VX7 Reference Guide

E-EQ-VX7RG-F

Notices

Notice:

LXE Inc. reserves the right to make improvements or changes in the products described in this manual at any time without notice. While reasonable efforts have been made in the preparation of this document to assure its accuracy, LXE assumes no liability resulting from any errors or omissions in this document, or from the use of the information contained herein. Further, LXE Incorporated, reserves the right to revise this publication and to make changes to it from time to time without any obligation to notify any person or organization of such revision or changes.

Copyright Notice:

125 Technology Parkway, Norcross, GA 30092 U.S.A. (770) 447-4224

Trademarks:

Revision Notice

VX7 Reference Guide
Upgrade From Revision E to Revision F

Section	**Explanation**
Entire Manual	Added CE 5.0 information and instruction where applicable.
Chapter 1 – Introduction	Added Bluetooth information. Revised Accessories listing.
Chapter 2 – Physical Description and Layout	Added Bluetooth information. Revised “Vehicle 12-80VDC Power Connection” with updated graphic.
Chapter 3 – System Configuration	Added Bluetooth information. Revised “Mixer” and “Step 3: Check Barcode Length” sections. Revised “Enabling GrabTime”. Revised “Wavelink Avalanche Enabler Configuration” for Avalanche Mobility Center.
Chapter 5 – Wireless Network Configuration	Updated chapter for EAP-FAST support, tray icon, help feature, etc. included in latest version of SCU. Revised section: “Admin login”.

Note: A complete revision history is included in Appendix C, “Reference Material”.

Table of Contents

Appendix A Key Maps 283

Appendix B Technical Specifications 291

Appendix C Reference Material 297

Illustrations

Chapter 1 Introduction

Overview

The VX7 Vehicle Mount Computer (VMC) is a rugged, vehicle mounted, PC (Personal Computer) running a Microsoft® Windows® CE operating system and capable of wireless data communications from a fork-lift truck or any properly configured vehicle. The VX7 provides power and functionality in a vehicle mounted unit, with a wide range of options:

CPU	400MHz Intel® PXA255
Memory	64 or 128MB SDRAM
Display	Indoor or Outdoor 12.1" display, integrated Touchscreen, adjustable brightness
Network connectivity	2.4 Wireless LAN radio (single or dual antenna) Ethernet port Optional Bluetooth module
Audio	Speakers in front bezel, audio jack for headset with microphone
Storage media	Compact Flash PCMCIA Secure Digital (SD)
Operating system	Microsoft Windows CE .NET 4.2 or CE 5.0
Other options	Extended temperature version RAM Mount™ vehicle mounting

When to Use this Guide

The “VX7 User’s Guide” is directed toward the VX7 user. It is delivered on the LXE Documentation CD. It contains safety warnings, descriptions of the controls and connectors, instruction on installing antennas, and day to day operation.

As the reference for LXE’s VX7 equipped with a Microsoft Windows CE operating system, this guide provides detailed information on its features and functionality. Use this guide as you would any other source book -- reading portions to learn about the VX7, and then referring to it when you need more information about a particular subject.

This chapter, **“Introduction”,** briefly describes this reference guide structure, contains setup and installation instruction, briefly describes data entry processes, and explains how to get help.

Chapter 2 “Physical Description and Layout” describes the function and layout of the controls and connectors on the VX7. Describes AC power and DC power connections.

Chapter 3 “System Configuration” takes you through the system setup and file structure, covering all components except the 2.4GHz radio, AppLock and Scanner.

Chapter 4 “Scanner” contains information on the scanner keyboard wedge, active scanner port, and COM port settings such as baud rate, parity, stop bits and data bits.

Chapter 5, “Wireless Network Configuration” details 2.4GHz radio setup. Configuration for WEP and WPA is included.

Chapter 6, “AppLock” contains explanation and instruction when working with VX7’s running AppLock.

Appendix A “Key Maps” describes the keypress sequences for the VX7 keyboard options.

Appendix B “Technical Specifications” lists technical specifications including physical, environmental, display and the radios.

Appendix C, “Reference Material” includes parameter programming charts and other reference information.

Document Conventions

This reference guide uses the following document conventions:

ALL CAPS	All caps are used to represent disk directories, file names, and application names.
Menu|Choice	Rather than use the phrase "choose the **Save** command from the **File** menu", this guide uses the convention "choose **File|Save**".
"Quotes"	Indicates the title of a book, chapter or a section within a chapter (for example, "Document Conventions").
< >	Indicates a key on the keyboard (for example, <Enter>).
📖	Indicates a reference to other documentation.
Ⓟ	Differences in operation or commands due to platform type.
Ⓢ	Differences in operation or commands due to software revision.
ATTENTION	Keyword that indicates vital or pivotal information to follow.
⚠	Attention symbol that indicates vital or pivotal information to follow. Also, when marked on product, means to refer to the manual or user's guide.
△	International fuse replacement symbol. When marked on the product, the label includes fuse ratings in volts (v) and amperes (a) for the product.
Note:	Keyword that indicates immediately relevant information.
Caution ⚠	Keyword that indicates a potentially hazardous situation, which, if not avoided, may result in minor or moderate injury.
WARNING ⚠	Keyword that indicates a potentially hazardous situation, which, if not avoided, could result in death or serious injury.
DANGER ⚠	Keyword that indicates an imminent hazardous situation, which, if not avoided, will result in death or serious injury.

Quick Start

This section's instructions are based on the assumption that your new system is pre-configured and requires only accessory installation (e.g. antenna, external keyboard and/or barcode scanner) and a power source.

In general, the sequence of events is:

1. Install Vehicle Mounting Bracket on vehicle and secure VX7 in Mounting Bracket Assembly (see "VX7 User's Guide").
2. Connect power cable to the VX7. The power cable can also be connected to a UPS battery pack, which is then connected to the VX7 (see "VX7 User's Guide").
3. Connect accessories to VX7, e.g. scanner, antenna, etc. (see "VX7 User's Guide).
4. Secure all cables to the VX7 with the Strain Relief Cable Clamps.
5. Turn the VX7 on.
6. When instructed, calibrate the touchscreen (see Chapter 3, "System Configuration").
7. The screen may appear white while applications and drivers are loading. When complete, set Date and Time (see Chapter 3, "System Configuration").
8. Pair Bluetooth devices.
9. Configure radio (see Chapter 5, "Wireless Network Configuration").
10. Warmboot to ensure all registry settings are saved.
11. Device is ready for use.

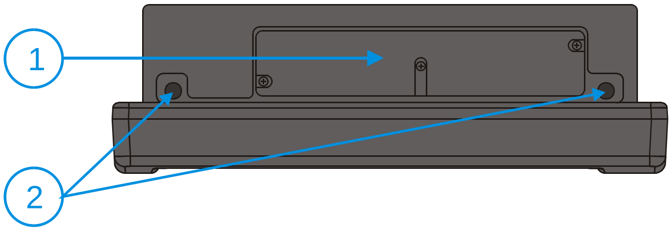
The VX7 and its keyboard should be mounted in an area in the vehicle where it:

- Does not obstruct the vehicle driver's vision or safe vehicle operation.
- Can be easily accessed by anyone seated in the driver's seat.

Troubleshooting

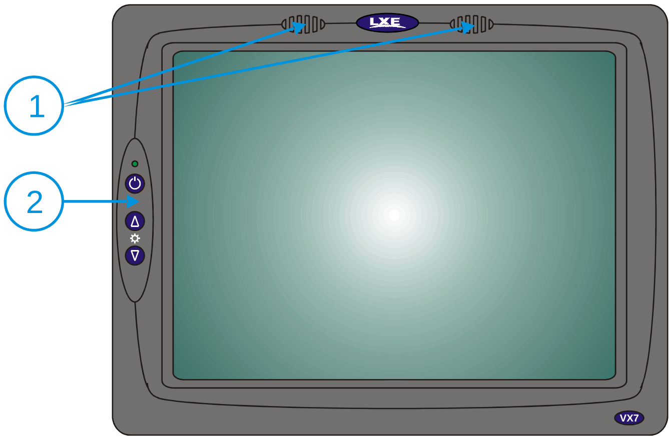
Can't calibrate the touch screen, change the date/time or adjust the volume.	AppLock is installed and running on the mobile device. AppLock restricts User access to running programs. Changes or modifications require Administrator access. Refer to "Chapter 6 – AppLock" for setup and processing information.
RFTerm opens and runs upon each cold reset and warm reset.	Tap **File | Exit** to close the RFTerm application.
VX7 seems to lockup as soon as it is warmbooted.	There may be small delays while the wireless client connects to the network, authorization for Voxware-enabled applications complete, Wavelink Avalanche management of the VX7 startup completes, and Bluetooth relationships establish or re-establish.

Components



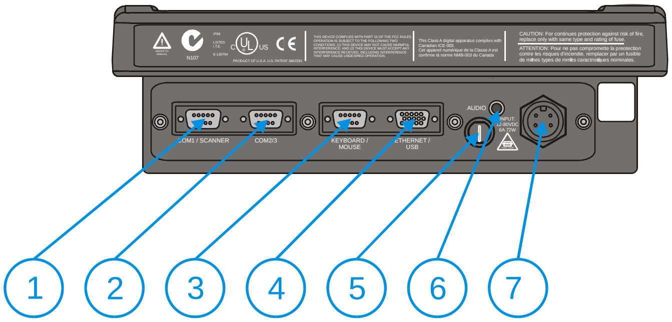
1. Access Panel Cover (See Following Illustrations for Detail)
2. Antenna Connectors or Hole Plugs

Figure 1-1 VX7 Components, Top View



1. Speakers
2. Control Panel (See Following Illustrations for Detail)

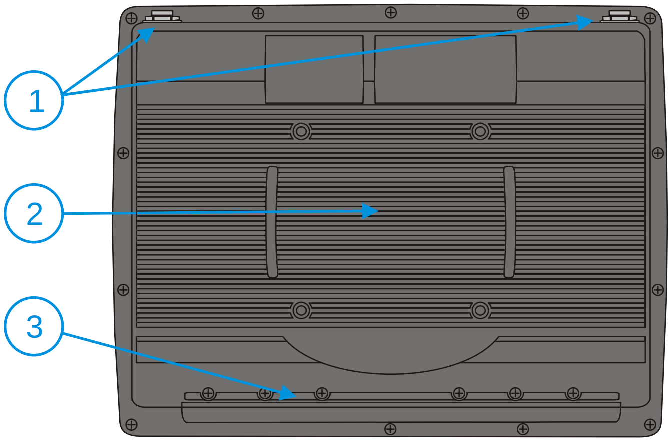
Figure 1-2 VX7 Components, Front View



1. COM1/Scanner Connector
2. COM3 Connector
3. Keyboard/Mouse Connector
4. Ethernet/USB Cable Connector (USB-Host and USB-Client)
5. Fuse
6. Audio Connector
7. Power Cable Connector

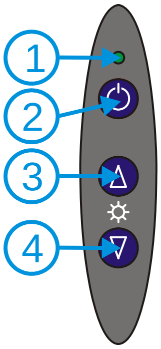
Figure 1-3 VX7 Components, Bottom View

Note: *COM1 is configured with Pin 9 +5V. COM3 is labeled “COM2/3” and is configured with Pin 9 RI. Please see Chapter 4, “Scanner”, for details on configuring Pin 9 of the serial ports.*



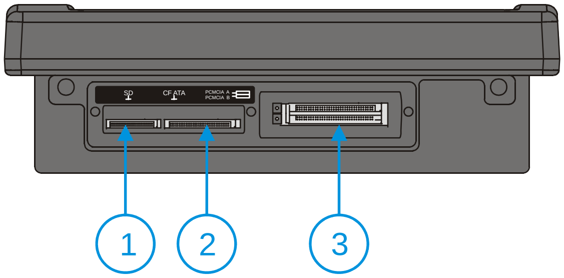
1. Antenna Connectors
2. Bracket Mounting Area
3. Strain Relief Bracket and Screws

Figure 1-4 VX7 Components, Back View



1. Power LED
2. Power Switch
3. Brightness Increase
4. Brightness Decrease

Figure 1-5 VX7 Control Panel



1. SD Memory Card Slot
2. Compact Flash Hard Drive
3. PCMCIA Slots

Figure 1-6 VX7 Access Panel

Note: The tethered access panel cover is not shown in the illustration above.

Data Entry

You can enter data into the VX7 through several different methods. A tethered scanner connected to the COM1 serial port provides barcode data entry, the serial ports are used to input/output data, keyboards provide manual entry and the touchscreen also provides manual entry (simulating a desktop PC's mouse).

Keyboard Data Entry

Refer to Appendix A "Key Maps" for 101-key keyboard equivalent keypresses.

The keyboard is used to manually input data that is not collected otherwise. Almost any function that a full sized computer keyboard can provide is duplicated on the LXE VMT keyboard but it may take a few more keystrokes to accomplish a keyed task.

When using the LXE 60-key keyboard, almost every key has two or three different functions. The primary alpha or numeric character is printed on the key.

For example, when the <2nd> key is selected pressing the desired second-function key produces the <2nd> character i.e. <2nd> + <F1> toggles the CAPS Lock function. The specific <2nd> character is printed above the corresponding key.

Please refer to Appendix A "Key Maps" for instruction on the specific keypresses to access all PC-compatible keyboard functions.

Tethered Scanners

The VX7 supports an accessory barcode label reading device. Keyboard data entries can be mixed with barcode data entries. Any scanner that decodes the barcode internally and outputs an RS-232 data stream may be used. COM port 1 is designed to be used with a hand held tethered barcode scanner.

> COM1 is set to +5V on pin 9 up to accept input from a barcode scanner by default. To change the setting for pin 9, refer to Chapter 4: "Scanner" section titled "Serial Port Pin 9" for details.

Bluetooth Scanners

Bluetooth scanners are paired to the VX7 wirelessly using the VX7 Bluetooth wireless client. The VX7 does not have a Bluetooth LED.

See previous sections on Bluetooth for more information.

Only LXE Bluetooth scanners and LXE Bluetooth printers are supported by LXE. See *Accessories*.

RS-232 Data Entry

The VX7 accepts input from an RS-232 device connected to either RS-232 port, COM1 or COM3 (labeled "COM2/3"). The data is entered at the cursor position, and the data is subject to all of the barcode/RS-232 input menu parameters, such as truncate.

Touchscreen Entry

Note: The touchscreen should be calibrated before initial use. See "Touchscreen Calibration" in Chapter 3, "System Configuration".

Note: Always use the point of the stylus for tapping or making strokes on the display. Never use an actual pen, pencil or sharp object to write on the touchscreen.

The touchscreen input performs the same function as the mouse that is used to point to and click elements on a desk top computer. A stylus is used in the same manner as a mouse – single tap or double tap to select menu options, drag the stylus across text to select, hold the stylus down to activate slider bars, etcetera. Right click is accomplished via a tap and hold on the touchscreen.

Hold the stylus as if it were a pen or pencil. Touch an element on the screen with the tip of the stylus then remove the stylus from the screen. The touchscreen responds to an actuation force (touch) of up to 4 oz. of pressure.

The touchscreen can be used in conjunction with the keyboard and scanner and an input/output device connected to one of the VX7's serial ports.

- Touch the stylus to the field of the data entry form to receive the next data feed.
- The cursor begins to flash in the field.
- The unit is ready to accept data from either the keyboard, integrated scanner or a device connected to a serial port.

Note: The touchscreen may be disabled. Please refer to "Disabling the Touchscreen" in Chapter 3, "System Configuration" for details.

Right Click

A right click can be simulated on the touchscreen. To perform a right click, touch the touchscreen with the stylus and hold it in the same location for a short time.

Note: Some applications may not support this right click method. Please review documentation for the application to see if it provides for right mouse click configuration.

Input Panel (Virtual Keyboard)

Data may be entered via the input panel (virtual keyboard) on the touchscreen. For more details on the input panel, please refer to Chapter 2, "Physical Description and Layout".

Touchscreen and Mouse

The behavior of the mouse pointer on the touchscreen varies by VX7 construction.

P To identify your VX7 platform type, please see "Identifying Your VX7", in Chapter 2, "Physical Description and Layout".

Platform 1 VX7's

Because the touchscreen also functions as a mouse, the pointer for on the 95-key keyboard, a USB mouse or a PS/2 mouse pointer may not always be visible on the screen. The mouse pointer reappears when the 95-key keyboard pointer or external mouse is moved or clicked. Please see "USB Mouse" earlier in this manual for more details.

- When a USB mouse is first attached to the VX7, the mouse pointer may not be visible. However, moving or clicking the mouse causes the pointer to appear.
- When the USB mouse is unplugged, the pointer may remain visible until the touchscreen is tapped.
- If the touchscreen is used for input, the mouse pointer may disappear. However, moving or clicking the mouse or pointing device on the 95-key keyboard causes the pointer to reappear.

Platform 2 VX7's

The mouse pointer is not visible unless a mouse (P/S2 or USB mouse or 95-key keyboard with pointing device) is attached.

If a mouse of any kind is attached, the mouse pointer is displayed on screen.

Setup the Radio and Network

Prerequisites

- Network SSID or ESSID number of the Access Point
- WEP or LEAP Authentication Protocol Keys

See “Chapter 5, “Wireless Network Configuration” for complete information.

Setup Terminal Emulation Parameters

Before you make a host connection, you will, at a minimum, need to know:

- the alias name or IP address (Host Address) and
- the port number (Telnet Port) of the host system

to properly set up your host session.

1. Make sure the mobile client network settings are configured and functional. If you are connecting over wireless LAN, make sure your mobile client is communicating with the Access Point.
2. From the **Start | Programs**, run **LXE RFTerm** or tap the **RFTerm** icon on the desktop.
3. Select **Session | Configure** from the application menu and select the “host type” that you require. This will depend on the type of host system that you are going to connect to; i.e. 3270 mainframe, AS/400 5250 server or VT host.
4. Enter the “Host Address” of the host system that you wish to connect to. This may either be a DNS name or an IP address of the host system.
5. Update the telnet port number, if your host application is configured to listen on a specific port. If not, just use the default telnet port.
6. Select **OK**
7. Select **Session | Connect** from the application menu or tap the “Connect” button on the Command Bar. Upon a successful connection, you should see the host application screen displayed.

To change options such as Display, Colors, Cursor, Barcode, etc., please refer to the “RFTerm Reference Guide” on the LXE Manuals CD.

ActiveSync – Initial Setup

The following instructions relate to initial setup of ActiveSync. When there is a Connect icon on the VX7 desktop, this section can be bypassed.

USB Connection

The VX7 is configured to use USB-C by default. No configuration is necessary

Connect the cable to the PC (the host) and to the dongle cable on the VX7 (the client). The ActiveSync connection is established automatically when the cable is connected.

Cables for USB ActiveSync Connection:

USB Client to PC/Laptop	Dongle cable w/USB-C connector	9000A075CBLUSBHCETH
	Also requires a standard USB cable with a type A plug on one end, and a type B plug on the other.	

Serial Connection

Select **Start | Settings | Control Panel | PC Connection**. Click the Change button. From the popup list, choose the appropriate COM port and baud rate.

This will set up the VX7 to use the USB or designated COM port. Click OK and ensure the check box for “Allow connection with desktop computer when device is attached” is checked.

Click OK to return to the Control Panel.

Note: By default COM3 (labeled “COM2/3”) is configured to use ActiveSync (Pin 9 = RI). Please refer to “Serial Port Pin 9” in Chapter 4, “Scanner” fore details on configuring Pin 9 of the serial ports.

Connect

Connect the correct cable to the PC (the host) and the VX7 (the client). Select “Connect” from the Start Menu on the VX7 (**Start | Programs | Communications | Connect**).

Note: Run “Connect” when the “Get Connected” wizard on the host PC is checking COM ports to establish a connection for the first time.

Cable for Serial ActiveSync Connection:

Serial Client to PC/Laptop	RS-232 9 Pin to 9 Pin	9000A054CBL6D9D9

Radio

Note: You must establish a partnership with a desktop computer prior to running ActiveSync on the VX7. The initial partnership must be done using direct serial / USB cable connection.

Once the relationship is established using the serial port, the ActiveSync link in the Start Menu gives a choice of connections, one of which is radio.

Select **Start | Settings | Programs | Communication | ActiveSync**. From the popup list, choose Network and then click the Connect button.

Bluetooth

Access: **Start | Settings | Control Panel | Bluetooth or Bluetooth icon in taskbar or Bluetooth icon on desktop**

or Tap the Bluetooth icon in the taskbar to open the Bluetooth LXEZ Pairings application.

The VX7 default Bluetooth setting is Enabled.

The LXE VX7 *Bluetooth*® module is designed to Discover and pair with nearby LXE Bluetooth devices. Only LXE printers or scanners are recognized and displayed in the Bluetooth panel. All other Bluetooth devices are ignored.

Prerequisite The Bluetooth devices (printers and/or scanners) have been setup to allow them to be "Discovered" and "Connected/Paired". The SysAdmin is familiar with the pairing function of the Bluetooth devices.

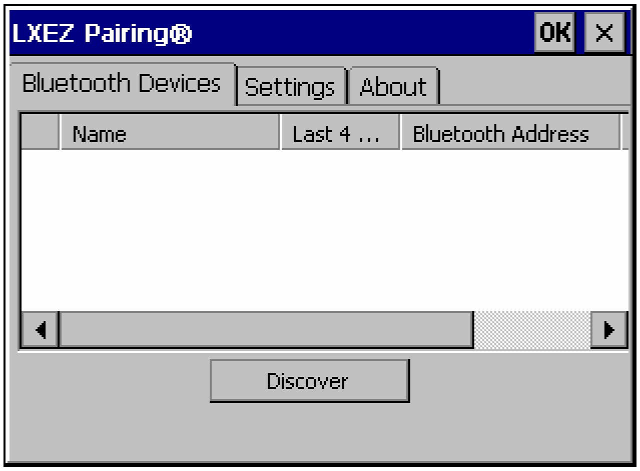


Figure 1-7 Bluetooth Devices Display – Before Discovering Devices

Initial Use

1. Select **Start | Settings | Control Panel | Bluetooth** or tap the Bluetooth icon in the taskbar or on the desktop.
2. Tap the **Settings** Tab.
3. Change the **Computer Friendly Name** at the bottom of the Settings display. The Bluetooth VX7 default name is determined by the LXE factory installed software version. LXE strongly urges assigning every VX7 a unique name (up to 32 characters) before Bluetooth Discovery is initiated.
4. Check or uncheck the VX7 Bluetooth options on the Settings tab.
5. Tap the OK button to save your changes or the X button to discard any changes.

See Also: *Chapter 3 – System Configuration*, section titled *Bluetooth.*

Settings Tab | Bluetooth Options

Note: These options can still be checked or unchecked whether Bluetooth connection is enabled or disabled.

As Bluetooth devices pair with the VX7, the name of the device and an icon representing the type of device is displayed in the Devices window. The icon state changes as the paired Bluetooth devices connect and disconnect from the VX7. When the Bluetooth devices are disconnected, the device icon has a red background.

Report when connection lost

A dialog box appears on the VX7 display notifying the user the connection between one (or all) of the paired Bluetooth devices has stopped. This option is enabled by default.

Click the OK button or the X button to remove the dialog box from the screen.

Report when reconnected

A dialog box appears on the VX7 display notifying the user a connection between one (or all) of the previously-paired Bluetooth devices is complete. This option is disabled by default.

Click the OK button or the X button to remove the dialog box from the screen.

Report failure to reconnect

If the reconnect timeout (30 minutes) expires, a dialog box appears on the VX7 display notifying the end-user the connection between one (or all) of the previously-paired Bluetooth devices has failed. This option is enabled by default.

Click the OK button to remove the dialog box from the screen.

Computer is connectable

There is no dialog connected to this checkbox. Enable this checkbox when you want the VX7 to be able to pair with other Bluetooth devices. This option is enabled by default.

Computer is discoverable

There is no dialog connected to this checkbox. Enable this checkbox when you want the VX7 to be Discovered by other Bluetooth devices. This option is disabled by default.

Prompt if devices request to pair

A dialog box appears on the VX7 screen notifying the user a Bluetooth device requests to pair with the VX7. This option is disabled by default.

The requesting Bluetooth device does not need to have been Discovered by the VX7 before the pairing request is received.

Click the Accept button or the Decline button to remove the dialog box from the screen.

Continuous search

When enabled, the VX7 never stops searching for a device it has paired with once the connection is broken (such as the paired device entering Suspend mode, going out of range or being turned off).

When disabled, the VX7 stops searching after one half hour. The search can be restarted by putting the VX7 through a Suspend/Resume cycle or accessing the Bluetooth control panel.

This option is disabled by default.

Subsequent Use

Note: Taskbar and Bluetooth device Icon states change as Bluetooth devices are discovered, pair, connect and disconnect. A taskbar Bluetooth icon with a red background indicates Bluetooth is active and not paired with any device. A device icon with a red background indicates a disconnected paired device.

1. Tap the **Bluetooth icon** in the taskbar or on the desktop to open the Bluetooth LXEZ Pairing application.
2. Tap the **Bluetooth Devices** tab.
3. Tap the **Discover** button. When the Bluetooth module begins searching for in-range Bluetooth devices, the button name changes to Stop. Tap the Stop button to cancel the Discover function at any time.
4. The discovered devices are listed in the Bluetooth Devices window.
5. **Doubletap** a Bluetooth device in the Discovered window to open the device properties menu.
6. Tap **Pair as Scanner** to set up the VX7 to receive scanner data.
7. Tap **Pair as Printer** to set up the VX7 to send data to the printer.
8. Tap **Disconnect** to stop pairing with the device. Once disconnected, tap **Delete** to remove the device name and data from the VX7 Bluetooth Devices list. The device is deleted after the user taps **OK**.
9. Upon successful pairing, the selected device may react to indicate a successful connection. The reaction may be an audio signal from the device, flashing LED on the device, or a dialog box is placed on the VX7 display.
10. Whenever the VX7 is turned On, all previously paired, live, Bluetooth devices in the vicinity are paired, one at a time, with the VX7. If the devices cannot connect to the VX7 before the re-connect timeout time period expires (default is approximately 20 seconds for each paired device) there is no indication of the continuing disconnect state if Report Failure to Reconnect is disabled.

See Also: *Chapter 3 – System Configuration,* section titled *Bluetooth.*

Bluetooth Devices

Assumption: The System Administrator has Discovered and Paired targeted Bluetooth devices for each VX7. The System Administrator has also enabled / disabled Bluetooth settings and assigned a Computer Friendly Name for each VX7. See *Chapter 3 System Configuration, Bluetooth control panel applet* and supported Bluetooth printers and scanners.

The Bluetooth taskbar Icon state and Bluetooth LED states change as Bluetooth devices are discovered, pair, connect and disconnect. There may be audible or visual signals as paired devices re-connect with the VX7. Only LXE printers or scanners are recognized and displayed in the Bluetooth panel. All other Bluetooth devices are ignored.

Taskbar Icon	Legend
ᛒ	Bluetooth module is connected to one or more of the targeted Bluetooth device(s).
ᛒ	VX7 is not connected to any Bluetooth device. VX7 is ready to connect with any Bluetooth device. VX7 is out of range of all paired Bluetooth device(s). Connection is inactive.

Note: When an active paired device enters Suspend Mode, is turned Off or leaves the VX7 Bluetooth scan range, the Bluetooth connection between the paired device and the VX7 is lost. There may be audible or visual signals as paired devices disconnect from the VX7.

See *Accessories* for supported Bluetooth printers and scanners.

AppLock, if installed, does not stop the end-user from using Bluetooth applications, nor does it stop authorized Bluetooth-enabled devices from pairing with the VX7 while AppLock is in control. See *Chapter 6 – AppLock* for more information.

See Also: *Chapter 3 – System Configuration*, section titled *Bluetooth*.

Bluetooth Barcode Reader Setup

Please refer to the Bluetooth scanner manufacturer's User Guide; it may be available on the manufacturer's web site. Contact your LXE representative for Bluetooth product assistance.

Introduction

LXE supports several different types of barcode readers. This section describes the interaction and setup for a mobile Bluetooth laser scanner or laser imager connected to the VX7 using Bluetooth functions.

- The VX7 must have the Bluetooth hardware and software installed. An VX7 operating system upgrade may be required. Contact your LXE representative for details.
- If the VX7 has a Bluetooth address identifier barcode label affixed, then Bluetooth hardware and software is installed.
- The mobile Bluetooth laser scanner / laser imager battery is fully charged.
- The VX7 batteries are fully charged. Alternatively, the VX7 may be in a powered cradle or cabled to AC/DC power.
- The barcode numbering examples in this segment are not real and should not be created nor scanned with a Bluetooth scanner.
- To open the LXEZ Pairing program, tap **Start | Settings | Control Panel | Bluetooth** or tap the **Bluetooth icon on the desktop** or tap the **Bluetooth icon in the taskbar**.

Figure 1-8 Sample Bluetooth Address Barcode Label

Locate the barcode label, similar to the one shown above, attached to the mobile device. The label is the Bluetooth address identifier for the VX7.

The mobile Bluetooth scanner / imager requires this information before discovering, pairing, connecting or disconnecting can occur.

Important: The VX7 Bluetooth address identifier label should remain protected from damage (rips, tears, spills, soiling, erasure, etc.) at all times. It may be required when pairing, connecting, and disconnecting new Bluetooth barcode readers.

VX7 with Label

If the VX7 has a Bluetooth address barcode label attached, follow these steps:

1. Scan the Bluetooth address barcode label, attached to the VX7, with the LXE Bluetooth mobile scanner.
2. If this is the first time the Bluetooth scanner has scanned the VX7 Bluetooth label, the devices are paired. See section titled "Bluetooth Beep and LED Indications". If the devices do not pair successfully, go to the next step.
3. Open the LXEZ Pairing panel [**Start | Settings | Control Panel | Bluetooth**].
4. Tap Discover. Locate the Bluetooth scanner in the Discovery panel.

5. Doubletap the stylus on the Bluetooth scanner. The right-mouse-click menu appears.
6. Select Pair as Scanner to pair the VX7 with the Bluetooth mobile scanner.

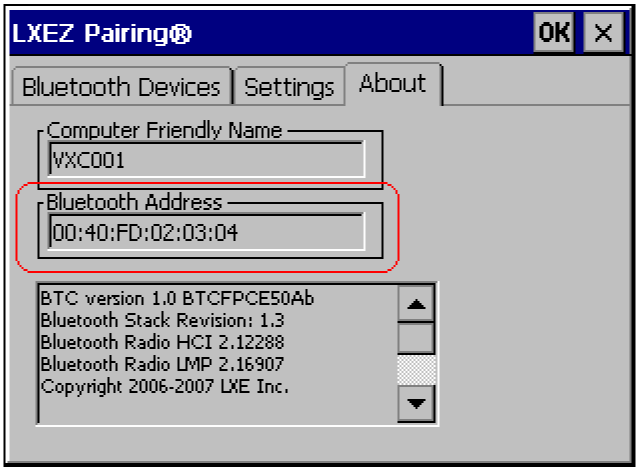
The devices are paired. The Bluetooth barcode reader responds with a series of beeps and LED flashes. Refer to the following section titled “Bluetooth Beep and LED Indications”.

Note: After scanning the VX7 Bluetooth label, if there is no beep and no LED flash from the Bluetooth device, the devices are currently paired.

VX7 without Label

If the VX7 Bluetooth address barcode label does not exist, follow these steps to create a unique Bluetooth address barcode for the VX7:

First, locate the VX7 Bluetooth address by tapping **Start | Settings | Control Panel | Bluetooth | About** tab.



Computer Friendly Name: VXC001

Bluetooth Address: 00:40:FD:02:03:04

BTC version 1.0 BTCFPCE50Ab
Bluetooth Stack Revision: 1.3
Bluetooth Radio HCI 2.12288
Bluetooth Radio LMP 2.16907
Copyright 2006-2007 LXE Inc.

Figure 1-9 About Tab and Bluetooth Address

Next, create a Bluetooth address barcode label for the VX7 [1].

The format for the barcode label is as follows:

- Barcode type must be Code 128.
- FNC3 character followed by string Uppercase L, lowercase n, lowercase k, uppercase B and then the Bluetooth address (12 hex digits, no colons). For example, LnkB0400fd002031.

Create and print the label.

Scan the VX7 Bluetooth address barcode label with the Bluetooth barcode reader.

The devices are paired. The Bluetooth barcode reader responds with a series of beeps and LED flashes. Refer to the following section titled “Bluetooth Beep and LED Indications”.

Note: After scanning the VX7 Bluetooth label, if there is no beep and no LED flash from the Bluetooth device, the devices are currently paired.

[1] Free barcode creation software is available for download on the World Wide Web. Search using the keywords “barcode create”.

Bluetooth Beep and LED Indications

Beep Type from Bluetooth Device	**Behavior**
Acknowledge label	1 beep
Label rejected	2 beeps at low frequency
Transmission error	Beep will sound high-low-high-low
Link successful	Beep will sound low-medium-high
Link unsuccessful	Beep will sound high-low-high-low

LED on Bluetooth Device	**Behavior**
Yellow LED blinks at 2 Hz	Linking in progress
Off	Disconnected or unlinked
Yellow LED blinks at 50 Hz	Bluetooth transmission in progress
Yellow LED blinks at the same rate as the paging beep (1 Hz)	Paging
Green LED blinks once a second	Disabled indication

Upon startup, if the scanner sounds a long tone, this means the scanner has not passed its automatic Selftest and has entered isolation mode. If the scanner is reset, the sequence is repeated. Contact LXE Support for assistance.

Saving Changes to the Registry

The VX7 saves the registry when you:

- Tap **Start** | **Run** then type **Warmboot**. Tap OK.
- Install Restart in the Start menu by **Start | Run** then type CTL RESTART=1 and tap the **OK** button. Tap **Start | Restart**.

The registry save process takes 0 – 3 seconds. If nothing has been changed, nothing is saved (e.g. 0 seconds)

The registry is automatically saved every 20 minutes. It is also saved every tenth time the registry settings are changed. Registry settings are changed when control panel applet (e.g. Date/Time) parameters are changed by the user and a warm boot was not performed afterward.

When you tap the **Start** | **Run** then type **Coldboot** and tap the OK button, factory default registry settings are loaded during coldboot. All changes and settings are lost.

Getting Help

All LXE manuals are now available on one CD and they can also be viewed/downloaded from the LXE website. Contact your LXE representative to obtain the LXE Manuals CD.

You can also get help from LXE by calling the telephone numbers listed on the LXE Manuals CD, in the file titled “Contacting LXE”. This information is also available on the LXE website www.lxe.com.

Explanations of terms and acronyms used in this guide are located in the file titled “Glossary” on the LXE Manuals CD.

Manuals and Accessories

Manuals

The following manuals are available on the LXE Manuals CD:

- VX7 User’s Guide
- RFTerm® Reference Guide
- Contacting LXE
- LXE Technical Glossary

Accessories

The table below lists the available VX7 accessories.

- Where two parts numbers are listed for a given part, the part number ending in “-R” is the RoHS compliant version.
- When only one part number is listed, the part is RoHS compliant unless otherwise noted.

VX7 Brackets	
Bracket, U Style, VX6 VX7	9000A021UBRACKET-R
Bracket, U Style w/ Integrated Keyboard Mount, VX7	9000A025UBRKTWKBDMNT-R
Kit, VXX U-Bracket to VX6 VX7 Adapter	9000A022BRKTADPTKIT-R
Kit, VXX U-Bracket to VX7 Adapter w/ Keyboard Mount	9000A026BRKTADPKBDMN-R
Bracket, RAM Mount VX6 VX7	9000A023BRKTRAMMOUNT-R
Bracket, Combo RAM VMT Mount w/ Keyboard Mount, VX7	9000A027BRKTRAMWKBMN-R
Bracket, VXX RAM ball on plate	9000A028RAMPLATEBALL-R
Bracket, RAM keyboard mounting plate	9000A029RAMKBDPLATE-R
Bracket, RAM keyboard arm	9000A030RAMKBDARM-R
Bracket, RAM Squeeze Mount, VX6 VX7	9000A031BRKTRAMSQZMT-R
Bracket, Combo RAM Squeeze Mount w/Keyboard Mount	9000A032BRKTRAMSQKBMT-R

Keyboard Brackets	
Bracket, Remote, Keyboard, LXE	9000A012BRKTRMTLXE-R
Bracket, Remote, Mouse Keyboard	9000A018BRKTMKBDRMT 9000A018BRKTMKBDRMT-R
Keyboards	
Keyboard, LXE Standard, D9, ANSI/PC Overlay, QWERTY	9000A157KBDSTDD9ANSI 9000A157KBDSTDD9ANSI-R
Keyboard, LXE Standard, D9, IBM 5250 Overlay, QWERTY	9000A158KBDSTDD95250 9000A158KBDSTDD95250-R
Keyboard, LXE Standard, D9, IBM 3270 Overlay, QWERTY	9000A159KBDSTDD93270 9000A159KBDSTDD93270-R
Keyboard, Rugged PC Style w/Mouse, PS2 D9	9000A160MOUSEKBDD9 9000A160MOUSEKBDD9-R
Data Cables	
Cable, Combo D15 to USB and Ethernet Adapter 1 Ft	9000A071CBLD15USBETH
Cable, Combo D15 to USB-H, USB-C and Ethernet Adapter	9000A075CBLUSBHCETH
Cable, Keyboard/Mouse Dual PS2 Adapter 1 Ft	9000A072CBLD9DUALPS2
Cable, Printer/PC, D9 to D25	9000A053CBL6D9D25 (above part is ***not*** RoHS compliant)
Cable, PC, D9 to D9	9000A054CBL6D9D9
Power Cables	
Cable, Input Power, 12 FT, VX5 VX6 VX7	9000A073CBLPWR12FT-R
Adapter Cable, VX1 VX2 VX4 Power Cable to VX5 VX6 VX7	9000A077CBLPWRADPTR
Power Supplies	
Power Supply, External, AC, W/US Power Cord VX5 VX6 VX7	9000A318PSACUS-R
Power Supply, External, AC, No Power Cord VX5 VX6 VX7	9000A318PSACWW-R
UPS Battery and Cables	
Battery, UPS Lead Acid, VX5 VX6 VX7	9000A378UPSBATTPACK-R
Cable, UPS Battery, Remote Mount Extender, 6 Ft	9000A074CBLUPSEXTNDR
Antenna and Antenna Mount Kits	
Replacement antenna, 2.4GHz	153180-0001
Remote Mount Antenna Assembly Kit, 8 Ft Cable	9000A279ANTREMOTE8-R
Remote Mount Antenna Assembly Kit, 6 Ft Cable	9000A278ANTREMOTE6-R
Right Angle Remote Mount Antenna Assembly Kit, 6 Ft Cable	9000A280ANTREMOTE6RT
Right Angle Remote Mount Antenna Assembly Kit, 15 Ft Cable	9000A281ANTREMOT15RT
Miscellaneous	
Stylus, with Tethers and Sleeves, 5 Pack	9000A510STYLUS
Protective Film, 12 in Display, 10 Pack, VX5 VX7	9000A511PROTFILM12IN

Voice Recognition Accessories	
Headset coiled adapter cable, with quick disconnect connector to a 2.5 mm audio jack. A headset (see below) is required	9000A076CBLHEADSET1
Headset, Single Band	HX1A501SINGHEADSET
Headset, Dual Band	HX1A502DUALHEADSET
Headset, Behind the Ear, Dual Ear	HX1A503BTHHEADSET
Foam, Replacement Block, Headset	HX1A504HSBLOCKFOAM
Yoke, Replacement for Dual Band Headset	HX1A505DUALYOKE
Yoke, Replacement for Single Band Headset	HX1A506SINGLEYOKE
Replacement Microphone Foam, Wind Screen, 10 pack	HX1A508WINDSREEN10
Replacement Microphone Foam, Wind Screen, 50 pack	HX1A509WINDSREEN50
Replacement Headset Foam, Ear Cover, 10 pack	HX1A510FOAMEAR10
Replacement Headset Foam, Ear Cover, 50 pack	HX1A511FOAMEAR
Tethered Scanners	
Scanner, Powerscan, SR, 8’ Cbl, WW	8300A326SCNRPWRSR8DA9F 8300A326SCNRPWRSR8DA9F-R
Scanner, Powerscan, SR, 12’ Cbl, US	8300A327SCNRPWRSR12DA9F (above part is ***not*** RoHS compliant)
Scanner, Powerscan, SR, Low Temp, 8’ Cbl	8300A332SCNRS8D9FLT (above part is ***not*** RoHS compliant)
Scanner, Powerscan, SR, Low Temp, 12’ Cbl	8300A333SCNRS12D9FLT (above part is ***not*** RoHS compliant)
Scanner, Powerscan, LR, 8’ Cbl, WW	8310A326SCNRPWRLR8DA9F 8310A326SCNRPWRLR8DA9F-R
Scanner, Powerscan, LR, 12’ Cbl, US	8310A3 27SCNRPWRLR12DA9F 8310A327SCNRPWRLR12DA9F-R
Scanner, Powerscan, LR, Low Temp, 8’ Cbl	8310A332SCNRL8D9FLT (above part is ***not*** RoHS compliant)
Scanner, Powerscan, LR, Low Temp, 12’ Cbl	8310A333SCNRL12D9FLT (above part is ***not*** RoHS compliant)
Scanner, Powerscan, XLR, 8’ Cbl, WW	8320A326SCNRPWRXLR8DA9F 8320A326SCNRPWRXLR8DA9F-R
Scanner, Powerscan, XLR, 12’ Cbl, US	8320A327SCNRPWRXLR12DA9F (above part is ***not*** RoHS compliant)
Scanner, Powerscan, XLR, Low Temp, 8’ Cbl	8320A332SCNRX8D9FLT (above part is ***not*** RoHS compliant)
Scanner, Powerscan, XLR, Low Temp, 12’ Cbl	8320A333SCNRX12D9FLT (above part is ***not*** RoHS compliant)
Scanner, LS3408 Fuzzy Logic SR, D9 Interface Cable, 8ft	8510A326SCNRFZYDA9F 8510A326SCNRFZYDA9F-R
Scanner, LS3408 Extended Range, D9 Interface Cable, 8ft	8520A326SCNRERDA9F-R

Bluetooth Scanner and Accessories	
PowerScan 7000BT Scanner RS-232 with pointer	8700A301SCNRBTSRI
PowerScan 7000BT Base Station, RS232, without universal power supply.	8700A501BASERS232
PowerScan 7000BT Base Station Power Supply, Std US, 120V	8700A502PSACUS
PowerScan 7000BT, RS232 Cable for Base Station, DB9S, Coil, 8'	8700A001CBL8DA9F
PowerScan 7000BT Battery Charger with Power Supply, Four Station, US Std	8700A503CHGR4US
PowerScan 7000BT Battery Pack	8700A504BATT
Bluetooth Standard Range Fuzzy Logic laser scanner	8810A326SCNRBTFZ
Bluetooth Auto range "LORAX" scanner	8820A327SCNRBTER
Desk Cradle, Radio/Charging, Multi-Interface	8800A001CRADLERCMI
Desk Cradle, Charge Only, Mulit-Interface	8800A002CRADLECMI
Forklift Cradle, Radio/Charging, Multi-Interface	8800A003CRADLEVRCMI
Forklift Cradle, Charge Only, Multi-Interface	8800A004CRADLEVCMI
US AC Power Cord	8800A051POWERCORD
Universal Desktop Power Supply 90-264VAC	8800A301ACPS
9-60VDC Forklift Power Supply	8800A302DCPS
Power Cable (connects Power Supply to Forklift)	8800A052DCPWRCABLE
Cable Assembly, DA9F, 9 ft, Cradle to Terminal	8500A051CBL9DA9F
Forklift Rugged Scanner Holder with RAM mount	8800A005STAND
8800 Spare Battery	8800A376BATTERY
Single slot Universal Battery Charger Adapter Cup	8800A377CHGRADPTRCUP
Single Slot Battery Charger w/International Power	8800A378CHGR1SLOT
Universal Battery Charger, 4 slot. Requires 4 adapter cups	8800A379CHGRBASE
Scanner Holster for Belt	8200A501HOLSRBELT
Mounted take up Reel	8000A501INDREEL
Auto Sense Intellistand, Hands Free Scanning	8500A505STANDSMT
Strap with Scanner Clip	9000A411SCNRSTRAP

Chapter 2 Physical Description and Layout

Identifying Your VX7

Some features discussed in this document may not be available for all VX7's. Additionally, some features require a certain revision level of system software.

Any feature that is not identified as platform specific or requiring a certain level of system software is available to all VX7's.

Hardware Platforms

P

To determine the platform level of your VX7, please refer to the VX7 serial number decal.

Platform 1 VX7

VX7's identified as Platform 1 by a P1 notation on the serial number decal (and VX7's with no platform identification on the serial number decal) are referred to as Platform 1 VX7's. These VX7's DO NOT support the features identified as "Platform 2" throughout this manual.

Note: If software revision 1ED or greater is installed, "LXE VX7 Platform 1" is displayed during boot up. See "Software Revisions", below, to determine the software revision installed on the VX7. If no software revision is displayed during bootup, the VX7 is a Platform 1 type as all Platform 2 VX7's ship with software revision 1ED or greater.

Platform 2 VX7

VX7's identified as Platform 2 by a P2 notation on the serial number decal support all features, including those noted as Platform 2 specific.

Note: If software revision 1ED or greater is installed, "LXE VX7 Platform 2" is displayed during boot up. See "Software Revisions", below, to determine the software revision installed on the VX7.

Software Revisions

S

Some features described in this manual require a certain minimum revision level of system software. These features are available on all VX7's if the proper revision level (or newer) of system software is installed.

The software revision is displayed during boot up and on the default desktop wallpaper. The revision can also be viewed using the **Start | Settings | Control Panel | About** icon. For more information, please refer to Chapter 3, "System Configuration".

To upgrade the VX7 with a newer revision of system software, please refer to "Reflash the VX7" in Chapter 3, "System Configuration".

Hardware Configuration

System Hardware

The VX7 hardware configuration is shown in the following figure.

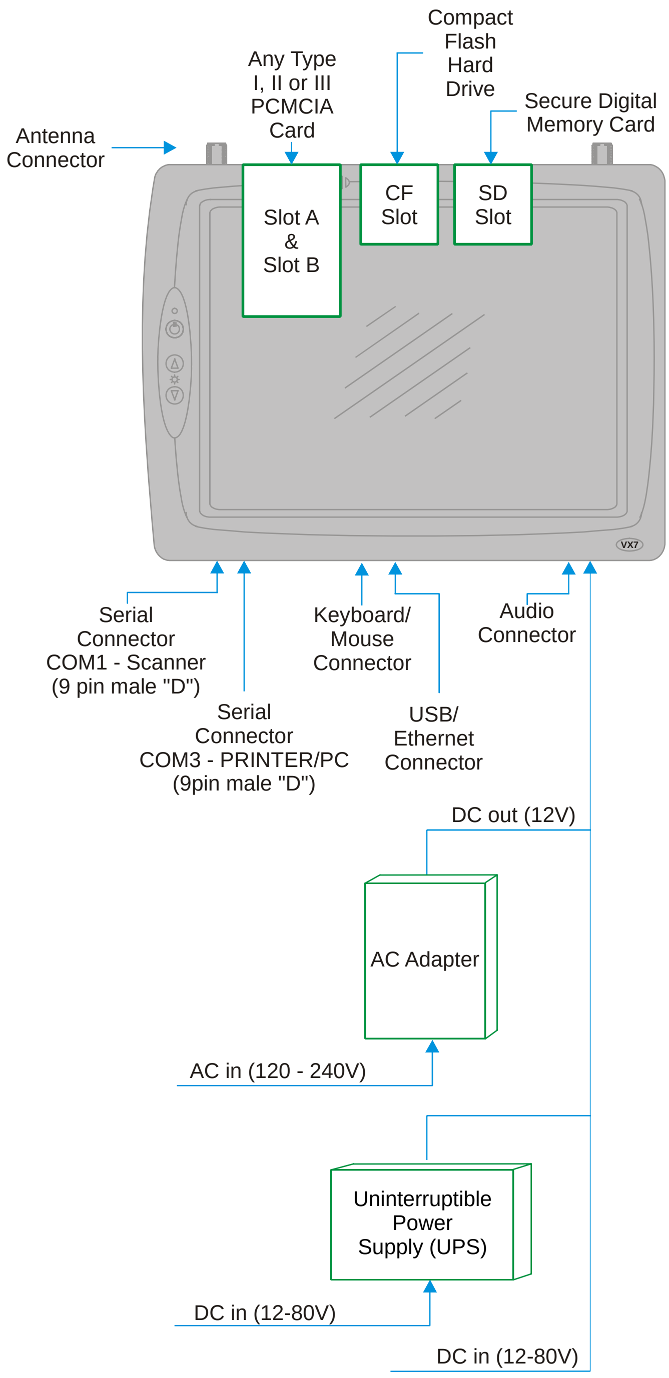


Figure 2-1 VX7 Hardware Configuration

Central Processing Unit

The LXE VX7 contains an 400MHz Intel PXA255 CPU.

I/O Components

The VX7 supports the following I/O components:

- Two 9-pin RS-232 serial ports configured as:
  - COM1
  - COM3 (labeled “COM2/3”)

  Note: There is no COM2 port on the VX7.
- Two PCMCIA slots (supporting Type I or II PCMCIA cards).
- One slot for SD memory card.
- Compact flash drive.
- LXE VMT or standard PS/2 keyboard (via a watertight connector).
- Ports available via dongle cable:
  - USB Host port
  - USB Client Port
  - Ethernet port
- One audio jack providing monaural audio output.

System Memory

Main system memory is 64 or 128MB DRAM.

Video Subsystem

The LXE VX7 video subsystem consists of a color TFT display. The video subsystem complies with the VESA VL bus standard.

The display supports screen blanking to eliminate driver distraction when the vehicle is in motion. Please see “Technical Specifications – Screen Blanking Cable” later in this chapter and “Screen Blanking” in Chapter 4, “Scanner” for details.

To identify your VX7 platform type, please see “Identifying Your VX7”, earlier in this chapter.

Platform 1 VX7’s

The display resolution is 800 x 600 pixels. This resolution complies with the SVGA graphics industry standard.

Platform 2 VX7’s

The default resolution of this display is 800 by 600 pixels. This resolution complies with the SVGA graphics industry standard. The display can also be configured for 640 by 480 pixels.

To change the display resolution, please refer to “Changing the Display Resolution” in Chapter 3, “System Configuration”.

Power Supply

Vehicle power input for the VX7 is 12V to 80V DC nominal and is accepted without the need to perform any manual operation within the VX7.

If 12V to 60V DC power is not available – for example, in an office environment – an optional external Universal Input Power Supply can be used to convert AC wall power to an appropriate DC level. See “External Power Supply”, later in this chapter.

Power input is fused for protection and the fuse is externally accessible.

Uninterruptible Power Supply

A DC uninterruptible power supply (UPS) battery is available to maintain power to the VX7 for a minimum of 15 minutes when vehicle power is not available (such as when a vehicle battery is being swapped).

Backup Battery

The LXE VX7 has a permanent lithium battery installed to maintain time and date. The backup battery is not user serviceable and should last five years with normal use before it requires replacement.

Note: This battery should only be changed by authorized service personnel.

PCMCIA Slots

Microsoft Windows CE Plug and Play operating system controls the PCMCIA cards. These cards are hot swappable per the PCMCIA specifications.

CF Slot

The CF ATA slot is not hot swappable. The VX7 must be powered down to insert or remove an ATA card. Since the operating system is stored on the ATA card, the VX7 cannot operate without the ATA card.

SD Slot

The SD slot accepts an SD memory card. These cards are hot swappable.

Bluetooth LXEZ Pairing

The VX7 contains Bluetooth version 2.0 with Enhanced Data Rate (EDR) up to 3.0 Mbit/s over the air. Bluetooth device connection (or pairing) can occur at distances up to 32.8 ft (10 meters) Line of Sight. The wireless client retains wireless connectivity while Bluetooth is active.

The user will not be able to select PIN authentication or encryption on connections from the HX3. However, the HX3 supports authentication requests from pairing devices. If a pairing device requests authentication or encryption, the HX3 displays a prompt for the PIN or passcode. Maximum encryption is 128 bit. Encryption is based on the length of the user's passcode.

Bluetooth will simultaneously support one printer as a slave Bluetooth device and one scanner, either as a slave or as a master Bluetooth device.

See *Chapter 3 System Configuration*, control panel section titled *Bluetooth*.

Notes

- The VX7 does not have a Bluetooth managed LED.
- The LED on the Bluetooth scanner illuminates during a scanning operation.
- Barcode data captured by the Bluetooth scanner is manipulated by the settings in the VX7 Scanner Properties control panel applet.
- Multiple beeps may be heard during a barcode scan using the Bluetooth scanner; beeps from the Bluetooth scanner as the barcode data is accepted/rejected, and other beeps from the VX7 during final barcode data manipulation.

Power Modes

The VX7 has several distinct power modes.

- **On Mode** – When the VX7 is attached to either vehicle 12-80 VDC or an external power supply and the power button is pressed, the VX7 is in the On mode. In this mode, the keypad, touchscreen and any attached peripherals such as a scanner function normally. The display remains on until the backlight timer (if enabled) expires.
- **User Idle Mode** – If the Display Backlight Timer is enabled (see the Display section in the Windows CE Control panel), the VX7 enters User Idle Mode when the display backlight timer expires without any Primary Event (see below) to reset the timer. The VX7 exits User Idle Mode with any Primary Event. The keypress or screen touch that exits User Idle Mode is sent to the operating system. The VX7 then transitions to On Mode.

Primary Events

Any key on the keypad	COM1 activity
Stylus touch on the touchscreen	Scanner activity
Power button tap	USB client connection
Bluetooth device reconnect / disconnect message	

- **System Idle Mode** – The VX7 does not support System Idle mode.
- **Suspend Mode** – TheVX7 does not support Suspend mode. However, if the Suspend timer is enabled, the VX7 transitions to Off mode when the Suspend timer expires.
- **Off Mode** – The VX7 turns off if the user presses the power button when the VX7 is On. The VX7 is also off when it is not connected to a power source. However, an internal Real Time Clock (RTC) powered by an internal battery maintains the date and time while the VX7 is off.

Physical Controls

On/Off Switch

The power (on/off) switch is a push button switch located on the front control panel of the VX7. The switch is a momentary switch. If the VX7 is Off, pressing the power switch turns the VX7 On.

For Platform 2 VX7's, the keyboard LEDs turn on for about one second when the operating system loads the keyboard driver. If the LEDs blink more than once, this indicates a keyboard problem.

- On a USB or PS/2 keyboard, the NumLock, CapsLock and Scroll Lock keys blink the same as a desktop PC.
- On the 95-key keyboard, the CapsLock, NumLock and Scroll Lock keys are backlit amber. However, the keyboard backlight must be On for this feature to be used. The brief illumination may not be visible unless the room is dark.
- On the 60-key keyboard, only the CAPs led is lit during this process.

To identify your VX7 platform type, please see "Identifying Your VX7", earlier in this chapter.

If the VX7 is On, pressing and releasing the power switch turns the VX7 Off. An orderly shutdown is preformed. Any open programs are closed, the Windows CE operating system shuts down and then the VX7 powers off.

If a software lockup should occur and the VX7 is unresponsive to keyboard or touchscreen input, pressing and holding the power button for several seconds forces a shutdown. However, the forced shutdown is not an orderly shutdown. All unsaved data and any registry settings not saved to persistent storage are lost.

The Status LED, located on the keyboard of the VX7, is lit when the power is on:

- **Green** – VX7 is operating from vehicle power or AC power.
- **Solid Yellow** – VX7 is operating from the UPS, UPS battery is good.
- **Flashing Yellow** – VX7 is operating from the UPS, UPS battery is critically low.

Note: Always turn the computer off prior to removing power cables.

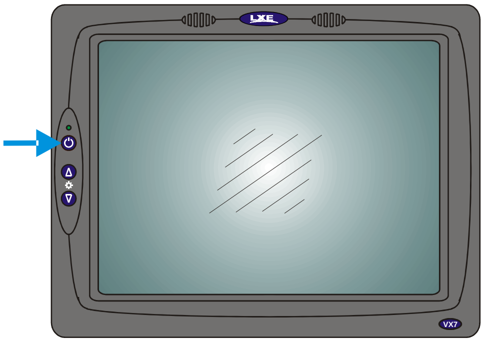


Figure 2-2 The Power (On/Off) Switch

Caution ⚠	**The VX7 has voltage on it even when power is off. Always disconnect input power before working on the VX7 (changing fuse, opening access panel, etc).**

External Connectors

Most external connectors for the VX7 are located on the bottom of the unit.

- The Keyboard/Mouse connector accepts an LXE VMT keyboard or a dongle cable for a PS/2 keyboard and mouse.
- COM1 connects to a serial barcode scanner.
- COM3 (labeled “COM2/3”) connects to a serial printer or PC with the appropriate cables.
- The USB/Ethernet connector accepts dongle cables, offering a combination of the following ports:
  - An Ethernet port
  - A USB Host port
  - A USB Client port
- Audio connects to a mono or stereo telephone headset/microphone.

Other external connectors are located as follows:

- Antenna connectors are located on the top of the VX7. VX7’s can be configured for a single antenna or dual antennas.

Scanner Serial Connector (COM1)

The serial connector, labeled "SCANNER", (configured as COM1) is industry-standard RS-232. The connector includes a PC/AT standard 9–pin "D" male connector. By default, Pin 9 is configured to supply +5 VDC at 0.4A (max) for an external bar code scanner. Pin 9 may also be configured to provide RI. Refer to Chapter 4, "Scanner", section titled "Serial Port Pin 9" for more information on configuring Pin 9.

If Pin 9 is powered off, please see "Technical Specifications – Connection Cable" in the following section for information on using a serial cable.

If COM1 is not being used for a scanner, it can also be used for screen blanking when the vehicle is in motion. Please see "Technical Specifications – Screen Blanking Cable" in the following section for more details.

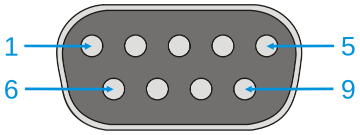


Figure 2-3 Scanner Serial Connector (COM1)

Note: Power the VX7 off before attaching a cable or device to the COM1 serial port.

Pinout

Pin	Signal	Description
1	DCD	Data Carrier Detect – Input
2	RXD	Receive Data – Input
3	TXD	Transmit Data – Output
4	DTR	Data Terminal Ready – Output
5	GND	Signal/Power Ground
6	DSR	Data Set Ready – Input
7	RTS	Request to Send – Output
8	CTS	Clear to Send – Input
9	+5VDC or RI	Barcode Scanner Power – 400mA max (Default) or Ring Indicator – Input
Shell	CGND	Chassis Ground

Printer/PC Serial Connector (COM3)

The serial connector (labeled "COM2/3") is an industry-standard RS-232 9-pin "D" connector. The connector and its pin assignments are shown below. By default, Pin 9 provides RI. Pin 9 may also be configured to supply +5 VDC at 0.4A (max) for an external bar code scanner. Refer to Chapter 4, "Scanner", section titled "Serial Port Pin 9" for more information on configuring Pin 9.

Please see "Technical Specifications – Connection Cable" below for information on using a serial cable.

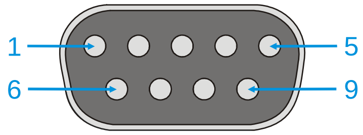


Figure 2-4 Printer/PC Serial Connector (COM3)

Note: Power the VX7 off before attaching a cable or device to the COM3 serial port.

Pinout

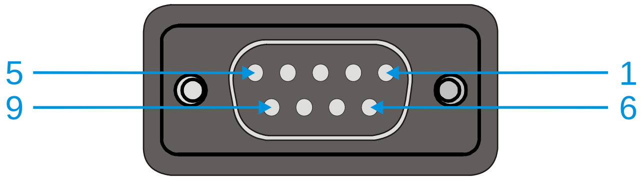
Pin	Signal	Description
1	DCD	Data Carrier Detect – Input
2	RXD	Receive Data – Input
3	TXD	Transmit Data – Output
4	DTR	Data Terminal Ready – Output
5	GND	Signal/Power Ground
6	DSR	Data Set Ready – Input
7	RTS	Request to Send – Output
8	CTS	Clear to Send – Input
9	RI or +5VDC	Ring Indicator – Input (default) or Bar Code Scanner Power – 400mA max
Shell	CGND	Chassis Ground

Technical Specifications – Connection Cable

The exact serial cable is crucial. Many commercial null modem cables will not work. LXE recommends the following cable:

Serial cable:

9000A054CBL6D9D9



Pinout:

DB9 female	DB9 female
1	7
2	3
3	2
4	6, 8
5	5
6, 8	4
7	1
9	no connection

Figure 2-5 Pinout – Serial Cable

Some laptop devices do not properly implement all control lines on the serial port – the laptop connection will not work.

RTS/CTS Handshaking and the Serial Port

RTS	Ready to Send	CTS	Clear to Send
DTR	Data Terminal Ready	DSR	Data Set Ready
Remote Side	The device sending data to and receiving data from the VX7 through the LXE serial cable connected to the RS-232 ports on both devices.		
LXE Serial Cable	9000A054CBLD9D9		

The VX7 serial port supports four types of handshaking via the LXE serial cable: None, standard Xon/Xoff, standard DTR/DSR, and a form of RTS/CTS.

To use RTS/CTS, the remote side computer must clear the DTR line which sets the VX7 CTS line and allows the VX7 to send data to the remote side.

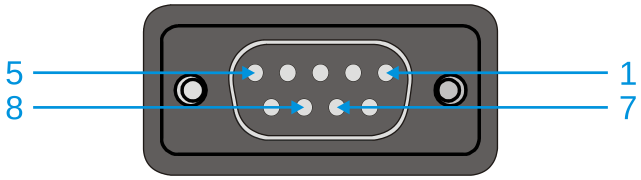
This allows signals and data to travel smoothly between both devices.

Technical Specifications – Screen Blanking Cable

The customer must supply their own cable. The cable must be designed so that pin 7 (RTS – Request to Send Output) and pin 8 (Clear to Send Input) of a D9 female connector provide continuity only when the vehicle is stopped (for example, via a switch on the accelerator pedal of the fork truck). All other pins on the connector must be left unconnected. If pins 7 and 8 do not provide continuity (or the cable is removed), the VX7 screen remains blank.

Serial cable:

Customer built cable with the following specifications:



Pinout:

DB9 female	Function
1	Not Used
2	Not Used
3	Not Used
4	Not Used
5	Not Used
6	Not Used
7	No signal when in motion, Continuity to Pin 8 when stopped
8	No signal when in motion, Continuity to Pin 7 when stopped
9	Not Used

Figure 2-6 Pinout – Screen Blanking Cable

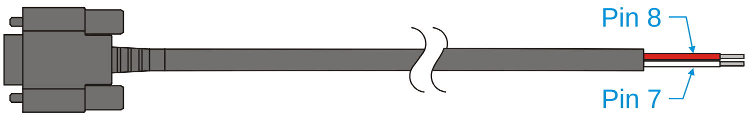


Figure 2-7 Sample Cable for Screen Blanking

Please refer to “Scanner” in Chapter 4, “Scanner”, for the proper COM port settings to support screen blanking.

Keyboard/Mouse Connector

The VX7 external keyboard connector accepts:

- An LXE VMT keyboard with integrated pointing device
- An LXE VMT keyboard without integrated pointing device
- A dongle cable providing PS/2 connections for a standard PS/2 keyboard and mouse.

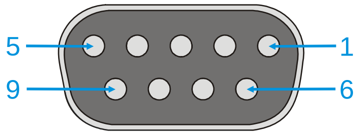


Figure 2-8 VX7 Keyboard Connector and External Keyboard Cable Connector

The +5V supply available from the connector is current limited at 400mA.

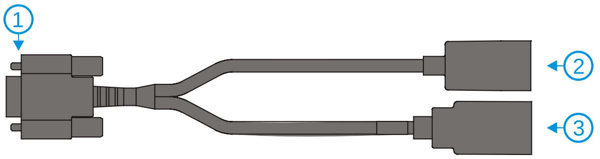
Note: Power the VX7 off before attaching a cable or device to the Keyboard/Mouse connector.

Pinout

Pin	Signal	Description
1	KBDAT_A	Keyboard Data
2	MSDAT_A	Mouse Data
3	–	Not Connected
4	MSCLK_A	Mouse Clock
5	DGND	System Ground
6	–	Not Connected
7	KBCLK_A	Keyboard Clock
8	/BL_ENABLE	Keyboard Backlight Enable
9	KDB_PWR	Keyboard Power, 5V
Shell	CGND	Chassis Ground

PS/2 Keyboard/Mouse Dongle Cable

The PS/2 keyboard/mouse dongle cable allows a standard PS/2 keyboard and/or mouse to be attached to the VX7. The PS/2 connectors on the dongle cable are labeled for keyboard and mouse.



1	D9 Connector
2	PS/2 Keyboard Connector
3	PS/2 Mouse Connector

Figure 2-9 VX7 PS/2 Keyboard/Mouse Dongle Cable

Note: Power the VX7 off before attaching the cable to the Keyboard/Mouse connector. The VX7 must also be powered off to add or remove a PS/2 keyboard or mouse.

D9 Male Connector

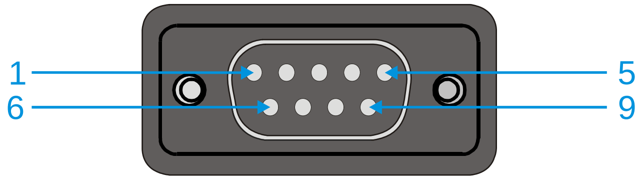


Figure 2-10 D9 Male Connector

Pinout

Pin	Signal	Description
1	KBDAT_A	Keyboard Data
2	MSDAT_A	Mouse Data
3	–	Not Connected
4	MSCLK_A	Mouse Clock
5	DGND	System Ground
6	–	Not Connected
7	KBCLK_A	Keyboard Clock
8	/BL_ENABLE	Keyboard Backlight Enable
9	KB_PWR	Keyboard Power, 5V
Shell	CGND	Chassis Ground

PS/2 Keyboard Connector

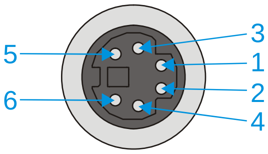


Figure 2-11 PS/2 Keyboard Connector

Pinout

Pin	Signal	Description
1	KBDAT_A	Keyboard Data
2	–	Not Connected
3	DGND	System Ground
4	KBD_PWR	Keyboard Power, 5V
5	KBCLK_A	Keyboard Clock
6	–	Not Connected
Shell	CGND	Chassis Ground

PS/2 Mouse

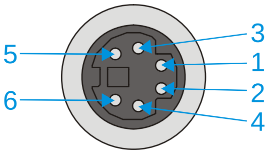


Figure 2-12 PS/2 Mouse Connector

Pinout

Pin	Signal	Description
1	MSDAT_A	Mouse Data
2	–	Not Connected
3	DGND	System Ground
4	KBD_PWR	Keyboard Power, 5V
5	MSCLK_A	Mouse Clock
6	–	Not Connected
Shell	CGND	Chassis Ground

Ethernet/USB Connector

The VX7 Ethernet/USB connector accepts dongle cables that provide combinations of the following connections:

- an Ethernet port, via an RJ45 connector
- a USB Host port for connecting a USB device to the VX7
- a USB Client port to connect the VX7 to a USB host or hub.

Note: Please refer to the diagrams later in this chapter for details on available ports with the dongle cable options.

The connector is shown below.

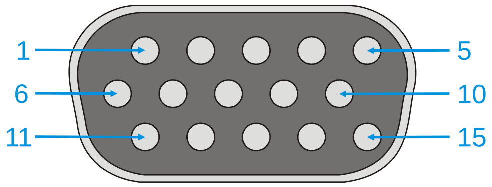


Figure 2-13 VX7 USB Connector and External USB Adapter Cable Connector

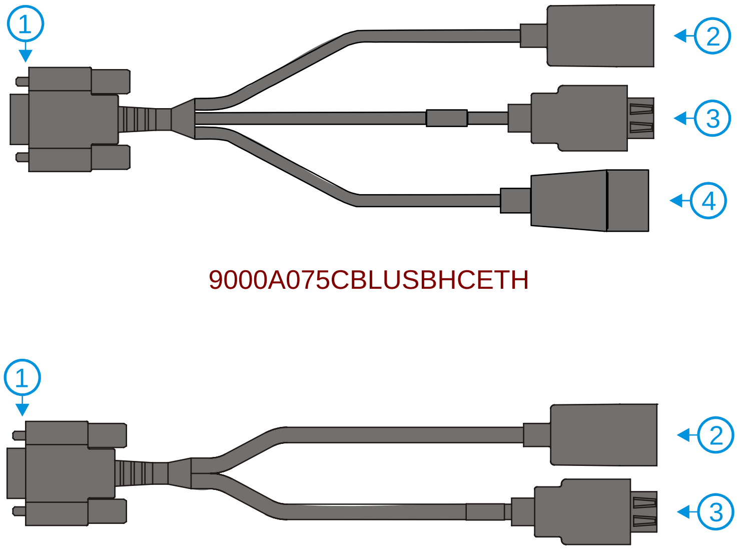
Note: Power the VX7 off before attaching a cable or device to the Ethernet/USB connector.

Pinout

Pin	Signal	Description
1	USB2N_A	USB D –
2	–	Not Connected
3	–	Not Connected
4	RXP	Receive +
5	RXN	Receive –
6	USB2P_A	USB D +
7	DGND	USB Power Return
8	–	Not Connected
9	RJ45_45	RJ45, Pins 4 and 5 Connections
10	RJ45_78	RJ45, Pins 7 and 8 Connections
11	5V_USB_23	USB Power, Current Limited
12	–	Not Connected
13	–	Not Connected
14	TXN	Transmit –
15	TXP	Transmit +
Shell	CGND	Chassis Ground

Ethernet/USB Dongle Cables

The available dongle cables are shown below.



1 D15 Connector

2 RJ45 Connector

3 USB Host Connector

4 USB Client Connector

9000A075CBLUSBHCETH

1 D15 Connector

2 RJ45 Connector

3 USB Host Connector

9000A071CBLD15USBETH

Figure 2-14 VX7 Ethernet/USB Dongle Cables

Note: Power the VX7 off before attaching a cable or device to the Ethernet/USB connector.

The connectors and pinouts for the dongle cables are detailed below.

⚠	9000A075CBLUSBHCETH is required when using ActiveSync via USB on the VX7.

D15 Female Connector

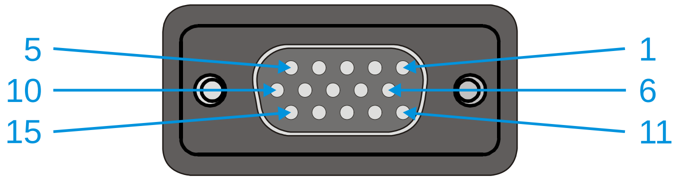


Figure 2-15 D15 Female Connector

Pinout

Pin	Signal	Description
1	USB2N_A	USB-H D –
2	–	Not Connected
3		USB-D Power
4	RXP	Receive +
5	RXN	Receive –
6	USB2P_A	USB-H D +
7	DGND	USB-H Power Return
8		USB-D D –
9	RJ45_45	RJ45, Pins 4 and 5 Connections
10	RJ45_78	RJ45, Pins 7 and 8 Connections
11	5V_USB_23	USB-H Power, Current Limited
12		USB-D Power Return
13		USB-D D +
14	TXN	Transmit –
15	TXP	Transmit +
Shell	CGND	Chassis Ground

USB Host Connector

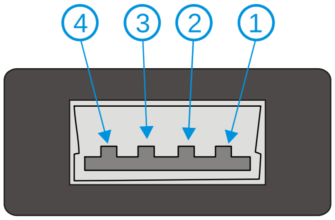


Figure 2-16 Dongle Cable USB Host Port

Pinout

Pin	Signal	Description
1	5V_USB_23	USB Power, Current Limited
2	USB2N_A	USB D –
3	USB2P_A	USB D +
4	DGND	USB Power Return
Shell	CGND	Chassis Ground

USB Client Connector

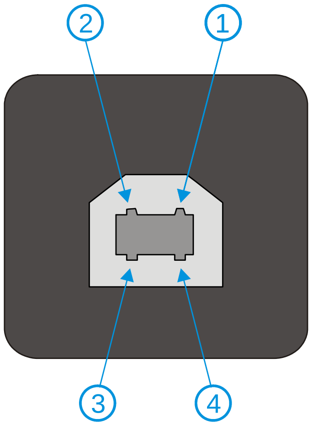


Figure 2-17 Dongle Cable USB Client Port

Pinout

Pin	Signal	Description
1	5V_USB_23	USB Power, Current Limited
2	USB2N_A	USB D –
3	USB2P_A	USB D +
4	DGND	USB Power Return

RJ45 Connector

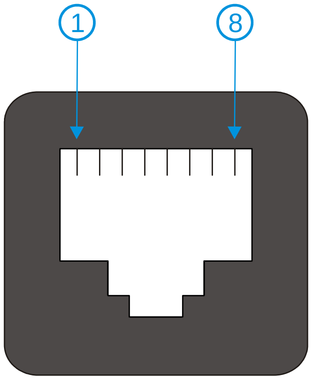


Figure 2-18 Dongle Cable Ethernet Port

Pinout

Pin	Signal	Description
1	TXP	Transmit +
2	TXN	Transmit –
3	RXP	Receive +
4	–	Not Connected
5	–	Not Connected
6	RXN	Receive –
7	–	Not Connected
8	–	Not Connected

Audio Connector

The VX7 audio connector accepts a headset with a 2.5mm plug, such as a mono telephone headset with microphone or a stereo headset.

Please refer to “Mixer” in Chapter 3, “System Configuration” for information on configuring the audio port for either a mono headset with microphone or a stereo headset.

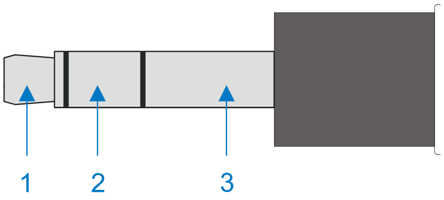


Figure 2-19 VX7 Audio Jack for External Speaker or Headphones

Note: The VX7 is not configured for standard PC speakers.

Pinout

Pin	Description
1	Microphone (Not connected in VX7)
2	Speaker
3	Ground

Power Supply Connector

Power is supplied to the VX7 through the power connector. Additionally this assembly provides a connection point for the vehicle's chassis ground to be connected internally to the conductive chassis of the computer.

The VX7 internal power supply can accept DC input voltages in the range of 12 to 80 Volts.

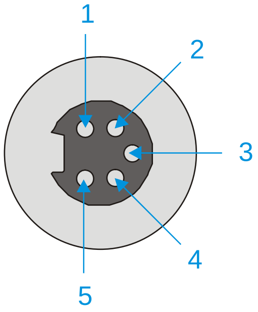


Figure 2-20 The Power Connector

Pinout

Pin	Signal
1	DC Positive (+)
2	UPS Battery Positive (+)
3	Chassis Ground
4	UPS Battery Negative (–)
5	DC Negative (–)

UPS Battery Pack Connectors

Input

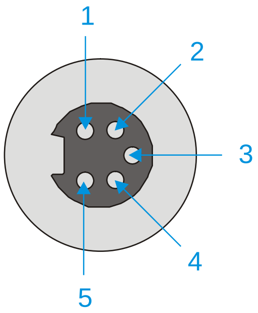


Figure 2-21 The UPS Battery Pack Input Connector

Pinout

Pin	Signal
1	DC Positive (+)
2	Not used
3	Chassis Ground
4	Not used
5	DC Negative (–)

Output

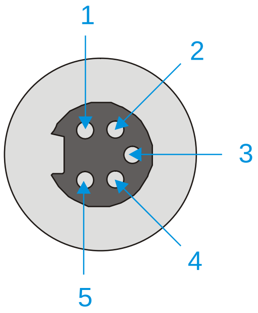


Figure 2-22 The UPS Battery Pack Output Connector

Pinout

Pin	Signal
1	DC Positive (+)
2	UPS Battery Positive (+)
3	Chassis Ground
4	UPS Battery Negative (–)
5	DC Negative (–)

UPS Battery Extension Cable Connectors

Input

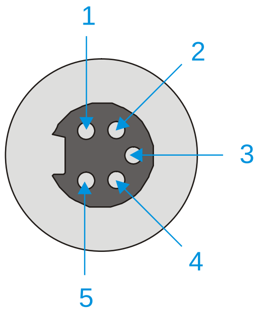


Figure 2-23 The UPS Battery Extension Cable Input Connector

Pinout

Pin	Signal
1	DC Positive (+)
2	UPS Battery Positive (+)
3	Chassis Ground
4	UPS Battery Negative (–)
5	DC Negative (–)

Output

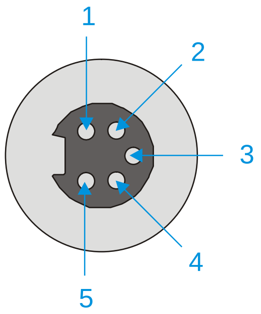


Figure 2-24 The UPS Battery Extension Cable Output Connector

Pinout

Pin	Signal
1	DC Positive (+)
2	UPS Battery Positive (+)
3	Chassis Ground
4	UPS Battery Negative (–)
5	DC Negative (–)

Antenna Connections

Note: VX7's are equipped with a radio and require an either an external or an internal antenna. Some VX7's may be equipped with a dual antenna option. For these VX7's, an external antenna must be connected to each antenna connector.

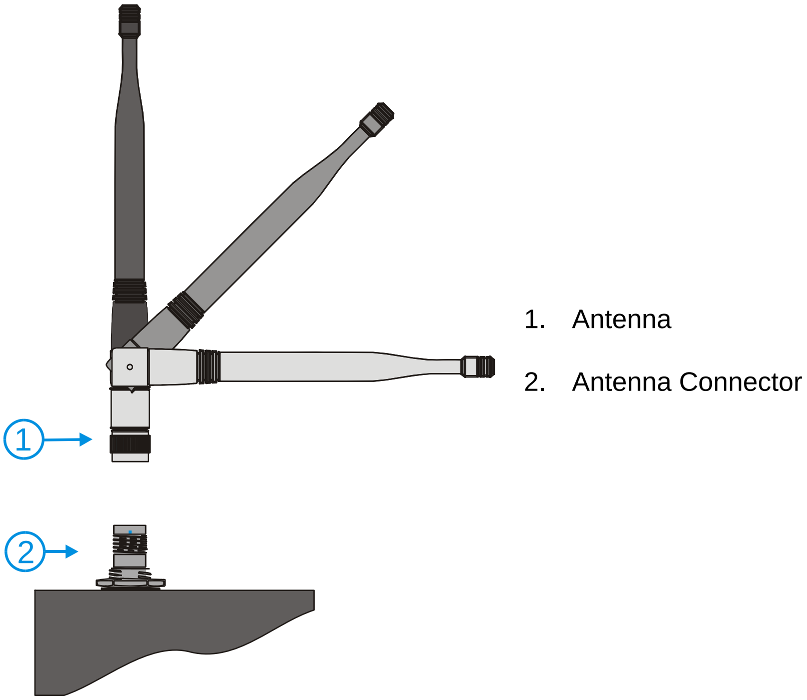


Figure 2-25 2.4GHz External Antenna

Spread Spectrum RF Antenna Connector Pin

VX7's ordered with an external antenna option have either one or two antenna connectors located on top of the unit. VX7's ordered with the internal antenna option do not have an external antenna connector.

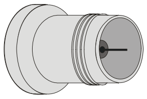


Figure 2-26 RF Antenna SS Connector

Vehicle Remote Antenna Mount

The external antenna (or antennas) can be remotely mounted on the vehicle. Please refer to the "Vehicle Remote Mount Antenna Installation Sheet" for details.

Internal Antenna

If the internal antenna option is ordered, an antenna is mounted on the inside of the user access panel cover.

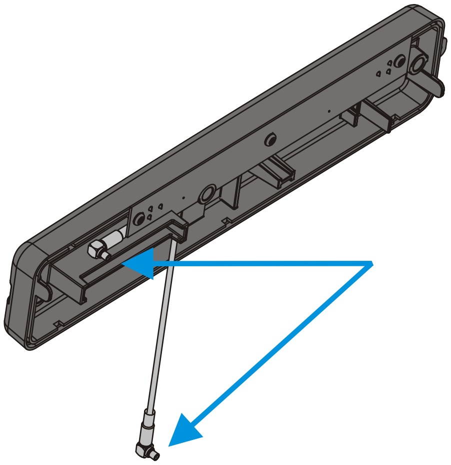


Figure 2-27 Internal Antenna Cables

The internal antenna assembly has two antenna cables which are attached to the radio card.

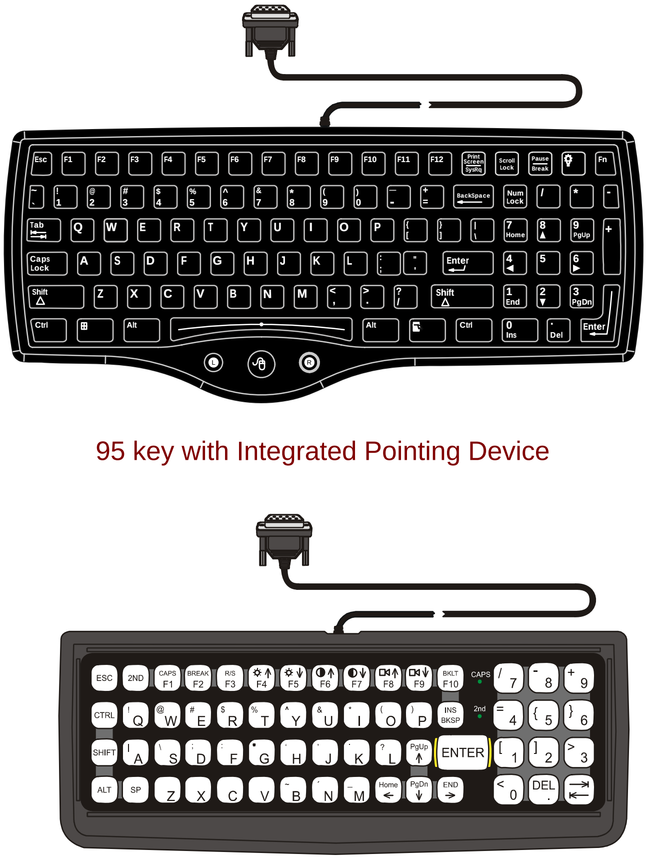
The Keyboards

The following keyboard options are available for the VX7:

The LXE VMT keyboards are customized rugged keyboards, connected to the VX7 via a watertight connector. The keyboards are available in the following configurations:

- LXE VMT 95-key QWERTY keyboard with integrated pointing device – a customized rugged keyboard connected to the VX7 via a watertight connector.
- LXE VMT 60-key QWERTY keyboard – a customized rugged keyboard connected to the VX7 via a watertight connector
- A standard PS/2 keyboard via an adapter cable attached to the “Keyboard/Mouse” port on the VX7. The adapter cable also provides a connector for a PS/2 mouse.
- A USB keyboard via a dongle cable attached to the “Ethernet/USB” connector.
- A software keyboard, or virtual keyboard, can be displayed on the touchscreen. The virtual keyboard can be used in place of, or in addition to, a physical keyboard.

For more details on each keyboard type, please refer to the appropriate section later in this chapter.



95 key with Integrated Pointing Device

60 key

Figure 2-28 The LXE VMT Keyboards with Cable

The 95-key QWERTY Keyboard with Pointing Device

Designed for ease of use with the Windows CE operating system, the 95-key keyboard with pointing device connects via a cable to the keyboard port on the VX7. Additional Windows keys (the Windows logo key and the Application key) and an integrated pointing device are provided.

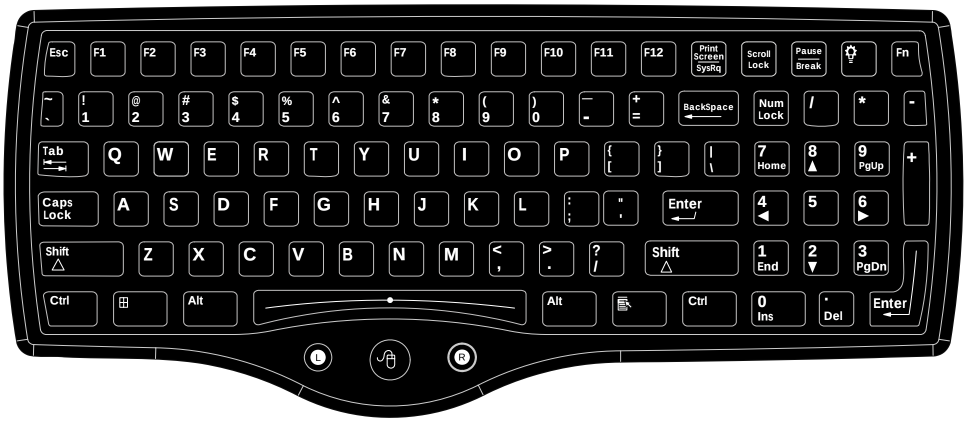

Esc F1 F2 F3 F4 F5 F6 F7 F8 F9 F10 F11 F12 Print Screen SysRq Scroll Lock Pause Break Fn
~ ` ! 1 @ 2 # 3 $ 4 % 5 ^ 6 & 7 * 8 (9) 0 _ - + = BackSpace Num Lock / * -
Tab Q W E R T Y U I O P { [}] | \ 7 Home 8 ▲ 9 PgUp +
Caps Lock A S D F G H J K L : ; " ' Enter 4 ◀ 5 6 ▶
Shift Z X C V B N M < , > . ? / Shift 1 End 2 ▼ 3 PgDn
Ctrl Alt Alt Ctrl 0 Ins . Del Enter
L R

Figure 2-29 The 95-key QWERTY Keyboard

Key Maps

The 95-key keyboard supports all 104 keyboard functions (101 keyboard standard plus Windows keys) and includes an integrated pointing device and left and right mouse buttons. However, because the keyboard only has 95 keys, all functions are not visible (or printed on the keyboard). Therefore the VX7 keyboard supports what is called hidden keys -- keys that are accessible but not visible on the keyboard.

Note: The 95-key keyboard does not have a 2^{nd} key function.

NumLock and the VX7

For the 95-key keyboard, the NumLock key and the numeric keys are backlit **green** when NumLock is off. When NumLock is on, the backlight for the NumLock key and the numeric keys is **amber**.

For information on preserving NumLock configuration after a reboot, please see “Configuring NumLock Behavior” in Chapter 3, “System Configuration”.

CapsLock and the VX7

For the 95-key keyboard, the CapsLock key is backlit **green** when CapsLock is off. When CapsLock is on, the backlight for the CapsLock key is **amber**.

For information on preserving CapsLock configuration after a reboot, please see “Configuring CapsLock Behavior” in Chapter 3, “System Configuration”.

Scroll Lock and the VX7

The Scroll Lock key is backlit **green** when Scroll Lock is off. When Scroll Lock is on, the backlight for the Scroll Lock key is **amber**.

The default values for CapsLock and Scroll Lock are Off.

Keyboard Backlight

The 95-key keyboard backlights each key. The keyboard backlight is manually controlled using the “backlight” key in the upper right hand corner of the keyboard. Pressing the backlight key cycles the keyboard backlight through the levels of backlight intensity:

- Off
- Maximum intensity
- Medium intensity
- Low intensity.

The 60-key QWERTY Keyboard

The 60-key keyboard has 101 keyboard functions, including a numeric keyboard pad. Please refer to Appendix A, “Key Maps”, for keypress combinations. This keyboard is also available with either an IBM 3270 or IBM 5250 overlay.

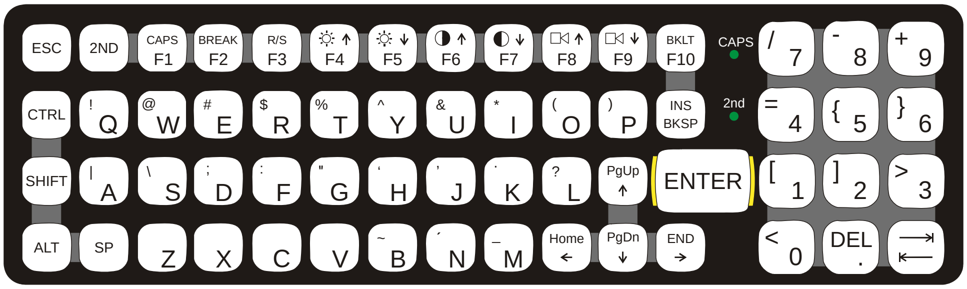

ESC 2ND CAPS F1 BREAK F2 R/S F3 F4 F5 F6 F7 F8 F9 BKLT F10 CAPS / 7 - 8 + 9
CTRL ! Q @ W # E $ R % T ^ Y & U * I (O) P INS BKSP 2nd = 4 { 5 } 6
SHIFT | A \ S ; D : F " G ' H ' J ` K ? L PgUp ENTER [1] 2 > 3
ALT SP Z X C V ~ B ´ N _ M Home PgDn END < 0 DEL .

Figure 2-30 The 60-key QWERTY Keyboard

IBM 3270 Keypad Overlay

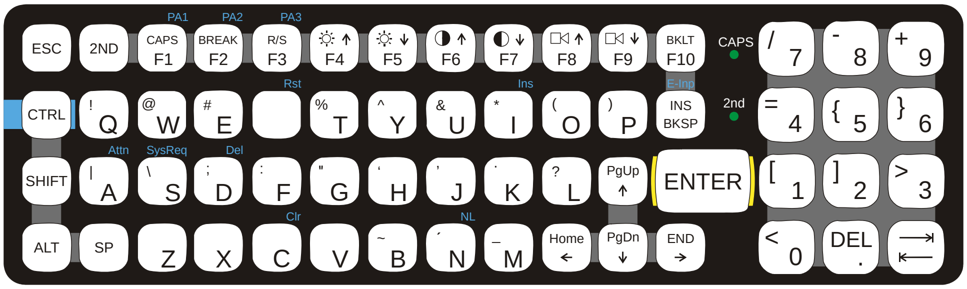

PA1 PA2 PA3
ESC 2ND CAPS F1 BREAK F2 R/S F3 F4 F5 F6 F7 F8 F9 BKLT F10 CAPS / 7 - 8 + 9
Rst Ins E-Inp
CTRL ! Q @ W # E % T ^ Y & U * I (O) P INS BKSP 2nd = 4 { 5 } 6
Attn SysReq Del
SHIFT | A \ S ; D : F " G ' H ' J ` K ? L PgUp ENTER [1] 2 > 3
Clr NL
ALT SP Z X C V ~ B ´ N _ M Home PgDn END < 0 DEL .

Figure 2-31 IBM 3270 Specific Keypad

The 60-key keypad is available with an IBM 3270 overlay designed to allow the user to enter terminal emulator commands when running LXE’s RFTerm™ program.

IBM 5250 Keypad Overlay

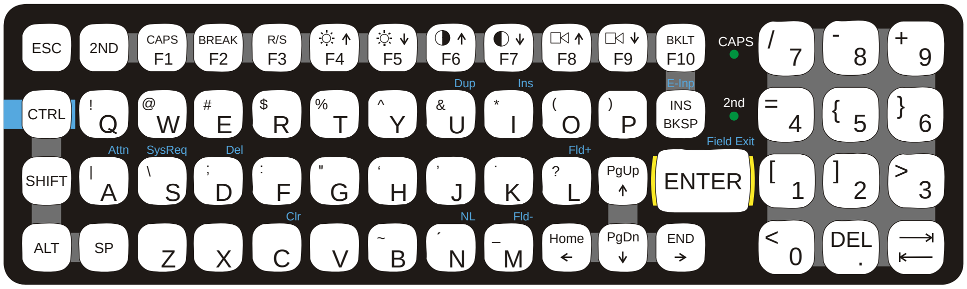

ESC 2ND CAPS F1 BREAK F2 R/S F3 F4 F5 F6 F7 F8 F9 BKLT F10 CAPS / 7 - 8 + 9
Dup Ins E-Inp
CTRL ! Q @ W # E $ R % T ^ Y & U * I (O) P INS BKSP 2nd = 4 { 5 } 6
Attn SysReq Del Fld+ Field Exit
SHIFT | A \ S ; D : F " G ' H ' J ` K ? L PgUp ENTER [1] 2 > 3
Clr NL Fld-
ALT SP Z X C V ~ B ´ N _ M Home PgDn END < 0 DEL .

Figure 2-32 IBM 5250 Specific Keypad

The 60-key keypad is available with an IBM 5250 overlay designed to allow the user to enter terminal emulator commands when running LXE’s RFTerm™ program.

Key Maps

The 60-key keyboard supports all 101 keyboard functions. However, because the keyboard only has 60 keys, all functions are not visible (or printed on the keyboard). Therefore the VX7 keyboard supports what is called hidden keys -- keys that are accessible but not visible on the keyboard.

The hidden keys supported by the VX7 are listed in Appendix A, “Key Maps”.

NumLock and the VX7

The 60-key keyboard does not have a NumLock indicator or key. NumLock can be toggled On or Off using the <2nd> <SHIFT> <F10> keypress sequence.

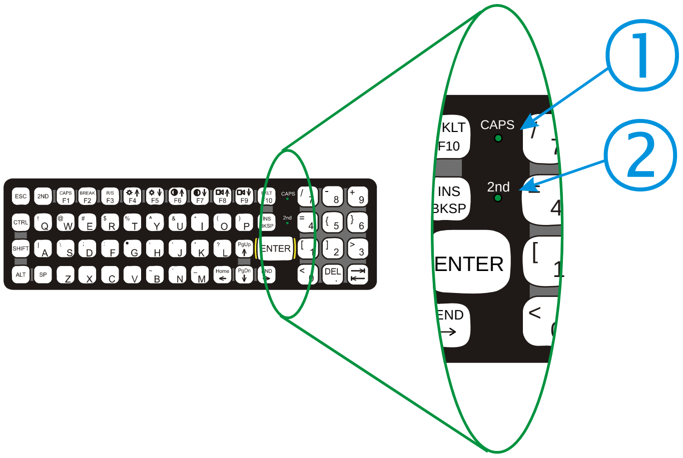
For information on preserving NumLock configuration after a reboot, please see “Configuring NumLock Behavior” in Chapter 3, “System Configuration”.

Keyboard Backlight

The LXE keyboard keys are backlit. The backlight is manually controlled using the <2nd> + <CTRL> + <F10> keypress sequence.

Keyboard LEDs

The VX7 keyboard has three (2) LED indicators.



1. CapsLock Mode LED Indicator
2. Secondary Mode LED Indicator

Figure 2-33 Keyboard LEDs

CAPS LED

This LED indicates the state of the keyboard CapsLock mode. If CapsLock is enabled this LED is illuminated green. When CapsLock is off, the LED is dark.

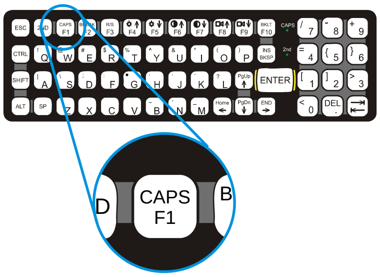


Figure 2-34 The CapsLock Key

Press <2nd> then <F1> to toggle CapsLock On and Off.

The default value of CapsLock is “Off”.

For information on preserving CapsLock configuration after a reboot, please see “Configuring CapsLock Behavior” in Chapter 3, “System Configuration”.

Secondary Keys LED

The VMT keyboard is equipped with several secondary keys. These keys are identified by the superscripted text found on the keyboard keys. The secondary keys are accessible by using two (2) keystrokes: the <2nd> key followed by the superscripted key.

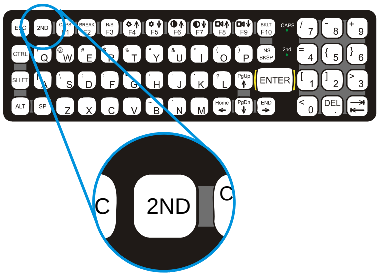


Figure 2-35 The Secondary Key

Once the <2nd> state is enabled (by pressing the <2nd> key) the Secondary Mode LED is illuminated and the <2nd> state is enabled until another key is pressed. The <2nd> key is toggled on with a <2nd> keypress and then immediately off with another <2nd> keypress.

For example:

Press <2nd> and <F1> to turn CapsLock on and off.

Press <2nd> and <↑> to initiate the PgUp command.

Press <2nd> and <Q> to type the "!" key.

Press <2nd> and <BkSp> to enter the Insert (Ins) mode.

Control Keys

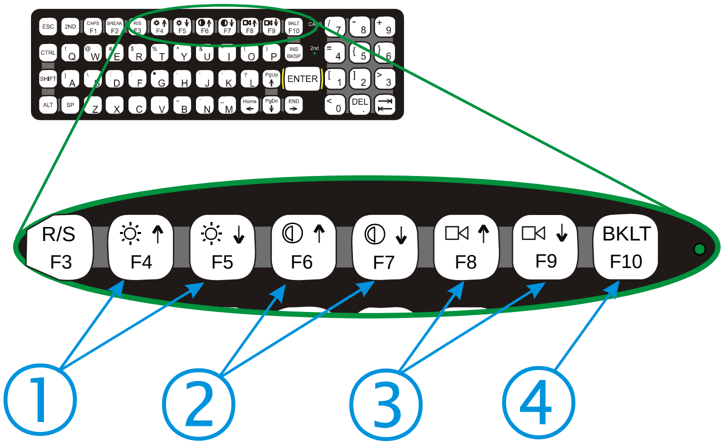
The VMT keyboard has several control keys. Because of the construction of the VX7 and the Microsoft Windows CE operating system, many of the Control Keys are not used on the VX7.

Note: *The 2nd functions of the <F4> and <F5>keys are not used as the display brightness is adjusted via the buttons on the VX7 Control Panel.*

The 2nd functions of the <F6>, and <F7> keys are not used as the VX7 has TFT LCD screen with no provision for contrast adjustments.

The 2nd functions of the <F8> and <F9> keys are not used as the sound volume on the VX7 is controlled with the Volume and Sounds icon in the Microsoft Windows CE Control Panel.

The <F10> key is used to toggle the backlight as part of the keypress sequence <2nd> + <CTRL> + <F10>. This key sequence immediately toggles the status of the keyboard backlight. Pressing <2nd> + <F10> has no effect on the keyboard backlight.



1. Display Brightness Control Keys (Not used)
2. Display Contrast Control Keys (Not used)
3. Speaker Volume Control Keys (Not used)
4. Backlight Control Key (See above)

Figure 2-36 The VMT Keyboard Display Controls

General Windows CE Keyboard Shortcuts

Use the keyboard shortcuts in the chart below to navigate with any VX7 keyboard. These are standard keyboard shortcuts for Windows CE applications.

Press these keys …	**To …**
CTRL + C	Copy
CTRL + X	Cut
CTRL + V	Paste
CTRL + Z	Undo
DELETE	Delete
SHIFT with any of the arrow keys	Select more than one item in a window or on the desktop, or select text within a document.
CTRL+A	Select all.
ALT+ESC	Cycle through items in the order they were opened.
CTRL+ESC	Display the Start menu.
ALT+Underlined letter in a menu name	Display the corresponding menu.
Underlined letter in a command name on an open menu	Carry out the corresponding command.
ESC	Cancel the current task.

The touchscreen provides equivalent functionality to a mouse:

- A touch on the touchscreen is equivalent to a left mouse click.
- Many items can be moved by the “drag and drop” method, touching the desired item, moving the stylus across the screen and releasing the stylus in the desired location.
- A double stylus tap is equivalent to a double click.
- A touch and hold is equivalent to a right mouse click.

Note: Some applications may not support this right click method. Please review documentation for the application to see if it provides for right mouse click configuration.

PS/2 Keyboard/Mouse

A standard PS/2 keyboard and mouse can be attached to the VX7 using the appropriate dongle cable. The dongle cable attaches to the VX7 and provides two PS/2 connectors, one labeled “Keyboard” and one labeled “Mouse”. Please refer to documentation provided with the PS/2 keyboard and mouse for more information on their operation.

USB Keyboard/Mouse

A standard USB mouse can be attached to the VX7 using the appropriate dongle cable. A standard USB keyboard cane be attached to Platform 2 VX7's using the appropriate dongle cable. The dongle cable attaches to the VX7 and provides a USB connector. Please refer to documentation provided with the USB keyboard and mouse for more information on their operation.

To identify your VX7 platform type, please see "Identifying Your VX7", earlier in this chapter.

Input Panel (Virtual Keyboard)

The Input Panel may be enabled via the Input Panel icon in the Microsoft Windows CE Control panel. The Input Panel can be displayed as a large or small keyboard.

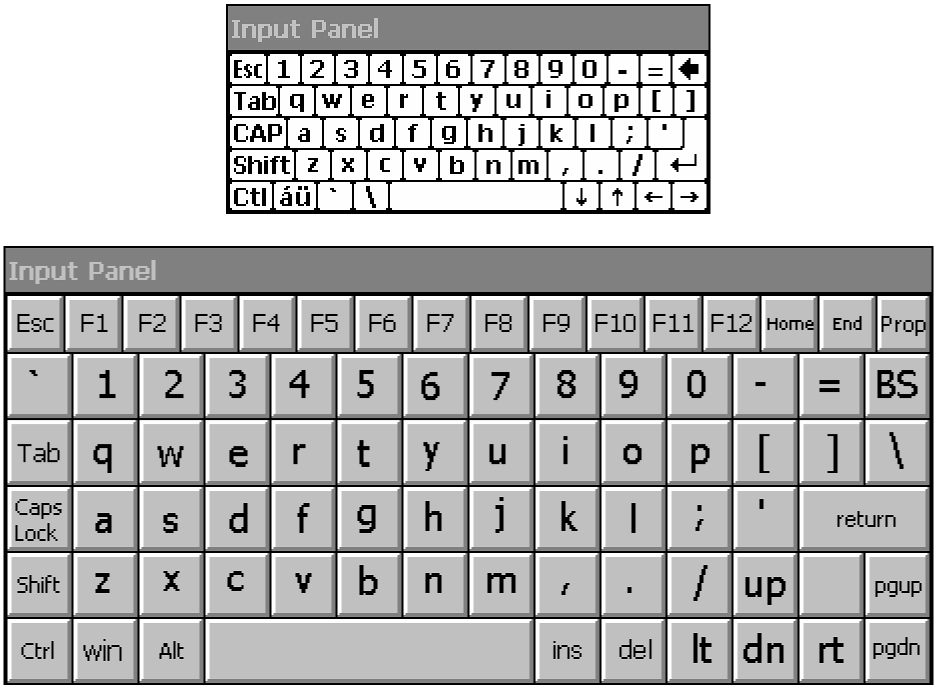

Input Panel
Esc 1 2 3 4 5 6 7 8 9 0 - =
Tab q w e r t y u i o p [ ]
CAP a s d f g h j k l ; '
Shift z x c v b n m , . /
Ctl áü ` \ ↓ ↑ ← →
Input Panel
Esc F1 F2 F3 F4 F5 F6 F7 F8 F9 F10 F11 F12 Home End Prop
` 1 2 3 4 5 6 7 8 9 0 - = BS
Tab q w e r t y u i o p [ ] \
Caps Lock a s d f g h j k l ; ' return
Shift z x c v b n m , . / up pgup
Ctrl win Alt ins del lt dn rt pgdn

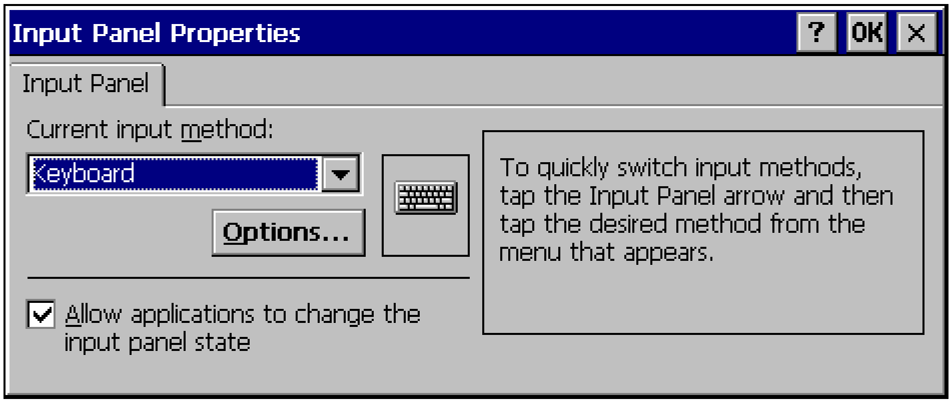
Figure 2-37 Small and Large Virtual Keyboards

Virtual keyboards display the actual character a keypress results in. For example, pressing the <Shift> key on the virtual keyboard toggles the characters displayed on the keys between upper and lower case. The <áü> key toggles the keys between standard and international symbols. The <Shift> and <áü> keys can be used in combination for capitalized international characters.

Note: When the virtual keyboard is displayed, the physical keyboard is still active, if attached. Therefore it is possible to input data from both keyboards.

Enabling the Input Panel

The Input Panel is disabled by default. To enable the Input Panel, select **Start | Settings | Control Panel |Input Panel** icon. Make sure the "Allow applications to change the input panel state" checkbox is checked and warmboot the VX7.



Input Panel Properties

Current input method: Keyboard

☑ Allow applications to change the input panel state

To quickly switch input methods, tap the Input Panel arrow and then tap the desired method from the menu that appears.

Figure 2-38 Input Panel Properties

The Display

The VX7 Display is a thin-film transistor display capable of supporting SVGA graphics modes. Display size is 800 x 600 pixels. The display covering is designed to resist stains. The touchscreen allows signature capture and touch input.

The display supports screen blanking to eliminate driver distraction when the vehicle is in motion. Please see "Technical Specifications – Screen Blanking Cable" earlier in this chapter and "Screen Blanking" in Chapter 4, "Scanner" for details.

Cleaning the Display

Keep fingers and rough or sharp objects away from the display. If the glass becomes soiled or smudged, clean only with a standard household cleaner such as Windex® without vinegar or use Isopropyl Alcohol. Do not use paper towels or harsh-chemical-based cleaning fluids since they may result in damage to the glass surface. Use a clean, damp, lint-free cloth. Do not scrub optical surfaces. If possible, clean only those areas which are soiled. Lint/particulates can be removed with clean, filtered canned air.

Touchscreen

The touchscreen is a Resistive Panel with a scratch resistant finish that can detect touches by a stylus, and translate them into computer commands. In effect, it simulates a computer mouse. Only Delrin or plastic styluses should be used. A right mouse click is simulated by touching and holding the screen for the appropriate time interval.

Note: Always use the point of the stylus for tapping or making strokes on the display. Never use an actual pen, pencil or sharp object to write on the touchscreen.

An extra or replacement stylus may be ordered from LXE. See the "Accessories" section for the stylus part number.

Please refer to Chapter 3, "System Configuration" for more information on:

- Calibrating the touchscreen
- Disabling the touchscreen.

LXE offers a replaceable touchscreen protective film to protect the touchscreen when the VX7 is used in an abrasive environment. For information on installing or removing the protective film, please refer to the "VX7 User's Guide".

Touchscreen Heater

Extended temperature versions of the VX7 contain a touchscreen heater. The touchscreen heater can be disabled on Platform 2 VX7's when not needed. Please see "Disabling the Touchscreen Heater" in Chapter 3, "System Configuration".

Note: To identify your VX7 platform type, please see "Identifying Your VX7", earlier in this chapter.

PCMCIA, CF and SD Slots

The VX7 has two PCMCIA slots, one Compact Flash slot and one Secure Digital slot. The PCMCIA slots are stacked on top of each other and located on the right hand side of the opening. The PCMCIA slots support the Personal Computer Memory Card International Association (PCMCIA) 2.1 standards. The upper slot is designated as Slot A and the lower slot is designated as Slot B.

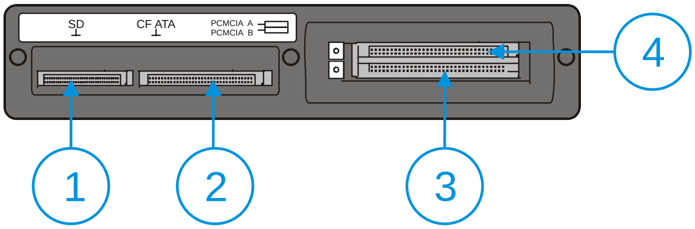
Slot A accepts Type I or II PCMCIA cards. If a radio card is used, it must be installed in Slot A to prevent damage to the internal radio cables. LXE supports only Type II 2.4GHz Spread Spectrum radios.

Slot B accepts Type I or II PCMCIA cards.

The PCMCIA slots may be disabled by the user. To enable or disable a PCMCIA slot, select **Start | Settings | Control Panel |PCMCIA** icon.

The center slot is a Compact Flash slot, containing the CF ATA hard drive. This drive contains the operating system and settings.

The left slot is used for Secure Digital (SD) memory cards.



1. SD Card Slot
2. Compact Flash Hard Drive
3. PCMCIA Slots

Figure 2-39 The PCMCIA and ATA Slots

PCMCIA Slots

Slot A and B PCMCIA Card Management is handled by the Microsoft Windows CE operating system. The PCMCIA cards are Plug and Play devices and can be “hot swapped”. For more details, refer to the Windows CE help screens or refer to the documentation delivered with the PCMCIA card.

Note: Although cards in the PCMCIA slots may be hot swapped, the VX7 is not environmentally sealed while the access panel cover is removed to hot swap PCMCIA cards.

PCMCIA Pinout

Pin	Signal	Pin	Signal
1	GND	35	12V_RF_POWER
2	D3	36	-CDI
3	D4	37	D11
4	D5	38	D12
5	D6	39	D13
6	D7	40	D14
7	-CE1	41	D15
8	A10	42	-CE2
9	-OE	43	n.c. or VS1#
10	A11	44	-IORD
11	A9	45	-IOWR
12	A8	46	A17
13	A13	47	A18
14	A14	48	A19
15	-WE	49	A20
16	RDY/-IREQ	50	A21
17	SLOT_VCC	51	SLOT_VCC
18	SLOT-VPP	52	SLOT_VPP
19	A16	53	A22
20	A15	54	A23
21	A12	55	A24
22	A7	56	A25
23	A6	57	n.c. or VS2#
24	A5	58	RESET
25	A4	59	-WAIT
26	A3	60	-INPACK
27	A2	61	-REG
28	A1	62	BVD2/-SPKR
29	A0	63	BDV1/-STSCHG
30	D0	64	D8
31	D1	65	D9
32	D2	66	D10
33	WP/A_-IOIS16	67	-CD2
34	GND	68	GND

Install PCMCIA Cards

Equipment Needed: Phillips No. 1 screwdriver and a Torque wrench capable of measuring to 9±1 inch pounds (1.016±.11 N/m).

Note: The example below details installing a 2.4GHz radio card. Installation of other PCMCIA cards is similar, except there is no antenna.

The 2.4 GHz radio card is installed in slot A (the upper slot). When a second PCMCIA card is present, such as a Bluetooth CF card via a PCMCIA adapter, the second card is installed in Slot B (the lower slot).

Install the 2.4GHz Type II PCMCIA Radio

Caution ⚠	*The LXE Model VX7 Vehicle Mount Computer is specifically for use with LXE Model 6726, 6816 and 6830 2.4GHz Type II PCMCIA radios. Substitution of other PCMCIA radios will void the FCC, Industry Canada and other international radio certifications for the Model VX7 Vehicle Mount Computer and is strictly prohibited.*

1. Turn the VX7 off and detach the power cable.

2. Loosen the three (3) Phillips head screws securing the access panel cover so the cover can be removed. The screws are a captive part of the cover and cannot be removed.

   Partially insert the 2.4GHz Type II PCMCIA Radio into Slot A (the upper right slot).

   Caution ⚠ Slot A MUST BE used for the radio card. Installing a radio card in Slot B can result in pinching or other damage to the internal antenna cable.

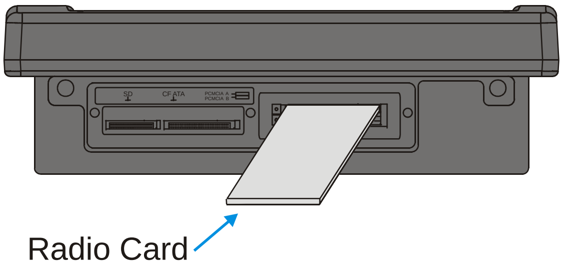


Figure 2-40 Inserting the 2.4GHz Type II PCMCIA Radio

Note: The tethered access panel cover is not shown in the illustration above.

3. Before completely inserting the 2.4GHz Radio, connect the Antenna Cable to the 2.4GHz Radio, using the port(s) indicated below:

   Note: Radio cards for single antenna units may have the unused antenna port covered with tape.

   The internal antenna is a dual (diversity) antenna.

Cisco Radio Card

Hold the radio card with the Cisco logo label facing up. Connect the antenna cable(s) as follows:

- Cisco radio with single antenna – Connect antenna cable to right port, as shown below.
- Cisco radio with dual antennas – Connect antenna cables to both ports.

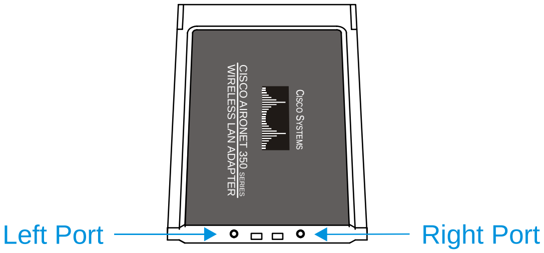


Figure 2-41 Cisco Antenna Cable Connections

Symbol 11Mb Radio Card

Hold the radio card with the Symbol logo label facing up. Connect the antenna cable(s) as follows:

- Symbol 11Mb radio with single antenna – Connect antenna cable to Port A (left port), as shown below.
- Symbol 11Mb radio with dual antennas – Connect antenna cables to both ports.

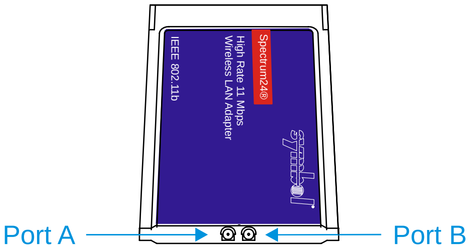


Figure 2-42 Symbol 11Mb Antenna Cable Connections

Summit CF Radio Card

The Summit CF radio is installed on a PCMCIA adapter. Hold the radio card with the antenna ports facing down. Connect the antenna cable(s) as follows:

- Summit radio with single antenna – Connect antenna cable to Main port. Auxiliary port is not used.
- Summit radio with dual antennas – Connect antenna cables to both Main and Auxiliary ports.

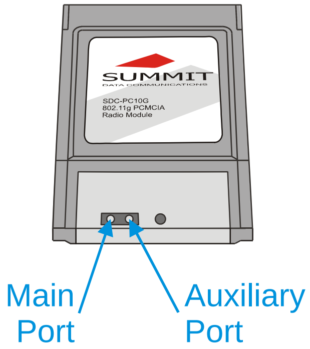


Figure 2-43 Summit Antenna Cable Connections

4. Now complete the insertion of the 2.4GHz Type II PCMCIA Radio into the slot.

   Note: When this process is complete, reattach the access cover screws using a torque wrench capable of measuring to 9±1 inch pounds (1.016±.11 N/m). The screws must be fastened to 9 inch pounds each. The screws require a Phillips size 1 driver head.

5. Re-connect the power cord/cable and turn the VX7 on.

6. For VX7's with a Summit radio, review RX Diversity and TX Diversity on the Global Settings tab of the Summit Client Utility to ensure these settings correspond to the VX7's antenna configuration.

CF Card Slot

This slot contains the Compact Flash (CF) hard drive.

⚠	The operating system and settings are stored on the CF card. The VX7 cannot operate without this card. Cards in this slot CANNOT be hot swapped.

Replace a CF Card

1. Turn the VX7 off and detach the power cable.
2. Loosen the three (3) Phillips head screws securing the access panel cover so the cover can be removed. The screws are a captive part of the cover and cannot be removed.
3. Remove the card currently installed present in the CF slot and replace it with the new CF card. The replacement CF card must contain the operating system in order for the VX7 to operate.

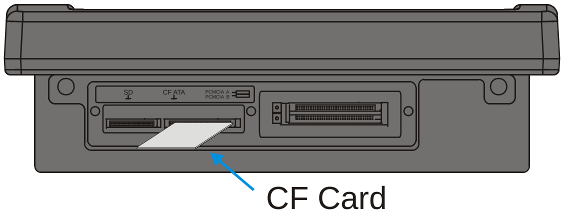


Figure 2-44 Inserting the CF ATA Card

Note: The tethered access panel cover is not shown in the illustration above.

Note: When this process is complete, reattach the access cover screws using a torque wrench capable of measuring to 9±1 inch pounds (1.016±.11 N/m). The screws must be fastened to 9 inch pounds each. The screws require a Phillips size 1 driver head.

4. Re-connect the power cord/cable and turn the VX7 on.

SD Card Slot

The slot accepts a Secure Digital (SD) memory card. The card in this slot can be hot swapped.

Note: Although cards in the SD slot may be hot swapped, the VX7 is not environmentally sealed while the access panel cover is removed to hot swap cards.

Install an SD Card

1. Turn the VX7 off and detach the power cable.
2. Loosen the three (3) Phillips head screws securing the access panel cover so the cover can be removed. The screws are a captive part of the cover and cannot be removed.
3. Insert the card into the ATA SD. This slot accepts an SD memory card only.

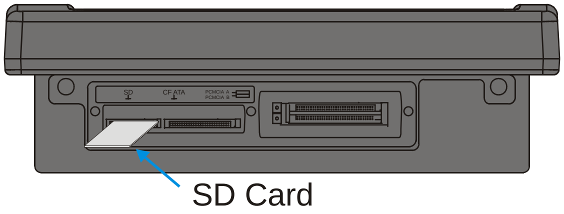


Figure 2-45 Inserting the ATA Card

Note: The tethered access panel cover is not shown in the illustration above.

Note: When this process is complete, reattach the access cover screws using a torque wrench capable of measuring to 9±1 inch pounds (1.016±.11 N/m). The screws must be fastened to 9 inch pounds each. The screws require a Phillips size 1 driver head.

4. Re-connect the power cord/cable and turn the VX7 on.

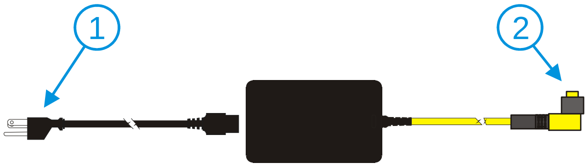
Power Supply

AC to DC power input for the VX7 is delivered via an optional external power supply. See "External Power Supply".

Vehicle power input for the VX7 is 12V to 80V DC nominal and is accepted without the need to perform any manual operation within the VX7. See "Vehicle 12-80VDC Direct Connection". An optional uninterruptible power supply (UPS) battery can be used with the vehicle DC power supply.

Power input is fused for protection and the fuse is externally accessible on the VX7.

External Power Supply



1. AC Input Cable (US only)
2. DC Output Cable

Figure 2-46 Optional Power Supply Cable

In North America, this unit is intended for use with a UL Listed ITE power supply with output rated 12 – 80 VDC, minimum 75 W. Outside North America, this unit is intended for use with an IEC certified ITE power supply with output rated 12 – 80 VDC, minimum 75 W.

The external power supply may be connected to either a 120V, 60Hz supply or, outside North America, to a 230V, 50Hz supply, using the appropriate detachable cordset. In all cases, connect the external AC supply to a properly grounded source of supply provided with maximum 15 Amp overcurrent protection (10 Amp for 230V circuits).

Note: Instructions for using this configuration are contained in "VX7 User's Guide" section titled "Installation".

Specifications

Feature	Specification
Dimensions	3.40” x 5.87” x 2.00”
Weight	<3.0 pounds
Input Power Switch	None
Power “ON” Indicator	None
Input Fusing	None
Input Voltage	90VAC min - 264VAC max
Input Frequency	47 - 63 Hz
Input Surge Current	50 Amps max @ 264VAC input
Input Connector	Standard IEC input power cord (included with US units only)
Output Connector	3 pin female connector
Output Voltage	+24VDC
Output Voltage Tolerance	+/- 8%, measured at the end of the output power cable
Output Current	0 Amps min, 1.87 Amps max
Safety and Emissions Compliance	FCC, Part 15, Radio Frequency Devices, Class B. EN 55022 UL1950 and IEC 950

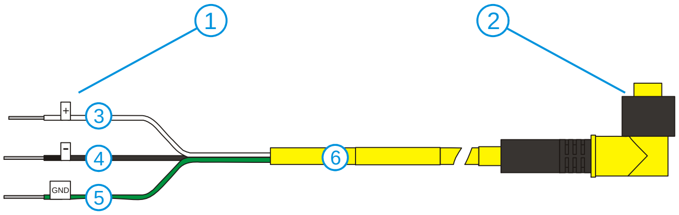
Environmental Specifications

The AC to DC adapter will withstand the following environmental characteristics:

Feature	Specification
Operating Temperature	see VX7 Environmental Specifications
Storage Temperature	see VX7 Environmental Specifications
Humidity	Operates in a relative humidity of: 5 – 95% (non-condensing)
ESD Immunity	Per IEC 801-1

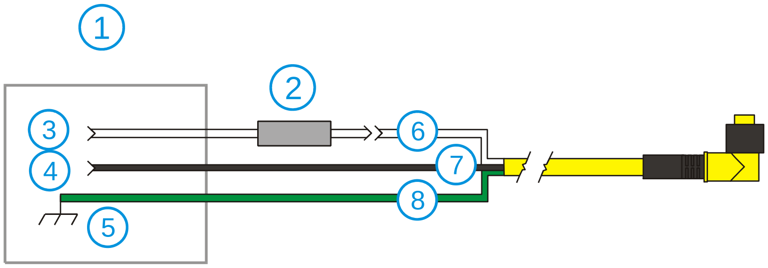
Vehicle 12-80VDC Direct Connection

Note: Instructions for using this configuration are contained in "VX7 User's Guide" section titled "Installation".



1. To Vehicle Battery
2. To Vehicle Mounted Device or UPS Battery Pack
3. White (DC+)
4. Black (DC-)
5. Green (GND)
6. 12 – 80 VDC

Figure 2-47 Direct Vehicle Power Connection Cable (12 Ft.)



1. Vehicle Electrical System
2. 5 Amp Slow Blow Fuse
3. DC +
4. DC -
5. Vehicle Chassis
6. Red / White
7. Red /Black
8. Green

Figure 2-48 Connecting the Power Cable to the Vehicle

Note: Correct electrical polarity is required for safe and proper installation. Connecting the cable to the VX7 with the polarity reversed will cause the VX7's fuse to be blown. See the following table for wire color-coding specifics.

Wiring color codes for LXE supplied DC input power cabling:

Vehicle Supply		Wire Color
+12 - 80VDC	(DC +)	White
Return	(DC -)	Black
Vehicle Chassis	(GND)	Green

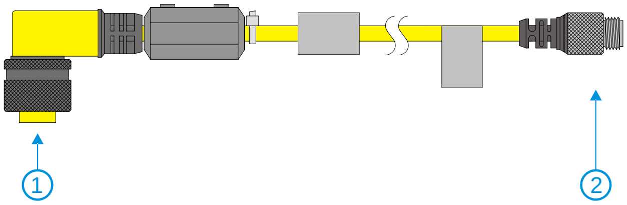
Figure 2-49 Vehicle Connection Wiring Color Codes

VX7 Input Power Specifications

Feature	Specification
DC Input Voltage	12 - 80 VDC
Input Current	3.5 Amps
Input Fuse	10A Time Delay
Input Power Switch	SPST 6 Amp 125VDC

Power Adapter Cable

LXE offers an adapter cable (part no. 9000A077CBLPWRADPTR) to adapt certain VX1, VX2 or VX4 DC power supplies to the VX7. Please read and follow all cautions in the "VX7 User's Guide" to determine if your present power supply can be used with the VX7.



1. VX7 Connector
2. VX1/2/4 Power Supply Connector

Figure 2-50 Power Adapter Cable, VX1/2/4 to VX7

Caution: ⚠	For use only with VX1/2/4 DC power cables with yellow colored cable containing 18AWG wires. Do not use this cable with VX1/2/4 DC power cables with gray colored cable containing 22AWG wires. These power cables must be replaced with a VX5/6/7 power cable.
Caution: ⚠	When a DC power cable that is eight feet or longer is in a 12V application, there may be an excessive voltage drop over the longer cable. If this occurs, a new power cable is required.
Caution: ⚠	Do not use this adapter with AC power supplies originally designed for the 1380, 1390, VX1, VX2 or VX4. These power supplies do not have sufficient power for the VX7.

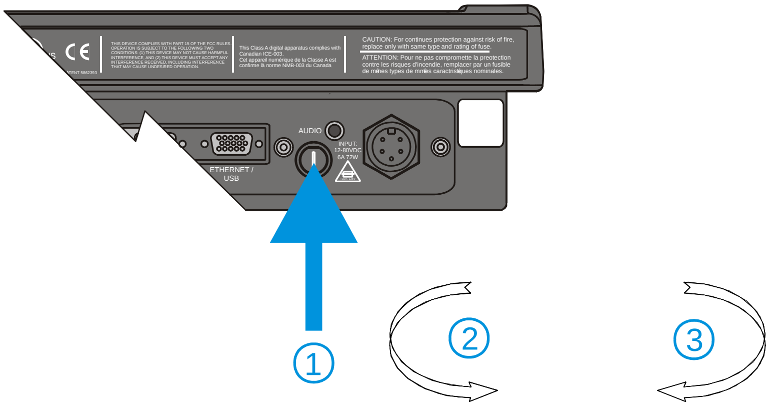
CMOS Battery

The LXE VX7 has a permanent 190 mAh Lithium battery installed to maintain time, date and CMOS setup information. The lithium battery is not user serviceable and should last five years with normal use before it requires replacement.

Note: This battery should only be changed by authorized service personnel.

Fuse

The VX7 uses a 100V, 10A time delay (slow blow), high current interrupting rating fuse that is externally accessible and user replaceable. Should it need replacement, replace with same size, rating and type of fuse – Littlefuse 0234010 or Optifuse MSC-10A (5x20mm).


CE
THIS DEVICE COMPLIES WITH PART 15 OF THE FCC RULES. OPERATION IS SUBJECT TO THE FOLLOWING TWO CONDITIONS: (1) THIS DEVICE MAY NOT CAUSE HARMFUL INTERFERENCE, AND (2) THIS DEVICE MUST ACCEPT ANY INTERFERENCE RECEIVED, INCLUDING INTERFERENCE THAT MAY CAUSE UNDESIRED OPERATION.
ATENT 5862393
This Class A digital apparatus complies with Canadian ICE-003.
Cet appareil numérique de la Classe A est confime là norme NMB-003 du Canada
CAUTION: For continues protection against risk of fire, replace only with same type and rating of fuse.
ATTENTION: Pour ne pas compromette la preotection contre les risques d'incendie, remplacer par un fusible de mêmes types de mmes caractristques nominales.
AUDIO
INPUT: 12-80VDC 6A 72W
ETHERNET / USB
1
2
3

1. Fuse
2. Twist in this direction to remove
3. Twist in this direction to insert

Figure 2-51 Fuse Replacement

Caution: **Fuse has voltage on it even when power is off. Always disconnect input power before changing fuse.**

Chapter 3 System Configuration

Introduction

There are several different aspects to the setup and configuration of the VX7. Many of the setup and configuration settings are dependent upon the optional features such as hardware and software installed on the unit. The examples found in this chapter are to be used *as examples only*, the configuration of your specific VX7 computer may vary. The following sections provide a general reference for the configuration of the VX7 and some of its optional features.

Your VX7 operating system may be Windows CE .NET or Windows CE 5.0. The VX7 operating system version is displayed on the Desktop in the default Desktop Display Background.

This chapter presents information and procedures that are common to both CE versions unless otherwise noted.

Windows CE Operating System

For general use instruction, please refer to commercially available Windows CE user's guides or the Windows CE on-line Help application installed with the VX7.

This chapter's contents assume the system administrator is familiar with Microsoft Windows options and capabilities loaded on most standard Windows computers.

Therefore, the sections that follow describe only those Windows capabilities that are unique to the VX7 and its Windows CE environment.

2.4 GHz Radio Configuration

All 2.4GHz radio configuration is included in Chapter 5, "Wireless Network Configuration".

Warmboot

A warmboot reboots the computer without erasing any registry data. However, any applications installed to RAM are lost, as is all data in RAM. This happens because the operating system is stored on the flash drive, but must be loaded into RAM to run.

All registry configurations are automatically preserved. Any applications stored as .CAB files in the System directory and configured in the registry to persist are reinstalled on boot up by the Launch utility.

Coldboot

A coldboot reboots the computer, erases all registry data and returns the computer to factory default settings. In order to be preserved, applications and data must be stored in the System folder. Registry information is not preserved. Only factory default applications and drivers stored as .CAB files in the System directory are loaded by Launch.

A cold boot is initiated by running the Coldboot application in the \Windows directory. This application automatically cold boots the VX7, erasing any customer applied registry changes and returning the VX7 to its factory settings.

Installed Software

When you order a VX7 you receive the software files required by the separate programs needed for operation and radio communication. The files are loaded by LXE and stored in subdirectories in the VX7.

This section lists the contents of the subdirectories and the general function of the files. Files installed in each VX7 are specific to the intended function of the VX7.

Files installed in each VX7 configured for an RF environment contain PCMCIA card radio specific drivers – the drivers for each type of radio are specific to the manufacturer (e.g. Summit, Cisco, Symbol) for the radios installed in the RF environment and are not interchangeable.

Software Load

The software loaded on the mobile computer consists of Windows CE .NET 4.2 or Windows CE 5.0 OS, hardware-specific OEM Adaptation Layer, device drivers, Internet Explorer 6.0 for Windows CE browser and utilities. The software supported is summarized below:

Operating System

- **Full Operating System License:** Includes all operating system components, including Windows CE 5.0 or CE .NET 4.2 kernel, file system, communications, connectivity (for remote APIs), device drivers, events and messaging, graphics, keyboard and touchscreen input, window management, and common controls.

Network and Device Drivers

Bluetooth (Optional)

Wavelink Avalanche (Optional)

LXE AppLock

Java (Optional)

- Java executables and browser components are handled by the Java option (when installed).

Terminal Emulation (Optional)

- RFTerm (VT220, TN5250, TN3270). Runs automatically at the conclusion of each reboot (if installed).

LXE API Routines (see “Accessories” for the LXE SDK Kit part number)

Note: Please contact your LXE representative for software updates and CAB files as they are released by LXE.

Software Applications

The following applications are included:

- WordPad (was PocketWord in previous versions of Windows CE)
- Pocket Inbox
- Word Viewer
- Excel Viewer

- PDF Viewer
- Image Viewer
- Scanner Wedge (LXE developed)
- ActiveSync
- Transcriber
- Media Player
- Internet Explorer

Note that the viewer applications allow viewing documents, but not editing them.

Java (Optional)

Installed by LXE. Files can be accessed by tapping **Start | Programs | JEM-CE**. Doubletap the EVM icon to open the EVM Console. A folder of Java examples and Plug-ins is also installed with the Java option. LXE does not support Java applications running on the mobile device.

LXE RFTerm (Optional)

Installed by LXE. The application can be accessed by tapping **Start** | **Programs** | **RFTerm**. Please refer to “Setup Terminal Emulation Parameters” earlier in this guide for RFTerm quick start instruction. Refer to the “RFTerm Reference Guide” on the LXE Manuals CD for complete information and instruction.

AppLock

Installed by LXE. Application is setup by the Administrator by tapping **Start** | **Settings** | **Control Panel** | **Administration**. Configuration parameters are specified by the AppLock Administrator for the mobile device end-user. AppLock is password protected by the Administrator. End-user mode locks the end-user into the configured application or applications. The end user can still reboot the mobile device and respond to dialog boxes. The administrator-specified application is automatically launched and runs in full screen mode when the device boots up.

See Also: Chapter 6 “AppLock” for instruction.

Wavelink Avalanche Enabler (Optional)

The following features are supported by the Wavelink Avalanche Enabler when used in conjunction with the Avalanche Mobility Center (MC) Console.

After configuration, Enabler files are installed upon initial bootup and after a hard reset. Network parameter configuration is supported for:

- IP address: DHCP or static IP
- RF network SSID
- DNS hosts (primary, secondary, tertiary)
- Subnet mask
- Enabler update

Related Manual: “Using Wavelink Avalanche on LXE Windows Computers”.

The VX7 has the Avalanche Enabler installation files loaded, but not installed, on the mobile device when it is shipped from LXE. The installation files are located in the System folder on CE devices. The installation application must be run manually the first time Avalanche is used.

After the installation application is manually run, a reboot is necessary for the Enabler to begin normal performance. Following this reboot, the Enabler will by default be an auto-launch application. This behavior can be modified by accessing the Avalanche Update Settings panel through the Enabler Interface. The designation of the mobile device to the Avalanche CE Manager is LXE_VXC.

LXE CE devices manufactured before October 2006 must have their drivers and system files upgraded before they can use the Avalanche Enabler functions. Please contact an LXE representative for details on upgrading the mobile device baseline.

If the user is NOT using Wavelink Avalanche to manage their mobile device, the Enabler should not be installed on the mobile device(s).

Desktop

For general use instruction, please refer to commercially available Windows CE user’s guides or the Windows on-line Help application installed in the mobile device.

The VX7 Desktop appearance is similar to that of a desktop PC running Windows 2000 or XP.

At a minimum, it has the following icons that can be double tapped with the stylus to access My Computer/My Device, Internet Explorer, and the Recycle Bin.

At the bottom of the screen is the Start button. Clicking the Start Button causes the Start Menu to pop up. It contains the standard Windows menu options: Programs, Favorites, Documents, Settings, Help, and Run.

Desktop Icon	Function
My Computer (CE .NET) My Device (CE 5.0)	Access files and programs.
Recycle Bin	Storage for files that are to be deleted.
Internet Explorer	Connect to the Internet/intranet (requires radio card and Internet Service Provider – ISP enrollment is not available from LXE).
Wireless Configuration Icon	Used for accessing the appropriate wireless configuration utility, either the SCU (Summit Client Utility) or ACU (Cisco Aironet Client Utility).
Bluetooth	Discover and then pair with nearby discoverable Bluetooth devices.
My Documents	Storage for downloaded files / applications.
Start	Access programs, select from the Favorites listing, documents last worked on, change/view settings for the control panel or taskbar, on-line help or run programs.

My Computer Folders (Windows CE .NET)

Folder	Description	Preserved upon Reboot?
System	Internal ATA Card	Yes
Network	Mounted network drive	No
Storage Card	ATA Card in Compact Flash or SD Card	No
Media Card	SD Memory Card	No
Windows	Operating System in ROM	No
Program Files	Applications	No
Application Data	Data saved by running applications	No
My Documents	Storage for downloaded files / applications	No
Temp	Location for temporary files	No

Folders Copies at Startup

The following folders are copied on startup:

System\Desktop => Windows\Desktop
System\Favorites => Windows\Favorites
System\Fonts => Windows\Fonts
System\Help => Windows\Help
System\Programs => Windows\Programs

This function copies only the directory contents, no sub-folders.

The following folders are NOT copied on startup:

Windows\AppMgr
Windows\Recent
Windows\Startup

Because copying these has no effect on the system or an incorrect effect.

Files in the Startup folder are executed, but only from System\Startup. Windows\Startup is parsed too early in the boot process so it has no effect.

Executables in System\Startup must be the actual executable, not a shortcut, because shortcuts are not parsed by launch.

My Device Folders (Windows CE 5.0)

Folder	Description	Preserved upon Reboot?
Application Data	Data saved by running applications	No
My Documents	Storage for downloaded files / applications	No
Network	Mounted network drive	No
Program Files	Applications	No
System	Internal SD Flash Card (CAB file storage)	Yes
Temp	Location for temporary files	No
Windows	Operating System in Secure Storage	No

Start Menu Program Options

The following options represent the factory default program installation. Your system may be different based on the software and hardware options purchased.

Access: **Start | Programs**

Cisco	**Set Cisco radio / network parameters**
	(Please see Chapter 5, "Wireless Network Configuration" for details)
Communication	**Stores Network communication options**
ActiveSync	Transfer files between a VX7 and a desktop computer
Connect	Run this command after setting up a connection
Start FTP Server	Begin connection to FTP server
Stop FTP Server	End connection to FTP server
Microsoft File Viewers	**View downloaded files** (see Note)
Excel Viewer	View Excel 97 and newer documents
Image Viewer	View BMP, JPEG and PNG images
PDF Viewer	View Adobe Acrobat documents
Word Viewer	View Word 97 and newer documents and RTF files
Summit	**Set Summit radio / network parameters**
	(Please see Chapter 5, "Wireless Network Configuration" for details)
Command Prompt	The command line interface in a separate window
Inbox	Microsoft Outlook mail inbox
Internet Explorer	Access web pages on the world wide Internet
Java	Option
LXE RFTerm	Option. Terminal emulation application.
Media Player	Music management program
Microsoft WordPad	Opens an ASCII notepad
Remote Desktop Connection	Log on to a Windows Terminal Server
Transcriber	Enter data using the stylus on the touchscreen
Avalanche	Option. Remote management for networked devices
Windows Explorer	File management program

Note: The Microsoft File Viewers cannot display files that have been password protected.

Communication

Access: Start | Programs | Communication

Note: Some communication menu options require an external modem connection to the VX7. Modems are not available from LXE nor supported by LXE.

ActiveSync

Once a relationship (partnership) has been established with Connect, ActiveSync will synchronize using the radio link on the VX7. See also: Chapter 1 “Introduction”, section “ActiveSync – Initial Setup”.

Requirement: ActiveSync version 3.7 (or higher) must be resident on the host (desktop/laptop) computer. ActiveSync is available from the Microsoft website. Follow their instructions to locate, download and install ActiveSync on your desktop computer.

For more information about using ActiveSync on your desktop computer, open ActiveSync, then open ActiveSync Help. See also section titled “Backup VX7 Files Using ActiveSync” for more ActiveSync information.

Synchronizing from the VX7 using a USB ActiveSync connection:

You must have set up ActiveSync on your desktop computer and completed the first synchronization process before you initiate synchronization from your device.

1. To initiate synchronization from your device, connect the USB cable to the PC and to the dongle cable on the VX7. The VX7 connects automatically.
2. Click the **Sync Now** button to synchronize with the PC.
3. Click the **Disconnect** button or remove the cable to disconnect.
4. To modify the Synchronization settings, see the **Options** icon on the ActiveSync window on the desktop PC.

Synchronizing from the VX7 using Serial or RF connection:

You must have set up ActiveSync on your desktop computer and completed the first synchronization process before you initiate synchronization from your device.

1. To initiate synchronization from your device, tap **Start | Programs | Communication | ActiveSync** to begin the process.
2. Click the **Connect** button.
3. Tap the **Sync Now** button to synchronize with the PC.
4. Tap the **Disconnect** button to disconnect.
5. To modify the Synchronization settings, see the **Options** icon on the ActiveSync window on the desktop PC.

Connect

Connect is used to initiate a hardwired connection to a host. Several pre-defined connect setups are included in the factory setup:

- COM1 direct connect at 57600 or 115200 baud
- COM3 [2] direct connect at 57600 or 115200 baud
- USB direct connect

The default connection is USB direct connect.

After a connect setup is selected, **Start | Programs | Communication | Connect** will start to connect to a host. After this connection is made and an ActiveSync relationship established, the ActiveSync menu item can be used to establish the connection over the radio link.

See Also: "Important Information – Cold Boot and Loss of Host Re-connection"

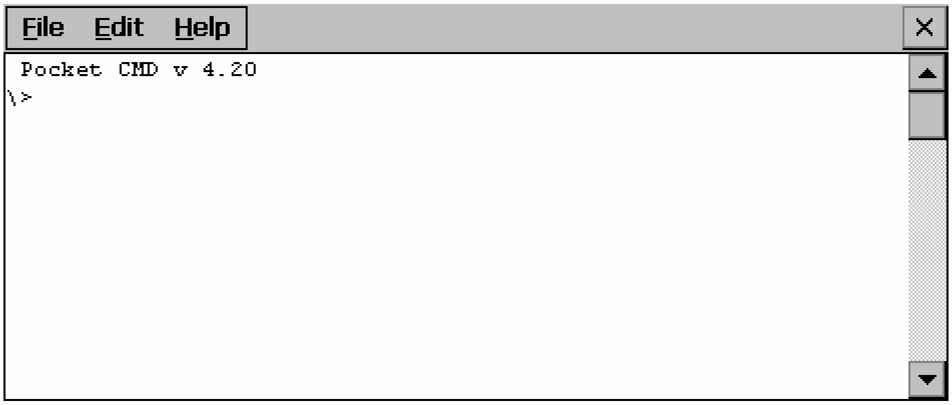
Start FTP Server / Stop FTP Server

These shortcuts call the Services Manager to start and stop the FTP server. The server defaults to Off (for security) unless it is explicitly turned on from the menu.

[2] The COM3 port is labeled "COM2/3".

Command Prompt

Access: **Start | Programs | Command Prompt**



```
Pocket CMD v 4.20
\>
```

Figure 3-1 Pocket CMD Prompt Screen

Type help at the command prompt for a list of available commands.

Exit the Command Prompt by typing exit at the command prompt or select **File** | **Close**.

Inbox

Access: **Start | Programs | Inbox**

This option requires a connection to a mail server. There are a few changes in the Windows CE version of Inbox as it relates to the general desktop Windows PC Microsoft Outlook Inbox options. Click the "?" button to access Inbox Help. ActiveSync can be used to transfer messages between the VX7 inbox and a desktop inbox.

Internet Explorer

Access: **Start | Programs | Internet Explorer**

This option requires a radio card and an Internet Service Provider. There are a few changes in the Windows CE version of Internet Explorer as it relates to the general desktop Windows PC Internet Explorer options. Click the "?" button to access Internet Explorer Help.

Media Player

Access: **Start | Programs | Media Player**

There are few changes in the Windows CE version of Media Player as it relates to the general desktop Windows PC Microsoft Media Player options. Click the "?" button to access Media Player Help.

Remote Desktop Connection

Access: **Start | Programs | Remote Desktop Connection**

There are few changes in the Windows CE version of Remote Desktop Connection as it relates to the general desktop Windows PC Microsoft Remote Desktop Connection options.

Select a computer from the drop down list or enter a host name and tap the Connect button.

Tap the **Options** >> button to access the General, Display, Local Resources, Programs and Experience tabs. Click the "?" button to access Remote Desktop Connection Help.

Transcriber

Access: **Start | Programs | Transcriber**

Select Transcriber on the **Start** | **Programs** menu. To make changes to the Transcriber application, enable or disable the current Transcriber session, etc., click the "hand with a pen" icon in the toolbar. Click the "?" button or the Help button to access Transcriber Help.

Windows Explorer

Access: **Start | Programs | Windows Explorer**

There are a few changes in the Windows CE version of Windows Explorer as it relates to the general desktop PC Windows Explorer options. Click the "?" button to access Windows Explorer Help.

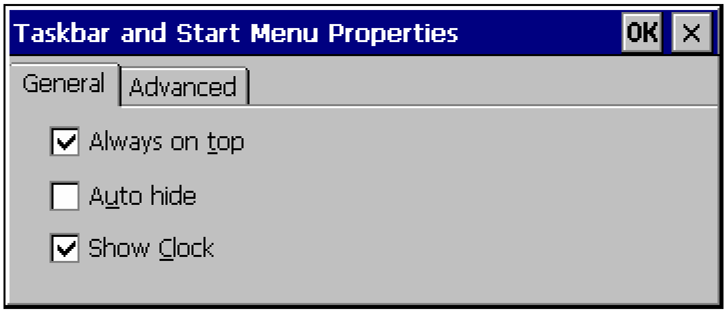
Taskbar

Access: Start | Settings | Taskbar and Start Menu

Factory Default Settings	
Always on Top	Enabled
Auto hide	Disabled
Show Clock	Enabled

There are a few changes in the Windows CE version of Taskbar as it relates to the general desktop PC Windows Taskbar options.

When the taskbar is auto hidden, press the **Ctrl** key then the **Esc** key to make the Start button appear.



☑ Always on top

□ Auto hide

☑ Show Clock

Figure 3-2 Taskbar Properties

Advanced Tab

Expand Control Panel

Tap the checkbox to have the Control Panel folders appear in drop down menu format from the **Settings | Control Panel** menu option.

Clear Contents of Document Folder

Tap the Clear button to remove the contents of the Document folder.

Control Panel Options

Access: **Start | Settings | Control Panel** or **My Computer | Control Panel**

Getting Help

Please click the “?” box to get Help when changing Control Panel options.

Option	Function
About	Displays hardware and software details.
Accessibility	Customize the way the keyboard, display or mouse functions.
Administrator Control	AppLock configuration. (See Chapter 6, “AppLock”.)
Aironet Client Utility	Set the parameters for a Cisco radio. (See section “Start Menu Program Options”, only present if Cisco radio software installed.)
Bluetooth	Discover and manage Bluetooth devices.
Certificates	Manage digital certificates used for secure communication.
Date/Time	Set Date, Time, Time Zone, and Daylight Savings.
Dialing	Set dialup properties for internal modems (not supplied/supported by LXE).
Display	Set background graphic, color scheme appearance, and power scheme properties.
Input Panel	Select the current key / data input method.
Internet Options	*CE .NET* - Set General, Connection, Security and Advanced options for Internet connectivity. *CE 5.0* – Set General, Connection, Security, Privacy, Advanced and Popups options for Internet connectivity.
Keyboard	Set key repeat delay and key repeat rate.
Mixer	Adjust the volume, record gain, and sidetone for microphone input.
Mouse	Set the double-click sensitivity for stylus taps on the touchscreen.
Network and Dial Up Options	Set network driver properties and network access properties.
Owner	Set VX7 owner details.
Password	Set VX7 access password properties.
PC Connection	Control the connection between the VX7 and a local desktop or laptop computer.
PCMCIA	Manage PCMCIA cards.
Power	Displays the status of all power managed devices.
Regional Settings	Set appearance of numbers, currency, time and date based on regional and language settings.
Remove Programs	Remove user installed programs in their entirety.

Option	Function
Scanner	Set scanner keyboard wedge, scanner icon appearance, active scanner port, and scan key settings. Assign baud rate, parity, stop bits and data bits for available COM ports. (See Chapter 4, "Scanner".)
Storage Manager	Manage storage devices, create partitions.
Stylus	Set double tap sensitivity properties and/or calibrate the touch panel.
System	Review System and Computer data and revision levels. Adjust Storage and Program memory settings.
Volume and Sounds	Set volume parameters and assign sound wav files to Windows CE events.

About

Access: **Start | Settings | Control Panel | About**

Displays hardware and software details.

Tab Title	Contents
Software	GUID, Windows Windows CE version, OAL Version, Bootloader Version, Compile Version, FPGA Version and Language
Hardware	CPU Type, Codec Type, FPGA Version, Scanner type, Display, Flash memory, and DRAM memory
Versions	LXE Utilities, LXE Drivers, LXE Image, LXE API, and Internet Explorer
Network IP	Current network connection IP and MAC address.

User application version information can be shown in the Version window. Version window information is taken from the registry.

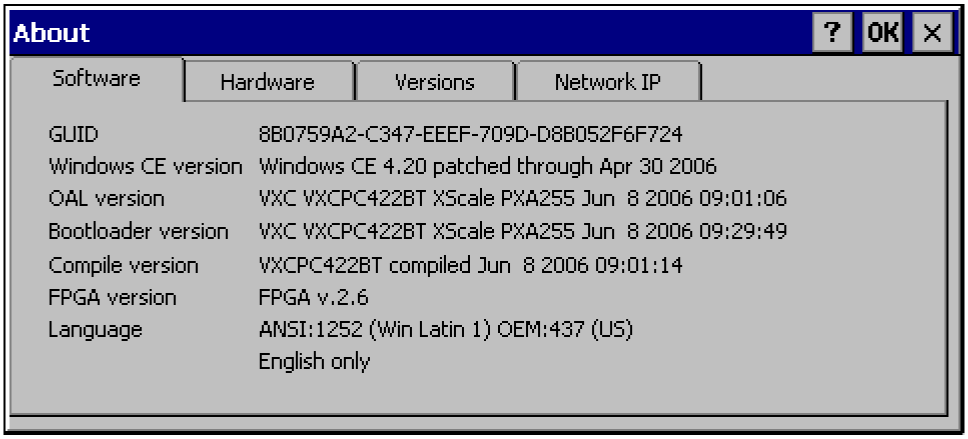
Modify the Registry using the Registry Editor (see section titled "VX7 Utilities"). LXE recommends **caution** when editing the Registry and also recommends making a backup copy of the registry before changes are made.

The registry settings for the Version window are under HKEY_LOCAL_MACHINE \ Software \ LXE \ Version in the registry.

Create a new string value under this key. The string name should be the Application name to appear in the Version window. The data for the value should be the version number to appear in the Version window.

Language and Fonts

The **Software** tab displays any fonts built into the OS image.



GUID	8B0759A2-C347-EEEF-709D-D8B052F6F724
Windows CE version	Windows CE 4.20 patched through Apr 30 2006
OAL version	VXC VXCPC422BT XScale PXA255 Jun 8 2006 09:01:06
Bootloader version	VXC VXCPC422BT XScale PXA255 Jun 8 2006 09:29:49
Compile version	VXCPC422BT compiled Jun 8 2006 09:01:14
FPGA version	FPGA v.2.6
Language	ANSI:1252 (Win Latin 1) OEM:437 (US) English only

Figure 3-3 About Properties, Software

The fonts built into the OS image are noted in the Language section of this tab:

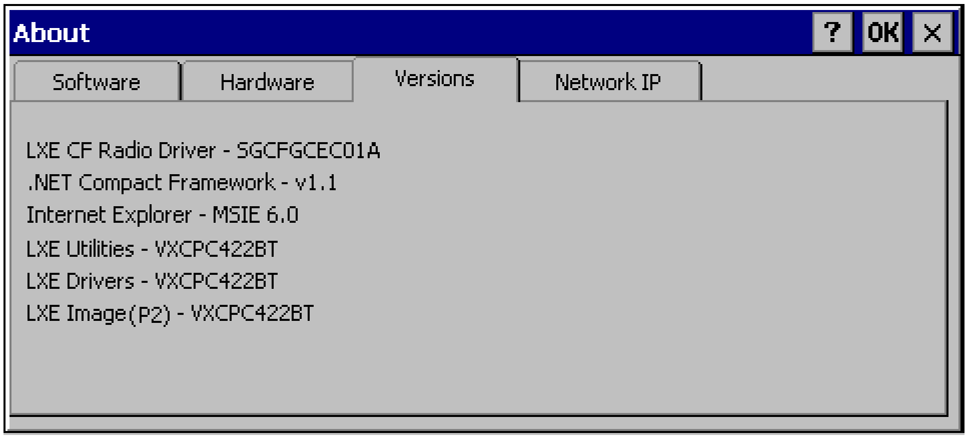
- English only – No additional fonts are built into the OS
- Japanese
- Simplified Chinese
- Traditional Chinese
- Korean

The listed Asian fonts are ordered separately and built-in to the VX7 OS image. Built-in fonts are added to registry entries and are available immediately upon startup. Thai, Hebrew, Arabic and Cyrillic Russian fonts are available in the (English only) default (extended) fonts.

When an Asian font is copied into the fonts folder on the /System folder; the font works for Asian web pages, the font works with RFTerm, the font does not work for Asian options in **Regional Settings** control panel, the font does not work for naming desktop icons with Asian names, the font does not work for third-party .NET applications, the font does not work for some third-party MFC applications.

Identifying Software Versions

The “Versions” tab displays the versions of many of the software programs installed. Not all installed software installed on the VX7 is included in this list and the list varies depending on the applications loaded on the VX7. The LXE Image line displays the revision of the system software installed. Please refer to the last three digits to determine the revision level (i.e.: in the example below, the revision level is 2BT).

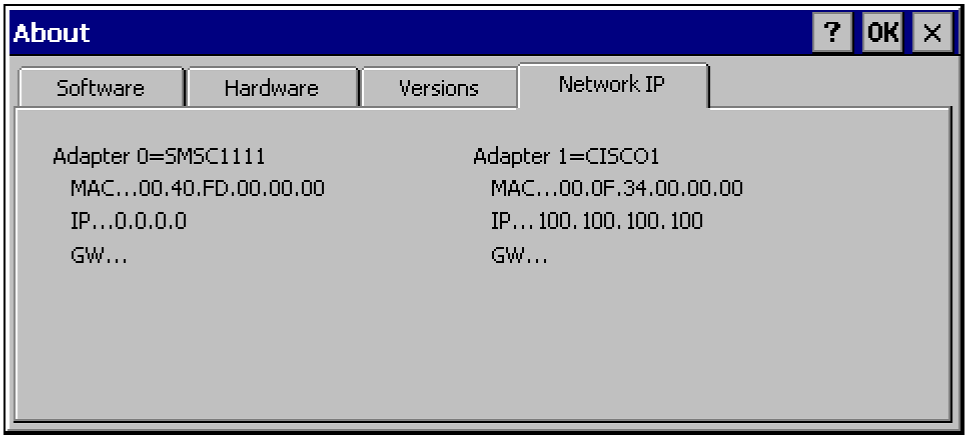


LXE CF Radio Driver - SGCFGCEC01A
.NET Compact Framework - v1.1
Internet Explorer - MSIE 6.0
LXE Utilities - VXCPC422BT
LXE Drivers - VXCPC422BT
LXE Image(P2) - VXCPC422BT

Figure 3-4 About Properties, Versions

Radio MAC Address

The “Network IP” tab displays the MAC address of the radio card.



Adapter 0=SMSC1111
MAC...00.40.FD.00.00.00
IP...0.0.0.0
GW...

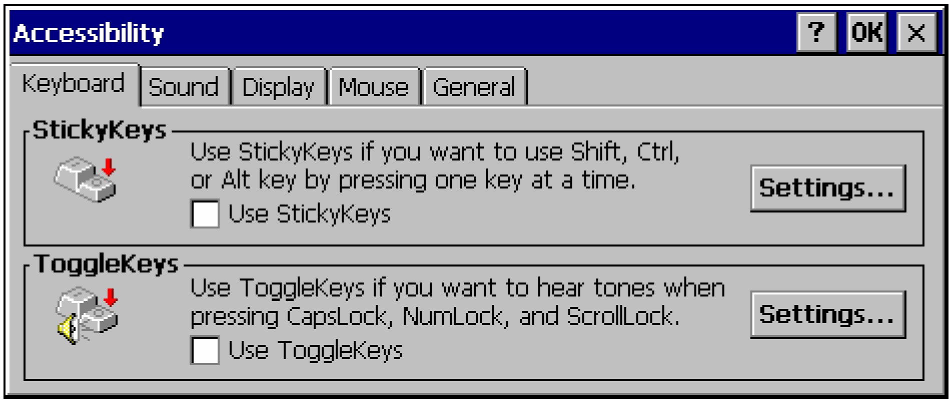
Adapter 1=CISCO1
MAC...00.0F.34.00.00.00
IP...100.100.100.100
GW...

Figure 3-5 About Properties, Network IP

Accessibility

Access: Start | Settings | Control Panel | Accessibility

Customize the way the keyboard, sound, display, mouse, automatic reset and notification sound function. There is no change from general desktop Accessibility options. Adjust the settings and click the OK box to save the changes. The changes take effect immediately.



Use StickyKeys if you want to use Shift, Ctrl, or Alt key by pressing one key at a time.

□ Use StickyKeys

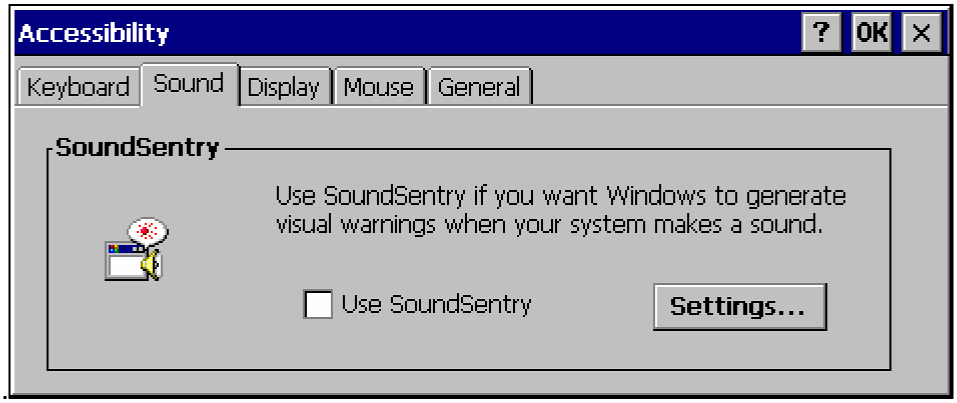
Use ToggleKeys if you want to hear tones when pressing CapsLock, NumLock, and ScrollLock.

□ Use ToggleKeys

Figure 3-6 Accessibility Properties, Keyboard

If the StickyKeys option is selected, the Shift, Ctrl and Alt keys become sticky keys. When a sticky key is pressed and released, the key remains in effect to modify the next keypress.

If the ToggleKeys option is selected, please note that Scroll Lock key does not produce a sound as the CapsLock and NumLock keys do. This is due to a limitation in the Microsoft Windows CE operating system.



Use SoundSentry if you want Windows to generate visual warnings when your system makes a sound.

□ Use SoundSentry

Figure 3-7 Accessibility Properties, Sound

If the SoundSentry option is selected, please note that Scroll Lock does not produce a visual warning as the CapsLock and NumLock keys do. This is due to a limitation in the Microsoft Windows CE operating system.

Administrator Control

Access: Start | Settings | Control Panel | PC Connection

Use this option to set parameters for computers intended to be used as dedicated, single (or multi) application devices. In other words, only the application(s) or feature(s) specified in the AppLock configuration by the Administrator are available to the user.

LXE devices with the AppLock feature are shipped to boot in Administration mode with no default password, thus when the device is first booted, the user has full access to the device and no password prompt is displayed. After the administrator specifies an application to lock, a password is assigned and the device is rebooted or the hotkey is pressed, the device switches to end-user mode.

AppLock also contains a component which sets configuration parameters as specified by the Administrator.

To set the AppLock parameters, please see Chapter 6, “AppLock” for details.

Bluetooth

Access: Start | Settings | Control Panel | Bluetooth

Discover and manage pairing with nearby Bluetooth devices.

Factory Default Settings	
Discovered Devices	None
Settings	
Turn Off Bluetooth	Disabled
Report when connection lost	Enabled
Report when connected	Disabled
Report failure to reconnect	Enabled
Computer is connectable	Enabled
Computer is discoverable	Disabled
Prompt if devices request to pair	Disabled
Continuous search	Disabled

Bluetooth taskbar Icon state and Bluetooth device Icon states change as Bluetooth devices are discovered, pair, connect and disconnect. There may be audible or visual signals as paired devices re-connect with the mobile device.

- The default Bluetooth setting is On and all options on the Settings Panel are enabled.
- The VX7 cannot be discovered by other Bluetooth devices when the Computer is discoverable option is disabled (unchecked) on the Settings panel.
- Other Bluetooth devices cannot be discovered if they have been set up to be Non-Discoverable or Invisible.
- The mobile device can pair with one Bluetooth scanner and one Bluetooth printer.
- It is not necessary to disconnect a paired scanner and printer before a different scanner or printer is paired with the VX7.
- The Bluetooth device should be as close as possible (line of sight) to the mobile device during the pairing process.

Assumption: The System Administrator has Discovered and Paired targeted Bluetooth devices for the VX7. The VX7 operating system has been upgraded to the revision level required for Bluetooth client operation.

Discover

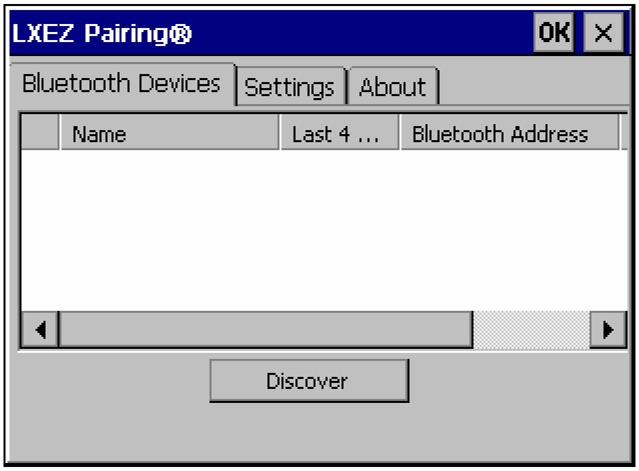
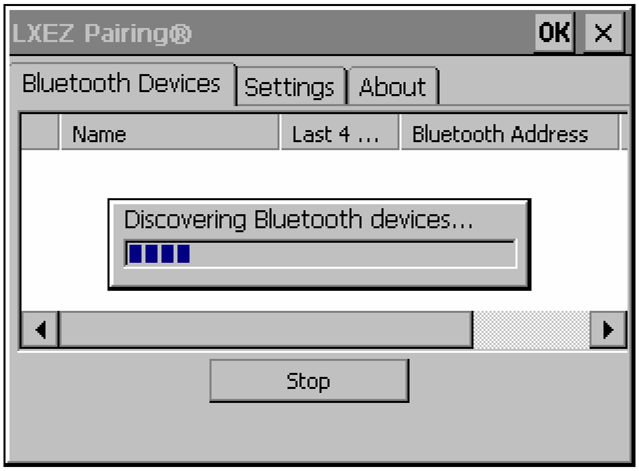


Figure 3-8 Control Panel - Bluetooth

Tap the **Discover** button to locate all discoverable Bluetooth devices in the vicinity. The Discovery process also queries for the unique identifier for each device discovered.



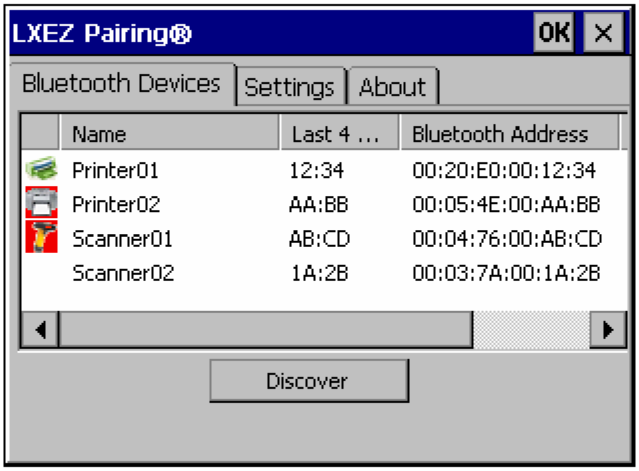
Discovering Bluetooth devices...

Figure 3-9 Discover Bluetooth Devices

Tap Stop at any time to end the Discover and Query for Unique Identifier functions.

Bluetooth Devices

A device previously discovered and paired with the VX7 is shown in the Bluetooth Devices panel.



Name	Last 4 ...	Bluetooth Address
Printer01	12:34	00:20:E0:00:12:34
Printer02	AA:BB	00:05:4E:00:AA:BB
Scanner01	AB:CD	00:04:76:00:AB:CD
Scanner02	1A:2B	00:03:7A:00:1A:2B

Figure 3-10 Bluetooth Devices Panel

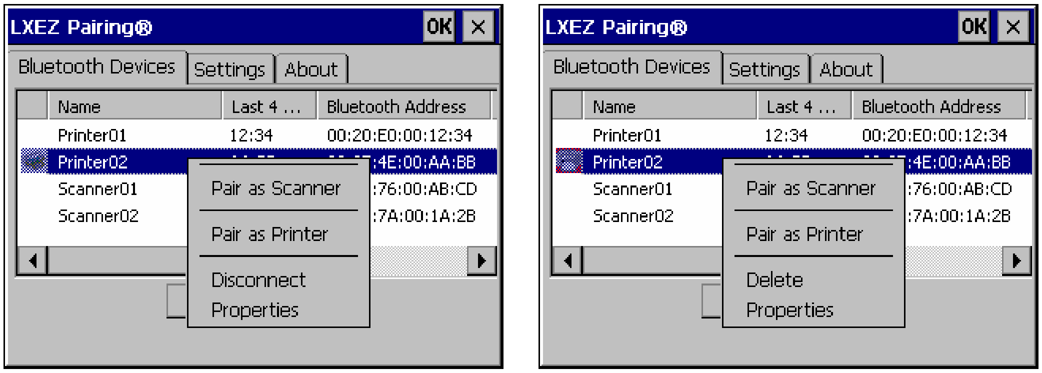
Note: When an active paired device enters Suspend Mode, is turned Off or leaves the VX7 Bluetooth scanning range, the Bluetooth connection between the paired device and the VX7 is lost. There may be audible or visual signals as paired devices disconnect from the VX7.

The discovered paired devices may or may not be identified with an icon. Discovered devices without an icon can be paired as printers or scanners; the Bluetooth panel will assign an icon to the device name.

An icon with a red background indicates the device Bluetooth connection is inactive.

An icon with a white background indicates the device is connected to the VX7 and the device Bluetooth connection is active.

Doubletap a device in the list to open the device properties menu. The targeted device does not need to be active.



Name	Last 4 ...	Bluetooth Address
Printer01	12:34	00:20:E0:00:12:34
Printer02		:4E:00:AA:BB
Scanner01		:76:00:AB:CD
Scanner02		:7A:00:1A:2B

Figure 3-11 Bluetooth Device Disconnect / Delete

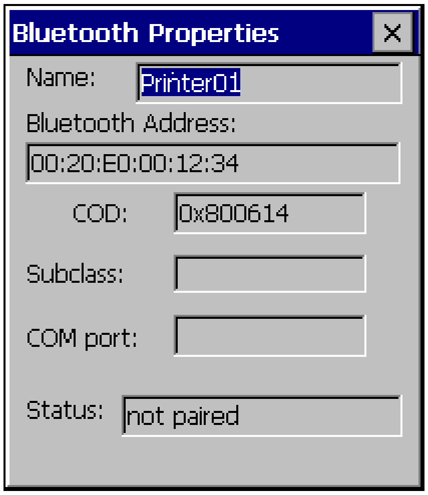
Tap Pair as Scanner to set up the VX7 to receive data from the scanner.

Tap Pair as Printer to set up the VX7 to send data to the printer.

Tap Disconnect to stop the connection between the VX7 and a paired Bluetooth device.

Tap Delete to remove an unpaired device from the Bluetooth device list. The device name and identifier is removed from the VX7 Bluetooth Devices panel after the user taps OK.

Bluetooth Device Properties



Name: Printer01

Bluetooth Address: 00:20:E0:00:12:34

COD: 0x800614

Subclass:

COM port:

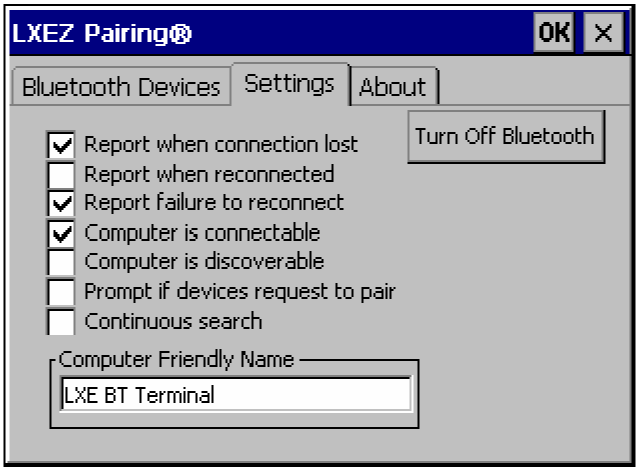
Status: not paired

Figure 3-12 Bluetooth Device Properties Menu

Data on the Bluetooth Properties panel cannot be changed by the user. The data displayed is the result of the device Query performed during the Discovery process.

The Status dialog box reflects the current state of the highlighted device.

Settings



☑ Report when connection lost
□ Report when reconnected
☑ Report failure to reconnect
☑ Computer is connectable
□ Computer is discoverable
□ Prompt if devices request to pair
□ Continuous search

Computer Friendly Name: LXE BT Terminal

Figure 3-13 Bluetooth Device Settings Panel

Turn Off Bluetooth Button

Tap the button to toggle Bluetooth hardware On or Off. The default value is Bluetooth On.

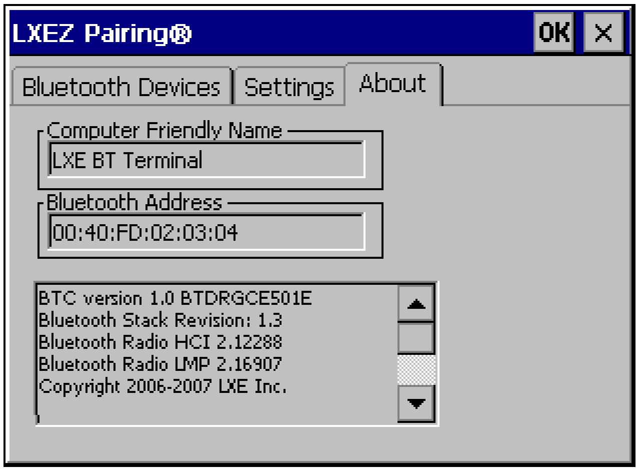
Options

Option	Default	Information
Report when connection lost	Enabled	There may be an audio or visual signal when a connection between a paired, active device is lost. A visual signal may be a dialog box placed on the display. Tap the X button or OK button to close the dialog box.
Report when reconnected	Disabled	There may be an audio or visual signal when a connection between a paired, active device is re-connected. A visual signal may be a dialog box placed on the display. Tap the X button or OK button to close the dialog box.
Report failure to reconnect	Enabled	The time delay is 30 minutes. This value cannot be changed by the user. There may be an audio or visual signal when a connection between a paired, active device is re-connected. A visual signal may be a dialog box placed on the display. Tap the X button or OK button to close the dialog box. Possible reasons for failure to reconnect: Timeout expired without reconnecting; attempted to pair with a device that is currently paired with another device; attempted to pair with a known device that moved out of range or was turned off; attempted to pair with a known device but the reason why reconnect failed is unknown.

Option	Default	Information
Computer is connectable	Enabled	Disable this option to inhibit VX7 connection with all Bluetooth devices.
Computer is discoverable	Disabled	Enable this option to ensure other devices can discover the VX7.
Prompt if devices request to pair	Disabled	When enabled, a dialog box is placed on the display. Tap the X button, OK button or No button to close the dialog box.
Continuous Search	Disabled	When enabled, the VX7 never stops searching for paired Bluetooth devices that have lost connection. When disabled, the VX7 stops searching after ½ hour.
Computer Friendly Name	Empty	The name, or identifier, entered in this space by the System Administrator is used exclusively by Bluetooth devices and during Bluetooth communication.

Note: The Device Name listed in ***Start*** *|* ***Settings*** *|* ***Control Panel*** *|* ***System*** *|* ***Device Name*** *is not used during Bluetooth operation. Owner Identification name listed in* ***Start*** *|* ***Settings*** *|* ***Control Panel*** *|* ***Owner*** *|* ***Identification*** *is not used during Bluetooth operation.*

About



Computer Friendly Name: LXE BT Terminal

Bluetooth Address: 00:40:FD:02:03:04

BTC version 1.0 BTDRGCE501E
Bluetooth Stack Revision: 1.3
Bluetooth Radio HCI 2.12288
Bluetooth Radio LMP 2.16907
Copyright 2006-2007 LXE Inc.

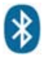
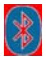
Figure 3-14 Bluetooth About Panel

This panel lists the assigned Computer Friendly Name (that other devices may discover during their Discovery and Query process), the Bluetooth MAC address, and software version levels. The data cannot be edited by the user.

Easy Pairing and Auto-Reconnect

The Bluetooth module can establish relationships with new devices after the end-user taps the Discover button. It can auto-reconnect to devices previously known but which have gone out of and then returned within range. Pairing supports SPP devices only.

Up to two Bluetooth devices can be connected to the VX7 at a time; LXE supports one scanner and one printer (see *Accessories*).

Taskbar Icon	Legend
	Bluetooth is ready to connect or Bluetooth module is connected to one or more of the targeted Bluetooth device(s).
	VX7 is not connected to another Bluetooth device or VX7 is out of range of all targeted Bluetooth device(s). Connection is inactive.

Note: Configuration elements are persistent and stored in the registry.

Setup the Bluetooth module to establish how the user is notified by easy pairing and auto-reconnect events.

AppLock, if installed, does not stop the end-user from using the Bluetooth application, nor does it stop other Bluetooth-enabled devices from pairing with the VX7 while AppLock is in control. See *Chapter 6 – AppLock* for more information.

Certificates

Access: **Start | Settings | Control Panel | Certificates**

Manage digital certificates used for secure communication.

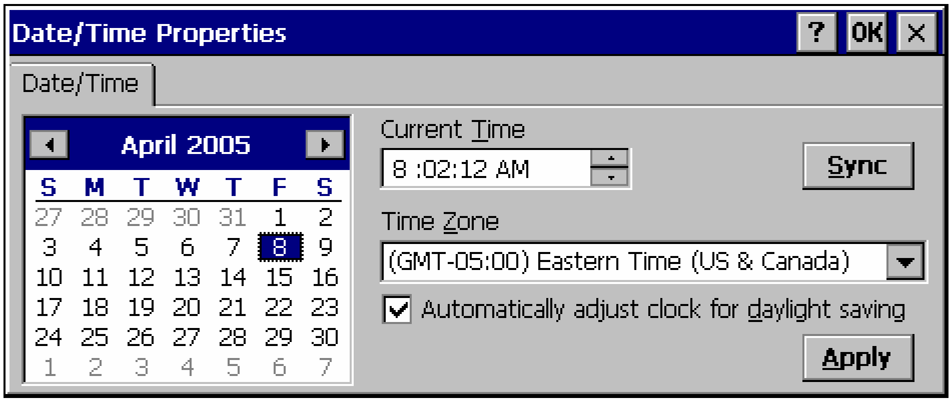
Lists the Stored certificates trusted by the VX7 user. These values may change based on the type of radio security resident in the client, access point or the host system.

Date/Time

Access: **Start | Settings | Control Panel | Date/Time Icon**

Set Date, Time, Time Zone, and Daylight Savings.

Factory Default Settings	
Current Time	Midnight
Time Zone	GMT-05:00
Daylight Savings	Disabled



Current Time: 8 :02:12 AM

Time Zone: (GMT-05:00) Eastern Time (US & Canada)

☑ Automatically adjust clock for daylight saving

Figure 3-15 Date/Time Properties

There is little change from general desktop PC Date/Time Properties options. Adjust the settings and click the OK box or the Apply button to save the changes. The changes take effect immediately. Double tapping the time displayed in the Taskbar causes this display to appear.

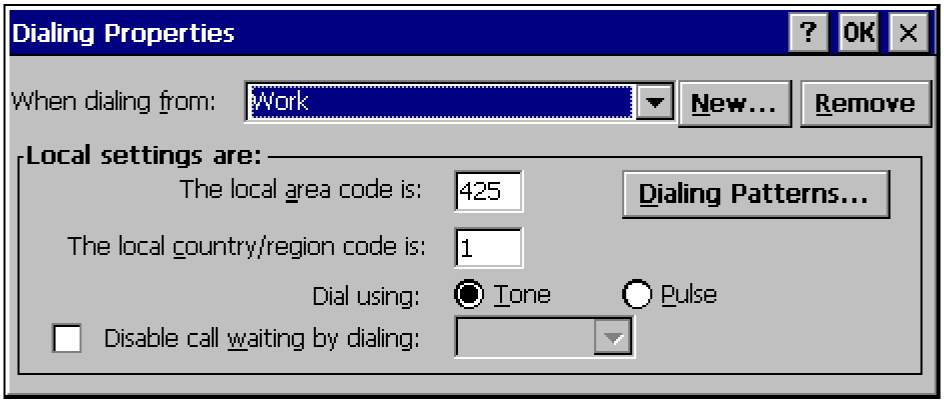
If an Internet connection is available, click the Sync button to synchronize time with a time server.

The VX7 includes a GrabTime utility:

- GrabTime can be executed manually at any time by clicking the **Sync** button on this control panel.
- GrabTime can be configured to synchronize the time at boot up. Please see "Enabling GrabTime", later in this chapter, for details.

Dialing

Access: **Start | Settings | Control Panel | Dialing**



Dialing Properties

When dialing from: Work

Local settings are:

The local area code is: 425

The local country/region code is: 1

Dial using: ● Tone ○ Pulse

□ Disable call waiting by dialing:

Figure 3-16 Dialing

Set dialup properties for internal modems (not supplied/supported by LXE). Tap the “?” and follow the instructions in Help.

Display

Access: Start | Settings | Control Panel | Display Icon

Set background graphic, color scheme appearance, and power scheme properties.

Factory Default Settings	
Background	Windowsce
Tile	Disable
Appearance	
Scheme:	Windows Standard
Backlight	
Battery Auto Turn Off	Enabled
Idle Time	30 seconds
External Auto Turn Off	Enabled
Idle Time	2 minutes

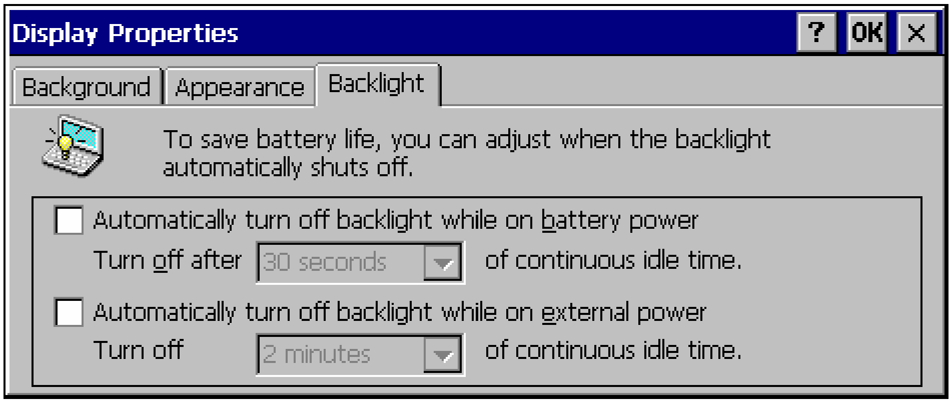
Background

There is no change from general desktop PC Display Properties / Background options. Adjust the settings and click the OK box to save the changes. The changes take effect immediately.

Appearance

No change from general desktop PC Display Properties / Appearance options. Adjust the settings and click the OK box to save the changes. The changes take effect immediately. The default is Windows Standard.

Backlight



To save battery life, you can adjust when the backlight automatically shuts off.

□ Automatically turn off backlight while on battery power

Turn off after 30 seconds ▾ of continuous idle time.

□ Automatically turn off backlight while on external power

Turn off 2 minutes ▾ of continuous idle time.

Figure 3-17 Display Properties / Backlight Tab

Adjust the settings and click the OK box to save the changes. The changes take effect immediately. When the backlight timer expires, the monochrome screen is turned off, the color transmissive backlight is dimmed not turned off.

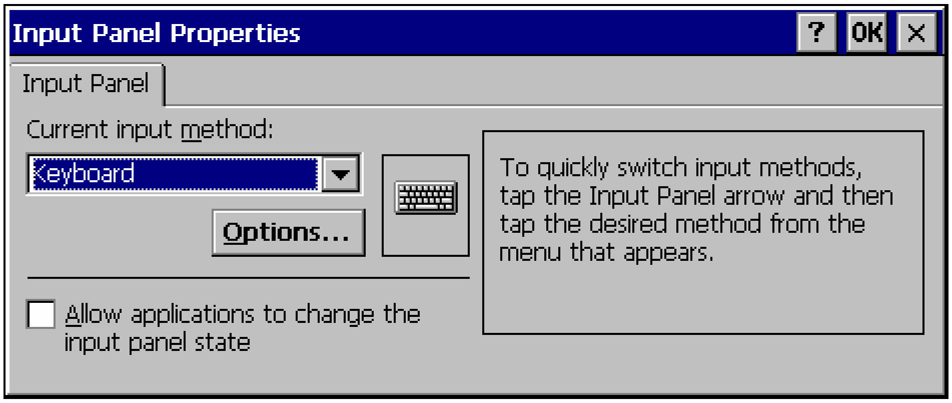
Note: The display can also be configured to turn off when the vehicle to which the VX7 is mounted is in motion. This feature required a serial cable connection and is enabled using the Scanner control panel. Please see "Screen Blanking", later in this chapter, for details.

Input Panel

Access: Start | Settings | Control Panel | Input Panel

Select the current key / data input method.

Factory Default Settings	
Input Method	Keyboard
Allow applications to change input panel state	Disabled
Keys	Small keys
Use gestures	Disabled



Input Panel Properties

Current input method: Keyboard

To quickly switch input methods, tap the Input Panel arrow and then tap the desired method from the menu that appears.

□ Allow applications to change the input panel state

Figure 3-18 Input Panel Properties

Use this option to make the Soft Keyboard or the keypad primarily available when entering data. Selecting Keyboard enables both.

The Input Panel is disabled by default. To enable the input panel, make sure the checkbox for “Allow applications to change input panel state” is checked and warmboot the VX7.

Internet Options

Windows CE .NET

Set General, Connection, Security and Advanced options for Internet connectivity.

Factory Default Settings	
General	
Start Page	http://www.lxe.com/
Search Page	http://www.google.com
Cache Size	512 Kb
Connection	
Use LAN	Disabled
Autodial Name	Blank
Proxy Server	Disabled
Security	
Allow cookies	Enabled
Allow TLS 1.0 security	Disabled
Allow SSL 2.0 security	Enabled
Allow SSL 3.0 security	Enabled
Warn when switching	Enabled
Advanced	
Display web images	Enabled
Play web sounds	Enabled
Enable web scripting	Enabled
Display script error note	Disabled
Underline links	Never

Select a tab. Adjust the settings and click the OK box to save the changes. The changes take effect immediately.

Windows CE 5.0

Set General, Connection, Security, Privacy, Advanced and Popups options for Internet connectivity.

Factory Default Settings	
General	
Start Page	http://www.lxe.com/
Search Page	http://www.google.com
Cache Size	512 Kb
User Agent	Windows CE
Connection	
Use LAN	Disabled
Autodial Name	Blank
Proxy Server	Disabled
Bypass Proxy	Disabled
Security	
Allow cookies	Enabled
Allow TLS 1.0 security	Disabled
Allow SSL 2.0 security	Enabled
Allow SSL 3.0 security	Enabled
Warn when switching	Enabled
Privacy	
First party cookies	Accept
Third party cookies	Prompt
Session cookies	Always allow
Advanced	
Stylesheets	Enable
Theming Support	Enable
Multimedia	All options enabled
Security	All options enabled
Popups	
Block popups	Disabled
Display notification	Enabled
Use same window	Disabled

Select a tab. Adjust the settings and click the OK box to save the changes. The changes take effect immediately.

Keyboard

Access: Start | Settings | Control Panel | Keyboard Icon

Set key repeat delay and key repeat rate.

Factory Default Settings	
Repeat	Enable
Delay	Short
Rate	Slow
Key Map	Default (Windows CE 5.0) 0409 (Windows CE .NET)

There is no change from general desktop PC Keyboard Properties options. Adjust the settings and click the OK box to save the changes. The changes take effect immediately.

When new key maps are added to the registry, they will appear in the Key Map dropdown list on the Keyboard Panel.

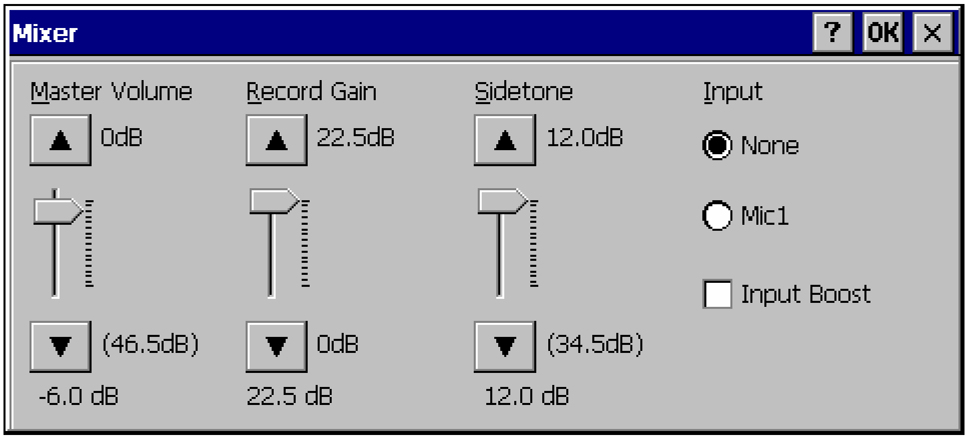
These values do not affect virtual keyboard taps.

Mixer

Access: Start | Settings | Control Panel | Mixer Icon

Adjust the volume, record gain, and sidetone for microphone input.

Factory Default Settings	
Master Volume	0dB
Record Gain	22.5dB
Sidetone	12.0dB
Input	None
Input Boost	Disabled



Mixer

Master Volume: 0dB (46.5dB) -6.0 dB

Record Gain: 22.5dB 0dB 22.5 dB

Sidetone: 12.0dB (34.5dB) 12.0 dB

Input: ● None ○ Mic1

□ Input Boost

Figure 3-19 Mixer

Select the Input for the mixer. Move the sliders to adjust the decibel level. Tap OK to save the settings.

The following options are available for **Input**

- None – No microphone. Use this setting when stereo headphones are attached to the device.
- Mic1 – Use this setting when a mono headset with microphone is attached to the device.
- Bluetooth – Reserved for future use.

When checked, (enabled) **Input Boost** provides increased sensitivity of the microphone by 20 dB. Input Boost can only be enabled after an Input type other than None is selected.

Mouse

Access: Start | Settings | Control Panel | Mouse

Set the double-click sensitivity for stylus taps on the touchscreen or an external mouse.

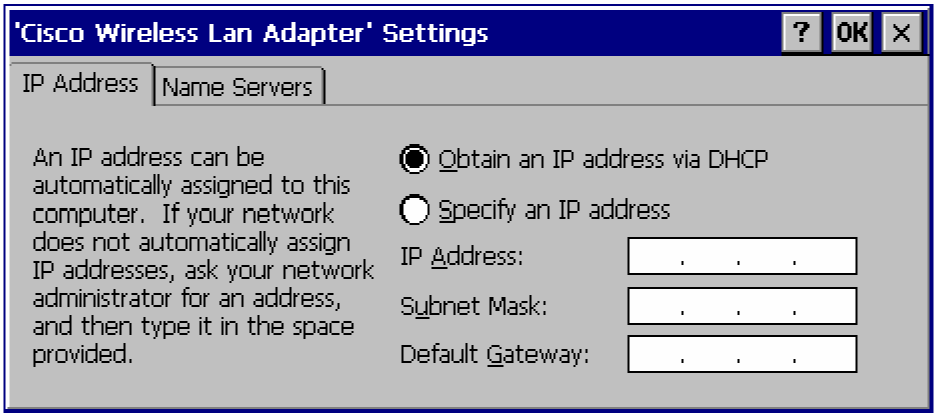
Network and Dialup Connections

Access: Start | Settings | Control Panel | Network and Dialup Connections

Create a dialup, direct, or VPN connection on the VX7.

To configure the VX7 to use DHCP or a fixed IP address, select the desired connection. The default is to obtain an IP address via DHCP.

A static IP address can be assigned by clicking the Specify an IP address radio button and entering the desired IP address, subnet mask and gateway.



An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space provided.

● Obtain an IP address via DHCP

○ Specify an IP address

IP Address: . . .

Subnet Mask: . . .

Default Gateway: . . .

Figure 3-20 Network Connection Properties

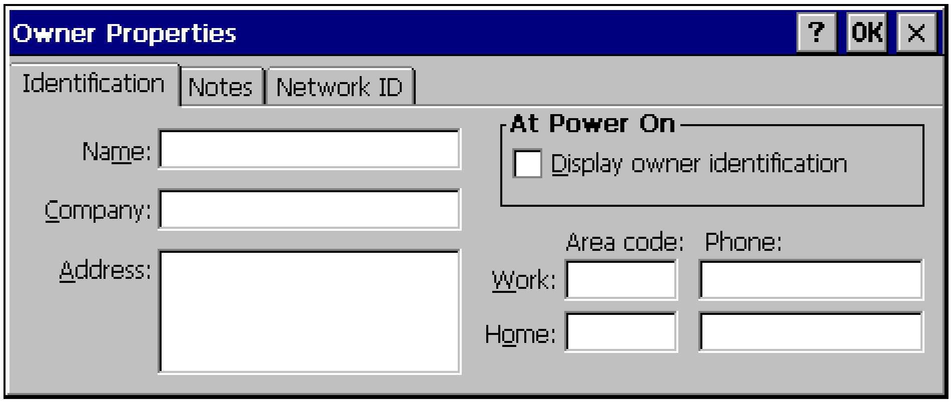
Owner

Access: Start | Settings | Control Panel | Owner Icon

Set VX7 owner details.

Factory Default Settings	
Identification	Blank
Notes	Blank

There is no change from general desktop PC Owner Properties display. Enter the information and click the OK box to save the changes. The changes take effect immediately.



Owner Properties

Identification | Notes | Network ID

Name:

Company:

Address:

At Power On

□ Display owner identification

	Area code:	Phone:
Work:		
Home:		

Figure 3-21 Owner Properties

Password

Access: Start | Settings | Control Panel | Password Icon

Set VX7 access/power up password properties.

Factory Default Settings	
Password	Blank
At Power On	Disabled

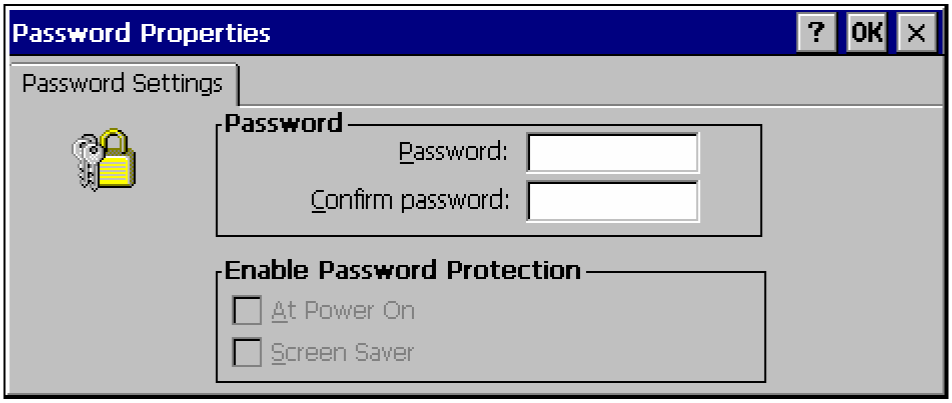
Note: *Once a password is assigned, the Owner and Password Control Panel options require the password to be entered before the Control Panel option can be accessed. If you forget the password, it cannot be restored without performing a cold boot on the unit (which erases all memory).*

Enter the password, then type it again to confirm it and click the OK box to save the changes. The password is immediately in effect.

Tap the Power On checkbox to set whether the user types a password at Power On.

Tap the Screen Saver checkbox to set whether the user types a password to clear the screensaver. If there is no screensaver chosen, this checkbox is ignored.

Note: *Screensaver option only works with Remote Desktop screensavers.*



Password

Password:

Confirm password:

Enable Password Protection

□ At Power On

□ Screen Saver

Figure 3-22 Password Properties

PC Connection

Access: Start | Settings | Control Panel | PC Connection

Control the connection between the VX7 and a nearby desktop/laptop computer.

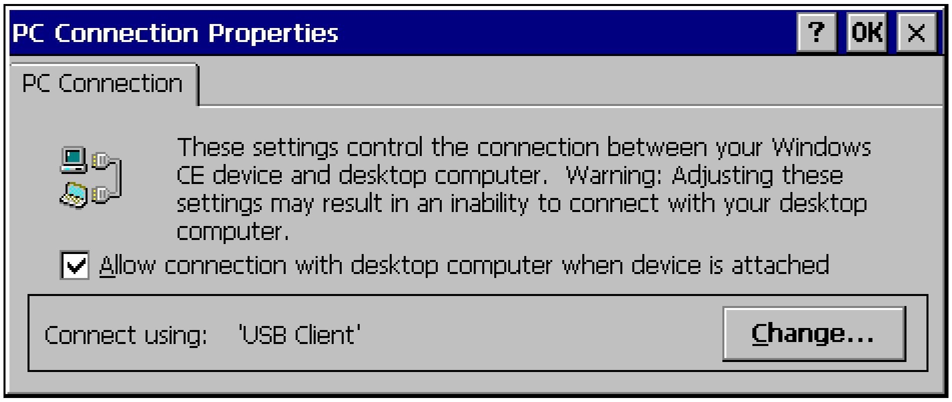
Factory Default Settings	
Allow Connection	Enabled
Connect Using	'USB Client'

Tap the Change button to adjust the settings and click the OK button to save the changes. The changes take effect immediately.

Unchecking the "Allow connection with ….." disables ActiveSync.

Change ….

Clicking Change lists configured ActiveSync connections. In addition, there is a checkbox for Automatic Connect. This option applies to USB connection only. If this checkbox is checked, when the USB cable is connected, the VX7 will automatically try to start ActiveSync over the USB port. Note that this interferes with processes on the configured port at the same time.



These settings control the connection between your Windows CE device and desktop computer. Warning: Adjusting these settings may result in an inability to connect with your desktop computer.

☑ Allow connection with desktop computer when device is attached

Connect using: 'USB Client'

Figure 3-23 Communication / PC Connection Tab

Please refer to the "Backup VX7 Files" section later in this chapter for parameter setting recommendations.

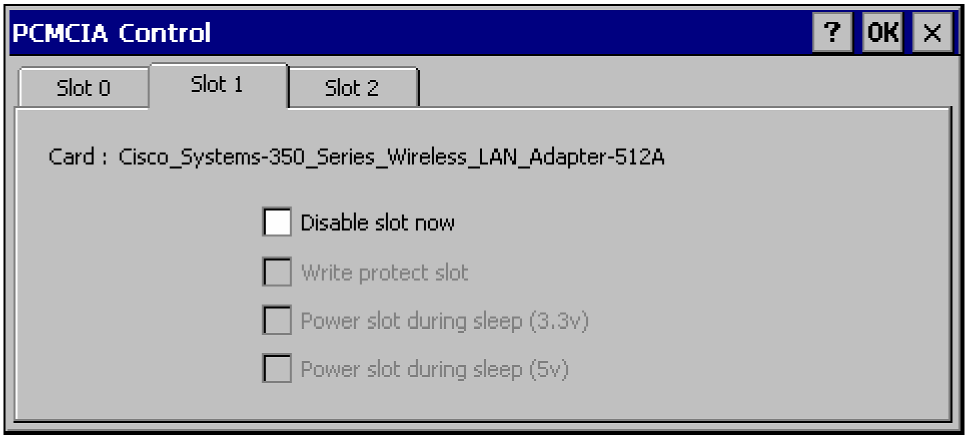
PCMCIA

Access: Start | Settings | Control Panel | PCMCIA

Enable or disable the PCMCIA slots. Information on the card currently in the PCMCIA slots and the Compact Flash slot is provided.

Factory Default Settings	
Disable slot now	Unchecked

The Slot 0 and Slot 1 Tabs contain the same parameters. If a card is present in the slot, a description of the card is displayed. To disable a slot, check the Disable slot now checkbox and tap OK. The change takes effect immediately. Slot 0 is the lower slot, labeled "PCMCIA B". Slot 1 is the upper slot, labeled "PCMCIA A".



Card : Cisco_Systems-350_Series_Wireless_LAN_Adapter-512A

☐ Disable slot now

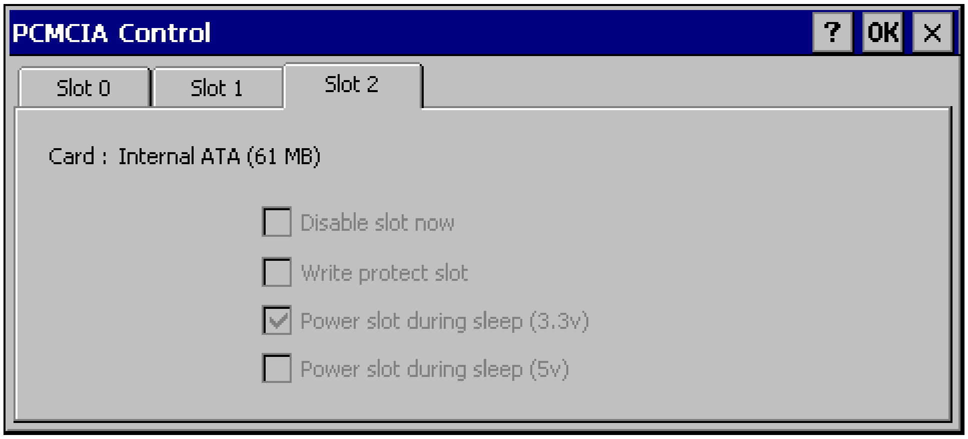
☐ Write protect slot

☐ Power slot during sleep (3.3v)

☐ Power slot during sleep (5v)

Figure 3-24 PCMCIA Control Tab, Slot 0 and Slot 1

The Slot 2 Tab provides information on the internal Compact Flash ATA drive. There are no user configurable options.



Card : Internal ATA (61 MB)

☐ Disable slot now

☐ Write protect slot

☑ Power slot during sleep (3.3v)

☐ Power slot during sleep (5v)

Figure 3-25 Compact Flash ATA Control Tab, Slot 2

Power

Depending on the Software Revision, some devices may have a **Schemes** tab.

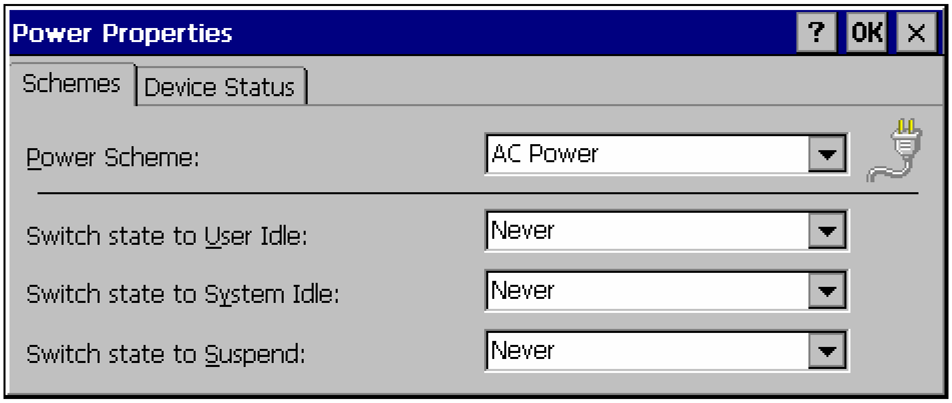
Factory Default Settings	
Switch state to User Idle	Never
Switch state to System Idle	Never
Switch state to Suspen	Never

The Schemes tab can be used to control the display backlight and shut the VX7 Off. The mode timers are cumulative. The System Idle timer begins the countdown after the User Idle timer has expired and the Suspend timer begins the countdown after the System Idle timer has expired. For example, if the User Idle timer is set to Never, the power scheme timers never place the device in User Idle, System Idle or Suspend modes.

For a VX7, the User Idle state turns off the display backlight. There is no System Idle mode so the VX7 remains in User Idle mode until the Suspend timer expires or a primary even occurs.

Please see “Power Modes” in Chapter 2, “Physical Description and Layout”.

IMPORTANT: There is no Suspend mode on the VX7. If the Suspend timer is enabled, the VX7 will **shut down** when the Suspend timer expires.



Power Scheme: AC Power

Switch state to User Idle: Never

Switch state to System Idle: Never

Switch state to Suspend: Never

Figure 3-26 Power Properties

The Device Status tab displays the status of power managed devices. Note that since the VX7 does not support power management, all devices show the “high” power level. There are no user options on this screen.

Regional Settings

Access: Start | Settings | Control Panel | Regional Settings

Set the appearance of numbers, currency, time and date based on regional and language settings.

No change from general desktop PC Regional Settings Properties options. Adjust the settings and click the OK box to save the changes. The changes take effect immediately.

Options (and defaults) for the regional settings depend on the fonts included in the OS image. Please refer to the section on the **About** control panel earlier in this chapter for more details.

Windows CE .NET2

Factory Default Settings	
Regional Setting	English (United States)
Number	123,456,789.00 / -123,456,789.00 neg
Currency	$123,456,789.00 pos / ($123,456,789.00) neg
Time	h:mm:ss tt (tt=AM or PM)
Date	M/d/yy short / dddd,MMMM,dd,yyyy long

Windows CE 5.0

A language must be installed before it can be selected. After selecting a language to use, and after all changes are made, tap OK to save your changes then warmboot the device.

Factory Default Settings	
Regional Settings	
Your Locale	English (United States)
Number	123,456,789.00 / -123,456,789.00 neg
Currency	$123,456,789.00 pos / ($123,456,789.00) neg
Time	h:mm:ss tt (tt=AM or PM)
Date	M/d/yy short / dddd,MMMM,dd,yyyy long
User Interface Language	
User Interface Language	Dimmed (default is Your Locale setting)
Input Language	
Input Language	Dimmed (default is Your Locale setting)
Installed Input Languages	English (US)

Tap the **Customize** button to set Number, Currency, Time and Date format for the selected Locale. User Interface Language determines the language used for the menus, dialogs and alerts. Select the Default Input Language to use when the device is rebooted.

Remove Programs

Access: Start | Settings | Control Panel | Remove Programs

No change from general desktop Remove Programs options. Select a program and click Remove. Follow the prompts on the screen to uninstall ***user-installed only*** programs. The change takes effect immediately.

Scanner

Access: Start | Settings | Control Panel | Scanner

Set scanner keyboard wedge, scanner icon appearance, active scanner port, and scan key settings. Assign baud rate, parity, stop bits and data bits for available COM ports.

To set the Scanner parameters, please see Chapter 4, "Scanner" for details.

Storage Manager

Access: Start | Settings | Control Panel | Storage Manager

Installed storage devices are listed by device name in the dropdown box. To view information about the disk or perform store operations, select a device from the list.

On-line help is available for this option.

Topics available are:

- Manage storage devices
- Manage disk partitions
- Creating a new partition
- Advanced partition features

LXE recommends **caution** when formatting or dismounting storage devices and when creating new partitions or deleting partitions on the storage device.

The internal ATA (System) card does not appear in the Storage Manager menu.

Stylus

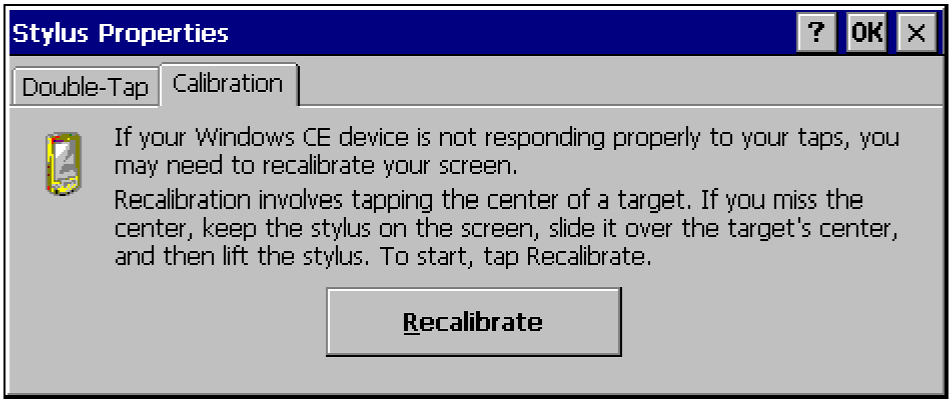
Access: Start | Settings | Control Panel | Stylus

Set double tap sensitivity properties and/or calibrate the touch panel.

Double Tap

Follow the instructions on the screen and click the OK box to save the changes. The changes take effect immediately.

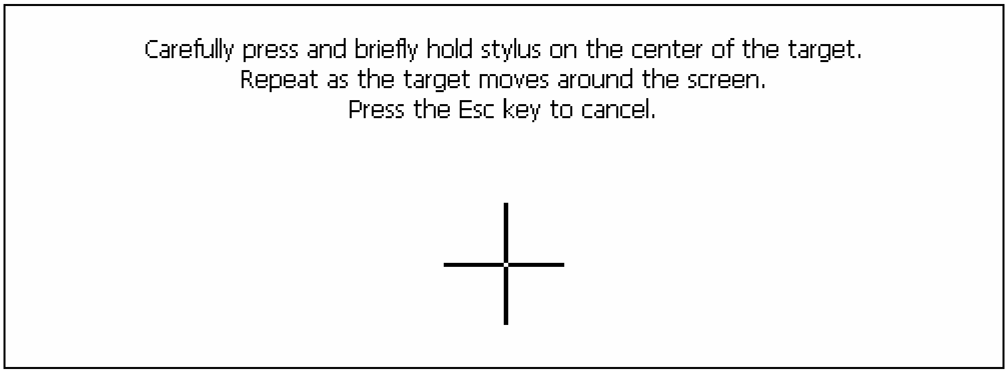
Calibration



If your Windows CE device is not responding properly to your taps, you may need to recalibrate your screen.

Recalibration involves tapping the center of a target. If you miss the center, keep the stylus on the screen, slide it over the target's center, and then lift the stylus. To start, tap Recalibrate.

Figure 3-27 Stylus Properties / Recalibration Start



Carefully press and briefly hold stylus on the center of the target.
Repeat as the target moves around the screen.
Press the Esc key to cancel.

Figure 3-28 Stylus Properties / Recalibration

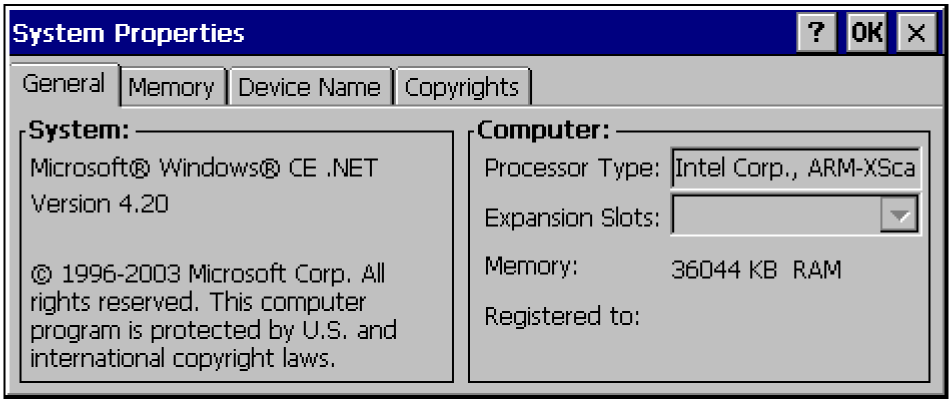
System

Access: Start | Settings | Control Panel | System Icon

Review System and Computer data and revision levels. Adjust Storage and Program memory settings.

Factory Default Settings	
General	N/A
Memory	1/3 storage, 2/3 program memory
Device Name	VXC0001
Device Description	LXE_VXC
Copyrights	N/A

General



System:
Microsoft® Windows® CE .NET
Version 4.20

© 1996-2003 Microsoft Corp. All rights reserved. This computer program is protected by U.S. and international copyright laws.

Computer:
Processor Type: Intel Corp., ARM-XSca
Expansion Slots:
Memory: 36044 KB RAM
Registered to:

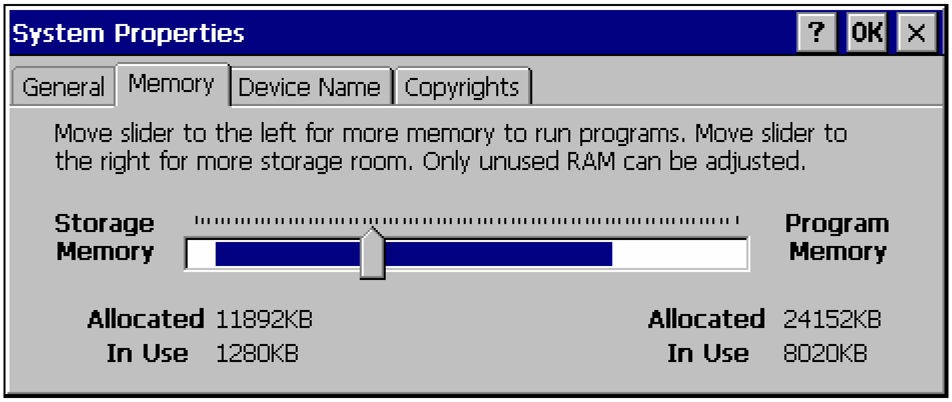
Figure 3-29 System / General tab

System: This screen is presented for information only. The System parameters cannot be changed by the user.

Computer: The processor type is listed. The type cannot be changed by the user. The name of the installed radio card is listed in the dropdown list. Total computer memory and the identification of the registered user is listed and cannot be changed by the user.

Memory sizes given do not include memory used up by the operating system. Hence, a system with 64 MB may only report 35 MB memory, since 29 MB is used up by the Windows CE .operating system. This is actual DRAM memory, and does not include internal flash or the internal ATA card used for storage.

Memory



Move slider to the left for more memory to run programs. Move slider to the right for more storage room. Only unused RAM can be adjusted.

Storage Memory

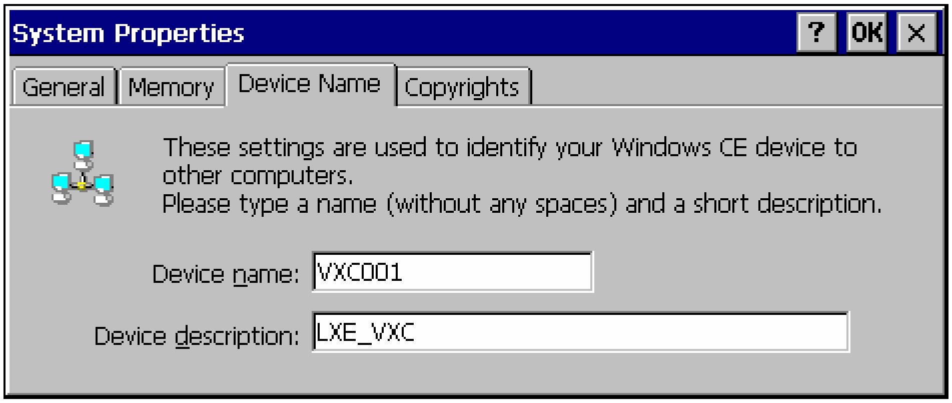
Program Memory

Allocated	11892KB	Allocated	24152KB
In Use	1280KB	In Use	8020KB

Figure 3-30 System / Memory

Move the slider to allocate more memory for programs or storage. If there isn't enough space for a file, increase the amount of storage memory. If the VX7 is running slowly, try increasing the amount of program memory. Adjust the settings and click the OK box to save the changes. The changes take effect immediately.

Device Name



These settings are used to identify your Windows CE device to other computers.
Please type a name (without any spaces) and a short description.

Device name: VXC001

Device description: LXE_VXC

Figure 3-31 System / Device Name

The device name and description can be changed. Enter the name and description using either the keypad or the Input Panel and tap OK to save the changes. The changes take effect immediately.

Copyrights

This screen is presented for information only. The Copyrights information cannot be changed by the user.

Terminal Server Client Licenses

(Windows *CE 5.0 only*) Select a server client license from a drop down list

Not available at this release.

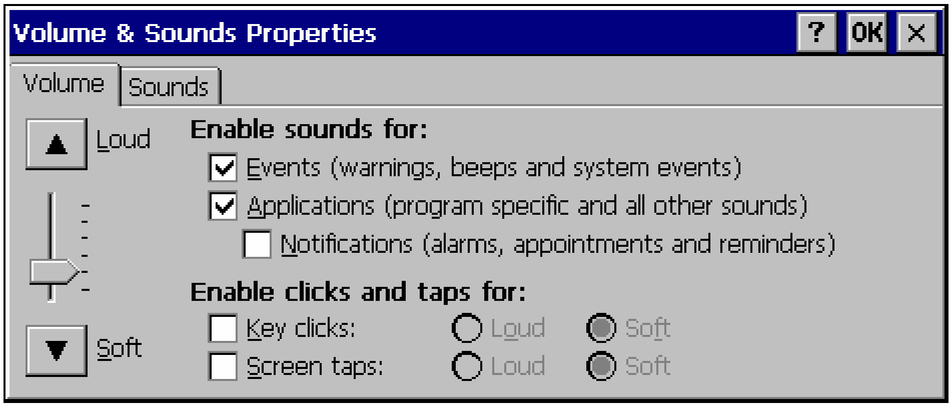
Volume and Sounds

Access: Start | Settings | Control Panel | Volume & Sounds Icon

Set volume parameters and assign sound wav files to Windows CE events.

Factory Default Settings	
Volume	
Events	Enabled
Application	Enabled
Notifications	Enabled
Volume	Middle of Bar
Key click	Loud
Screen tap	Loud
Sounds	
Scheme	LOUD!

Follow the instructions on the screen and click the OK box to save the changes. The changes take effect immediately.



Volume & Sounds Properties

Enable sounds for:

☑ Events (warnings, beeps and system events)

☑ Applications (program specific and all other sounds)

□ Notifications (alarms, appointments and reminders)

Enable clicks and taps for:

□ Key clicks: ○ Loud ● Soft

□ Screen taps: ○ Loud ● Soft

Figure 3-32 Volume and Sounds

CF Flash Cards, CAB Files and Programs

The Flash card, located under the main battery pack, is intended to protect the user from losing the LXE drivers and configuration information in the event of a cold boot. Also, on any boot, the contents of any registered CAB files are automatically unpacked.

Access Files on the Flash Card

Tap the **My Device** icon on the Desktop then tap the **System** icon.

Files

A flash card is used for permanent storage of the LXE drivers and utilities. It is also used for registry content back up. The flash card is located in the socket under the main battery pack.

CAB files, when executed, are not deleted.

SUMMIT.CAB	Summit Client files needed for network card operation.
The following CAB files are optional and may or may not be present:	
BLUETOOTH.CAB	Bluetooth Client files needed for LXEZ Pairing operation.
LXE_VX3C_ENABLER.CAB	Wavelink Avalanche Enabler.
RFTERM.CAB	RFTerm terminal emulation application.
JAVA.CAB	Java application.
APPLOCK.CAB	AppLock program. See Chapter 6 “AppLock”.

Note: Always perform a warm reset (Start / Run / Warmboot) when exchanging one flash card for another.

Backup VX7 Files using ActiveSync

Using Microsoft ActiveSync version 3.7 or higher, you can synchronize information on your desktop computer with the VX7 and vice versa. Synchronization compares the data on your VX7 with your desktop computer and updates both with the most recent data.

For example, you can:

- Back up and restore your device data.
- Copy (rather than synchronize) files between your device and desktop computer.
- Control when synchronization occurs by selecting a synchronization mode. For example, you can synchronize continually while connected to your desktop computer or only when you choose the synchronize command.

If the VX7 is connected to a PC by a RS-232 or USB cable, disconnect the cable from the VX7 and reconnect.

Check that the correct connection is selected (Serial or USB “Client”).

Note: By default, ActiveSync does not automatically synchronize all types of information. Use ActiveSync Options to specify the types of information you want to synchronize. The synchronization process makes the data (in the information types you select) identical on both your desktop computer and your device.

When installation of ActiveSync is complete on your desktop computer, the ActiveSync Setup Wizard begins and starts the following processes:

- connect your device to your desktop computer,
- set up a partnership so you can synchronize information between your device and your desktop computer, and
- customize your synchronization settings.

Because ActiveSync is already installed on your device, your first synchronization process begins automatically when you finish setting up your desktop computer in the ActiveSync wizard.

Prerequisites

VX7 and ActiveSync Partnership

A partnership between the VX7 and ActiveSync has been established. See section “ActiveSync – Initial Setup” in Chapter 1 “Introduction”, “Getting Started”.

Serial Port Transfer

- A desktop or laptop PC with an available serial port and a VX7 with a serial port. The desktop or laptop PC must be running Windows 95, 98, NT, 2000 or XP.
- Null modem cable with all control lines connected. LXE recommends using the null modem cable part number listed in Chapter 1 “Introduction”, subsection “Accessories”.

USB Transfer

- A desktop or laptop PC with an available USB port and a VX7 with a USB port. The desktop or laptop PC must be running Windows 98 SR2, 2000 or XP.
- A standard USB cable with a type A plug on one end, and a type B plug on the other.

Connect

Connect the modem cable to the PC (the host) and the VX7 (the client). Select "Connect" from the Start Menu on the VX7 (**Start | Programs | Communications | Connect)**.

Note: Run "Connect" when the "Get Connected" wizard on the host PC is checking COM ports to establish a connection for the first time.

Note: USB will start automatically when the cable is connected, not requiring you to select "Connect" from the Start menu.

Explore

From the ActiveSync Dialog on the Desktop PC, click on the Explore button, which allows you to explore the VX7 from the PC side, with some limitations. You can copy files to or from the VX7 by drag-and-drop. You will not be allowed to delete files or copy files out of the \Windows directory on the VX7. (Technically, the only files you cannot delete or copy are ones marked as system files in the original build of the Windows CE image. This, however, includes most of the files in the \Windows directory).

Disconnect

Serial Connection

- Disconnect the cable from the VX7.
- Click the status bar icon in the lower right hand corner of the status bar. Then click the Disconnect button.

USB Connection

- Disconnect the cable from the VX7.
- Click the status bar icon in the lower right hand corner of the status bar. Then click the Disconnect button.

Radio Connection

- Click the status bar icon in the lower right hand corner of the status bar. Then click the Disconnect button.

Important Information – Cold Boot and Loss of Host Re-connection

ActiveSync assigns a partnership between a client and a host computer. A partnership is defined by two objects -- a unique computer name and a random number generated when the partnership is first created. An ActiveSync partnership between a unique client can be established to two hosts.

If the VX7 is cold booted, the random number is deleted – and the partnership with the last one of the two hosts is also deleted. The host retains the random numbers and unique names of all devices having a partnership with it. Two clients cannot have a partnership with the same host if they have the same name. (**Control Panel | System | Device Name**)

If the cold booted VX7 tries to reestablish the partnership with the same host PC, a new random number is generated for the VX7 and ActiveSync will insist the unique name of the VX7 be changed. If the VX7 is associated with a second host, changing the name will destroy *that* partnership as well. This can cause some confusion when re-establishing partnerships with hosts.

Troubleshooting

ActiveSync on the host says that a device is trying to connect, but it cannot identify it

One or more control lines are not connected. This is usually a cable problem, but on a laptop or other device, it may indicate a bad serial port.

ActiveSync indicator on the host (disc in the toolbar tray) turns green and spins as soon as you connect the cable, before clicking the Connect icon (or REPLLOG.EXE in the Windows directory).

One or more control lines are tied together incorrectly. This is usually a cable problem, but on a laptop or other device, it may indicate a bad serial port.

ActiveSync indicator on the host turns green and spins, but connection never occurs

Baud rate of connection is not supported or detected by host. Try forcing ActiveSync on the desktop PC to use a specific baud rate and set the VX7 to use the same baud rate.

-or-

Incorrect or broken data lines in cable.

ActiveSync indicator on the host remains gray

The host doesn't know you are trying to connect. May mean a bad cable, with no control lines connected, or an incompatible baud rate. Try the connection again, with a known-good cable.

Testing connection with a terminal emulator program, or a serial port monitor

You can use HyperTerminal or some other terminal emulator program to do a rough test of ActiveSync. Set the terminal emulator to 8 bits, no parity, 1 stop bits, and the same baud rate as the connection on the CE device. After double-clicking REPLLOG.EXE on the CE device, the word “CLIENT” appears on the display in ASCII format. When using a serial port monitor, you see the host echo “CLIENT”, followed by “SERVER”. After this point, the data stream becomes straight (binary) PPP.

Create a Communication Option

1. On the VX7, select **Start | Settings | Control Panel | Network and Dialup Connections**. A window is displayed showing the existing connections.
2. Assuming the one you want does not exist, double-click **Make New Connection**.
3. Give the new connection an appropriate name. Click the **Direct Connection** radio button. Click the Next button.
4. From the popup menu, choose the port you want to connect to. Only the available ports are shown.
5. Click the **Configure...** button.
6. Under the **Port Settings** tab, choose the appropriate baud rate. Data bits, parity, and stop bits remain at 8, none, and 1, respectively.
7. Under the **Call Options** tab, be sure to turn off **Wait for dial tone**, since a direct connection will not have a dial tone. Set the timeout parameter (default is 90 seconds). Click OK.
8. **TCP/IP Settings** should not need to change from defaults. Click the **Finish** button to create the new connection.
9. Close the **Remote Networking** window.
10. To activate the new connection select **Start | Settings | Control Panel | PC Connection** and click the **Change** button.
11. Select the new connection. Click OK twice.
12. Close the Control Panel window.
13. Connect the desktop PC to the VX7 with the appropriate cable.
14. Click the desktop Connect icon to test the new connection.

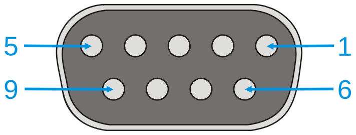
You can activate the connection by double-clicking on the specific connection icon in the Remote Networking window, but this will only start an RAS (Remote Access Services) session, and does not start ActiveSync properly.

Technical Specifications – Connection Cable

The exact serial cable is crucial. Many commercial null modem cables will not work. LXE recommends the following cable:

Serial cable:

9000A054CBL6D9D9



Pinout:

DB9 female	DB9 female
1	7
2	3
3	2
4	6, 8
5	5
6, 8	4
7	1
9	no connection

Figure 3-33 Pinout – Serial Cable for Synchronization

Some laptop devices do not properly implement all control lines on the serial port – the laptop connection will not work.

VX7 Utilities

The following files are pre-loaded by LXE.

LAUNCH.EXE

Launch works in coordination with registry settings to allow drivers or applications to be loaded automatically into DRAM at system startup. Registry settings control what gets launched; see the App Note for information on these settings. For examples, you can look at the registry key

HKEY_LOCAL_MACHINE \ Software \ LXE \ Persist

Launch will execute .CAB files, .BAT files, or .EXE files.

App Note

All applications to be installed into persistent memory must be in the form of Windows CE CAB files. These CAB files exist as separate files from the main installation image, and are copied to the CE device using ActiveSync, or using a Compact Flash ATA card. The CAB files are copied from ATA or using ActiveSync Explore into the folder System, which is the persistent storage virtual drive. Then, information is added to the registry, if desired, to make the CAB file auto-launch at startup.

The registry information needed is under the key HKEY_LOCAL_MACHINE \ Software \ LXE \ Persist, as follows. The main subkey is any text, and is a description of the file. Then 3 mandatory values are added:

FileName is the name of the CAB file, with the path (usually \System).

Installed is a DWORD value of **0**, which changes to **1** once auto-launch installs the file.

FileCheck is the name of a file to look for to determine if the CAB file is installed. This will be the name of one of the files (with path) installed by the CAB file. Since the CAB file installs into DRAM, when memory is lost this file is lost, and the CAB file must be reinstalled.

There are three optional fields that may be added:

Order is used to force a sequence of events. **Order=0** is first, and **Order=99** is last. Two items which have the same order will be installed in the same pass, but not in a predictable sequence.

Delay is used to add a delay after the item is loaded, before the next is loaded. The delay is given in seconds, and defaults to **0** if not specified. If the install fails (or the file to be installed is not found), the delay does not occur.

PCMCIA is used to indicate that the file (usually a CAB file) being loaded is a radio driver, and the PCMCIA slots should be started after this file is loaded. By default, the PCMCIA slots are off on powerup, to prevent the “Unidentified PCMCIA Slot” dialog from appearing. Once the drivers are loaded, the slot can be turned on. The value in the **PCMCIA** field is a DWORD, representing the number of seconds to wait after installing the CAB file, but before activating the slot (a latency to allow the thread loading the driver to finish installation). The default value of **0** means the slot is not powered on. The default values for the default radio drivers (listed below) is **1**, meaning one second elapses between the CAB file loading and the slot powering up.

The auto-launch process proceeds as follows:

- The launch utility opens the registry database and reads the list of CAB files to auto-launch.
- First it looks for **FileName** to see if the CAB file is present. If not, the registry entry is ignored. If it is present, and the Installed flag is not set, auto-launch makes a copy of the CAB file (since it gets deleted by installation), and runs the Microsoft utility WCELOAD to install it.
- If the Installed flag is set, auto-launch looks for the **FileCheck** file. If it is present, the CAB file is installed, and that registry entry is complete. If the **FileCheck** file is not present, memory has been lost, and the utility calls WCELOAD to reinstall the CAB file.
- Then, the whole process repeats for the next entry in the registry, until all registry entries are analyzed.
- To force execution every time (for example, for **AUTOEXEC.BAT**), use a **FileCheck** of **"dummy"**, which will never be found, forcing the item to execute.
- For persist keys specifying **.EXE** or **.BAT** files, the executing process is started, and then **Launch** will continue, leaving the loading process to run independently. For other persist keys (including **.CAB** files), **Launch** will wait for the loading process to complete before continuing. This is important, for example, to ensure that a .CAB file is installed before the .EXE files from the .CAB file are run.
- Note that the auto-launch process can also launch batch files (***.BAT**), executable files (***.EXE**), registry setting files (***.REG**), or sound files (***.WAV**). The mechanism is the same as listed above, but the appropriate CE application is called, depending on file type.

Registry information is already in the default image for the following:

Registry information is already in the default image for the following:

```
; these keys load the appropriate radio driver
[HKEY_LOCAL_MACHINE\SOFTWARE\LXE\Persist\Summit Radio]
      "FileName"="\SYSTEM\SUMMIT.CAB"
      "Installed"=dword:1
      "FileCheck"="\WINDOWS\SDCCFG10G.DLL"
      "Order"=dword:02
      "Delay"=dword:0
      "PCMCIA"=dword:1

[HKEY_LOCAL_MACHINE\SOFTWARE\LXE\Persist\Cisco Radio]
      "FileName"="\SYSTEM\CISCO.CAB"
      "Installed"=dword:0
      "FileCheck"="\WINDOWS\CISCO.DLL"
      "Order"=dword:02
      "Delay"=dword:0
      "PCMCIA"=dword:1

[HKEY_LOCAL_MACHINE\SOFTWARE\LXE\Persist\Symbol Radio]
      "FileName"="\SYSTEM\SYMBOL.CAB"
      "Installed"=dword:0
      "FileCheck"="\WINDOWS\NICTT.EXE"
      "Order"=dword:02
      "Delay"=dword:0
      "PCMCIA"=dword:1
; this key loads the RFID driver (N/A to VX7)
[HKEY_LOCAL_MACHINE\SOFTWARE\LXE\Persist\RFID]
      "FileName"="\WINDOWS\RFID.CAB"
      "FileCheck"="\WINDOWS\RFID_WDG.DLL"
      "Order"=dword:12
; this key installs RFTERM from the CAB file
[HKEY_LOCAL_MACHINE\SOFTWARE\LXE\Persist\LXE TE]
      "FileName"="\SYSTEM\RFTERM.CAB"
      "Installed"=dword:0
      "FileCheck"="\WINDOWS\LXE\RFTERM.EXE"
      "Order"=dword:10
      "Delay"=dword:0
; this key runs RFTERM as a startup app
[HKEY_LOCAL_MACHINE\SOFTWARE\LXE\Persist\RFTERM]
      "FileName"="\WINDOWS\LXE\RFTERM.EXE"
      "Installed"=dword:0
      "FileCheck"="dummy"
      "Order"=dword:40
      "Delay"=dword:0
[HKEY_LOCAL_MACHINE\SOFTWARE\LXE\Persist\Java]
      "FileName"="\SYSTEM\JEODE.CAB"
      "Installed"=dword:0
      "FileCheck"="\WINDOWS\EVM.EXE"
      "Order"=dword:30
      "Delay"=dword:0
; this key installs APPLOCK from the CAB file
[HKEY_LOCAL_MACHINE\SOFTWARE\LXE\Persist\AppLockInstall]
      "FileName"="\SYSTEM\APPLOCK.CAB"
      "FileCheck"="\WINDOWS\APPLOCK.EXE"
      "Order"=dword:0
; this key runs the APPLOCK prep app
[HKEY_LOCAL_MACHINE\SOFTWARE\LXE\Persist\AppLockPrep]
      "FileName"="\SYSTEM\APPLOCKPREP.EXE"
      "FileCheck"="dummy"
      "Order"=dword:1
; this key runs the APPLOCK main app
[HKEY_LOCAL_MACHINE\SOFTWARE\LXE\Persist\AppLockInstall]
      "FileName"="\SYSTEM\APPLOCK.EXE"
      "FileCheck"="dummy"
      "Order"=dword:63
[HKEY_LOCAL_MACHINE\SOFTWARE\LXE\Persist\AUTOEXEC]
      "FileName"="\SYSTEM\AUTOEXEC.BAT"
      "Installed"=dword:0
      "FileCheck"="dummy"
      "Order"=dword:50
      "Delay"=dword:0
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\LXE\Persist\Avalanche]
      "FileCheck"="\\System\\avalanche\\model.dat"
      "Installed"=dword:00000000
      "PCMCIA"=dword:00000000
      "Delay"=dword:00000000
      "Order"=dword:00000004
      "FileName"="\\System\\LXEAVA.CAB"
[HKEY_LOCAL_MACHINE\SOFTWARE\LXE\Persist\AvaLaunch]
      "Order"=dword:00000005
      "FileName"="\\System\\Avalanche\\Avainit.exe"
      "FileCheck"="dummy"
      "Delay"=dword:00000000
      "PCMCIA"=dword:00000000
      "Installed"=dword:00000000
```

;Avalanche

```
[HKEY_LOCAL_MACHINE\SOFTWARE\LXE\Persist\Avalanche]
      "FileName"="\SYSTEM\LXEAVA.CAB"
      "FileCheck"="\SYSTEM\AVALANCHE\MODEL.DAT"
      "Order"=dword:4
      "Installed"=dword:0
      "PCMCIA"=dword:0
      "Delay"=dword:0
[HKEY_LOCAL_MACHINE\SOFTWARE\LXE\Persist\AvaLaunch]
      "FileName"="\SYSTEM\AVALANCHE\AVAINIT.EXE"
      "FileCheck"="dummy"
      "Order"=dword:5
      "Delay"=dword:0
      "PCMCIA"=dword:0
      "Installed"=dword:0
```

Registry entries may vary depending on software revision level and options ordered with the VX7.

LAUNCH.EXE and Persistent Storage

If any of the following directories are created in the \System folder, Launch automatically copies all of the files in these directories to the respective folder on the flash drive:

- AppMgr
- Desktop
- Favorites
- Fonts
- Help
- Programs
- Recent

Note: Files in the Startup folder are executed, but only from \System\Startup. They are not copied to another directory.

REGEDIT.EXE

Registry Editor – LXE recommends **caution** when editing the Registry and also recommends making a backup copy of the registry before changes are made.

REGLOAD.EXE

Double-tapping a registry settings file (e.g. REG) causes RegLoad to open the file and make the indicated settings in the registry. This is similar to how RegEdit works on a desktop PC. The .REG file format is the same as on the desktop PC.

REGDUMP.EXE

Registry dump – Saves a copy of the registry as a text file. The file, REG.TXT, is located in the root folder.

Note: The REG.TXT file is not saved in persistent storage. To use the REG.TXT file as a reference in the even of a coldboot, LXE recommends copying the file to the \SYSTEM directory on the VX7 or storing a copy of the file on a PC.

WARMBOOT.EXE

Double click this file to warm boot the computer (i.e., all RAM is preserved). It automatically saves the registry before rebooting which means configuration changes are not lost.

WAVPLAY.EXE

Double tapping a sound file (e.g. WAV) causes WavPlay to open the file and run it in the background.

VX7 Command-line Utilities

Command line utilities can be executed by **Start | Run** | [program name].

COLDBOOT.EXE

Command line utility which performs a cold boot (all RAM is erased).

Passwords are lost upon cold boot. If a password is set, that password must be entered to begin the cold boot power cycle process.

PrtScrn.EXE

Command line utility which performs a screen print and saves the file in .BMP format in the \System folder. Tap **Start | Run** and type **prtscrn** and tap **OK**, or press **Enter**. There is a 10 second delay before the screen print is made. The device beeps and screen captured file (scrnnnnn.bmp) is placed in the \System folder. The numeric filename is incremented by 1 each time the PrtScrn function is activated. The command is not case-sensitive.

API Calls

See Also: LXE CE API Programming Guide E-SW-WINAPIPG

The LXE CE API Programming Guide documents only the LXE-specific API calls for the VX7. It is intended as an addition to the standard Microsoft Windows CE API documentation. Details of many of the calls in the LXE guide may be found in Microsoft's documentation.

The APIs documented in the programming guide are included in the file LXEAPI.DLL, which is in the standard Windows CE image on the VX7.

For ease of software development, the files LXEAPI.H and LXEAPI.LIB are available on the accessories CD, which are the C/C++ include files and the link library for the DLL, respectively.

A full SDK is now included for Microsoft Embedded Visual C++ 4.0 (which is available free on the Microsoft website).

Reflash the VX7

Note: When reflashing, LXE recommends using a Compact Flash (CF) card that is greater than 64MB. Files to be loaded on the CF card are: NK.BIN, EBOOT.NB0, XSCALE.BIT

Requirements:

- A screwdriver (not supplied by LXE)
- PCMCIA to CF card adapter

Preparation

- LXE recommends that installation of the CF card be performed on a clean, well-lit surface.
- Loosen the captive screws securing the user access panel cover. The cover is tethered to the VX7.

Caution ⚠	Make sure the VX7 has an uninterrupted power connection before beginning the reflash procedure. Loss of power during the reflash process can result in corrupted files.

IMPORTANT – Please contact LXE Customer Support for information on upgrading Windows CE .NET to Windows CE 5.0. These instructions are only valid for upgrading to another revision of the same operating system.

How To: Reflash using Keypress Method

Ⓟ For information on identifying the platform version of your VX7, please see “Identifying your VX7” in Chapter 2, “Physical Description and Layout”.

1. Place the PCMCIA adapter containing the CF card with new image files on it in the PCMCIA slot next to the radio.
2. Double-click **My Computer**, then **Storage Card** folder.
3. Select NK.BIN, EBOOT.NB0, XSCALE.BIT. Select **Edit | Copy**.
4. Tap **Back Arrow**. Doubleclick **\System** folder.
5. Select **Edit | Paste**. When asked “Overwrite ?”, click **Yes to All**.
6. When the copy process finishes, remove the he PCMCIA adapter containing the CF card.
7. Select **Start | Run** and type **Coldboot**.
8. Select one of the options below, as appropriate:

Platform 1 VX7’s

- Wait for the “Loading system from ATA” toolbar to appear. When it does, press and release the Power button. When the “Press power switch again for confirmation” message appears, the Power button must be pressed and released in the next three seconds to confirm the reload. If the Power button is not pressed during the three second period, the operating system resumes loading.

Platform 2 VX7's:

- Wait for the "Loading system from ATA" toolbar to appear. When it does, press and release the "A" key. When the "confirmation" message appears, "Y" key must be pressed and released in the next three seconds to confirm the reload. If the "Y" key is not pressed during the three second period, the operating system resumes loading.

9. The VX7 automatically reboots after flashing the bootloader. "Loading OS Image" is displayed on the screen and when the new OS finishes loading, all software upgrades are complete.
10. Secure the user access cover using the captive screws. The touchscreen must be re-calibrated.

How To: Reflash using TAG file Method

This method requires software revision 2BT or greater. To identify the software revision, please click on the "About" icon in the Windows CE Control Panel.

1. Place the PCMCIA adapter containing the CF card with new image files on it in the PCMCIA slot next to the radio.
2. Double-click **My Computer**, then **Storage Card** folder.
3. Select NK.BIN, EBOOT.NB0, XSCALE.BIT. Select **Edit | Copy**.
4. Tap **Back Arrow**. Doubleclick **\System** folder.
5. Select **Edit | Paste**. When asked "Overwrite ?", click **Yes to All**.
6. Additionally a REFLASH.TAG file is needed to trigger the reflash. This file can be created on the VX7 or copied to it along with the system files. The contents of the file are unimportant; but the file must be named REFLASH.TAG and it must be in the **\System** folder with the new system load.
7. When the copy process finishes, remove the he PCMCIA adapter containing the CF card.
8. Select **Start | Run** and type **Coldboot**.
9. When booting, the VX7 looks for a file named REFLASH.TAG in the \System folder.

   When this file is encountered, the VX7 loads a new bootloader image (eboot.nb0) into the boot flash. The tag file is deleted and the VX7 is rebooted to begin using the new boot loader. If there is no .nb0 file it does not re-flash and deletes the REFLASH.TAG.
10. The VX7 automatically reboots after flashing the bootloader. "Loading OS Image" is displayed on the screen and when the new OS finishes loading, all software upgrades are complete
11. Secure the user access cover using the captive screws. The touchscreen must be re-calibrated.

Clearing Persistent Storage

The coldboot utility sets all registry settings back to LXE factory defaults. No other clearing is available or necessary.

Keyboard Backlighting

This VX7 keyboards illuminate the individual keys

60-Key Keyboard

The keyboard is manually controlled by pressing <2nd> + <CTRL> + <F10> when using the 60-key keyboard. This key sequence immediately changes the state of the keyboard backlight as follows:

- Turns the backlight Off if it is currently On.
- Turns the backlight On if it is currently Off.

95-Key Keyboard

The keyboard backlight is manually controlled using the "backlight" key in the upper right hand corner of the keyboard. Pressing the backlight key cycles the keyboard backlight through the levels of backlight intensity:

- Off
- Maximum intensity
- Medium intensity
- Low intensity.

Changing the Display Resolution

The display resolution can only be changed on Platform 2 VX7's. For more information on identifying the platform version of your VX7, please see "Identifying your VX7" in Chapter 2, "Physical Description and Layout".

The default resolution of the VX7 display is 800 x 600 pixels. An optional resolution of 640 x 480 pixels is supported.

To change the display resolution to 640 x 480 pixels, run \Windows\dvx7_640x480.reg and perform a warmboot.

To change the display resolution to 800 x 600 pixels, run \Windows\dvx7_800x600.reg and perform a warmboot.

Note: These utilities configure the display resolution on warmboot. After a coldboot, the default resolution of 800 x 600 pixels is enabled.

Disabling the Touchscreen

To disable the touchscreen, run \Windows\TouchDisable.reg and perform a warmboot.

To enable the touchscreen, run \Windows\TouchEnable.reg and perform a warmboot.

Note: These utilities affect the behavior of the touchscreen on warmboot. After a coldboot, the touchscreen is enabled.

Disabling the Touchscreen Heater

Ⓟ The touchscreen heater can only be disabled on Platform 2 VX7's. For more information on identifying the platform version of your VX7, please see "Identifying your VX7" in Chapter 2, "Physical Description and Layout".

The touchscreen heater installed in extended temperature VX7's may be disabled.

To disable the touchscreen heater, run \Windows\HeaterDisable.reg and perform a warmboot.

To enable the touchscreen heater, run \Windows\HeaterEnable.reg and perform a warmboot.

Note: These utilities affect the behavior of the touchscreen heater on warmboot. After a coldboot, the touchscreen heater is enabled.

Configuring NumLock Behavior

To set NumLock status to On after a warmboot, run \Windows\NumLockOn.reg and perform a warmboot.

To set NumLock status to Off after a warmboot, run \Windows\NumLockOff.reg and perform a warmboot.

Note: The current status of NumLock can be changed with the <2^{nd}> <SHIFT> <F10> keypress sequence, however this method does not change NumLock behavior upon reboot.

Note: These utilities affect the behavior of the NumLock on warmboot. After a coldboot, NumLock is enabled.

Configuring CapsLock Behavior

The CapsLock behavior can only be changed on VX7's with software revision 1ED or greater. For more information on identifying the software version of your VX7, please see "Identifying your VX7" in Chapter 2, "Physical Description and Layout".

To set CapsLock status to On after a warmboot, run \Windows\CapsLockOn.reg and perform a warmboot.

To set CapsLock status to Off after a warmboot, run \Windows\CapsLockOff.reg and perform a warmboot.

Note: Setting CapsLock to On using this method does not display the CapsLock icon in the Windows CE taskbar,

Note: The current status of CapsLock can be changed with the CapsLock key (95-key keyboard) or the CAPS key (60—key keyboard), however this method does not change CapsLock behavior upon reboot.

Note: These utilities affect the behavior of the CapsLock on warmboot. After a coldboot, CapsLock is disabled.

Configuring IPv6

The ability to disable IPv6 is only present on VX7's with software revision 1ED or greater. For more information on identifying the software version of your VX7, please see "Identifying your VX7" in Chapter 2, "Physical Description and Layout".

By default, IPv6 is enabled and an IPv6 broadcast message is sent on power up.

To disable IPv6, run \Windows\ipv6Disable.reg and perform a warmboot.

To enable IPv6, run \Windows\ipv6Enable.reg and perform a warmboot.

Note: These utilities affect the behavior of IPv6 on warmboot. After a coldboot, IPv6 is enabled.

Enabling GrabTime

S The ability to enable GrabTime to run automatically is only present on VX7's with software revision 2BT or greater. For more information on identifying the software version of your VX7, please see "Identifying your VX7" in Chapter 2, "Physical Description and Layout".

The VX7 has a GrabTime utility which can automatically synchronize the VX7 with a time server (via an Internet connection or a local time server) at boot up.

By default, using GrabTime for time synchronization at boot up is Off. Grabtime can be run at any time (even when Off at boot up) using the Sync button on the Date/Time control panel.

To enable GrabTime to run automatically at boot up, run \Windows\tmsync.reg and perform a warmboot. For more detail, see "LAUNCH.EXE", earlier in this chapter.

Note: This utility affects the behavior of GrabTime at warmboot. After a coldboot, GrabTime is disabled.

Synchronize with a Local Time Server

By default, GrabTime synchronizes via an Internet connection. To synchronize with a local time server:

1. Use ActiveSync to copy **GrabTime.ini** from the **My Device | Windows** folder on the mobile device to the host PC.
2. Edit the copy of **GrabTime.ini** on the host PC. Add the local time server's domain name to the beginning of the list of servers. You can optionally delete the remainder of the list.
3. Copy the modified **GrabTime.ini** file to the **My Device | System** folder on the mobile device.

The System/GrabTime.ini file takes precedence over the Windows/GrabTime.ini file. System/Grabtime.ini also persists after a coldboot; Windows/Grabtime.ini does not persist.

Network Configuration

There are two networking options available for the VX7:

- 2.4GHz wireless radios
- Ethernet (RJ-45) connector.

2.4 GHz Wireless Radios

Please refer to the appropriate section in Chapter 5, “Wireless Network Configuration” for configuring the Summit, Cisco or Symbol radio.

Ethernet Connector

When the VX7 is networked using the Ethernet connector, the VX7’s networking options are set via the Microsoft Windows CE Control Panel.

For more information on configuring the Microsoft Windows CE network settings, please refer to the Help feature or commercially available Windows CE networking literature.

Wavelink Avalanche Enabler Configuration

A VX7 device manufactured before October 2006 must have drivers and system files upgraded before it can use the Avalanche Enabler functions. Please contact an LXE representative for details on upgrading the mobile device baseline.

If the user is NOT using Wavelink Avalanche to manage their mobile device, the Enabler should not be installed on the mobile device.

Briefly . . .

The Wavelink Avalanche Enabler installation file is loaded on the mobile device by LXE; however, the device is not configured to launch the installation file automatically. The installation application must be run manually the first time Avalanche is used. After the installation application is manually run, a reboot is necessary for the Enabler to begin normal performance. Following this reboot, the Enabler will by default be an auto-launch application. This behavior can be modified by accessing the Avalanche Update Settings panel through the Enabler Interface.

Enabler Install Process

- Doubletap the LXE_VXC_ENABLER.CAB file in the System folder.
- Warm boot the mobile device.

Because the VX7 has two possible network adapters (the internal adapter for a cabled network connection and the wireless network card), the Enabler uses the first network adapter it discovers. In order to assure the Enabler uses the wireless connection, perform one of the following actions:

- Select the Adapters tab in the Enabler setup (See “Enabler Configuration”, later in this chapter) and make sure the wireless adapter is selected for Current Adapter.
- To disable the internal network adapter, create a file in the **\system** directory named NoEther.tag. The contents of the file are unimportant; but the file must be named NoEhter.tag and it must be in the **\system** directory. (If the **\system** directory contains a file named Ether.tag, you can rename this file to NoEther.tag instead of creating a new file). After creating the file, coldboot the VX7. After the VX7 finishes booting, the internal Ethernet adapter is disabled. The restore the adapter, delete the NoEther.tag file and coldboot and the VX7.

Enabler Uninstall Process

To remove the LXE Avalanche Enabler from a Windows CE mobile device:

- Delete the Avalanche folder located in the System folder.
- Warm boot the mobile device.

The Avalanche folder cannot be deleted while the Enabler is running. See *Stop the Enabler Service*. If sharing errors occur while attempting to delete the Avalanche folder, warm boot the mobile device, immediately delete the Avalanche folder, and then perform another warm boot.

Stop the Enabler Service

To stop the Enabler from monitoring for updates from the Avalanche MC Console:

1. Open the Enabler Settings Panels by tapping the Avalanche icon on the desktop.
2. Select **File | Settings**. Enter the password.
3. Select the Startup/Shutdown tab.
4. Select the “Do not monitor or launch Enabler” parameter to prevent automatic monitoring upon startup.
5. Select Stop Monitoring for an immediate shutdown of all enabler update functionality upon exiting the user interface.
6. Click the OK button to save the changes.
7. Reboot the device if necessary.

Update Monitoring Overview

There are three methods by which the Enabler on an LXE device can communicate with the Mobile Device Server running on the host machine.

- Wired via a serial cable between the Mobile Device Server and the LXE device.
- Wired via a USB connection, using ActiveSync, between the Mobile Device Server and the mobile device.
- Wirelessly via the 2.4GHz radio and an access point

After installing the Enabler on the mobile unit, a reboot is required for the Enabler to begin normal functionality. Following a mobile device reboot, the Enabler searches for an Mobile Device Server, first by polling all available serial ports and then over the wireless network. The designation of the mobile device to the Avalanche Mobility Center Manager is LXE_VXC.

The Enabler running on LXE Windows CE devices will attempt to access COM1, COM2, and COM3. “Agent not found” will be reported if the Mobile Device Server is not located or a serial port is not present or available (COM port settings can be verified using the LXE scanner applet in the Control Panel).

The wireless connection is made using the default radio interface on the mobile device therefore the device must be actively communicating with the network for this method to succeed. If a Mobile Device Server is found, the Enabler will automatically attempt to apply all wireless and network settings from the active profile. The Enabler will also automatically download and process all available packages.

Mobile Device Wireless and Network Settings

Once the connection to the Mobile Device Server is established, the Enabler will attempt to apply all network and wireless settings contained in the active profile. The success of the application of settings is dependent upon the local configuration of control parameters for the Enabler. These local parameters cannot be overridden from the Avalanche Mobility Center Console.

The default Enabler adapter control setting are:

- Manage network settings – enabled
- Use Avalanche network profile – enabled
- Manage wireless settings – disabled for Windows CE Units

To configure the Avalanche Enabler management of the network and wireless settings:

1. Open the Enabler Settings Panels by tapping the Avalanche icon on the desktop.
2. Select **File** | **Settings**. Enter the password.
3. Select the Adapters tab.
4. Choose settings for the “Use Manual Settings” parameter.
5. Choose settings for “Manage Network Settings”, “Manage Wireless Settings” and “Use Avalanche Network Profile”.
6. Click the OK button to save the changes.
7. Reboot the device.

The designation of the mobile device to the Avalanche CE Manager is LXE_VXC.

See Also: “Using Wavelink Avalanche on LXE Windows Computers”.

Enabler Configuration

Avalanche Icon

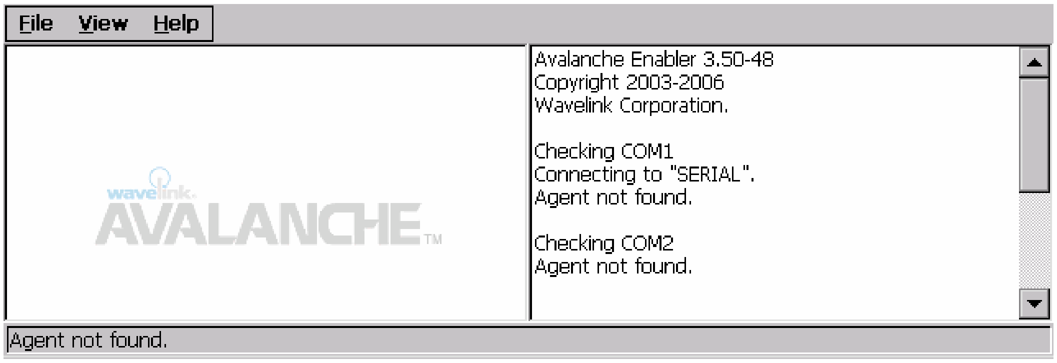
The Enabler user interface application is launched by clicking:

either the Avalanche icon on the desktop or Taskbar

or

selecting Avalanche from the Programs menu.

The opening screen presents the user with the connection status and a navigation menu.



```
Avalanche Enabler 3.50-48
Copyright 2003-2006
Wavelink Corporation.

Checking COM1
Connecting to "SERIAL".
Agent not found.

Checking COM2
Agent not found.
```

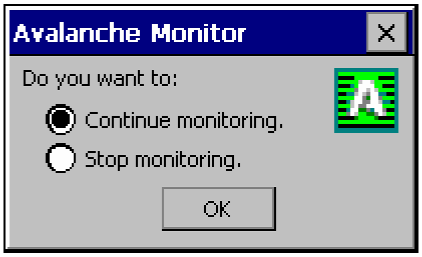
```
Agent not found.
```

Figure 3-34 Avalanche Enabler Opening Screen

File	View	Help
Connect Abort Settings Scan Config Exit	Updates Programs Icons List Details Launchable All Packages Time on Taskbar Device Status	Adapter Info About

File Menu Options

Connect	The Connect option under the File menu allows the user to initiate a manual connection to the Mobile Device Server. The connection methods, by default, are wireless and COM connections. Any updates available will be applied to the mobile device immediately upon a successful connection.
Abort	Stop transmission.
Settings	The Settings option under the File menu allows the user to access the control panel to locally configure the Enabler settings. The Enabler control panel is, by default, password protected. The default password is **system**. The password is not case-sensitive.

Scan Config	*Note: LXE does not support the Scan Configuration feature on Windows CE devices.* The Scan Config option under the File menu allows the user to configure Enabler settings using a special barcode that can be created using the Avalanche Mobility Center Console utilities. Refer to the *Wavelink Avalanche Mobility Center User's Guide* for details.
Exit	The Exit option is password protected. The default password is leave. The password is not case-sensitive. If changes were made on the Startup/Shutdown tab screen, then after entering the password, tap OK and the following screen is displayed:  Avalanche Monitor Do you want to: ● Continue monitoring. ○ Stop monitoring. Change the option if desired. Tap the X button to cancel Exit. Tap the OK button to exit the Avalanche applet.

Avalanche Update Settings

Access: Start | Avalanche | File | Settings

Use these menu options to setup the Avalanche Enabler on the mobile device. LXE recommends changing and then saving the changes (reboot) before connecting to the network.

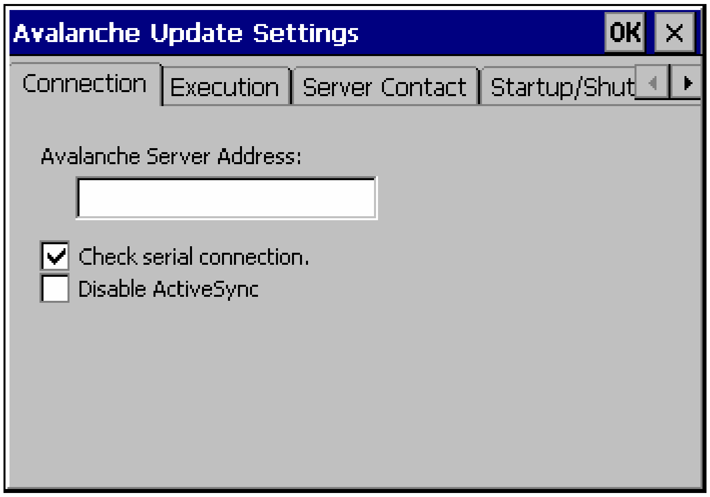
Alternatively, the Mobile Device Server on can be disabled until needed (refer to the *Wavelink Avalanche Mobility Center User's Guide*. for details).

Menu Options

Settings Tab	**Function**
Connection	Enter the IP Address or host name of the Mobile Device Server. Set the order in which serial ports or RF are used to check for the presence of the Mobile Device Server.
Execution	*Unavailable in this release.* LXE recommends using AppLock, which is resident on each Windows mobile device.
Server Contact	Setup synchronization, scheduled Mobile Device Server contact, suspend and reboot settings.
Startup/Shutdown	Set options for Enabler program startup or shutdown.

Scan Config	This option allows the user to configure Enabler settings using a special barcode that is created by the Avalanche Mobility Center Console. *Not currently supported by LXE.*
Display	Set up the Windows display at startup, on connect and during normal mode. The settings can be adjusted by the user.
Shortcuts	Add, delete and update shortcuts to user-allowable applications.
Adapters	Enable or disable network and wireless settings. Select an adapter and switch between the Avalanche Network Profile and manual settings.
Status	View the current adapter signal strength and quality, IP address, MAC address, SSID, BSSID and Link speed. The user cannot edit this information.

Connection



Avalanche Server Address:

☑ Check serial connection.

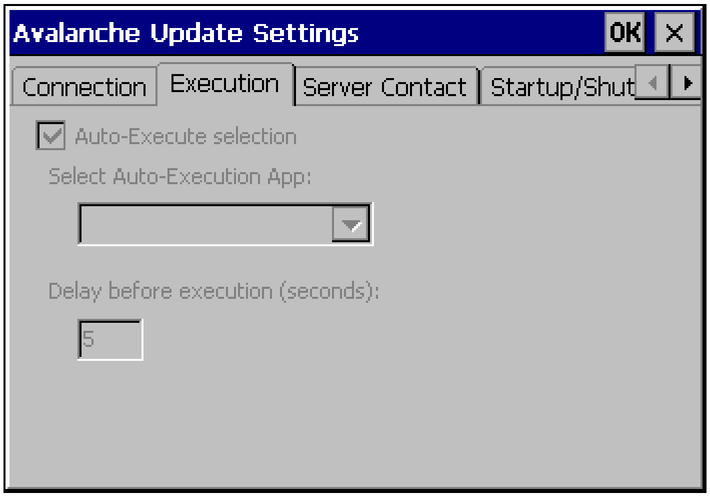
□ Disable ActiveSync

Figure 3-35 Connection Options

Avalanche Server Address	Enter the IP Address or host name of the Mobile Device Server assigned to the mobile device
Check Serial Connection	Indicates whether the Enabler should first check for serial port connection to the Mobile Device Server before checking for a wireless connection to the Mobile Device Server.
Disable ActiveSync	Disable ActiveSync connection with the Mobile Device Server.

Execution

Note the dimmed options on this panel. This menu option is designed to manage downloaded applications for automatic execution upon startup.



☑ Auto-Execute selection

Select Auto-Execution App:

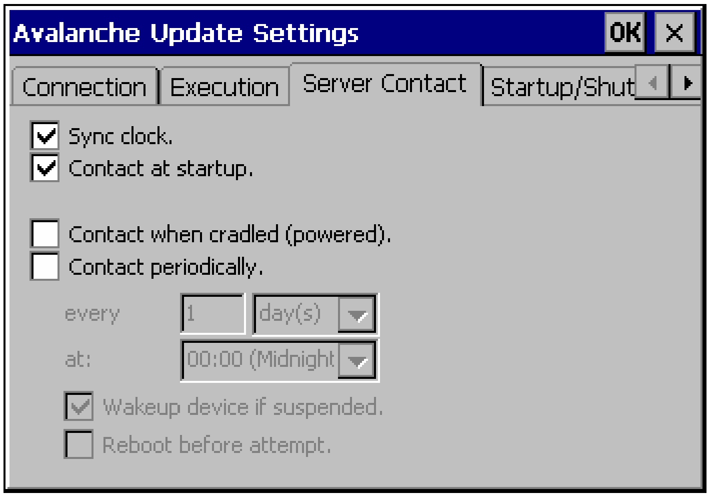
Delay before execution (seconds):

5

Figure 3-36 Execution Options (Dimmed)

Auto-Execute Selection	An application that has been installed with the Avalanche Mobility Center Console can be run automatically following each boot.
Select Auto-Execute App	The drop-down box provides a list of applications that have been installed by the Avalanche Mobility Center Console.
Delay before execution	Time delay before launching Auto-Execute application.

Server Contact



☑ Sync clock.

☑ Contact at startup.

☐ Contact when cradled (powered).

☐ Contact periodically.

every 1 day(s)

at: 00:00 (Midnight

☑ Wakeup device if suspended.

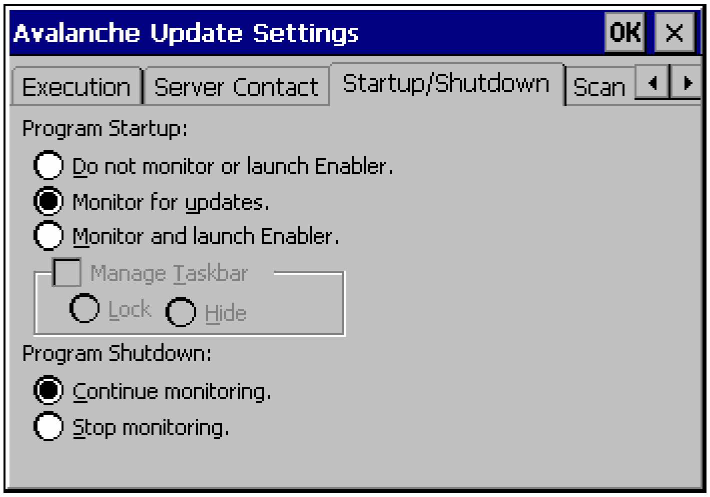
☐ Reboot before attempt.

Figure 3-37 Server Contact Options

Sync Clock	Reset the time on the mobile computer based on the time on the Mobile Device Server.
Contact at startup	Connect to the Mobile Device Server when the Enabler is accessed.
Contact when cradled	Initiate connection to the Mobile Device Server based on a docking event.
Contact Periodically	Allows the administrator to configure the Enabler to contact the Mobile Device Server and query for updates at a regular interval beginning at a specific time.
Wakeup device if suspended	If the time interval for periodic contact with the Mobile Device Server occurs, a mobile device that is in Suspend Mode can ‘wakeup’ and process updates.
Reboot before attempt	Reboot mobile device before attempting to contact Mobile Device Server.

Startup/Shutdown

LXE recommends using LXE AppLock to manage the taskbar. AppLock is resident on each mobile device with a Windows OS. AppLock configuration instructions are located in Chapter 6.



Program Startup:

○ Do not monitor or launch Enabler.

● Monitor for updates.

○ Monitor and launch Enabler.

□ Manage Taskbar

○ Lock ○ Hide

Program Shutdown:

● Continue monitoring.

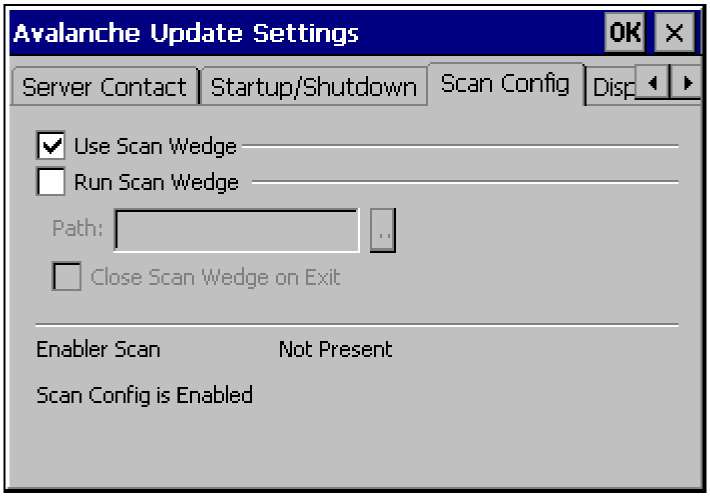
○ Stop monitoring.

Figure 3-38 Startup / Shutdown Options

Do not monitor or launch Enabler	When the device boots, do not launch the Enabler application and do not attempt to connect to the Mobile Device Server.
Monitor for updates	Attempt to connect to the Mobile Device Server and process any updates that are available. Do not launch the Enabler application.
Monitor and launch Enabler	Attempt to connect to the Mobile Device Server and process any updates that are available. Launch the Enabler application.
Manage Taskbar (Lock or Hide)	Note the dimmed options. The Enabler can restrict user access to other applications when the user interface is accessed by either locking or hiding the taskbar.
Program Shutdown (Continue or Stop monitoring)	The system administrator can control whether the Enabler continues to monitor the Mobile Device Server for updates once the Enabler application is exited.

Scan Config

Note: Scan Config functionality is a standard option of the Wavelink Avalanche System but is not currently supported by LXE on Windows CE.



Avalanche Update Settings

☑ Use Scan Wedge

□ Run Scan Wedge

Path:

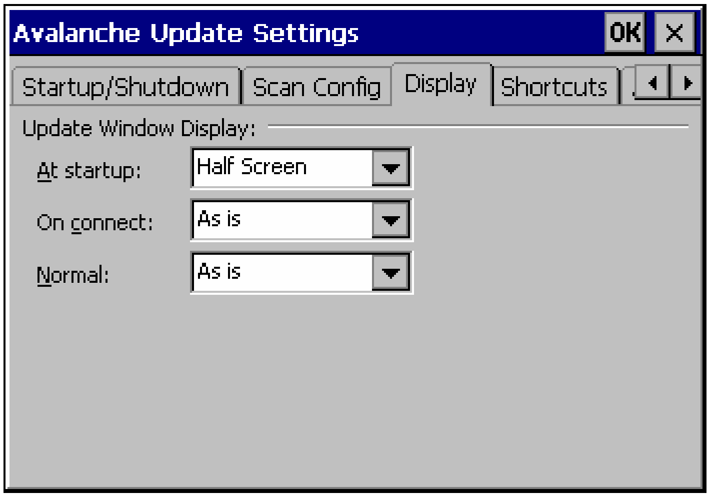
□ Close Scan Wedge on Exit

Enabler Scan Not Present

Scan Config is Enabled

Figure 3-39 Scan Config Option

Display



Avalanche Update Settings

Update Window Display:

At startup: Half Screen

On connect: As is

Normal: As is

Figure 3-40 Window Display Options

Update Window Display

The user interface for the Enabler can be configured to dynamically change based on the status of the connection with the Mobile Device Server.

At startup	Half screen, Hidden or Full screen. Default is Half screen.
On connect	As is, Half screen, full screen, Locked full screen. Default is As is.
Normal	Half screen, Hidden or As is. Default is As is.

Shortcuts

LXE recommends using LXE AppLock for this function. AppLock is resident on each mobile device with a Windows OS. AppLock configuration instructions are located in Chapter 6.

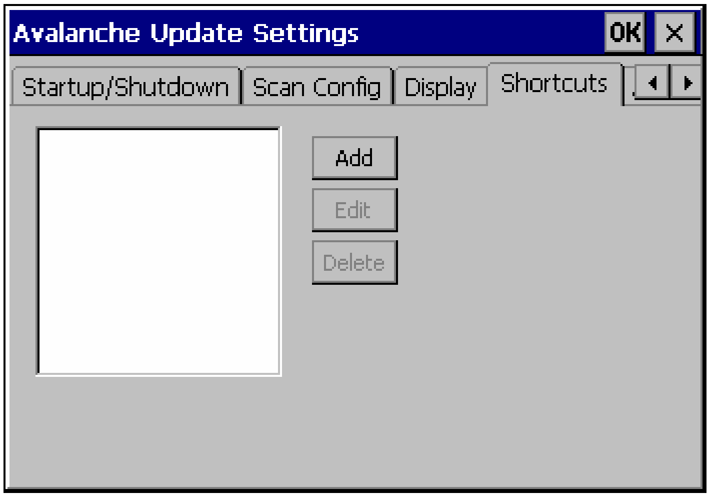


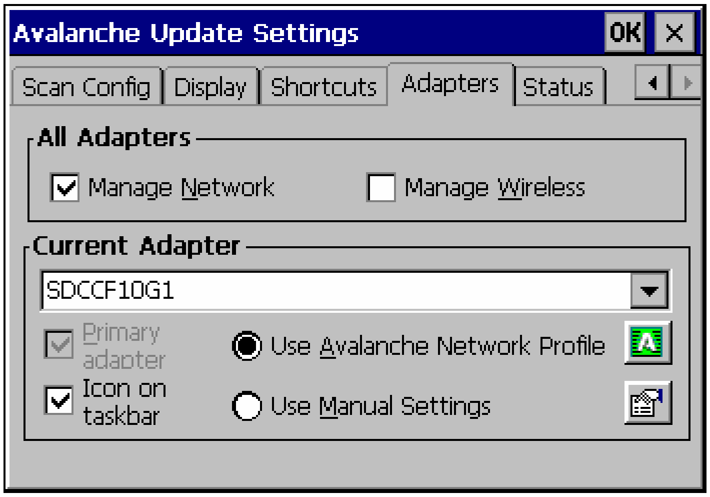
Figure 3-41 Application Shortcuts

Configure shortcuts to other applications on the mobile device. Shortcuts are viewed and activated in the Programs panel. This limits the user's access to certain applications when the Enabler is controlling the mobile device display.

LXE recommends using LXE AppLock for this function. See Chapter 6 "AppLock" for instruction.

Adapters

Note: LXE recommends the user review the network settings configuration utilities and the default values in Chapter 5 before setting All Adapters to Enable in the Adapters applet.


Avalanche Update Settings

All Adapters

☑ Manage Network □ Manage Wireless

Current Adapter

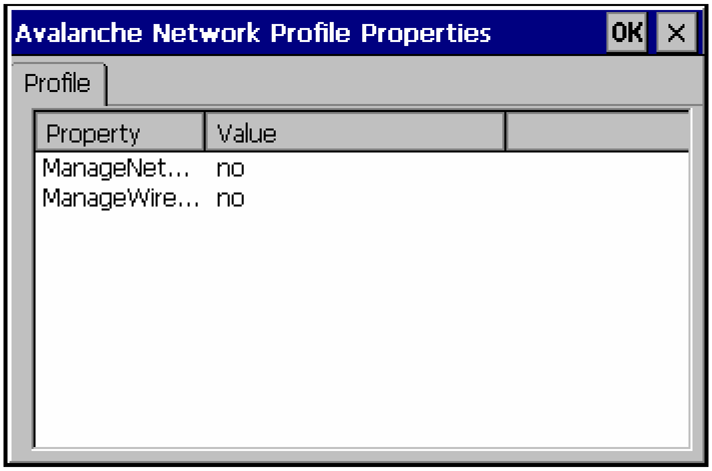
SDCCF10G1

☑ Primary adapter ● Use Avalanche Network Profile

☑ Icon on taskbar ○ Use Manual Settings

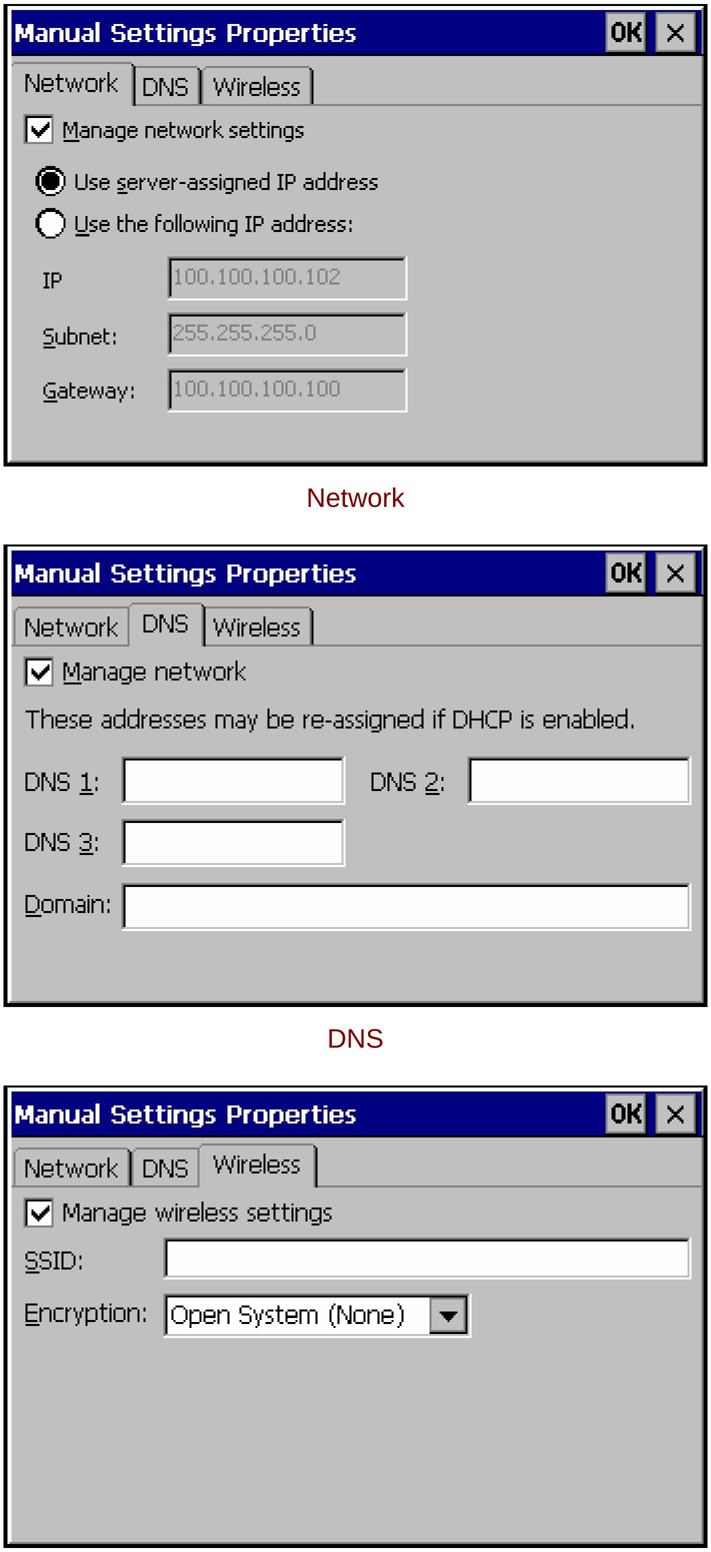
Figure 3-42 Adapter Options – Network

Manage Network Setting	When enabled, the Enabler will control the network settings. This parameter cannot be configured from the Avalanche Mobility Center Console and is enabled by default.
Manage Wireless Settings	When enabled, the Enabler will control the wireless settings. This parameter cannot be configured from the Avalanche Mobility Center Console and is disabled by default. This parameter setting **does not apply to Summit Clients *only***.
Current Adapter	Lists all network adapters currently installed on the mobile device.
Primary Adapter	Indicates if the Enabler is to attempt to configure the primary adapter (active only if there are multiple network adapters).
Icon on taskbar	Places the Avalanche icon in the Avalanche taskbar that may, optionally, override the standard Windows taskbar.
Use Avalanche Network Profile	The Enabler will apply all network settings sent to it by the Avalanche Mobility Center Console.

Avalanche Icon	Selecting the Avalanche Icon will access the Avalanche Network Profile tab which will display current network settings.  Avalanche Network Profile Properties Profile Property: Value ManageNet... : no ManageWire... : no Figure 3-43 Avalanche Network Profile Displayed

Use Manual Settings	When enabled, the Enabler will ignore any network or wireless settings coming from the Avalanche Mobility Center Console and use only the network settings on the mobile device.
Properties Icon	Selecting the Properties icon displays the Manual Settings Properties dialog applet. From here, the user can configure Network, DNS and Wireless parameters using the displays shown below:

Note: A reboot may be required after enabling or disabling these options.



Manual Settings Properties

☑ Manage network settings

● Use server-assigned IP address

○ Use the following IP address:

IP 100.100.100.102

Subnet: 255.255.255.0

Gateway: 100.100.100.100

Network

Manual Settings Properties

☑ Manage network

These addresses may be re-assigned if DHCP is enabled.

DNS 1:

DNS 2:

DNS 3:

Domain:

DNS

Manual Settings Properties

☑ Manage wireless settings

SSID:

Encryption: Open System (None)

Wireless

Figure 3-44 Manual Settings Properties Panels

For descriptions of these Enabler parameters, refer to Chapter 5 “Wireless Network Configuration”.

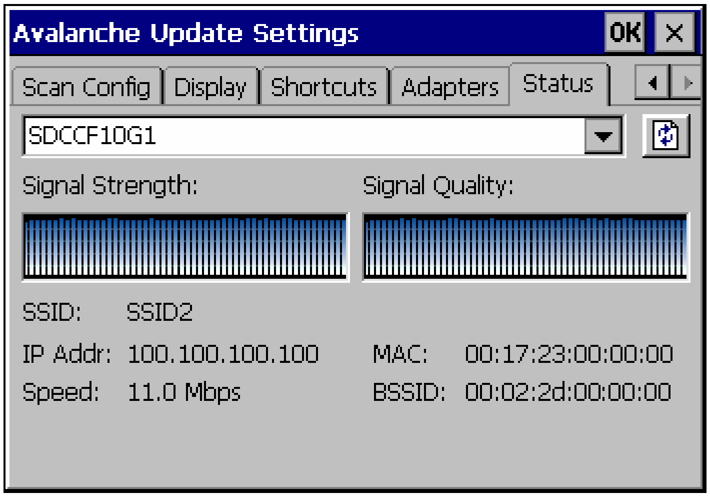
LXE does not recommend enabling “Manage Wireless Settings” for Summit Client devices.

When you download a profile that is configured to manage network and wireless settings, the Enabler will not apply the manage network and wireless settings to the adapter unless the global **Manage wireless settings** and **Manage network settings** options are enabled on the Adapters panel (see Figure titled Adapters Options – Network).

Until these options are enabled, the network and wireless settings are controlled by the third-party software associated with these settings.

Status

The Status panel displays the current status of the mobile device network adapter selected in the drop down box. Note the availability of the Windows standard Refresh button. When tapped, the signal strength, signal quality and link speed are refreshed for the currently selected adapter. It also searches for new adapters and may cause a slight delay to refresh the contents of the drop-down menu.



SDCCF10G1

Signal Strength:

Signal Quality:

SSID: SSID2

IP Addr: 100.100.100.100

Speed: 11.0 Mbps

MAC: 00:17:23:00:00:00

BSSID: 00:02:2d:00:00:00

Figure 3-45 Status Display

Link speed indicates the speed at which the signal is being sent from the adapter to the mobile device. Speed is dependent on signal strength.

Chapter 4 Scanner

Introduction

Access: Start | Settings | Control Panel | Scanner

Set scanner keyboard wedge, scanner icon appearance, active scanner port, and scan key settings. Assign baud rate, parity, stop bits and data bits for available COM ports.

Factory Default Settings		
Main		
Port 1	COM1	
Port 2	Disabled	
Send key messages WEDGE	Enabled	
Enable Internal Scanner Sound	Enabled	
On Delay Ms	3000	
COM Ports	COM1	COM3 [3]
Baud Rate	9600	9600
Parity	None	None
Stop Bits	1	1
Data Bits	8	8
Power on Pin 9	On	Off
Barcode		
Enable Code ID	None	
Symbology		
Symbology	All	
Enable	Checked	
Min	1	
Max	all	
Add Prefix	Disabled	
Add Suffix	Disabled	
Strip Leading	Disabled, 0 Characters	
Strip Trailing	Disabled, 0 Characters	
Strip CodeID	Disabled	
Strip Barcode Data	Disabled	
Control Character		
Translate All	Disabled	
Control Characters	None assigned	

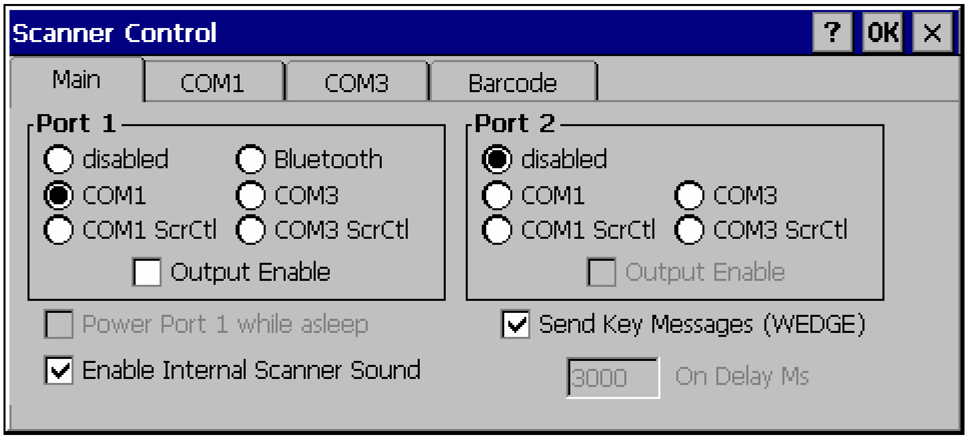
Scanner control panel options may vary with software revision level. To identify the software revision, please click on the “About” icon in the Windows CE Control Panel.

[3] The COM3 port is labeled “COM2/3”.

Notes:

- ActiveSync will not work over a COM port if that COM port is assigned to Port 1 or Port 2 in the Scanner applet as a scanner input. For example, if COM1 is being used by the scanner, COM1 can't be used by any other program.
- After scanning a Reset All or equivalent barcode for your specific external scanner, the next step is to select **Start | Control Panel | Scanner**. Click the **OK** button and close the scanner control panel. This action synchronizes all scanner formats.
- The scanner wedge does not configure an external scanner. Supported symbologies must be enabled for external scanner (see the documentation provided with the external scanner). Enabling or disabling a symbology in the scanner wedge only affects processing of the barcode data. It does not enable or disable the external scanner's ability to scan the symbology.
- LXE 8300 Tethered Scanners and Symbology Settings (AIM ID) – Before manipulating data received from an 8300 series scanner, and symbology settings are desired, the user must configure and append the Symbology ID as a prefix. See the documentation provided with the scanner for details.

Main



Port 1

○ disabled ○ Bluetooth
● COM1 ○ COM3
○ COM1 ScrCtl ○ COM3 ScrCtl
□ Output Enable

Port 2

● disabled
○ COM1 ○ COM3
○ COM1 ScrCtl ○ COM3 ScrCtl
□ Output Enable

□ Power Port 1 while asleep

☑ Enable Internal Scanner Sound

☑ Send Key Messages (WEDGE)

3000 On Delay Ms

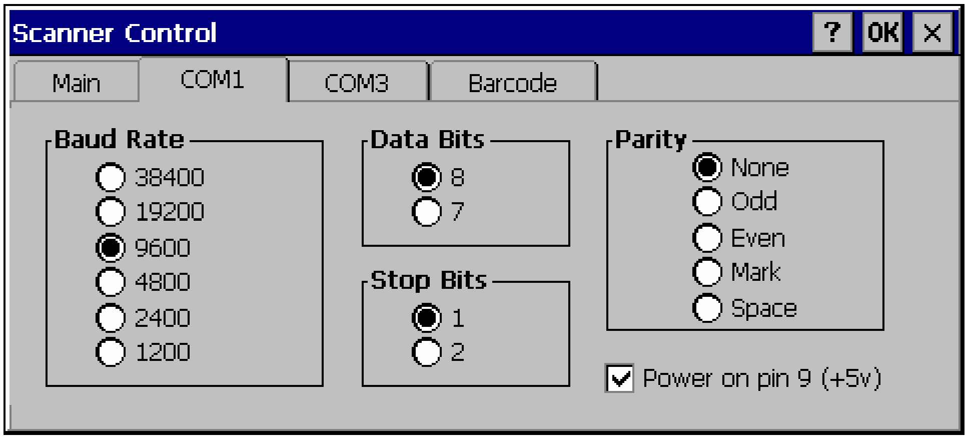
Figure 4-1 Scanner Properties / Main Tab

Adjust the settings and click the OK box to save the changes. The changes take effect immediately.

Two modes are determined by the configuration of "Send Key Messages (WEDGE)" setting.

- If "Send Key Messages (WEDGE)" is checked, the Scanner Driver is in "Key Message" (also known as "character") mode which sends the barcodes to the application with the focus as keystrokes. All data scanned is converted to keystrokes and sent to the active window.
- If "Send Key Messages (WEDGE)" is not checked, the Scanner Driver is in "Block" mode which buffers the data that can be read by an application from the WDG: device through the OS or LXE APIs. Note that this latter method is significantly faster than using "Wedge".
- Even if Send Key Messages is enabled ("key mode"), the data is still available using the scanner APIs ("block mode"). If two or more applications are reading the data in Block mode, ClearBuf must be set to Off so data is not erased when read. Please refer to the "CE API Programming Guide" for details on scanner APIs.

COM Ports



Baud Rate
○ 38400
○ 19200
● 9600
○ 4800
○ 2400
○ 1200

Data Bits
● 8
○ 7

Stop Bits
● 1
○ 2

Parity
● None
○ Odd
○ Even
○ Mark
○ Space

☑ Power on pin 9 (+5v)

Figure 4-2 Scanner Properties / COM Port Settings

Adjust the settings and click the OK box to save the changes. The changes take effect immediately.

The COM1 display contains the same parameters as the COM3 Tab. Adjust the settings and click the OK box to save the changes. The changes take effect immediately.

Note: This panel configures the VX7 for an external scanner. It DOES NOT configure the tethered scanner. Please refer to the documentation for the tethered scanner for information on configuring the tethered scanner.

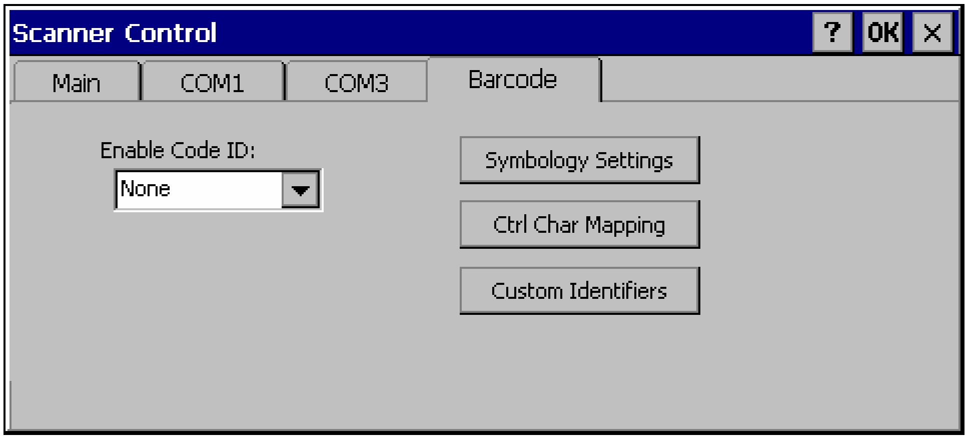
Serial Port Pin 9

To configure either COM port to have power (+5V) on Pin 9, check the “Power on pin 9 (+5V)” checkbox on the appropriate tab. This is required to supply power to an external scanner,

To configure either Com port to have RI on Pin 9, uncheck the “Power on pin 9 (+5V)” checkbox on the appropriate tab.

Barcode

The **Barcode** tab replaces the **Advanced** tab used in previous software revisions and adds several new features. Please contact your LXE support representative for details.



Enable Code ID: None

Figure 4-3 Scanner Properties / Barcode Settings

The Barcode tab contains several options to control barcode processing. Options include:

- Defining custom Code IDs
- Disable processing of specified barcode symbologies
- Rejecting barcode data that is too sort or too long
- Stripping characters including Code ID, leading or trailing characters and specified barcode data strings
- Replacing control characters
- Adding a prefix and a suffix.

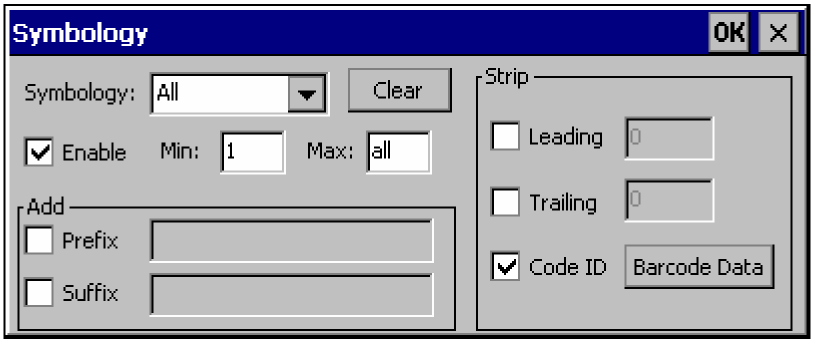
For examples of the barcode processing options in use, please refer to:

- "Control Code Replacement Examples"
- "Barcode Processing Examples"

later in this chapter.

Symbology Settings

Processing features such as the stripping of characters, rejection based on data length and addition of a prefix/suffix are specified by symbology allowing for different processing characteristics depending on the type of barcode scanned. These settings are configured by clicking the Symbology Settings button on the Barcode tab.



Symbology: All

☑ Enable Min: 1 Max: all

Add

□ Prefix

□ Suffix

Strip

□ Leading 0

□ Trailing 0

☑ Code ID

Figure 4-4 Scanner Properties / Barcode /Symbology Settings

The Symbology pulldown list determines the symbology which is being customized. The entries in the pulldown list are dependent on the Code ID type selected on the Barcode tab.

When All is selected, the changed settings become the defaults for all symbologies that have not been previously customized.

If any settings have been customized for an individual symbology, that symbology has an asterisk (*) beside its name in the list. Once configured, the specified symbology uses the entries on its individual screen. The default (All) settings have no effect on a previously customized symbology.

Symbology settings are saved when the OK button is clicked. Settings are also saved when a new Symbology is selected from the Symbology drop-down list.

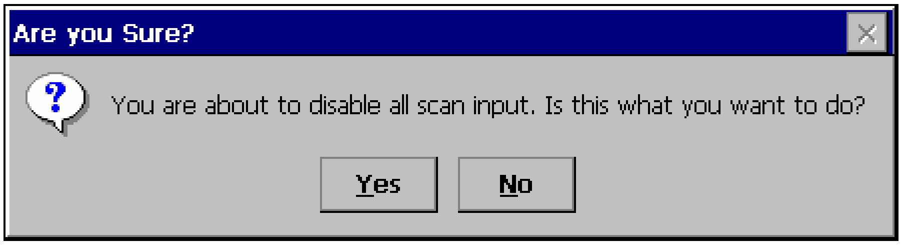
Use the Clear button to erase any customized entries, as follows:

- If the Clear button is clicked while a specific symbology is selected, any customization for that symbology is erased and the asterisk (*) is removed. The symbology then uses the settings specified for All.
- If the Clear button is clicked while All is selected, a confirmation box is displayed. If confirmed, the process clears all symbology customizations and all asterisk (*) indicators. All symbologies are reset to their factory defaults.

The following screen features are used during barcode processing. Please refer to "Barcode Processing", later in this section, for complete details:

- Enable – Determines if the specified symbology is enabled. Please see "Step 2: Reject Disabled Symbologies".

  When there are ***no** customized symbology settings*, and the Enable box is unchecked while All is selected, a warning message is displayed.



Are you Sure?

You are about to disable all scan input. Is this what you want to do?

Figure 4-5 Disable Scan Input Confirmation

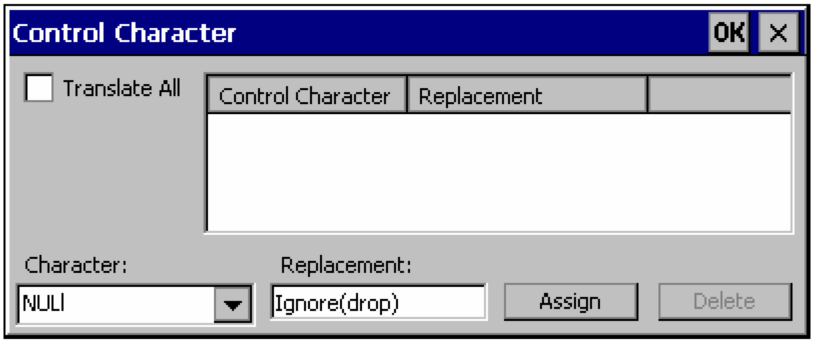
  Click **Yes** to disable all scan input. Click **No** to cancel.

  If there ***are** customized symbologies* and the **Enable** box is unchecked, all symbologies are disabled *except* the customized ones.

- Min – Specifies the minimum length the barcode data must be in able to be processed. Please see "Step 3: Check Barcode Length".
- Max – Specifies the maximum length the barcode data can be in able to be processed. Please see "Step 3: Check Barcode Length".
- Prefix – Specifies the string to be added to the beginning of barcode data. Please see "Step 8: Add Prefix String".
- Suffix – Specifies the string to be added to the end of barcode data. Please see "Step 11: Add Prefix String".
- Leading – Specifies the number of characters to strip from the beginning of the barcode data. Please see "Step 4: Strip Leading Characters".
- Trailing – Specifies the number of characters to strip from the end of the barcode data. Please see "Step 5: Strip Trailing Characters".
- Code ID – Specifies if the Code ID is stripped from the barcode data. Please see " "Step 1: Check Code ID and "Step 9: Add Code ID"
- Barcode Data – Specifies specific data to strip from the barcode. Please see "Step 6: Strip Barcode Data Strings".

Ctrl Char Mapping

Control character mapping is accessed by clicking on the Ctrl Char Mapping button on the Barcode tab.



Character: NUL

Replacement: Ignore(drop)

Figure 4-6 Scanner Properties / Barcode / Ctrl Char Mapping

This screen allows two functions to be configured, character translation and character replacement.

Character Translation

If "Translate All" is checked and "Send Key Messages" is checked, unprintable ASCII characters (characters below 20H) in scanned barcodes are assigned to their appropriate 2 keystroke CTRL code sequence (CTRL + letter) when the barcodes are sent in Key Message mode. Please see "Step 13: Start Key Output Thread".

When "Translate All" is not checked and "Send Key Messages" is checked, any CTRL code which has a keyboard equivalent is passed as a keystroke (enter, tab, escape, backspace, etc.); any CTRL code which does not have a keyboard equivalent is dropped. Please see "Step 13: Start Key Output Thread".

In Block mode ("Send Key Messages" is not checked) CTRL codes are always passed through as a single CTRL code value.

Character translation includes the barcode data and any prefix or suffix.

Character Replacement

Additionally, in both output modes control characters can be replaced with user defined data. The user-defined data can be text, hat-encoded or hex-encoded.

This mapping is independent of the "Translate All" function. If a control character is replaced by another control character, the replacement is performed only on the barcode data. Please see "Step 7: Replace Control Characters".

Custom Identifiers

This option allows the specification of custom Code IDs besides those using the standard AIM and Symbol IDs. To access the custom ID screen, click on the Custom Identifiers button on the Barcode tab.

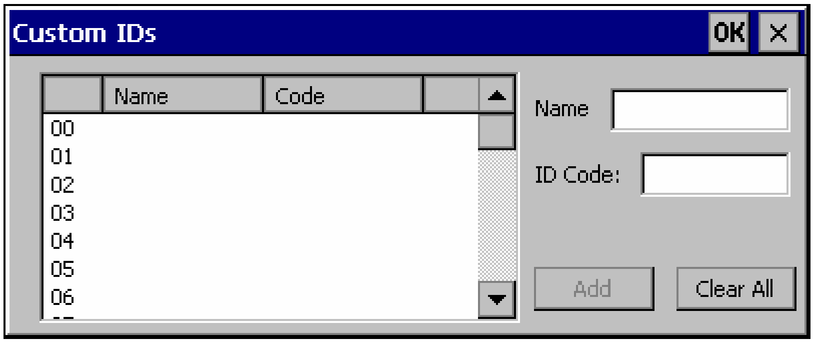


Figure 4-7 Scanner Properties / Barcode / Custom Identifiers

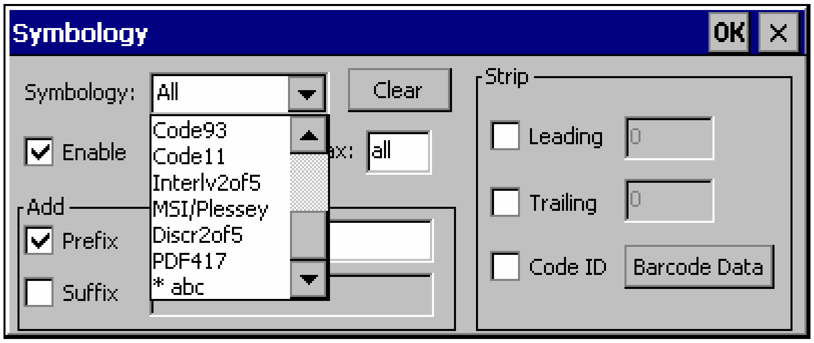
To add a custom ID, specify a Name and ID Code.

- Name is the descriptive name used to identify the custom ID. Names must be unique from each other. The value entered in the Name textbox is used in the symbology pulldown list to identify the custom ID.
- ID Code specifies the data at the beginning of the barcode that acts as an identifier (the actual Code ID).
- Both Name and ID Code must be specified before the custom ID can be added. The Name and ID Code boxes can have the same value, if desired.
- When incoming data is checked for a custom ID code, the list is compared in the order displayed on this screen.

Several functions are available:

- To add data to the list: Type the data into the Name and ID Code textboxes. The leftmost button is enabled and labeled Add. Click the Add button to add this data to the next available location in the list.
- To insert data into a blank entry: Click on the desired entry. The leftmost button is enabled and labeled Insert. Type the data into the Name and Code ID textboxes. When the Insert button is clicked, the data is added into the selected list entry.
- To edit data in the list: Double click on the item to edit. The current value of that item is copied into the textboxes for editing. The leftmost button is enabled and labeled Replace. When the Replace button is clicked, the values in the textboxes update the selected list item.
- To delete an item from the list: Click on the item to be deleted. The rightmost button is enabled and labeled Remove. Click the Remove button to remove the entry from the list. Deleting an entry does not move up items below in the list. A blank line (which is ignored during the processing) remains when an item is deleted.
- To erase all items from the list: When no items are selected in the list, the rightmost button is enabled and labeled Clear All. To clear all list items, click the Clear All button and confirm the delete.

Custom Code IDs are displayed in the Symbology pulldown box.



Symbology: All

☑ Enable

ax: all

Add

☑ Prefix

□ Suffix

Strip

□ Leading 0

□ Trailing 0

□ Code ID

Figure 4-8 Symbology List with Custom ID

If AIM or Symbol Code ID is selected from the Enable Code ID pulldown list, the custom IDs appear at the end of the symbology list.

If Custom is selected from the Enable Code ID pulldown list, only the custom IDs appear in the symbology list.

If None is selected from the Enable Code ID pulldown list, custom IDs are ignored.

Note: Custom symbologies appear at the end of the Symbology pulldown list, but are processed at the beginning of the list. This allows a custom ID based on a predefined Code ID to be processed before the predefined Code ID.

When the Code ID strip feature is enabled (please see “Step 1: Check Code ID and “Step 9: Add Code ID” later in this section), the entire custom ID string specified in the ID Code textbox earlier is treated as the Code ID and stripped.

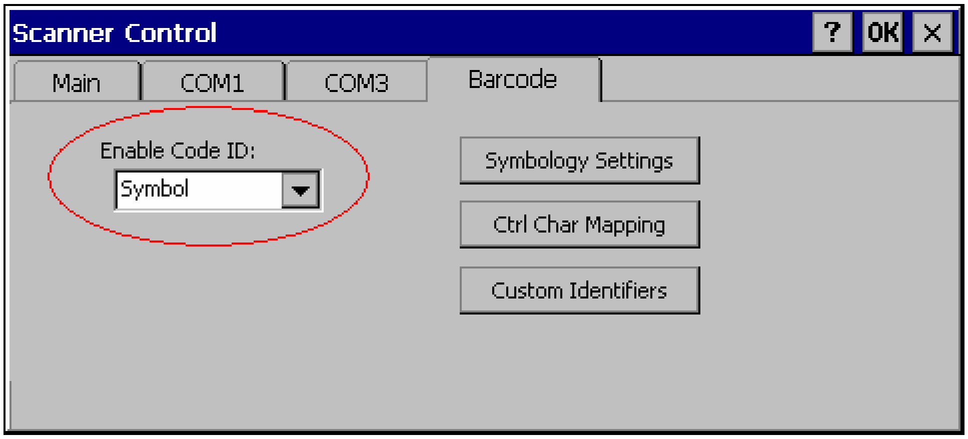
Barcode Processing

Barcode processing involves several steps. Some steps may be skipped during the processing depending on user selections on the various Scanner control panel screens. The steps are presented below in the order they performed on the barcode data.

Step 1: Check Code ID

Access: **Start | Settings | Control Panel | Scanner | Barcode**

The incoming scanned barcode data is checked for a Code ID. If the Code ID is present, it is stripped from the data and the settings for the specified symbology are used. To begin the process, select the appropriate Code ID from the pulldown list.



Enable Code ID: Symbol

Figure 4-9 Select Code ID

Note: *Since the VX7 does not contain an internal scanner, this feature requires that the external scanner be manually configured to include the Code ID as part of the incoming barcode data. Please refer to the scanner documentation to enable the Code ID.*

- **None:** Programs an internal scanner to disable transmission of a code ID (N/A on the VX7, see note above). After clicking the Symbology Settings button, the only entry on the Symbology listing is All, plus any configured custom IDs. Select this option to disable Code ID processing. The barcode data is received, but is not checked for a Code ID.
- **AIM:** Programs an internal scanner to transmit the AIM ID with each barcode (N/A on the VX7, see note above). After clicking the Symbology Settings button, the Symbology listing includes all AIM ID symbologies plus any configured custom Code IDs. Select this option to enable processing of barcodes with an AIM or custom Code ID.
- **Symbol:** Programs an internal scanner to transmit the Symbol ID with each barcode (N/A on the VX7, see note above). After clicking the Symbology Settings button, the Symbology listing includes all Symbol ID symbologies plus any configured custom Code IDs. Select this option to enable processing of barcodes with a Symbol or custom Code ID.
- **Custom:** Does not change the internal scanner’s code ID transmission (N/A on the VX7, see note above). After clicking the Symbology Settings button, the

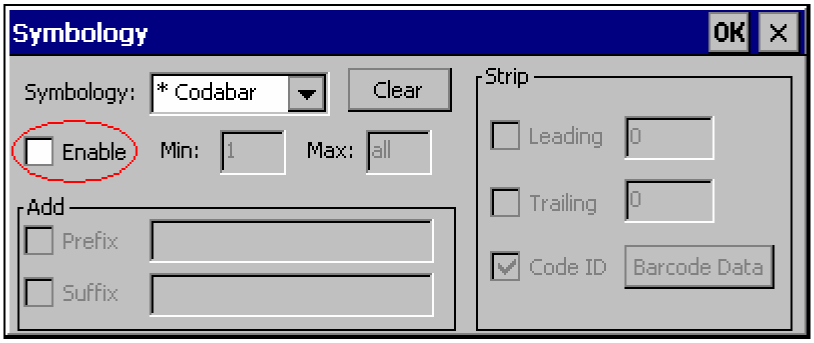
Symbology listing includes all Custom Code IDs. Select this option to enable processing of barcodes with a custom Code ID.

Note: **UPC/EAN Codes only**: *The Code ID for supplemental barcodes is not stripped.*

Step 2: Reject Disabled Symbologies

Access: Start | Settings | Control Panel | Scanner | Barcode | Symbology Settings

When a Code ID has been selected, individual symbologies for the Code ID may be disabled.



Symbology

Symbology: * Codabar

☐ Enable Min: 1 Max: all

Add

☐ Prefix

☐ Suffix

Strip

☐ Leading 0

☐ Trailing 0

☑ Code ID

Figure 4-10 Enable / Disable Symbologies

Note: Since the VX7 does not contain an internal scanner, this feature requires that the external scanner be manually configured to enable/disable symbologies as desired. This setting only affects the processing of barcode data, not the behavior of the external scanner. Please refer to the scanner documentation to enable the Code ID.

By default, all symbologies are enabled. To disable a particular symbology, select the symbology from the pulldown listing and uncheck the Enable box.

Note: The symbology is now shown with an asterisk (*) to indicate the default settings have been modified for this symbology.

When a symbology is disabled, any incoming scanned barcode data of that symbology is rejected. When a symbology is disabled, all other fields for that symbology are grayed out.

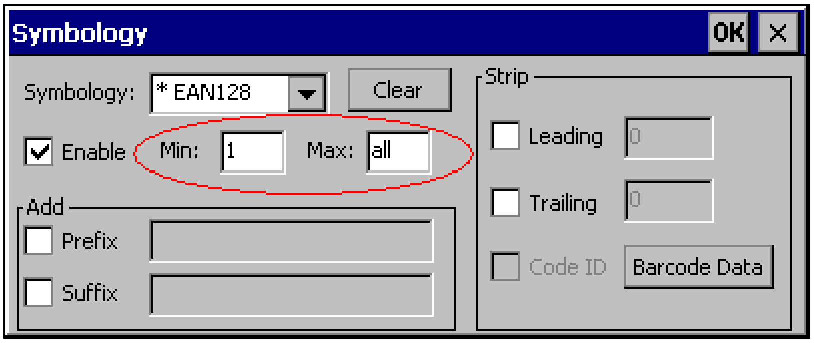
Note: Because external scanner operation cannot be controlled by the VX7's scanner driver, the scanner may still sound a "good scan" beep when scanning a disabled symbology. However, the VX7 sounds a "bad scan" beep to indicate the barcode has been rejected.

When None has been selected for Code ID, the Enable box cannot be unchecked (as this would disable the reading of all barcodes).

Step 3: Check Barcode Length

Access: Start | Settings | Control Panel | Scanner | Barcode | Symbology Settings

If the length of the barcode data (not counting the Code ID) is out of the specified minimum/maximum range, the scan is rejected.



Symbology: * EAN128

☑ Enable Min: 1 Max: all

□ Prefix

□ Suffix

□ Leading 0

□ Trailing 0

□ Code ID

Figure 4-11 Check Barcode Length

For the symbology selected from the pulldown list:

- The Min textbox specifies the minimum length the barcode data must be in order to be processed. The Code ID does not count when determining minimum length. Any barcode scanned that is less than the number of characters specified is rejected. The default value for this parameter is 1.
- The Max textbox specifies the maximum length the barcode data can be in order to be processed. The Code ID does not count when determining maximum length. Any barcode scanned that is more than the number of characters specified is rejected. The default value for this parameter is All (equivalent to 9999).

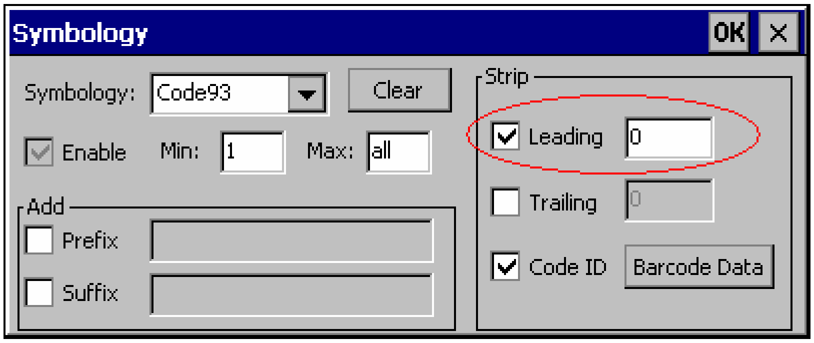
If 'All' is selected for Symbology, the Min and Max length requirements are applied to all symbologies not otherwise configured for the selected Code ID.

Note: If the value entered for Max is greater than the maximum length allowed for the specified symbology, the maximum valid length is used instead.

Step 4: Strip Leading Characters

Access: Start | Settings | Control Panel | Scanner | Barcode | Symbology Settings

Use this option to strip characters from the beginning of the barcode data.



Symbology: Code93

☑ Enable Min: 1 Max: all

Add

□ Prefix

□ Suffix

Strip

☑ Leading 0

□ Trailing 0

☑ Code ID

Figure 4-12 Strip Leading Characters

To enable, check the Leading checkbox and enter the desired number of characters to strip. The default is disabled (unchecked) and 0 characters.

The specified number of characters is stripped from the barcode data unconditionally for the Symbology selected from the pulldown list. If 'All' is selected, the character stripping is applied to all symbologies that have not been previously customized.

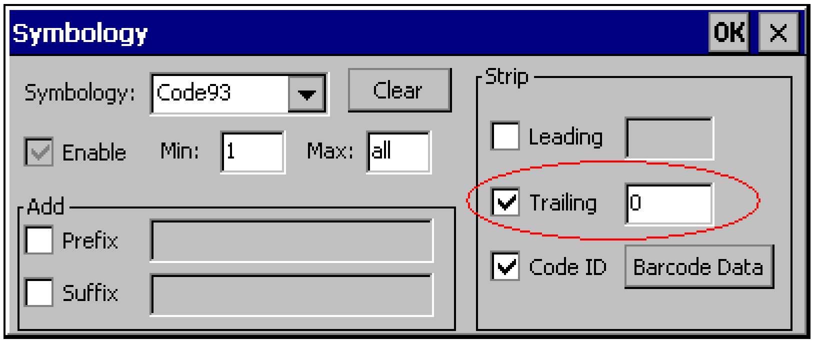
Code ID stripping (discussed earlier) is performed first. Next Leading and Trailing characters are stripped. Barcode data stripping (discussed later) is performed last.

Note: If the total number of characters being stripped is greater than the number of characters in the barcode data, the barcode data becomes a zero byte data string subject to any additional processing. If Strip Code ID is also enabled, and Prefix and Suffix are not programmed, this returns an empty scan which is rejected.

Step 5: Strip Trailing Characters

Access: Start | Settings | Control Panel | Scanner | Barcode | Symbology Settings

Use this option to strip characters from the end of the barcode data.



Symbology: Code93

☑ Enable Min: 1 Max: all

Add

□ Prefix

□ Suffix

Strip

□ Leading

☑ Trailing 0

☑ Code ID

Figure 4-13 Strip Trailing Characters

To enable, check the Trailing checkbox and enter the desired number of characters to strip. The default is disabled (unchecked) and 0 characters.

The specified number of characters is stripped from the barcode data unconditionally for the Symbology selected from the pulldown list. If ‘All’ is selected, the character stripping is applied to all symbologies that have not been previously customized.

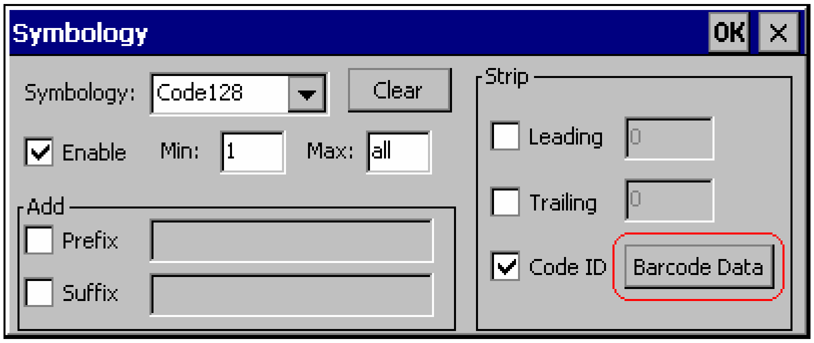
Code ID stripping (discussed earlier) is performed first. Next Leading and Trailing characters are stripped. Barcode data stripping (discussed later) is performed last.

Note: If the total number of characters being stripped is greater than the number of characters in the barcode data, the barcode data becomes a zero byte data string subject to any additional processing. If Strip Code ID is also enabled, and Prefix and Suffix are not programmed, this returns an empty scan which is rejected.

Step 6: Strip Barcode Data Strings

Access: Start | Settings | Control Panel | Scanner | Barcode | Symbology Settings

Use this option to strip specific data strings from the barcode data.



Symbology

Symbology: Code128

☑ Enable Min: 1 Max: all

Add

□ Prefix

□ Suffix

Strip

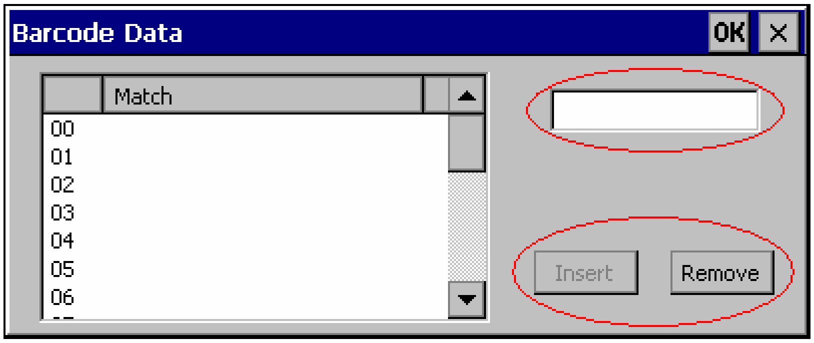
□ Leading 0

□ Trailing 0

☑ Code ID

Figure 4-14 Strip Barcode Data Strings

To specify the barcode strings to search for, click the Barcode Data button.



Barcode Data

	Match
00	
01	
02	
03	
04	
05	
06	

Figure 4-15 Define Barcode Data Strings

The specified string is stripped from the barcode for the Symbology selected from the pulldown list. If 'All' is selected, the data stripping is applied to all symbologies that have not been previously customized.

Use the text box to enter the desired search string. The rules are listed below:

- Strings are searched in the order they are listed. If the list contains ABC and AB in that order, incoming data is searched for ABC first, and then searched for AB.
- When a match between the first characters of the barcode and a string from the list is found, that string is stripped from the barcode data.
- Processing terminates when a match from the list is found. If no match is found, processing terminates when the end of the strip list is reached.
- If the wildcard * is not specified, the string is assumed to begin strip from the beginning of the data. The string ABC* strips off the prefix ABC. The string *XYZ strips off the suffix XYZ. The string ABC*XYZ strips both the ABC prefix and the XYZ suffix from the barcode data. Only one wildcard * is allowed per string. (The

user interface does not prevent multiple wildcards, but the result may not be as desired as only the first wildcard is processed).

- The wildcard ? may be used to match any single character in the incoming data. For example, AB?D would match ABcD, AB3D, but not ABDE). It is valid to use more than one wildcard ? in a string to match multiple characters.
- The barcode strip characters are saved per symbology.
- If the Code ID is enabled, but not stripped from the barcode data, the Code ID must be included in the data to match.
- Code ID stripping (discussed earlier) is performed first. Next Leading and Trailing characters (discussed earlier) are stripped. Barcode data stripping is performed last.

Several functions are available:

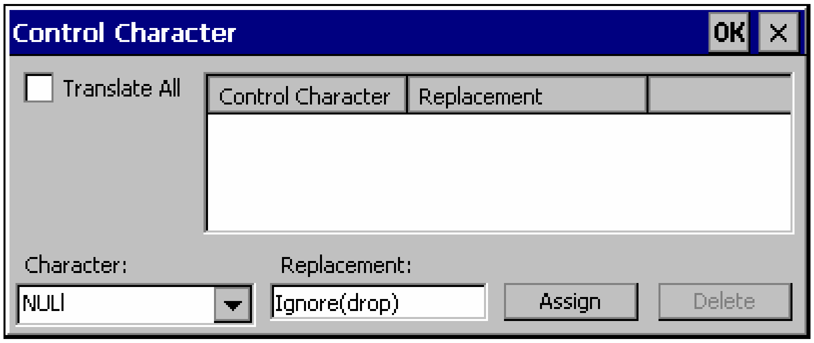
- To add data to the list: Type the data into the textbox. The leftmost button is enabled and labeled Add. Click the Add button to add this data to the next available entry.
- To insert data into a blank entry: Click on the desired entry. The leftmost button is enabled and labeled Insert. Type the data into the textbox. When the Insert button is clicked, the data is added into the selected list entry.
- To edit data in the list: Double click on the item to edit. The current value of that item is copied into the textbox for editing. The leftmost button is enabled and labeled Replace. When the Replace button is clicked, the value in the textbox updates the selected list item.
- To delete an item from the list: Click on the item to be deleted. The rightmost button is enabled and labeled Remove. Click the Remove button to remove the entry from the list. Deleting an entry does not move up items below in the list. A blank line (which is ignored during the processing) remains when an item is deleted.
- To erase all items from the list: When no items are selected in the list, the rightmost button is enabled and labeled Clear All. To clear all list items, click the Clear All button and confirm the delete.

When finished, click OK to save the barcode data strings.

Step 7: Replace Control Characters

Access: Start | Settings | Control Panel | Scanner | Barcode | Ctrl Char Mapping

Control characters may be replaced in the scanned barcode data.



□ Translate All

Character: NULl

Replacement: Ignore(drop)

Figure 4-16 Control Character Replacement

The specified control characters are replaced in the barcode data for the Symbology selected from the pulldown list. If 'All' is selected, the replacement is applied to all symbologies that have not been previously customized.

The Character pulldown list and the Replacement textbox are used to select the control character and its replacement value.

- Character is a drop down list that contains the control character name. Refer to the "ASCII Control Code" table later in this chapter for the list of control characters, their names and hex and hat-encoded values. When a character name is selected from the combo box, the text 'Ignore (drop)' is shown in the Replacement text box.
- Replacement is a text box where the user types the characters to be assigned as the replacement of the control character. Replacements for a control character are assigned by selecting the appropriate character from the Character combo box, typing the replacement in the Replacement text box and then selecting Assign. The assigned replacement is then added to the list box above the Assign button.

Replacement characters may be specified as follows:

- Ignore (drop) is the default. When selected, the specified control character is dropped from the barcode data. If the user defines a replacement for a control key, reselecting the character from Character combo box redisplays the 'Ignore (drop)' default in the Replacement edit control.
- A string of printable ASCII characters up to 19 characters in length.
- Hex encoded values may be specified (see "ASCII Control Codes" later in this chapter for a list).
- Hat-encoded control characters may be specified (see "ASCII Control Codes" later in this chapter for a list).

Available functions include:

- To add data to the list: Select an item from the Character pulldown list and enter a value in the Replacement text box. The leftmost button is labeled Assign and is active any time a control character is selected and a valid (non-blank) entry is made in the Replacement textbox. Clicking the Assign button adds the entry to the list.

- To delete an item from the list: Click on the item to be deleted. The rightmost button is enabled and labeled Remove. Click the Remove button to remove the entry from the list.

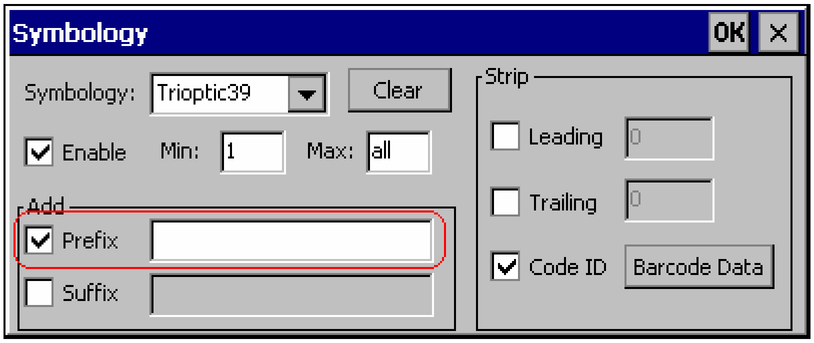
For examples, please see “Control Code Replacement Examples” later in this chapter.

Step 8: Add Prefix String

Access: Start | Settings | Control Panel | Scanner | Barcode | Symbology Settings

Use this option to specify a string to be added to the beginning of the barcode data. Up to 19 characters can be included in the string. The string can include any character from the keyboard plus characters specified by hex equivalent or entering in hat encoding. Please see the “Hat Encoding” section later in this chapter for a list of characters with their hex and hat-encoded values.

Using the Escape function allows entering of literal hex and hat values.



Symbology: Trioptic39

☑ Enable Min: 1 Max: all

Add

☑ Prefix

□ Suffix

Strip

□ Leading 0

□ Trailing 0

☑ Code ID

Figure 4-17 Specify Prefix

To enable a prefix, check the Prefix checkbox and enter the desired string in the textbox. The default is disabled (unchecked) and a blank text string.

When barcode data is processed, the Prefix string is sent to the output buffer before any other data.

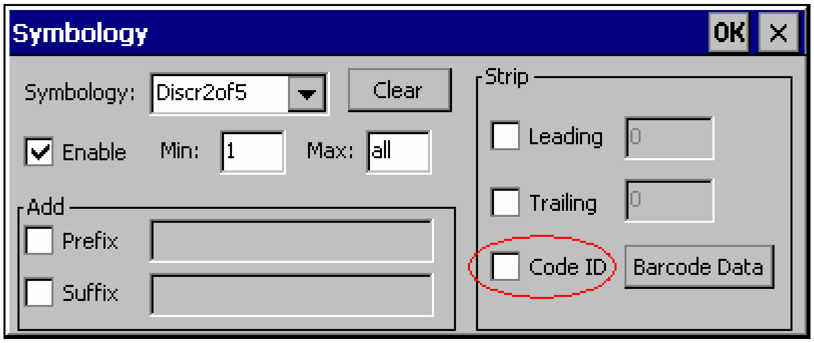
Because all stripping operations have already occurred, stripping settings do not affect the prefix.

The prefix is added to the output buffer for the Symbology selected from the pulldown list. If ‘All’ is selected, the prefix is added for all symbologies for the selected Code ID that have not been previously customized.

Step 9: Code ID

Access: Start | Settings | Control Panel | Scanner | Barcode | Symbology Settings

If the Code ID is not stripped, the Code ID is added to the output buffer after the Prefix string (if any).



Symbology: Discr2of5

☑ Enable Min: 1 Max: all

Add

□ Prefix

□ Suffix

Strip

□ Leading 0

□ Trailing 0

□ Code ID

Figure 4-18 Code ID Strip

The default is to enable Code ID stripping (the checkbox is enabled and the Code ID is not added to the output buffer).

The Code ID is stripped from the barcode data for the Symbology selected from the pulldown list. If ‘All’ is selected, the Code ID stripping is applied to all symbologies that have not been previously customized.

Step 10: Add Barcode Data

The processed barcode data is added to the output buffer. This is the scanned data minus any stripped characters and subject to any control character replacements. If the total number of characters stripped was greater than the number of characters in the barcode data, the barcode data becomes a zero byte data string subject to any additional processing. If Strip Code ID is also enabled, and Prefix and Suffix are not programmed, this returns an empty scan which is rejected.

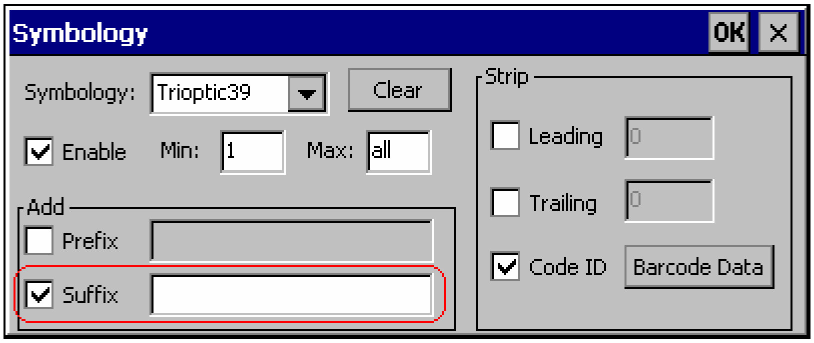
The barcode data follows the Prefix (if any) and the Code ID (if any) already placed in the output buffer.

Step 11: Add Suffix String

Access: Start | Settings | Control Panel | Scanner | Barcode | Symbology Settings

Use this option to specify a string to be added to the beginning of the barcode data. Up to 19 characters can be included in the string. The string can include any character from the keyboard plus characters specified by hex equivalent or entering in hat encoding. Please see the "Hat Encoding" section later in this chapter for a list of characters with their hex and hat-encoded values.

Using the Escape function allows entering of literal hex and hat values.



Symbology

Symbology: Trioptic39

☑ Enable Min: 1 Max: all

Add

□ Prefix

☑ Suffix

Strip

□ Leading 0

□ Trailing 0

☑ Code ID

Figure 4-19 Specify Suffix

To enable a suffix, check the Suffix checkbox and enter the desired string in the textbox. The default is disabled (unchecked) and a blank text string.

When barcode data is processed, the Suffix string is sent to the output buffer after the barcode data.

Because all stripping operations have already occurred, stripping settings do not affect the suffix.

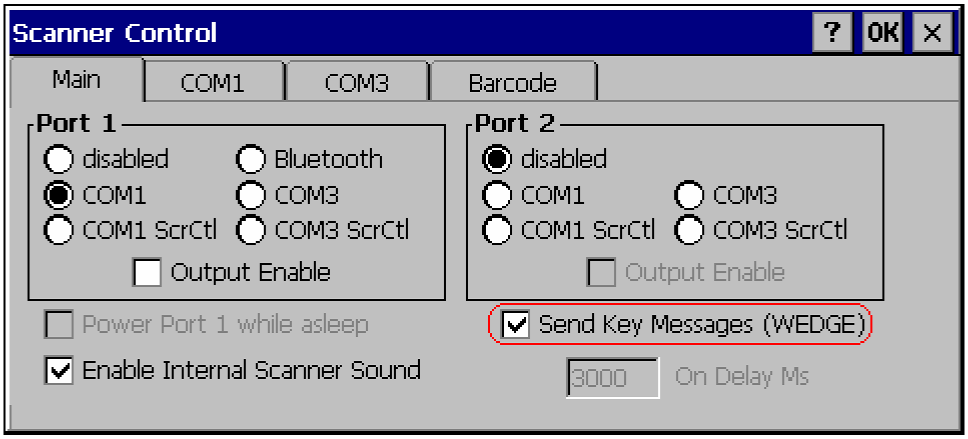
The suffix is added to the output buffer for the Symbology selected from the pulldown list. If 'All' is selected, the suffix is added for all symbologies for the selected Code ID unless otherwise configured.

Step 12: Add Terminating NUL

A terminating NUL is added to the output buffer after the Suffix (if any) in case the data is processed as a string.

Step 13: Start Key Output Thread

Access: **Start | Settings | Control Panel | Scanner | Main**



Scanner Control

Main | COM1 | COM3 | Barcode

Port 1
○ disabled ○ Bluetooth
● COM1 ○ COM3
○ COM1 ScrCtl ○ COM3 ScrCtl
□ Output Enable

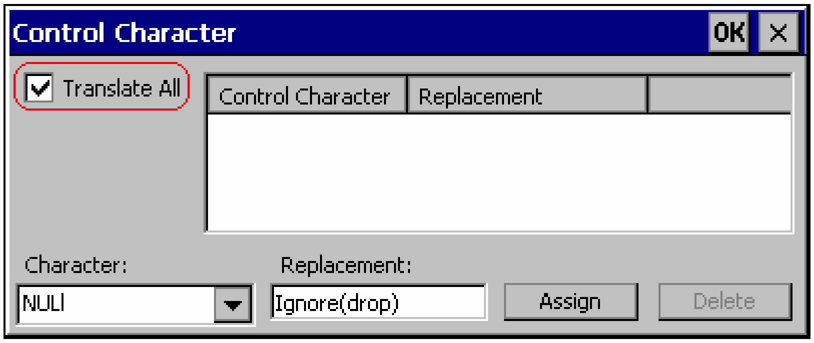
Port 2
● disabled
○ COM1 ○ COM3
○ COM1 ScrCtl ○ COM3 ScrCtl
□ Output Enable

□ Power Port 1 while asleep
☑ Send Key Messages (WEDGE)
☑ Enable Internal Scanner Sound
3000 On Delay Ms

Figure 4-20 Enable Key Messages

If key output is enabled, on the main tab, a thread is started to output the keys.

Access: **Start | Settings | Control Panel | Scanner | Barcode | Ctrl Char Mapping**



Control Character

☑ Translate All

Control Character	Replacement	

Character: NULl
Replacement: Ignore(drop)

Figure 4-21 Control Characters, Translate All

If “Translate All” is checked and “Send Key Messages” is checked, unprintable ASCII characters are assigned to their appropriate 2 keystroke CTRL code sequence (CTRL + letter) when the barcodes are sent in Key Message mode.

When “Translate All” is not checked and “Send Key Messages” is checked, any CTRL code which has a keyboard equivalent is passed as a keystroke (enter, tab, escape, backspace, etc.); any CTRL code which does not have a keyboard equivalent is dropped.

In Block mode (“Send Key Messages” is not checked) CTRL codes are always passed through as a single CTRL code value.

Examples

Control Code Replacement Examples

Configuration data	Translation	Example Control Character	Example configuration	Translated data
Ignore(drop)	The control character is discarded from the barcode data, prefix and suffix	ESCape	‘Ignore (drop)’	0x1B in the barcode is discarded.
Printable text	Text is substituted for Control Character.	Start of TeXt	‘STX’	0x02 in a barcode is converted to the text ‘STX’.
Hat-encoded text	The hat-encoded text is translated to the equivalent hex value.	Carriage Return	‘^M’	Value 0x0d in a barcode is converted to the value 0x0d.
Escaped hat-encoded text	The hat-encoding to pass thru to the application.	Horizontal Tab	‘\^I’	Value 0x09 in a barcode is converted to the text ‘^I’.
Hex-encoded text	The hex-encoded text is translated to the equivalent hex value.	Carriage Return	‘0x0A’	Value 0x0D in a barcode is converted to a value 0x0A.
Escaped hex-encoded text	The hex-encoding to pass thru to the application.	Vertical Tab	‘\0x0A’ or ‘0\x0A’	Value 0x0C is a barcode is converted to text ‘0x0A’

Barcode Processing Examples

The following table shows examples of stripping and prefix/suffix configurations. The examples assume that the scanner is configured to transmit an AIM identifier.

	Symbology				
	All	EAN-128 (]C1)	EAN-13 (]E0)	Intrlv 2 of 5 (]IO)	Code93
Enable	Enabled	Enabled	Enabled	Enabled	Disabled
Min length	1	4	1	1	
Max length	all	all	all	10	
Strip Code ID	Enabled	Enabled	Disabled	Enabled	
Strip Leading	3	0	3	3	
Strip Barcode Data		'*123'	'1*'	'456'	
Strip Trailing	0	0	3	3	
Prefix	'aaa'	'bbb'	'ccc'	'ddd'	
Suffix	'www'	'xxx'	'yyy'	'zzz'	

Provided that the wedge is configured with the above table, below are examples of scanned barcode data and results of these manipulations.

Barcode Symbology	Raw Scanner Data	Resulting Data
EAN-128	]C11234567890123	bbb1234567890xxx
EAN-128	]C111234567890123	bbb11234567890xxx
EAN-128	]C1123	< ***rejected*** > *(too short)*
EAN-13	]E01234567890987	ccc]E04567890yyy
EAN-13	]E01231234567890987	ccc]E0234567890yyy
EAN-13	]E01234	ccc]E0yyy
I2/5	]I04444567890987654321	< ***rejected*** > *(too long)*
I2/5	]I04444567890123	ddd7890zzz
I2/5	]I0444	dddzzz
I2/5	]I022245622	ddd45zzz
Code-93	]G0123456	< ***rejected*** > *(disabled)*
Code-93	]G0444444	< ***rejected*** > *(disabled)*
Code-39	]A01234567890	aaa4567890www
Code-39 full ASCII	]A41231234567890	aaa1234567890www
Code-39	]A4	< ***rejected*** > *(too short)*

Rejected barcodes generate a bad scan beep. In some cases, the receipt of data from the scanner triggers a good scan beep (from the external scanner), and then the rejection of scanned barcode data by the processing causes a bad scan beep on the same data.

Length Based Barcode Stripping Examples

Use this procedure to create symbology rules for two barcodes with the same symbology but with different lengths.

Note: The barcode length must be a discrete length, not a range of lengths.

Example 1:

- A normal AIM or Symbol symbology role can be created for the desired barcode ID.
- Next, a custom barcode symbology must be created using the same Code ID as the original AIM or Symbol ID rule and each rule would have unique length settings.

Example 2:

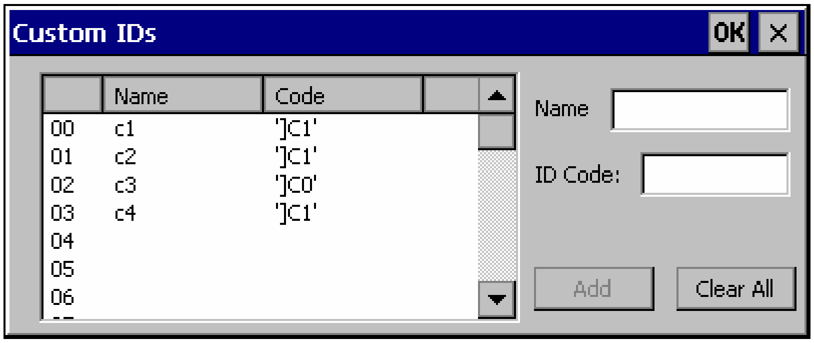
For the purposes of this example, the following sample barcode parameters will be used – EAN128 and Code128 barcodes. Some of the barcodes start with ‘00’ and some start with ‘01’. The barcodes are different lengths.

- 34 character length with first two characters = “01” (strip first 2 and last 18)
- 26 character length with first two characters = “01” (strip first 2 and last 10)
- 24 character length with first two characters = “01” (strip first 2 and last 8). This 24 character barcode is CODE128.
- 20 character length with first two characters = “00” (strip first 0 (no characters) and last 4)

On the Barcode tab, set Enable Code ID to AIM.

Create four custom IDs, using 1 for EAN128 barcode and 0 for Code128 barcode.

- c1 = Code = ‘]C1’
- c2 = Code = ‘]C1’
- c3 = Code = ‘]C0’ (24 character barcode is CODE128)
- c4 = Code = ‘]C1’



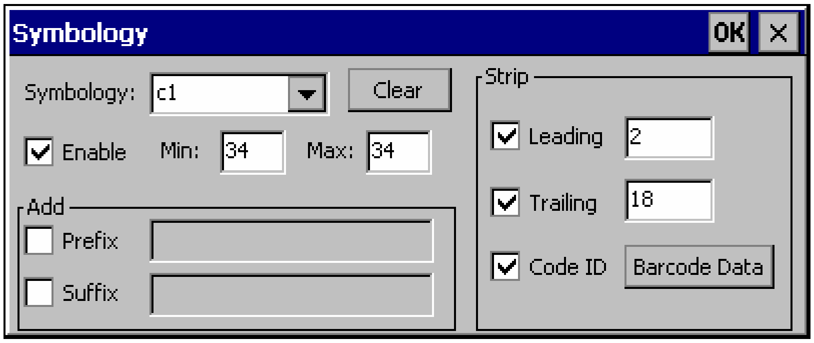
	Name	Code
00	c1	']C1'
01	c2	']C1'
02	c3	']C0'
03	c4	']C1'
04		
05		
06		

Figure 4-22 AIM Custom IDs

AIM custom symbology setup is assigned in the following manner:

- c1 min length = 34, max length = 34, strip leading 2, strip trailing 18, Code ID enabled, Barcode Data = "01"
- c2 min length = 26, max length = 26, strip leading 2, strip trailing 10, Code ID enabled, Barcode Data = "01"
- c3 min length = 24, max length = 24, strip leading 2, strip trailing 8, Code ID enabled, Barcode Data = "01"
- c4 min length = 20, max length = 20, strip leading 0, strip trailing 4, Code ID enabled, Barcode Data = "00"

Add the AIM custom symbologies. Refer to the previous section *Barcode – Symbology Settings* for instruction.



Symbology: c1

☑ Enable Min: 34 Max: 34

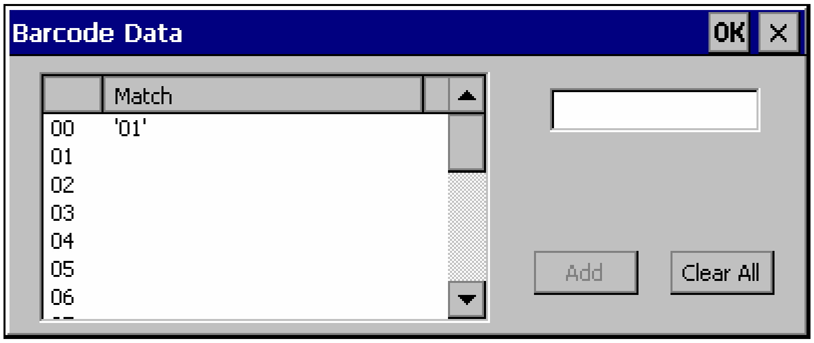
Add
□ Prefix
□ Suffix

Strip
☑ Leading 2
☑ Trailing 18
☑ Code ID

Figure 4-23 AIM Custom Setup for C1

Click the Barcode Data button. Click the Add button.

Add the data for the match codes.



	Match
00	'01'
01	
02	
03	
04	
05	
06	

Figure 4-24 Barcode Match Data for C1

Refer to the previous section *BarcodeData Match List* for instruction. Scan a barcode and examine the result.

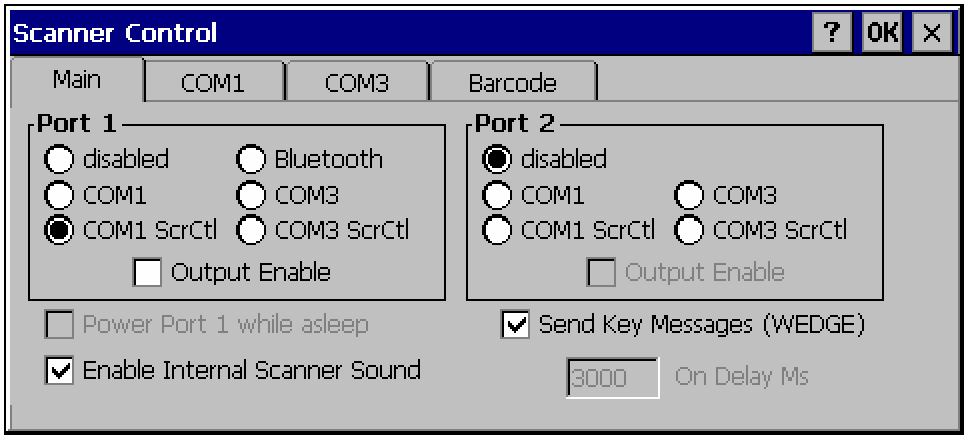
Screen Blanking

The VX7 can be configured to blank the display when the vehicle to which it is mounted is moving, eliminating a possible distraction for the driver. When configured properly, the screen blanking feature provides a tamper resistant method to blank the vehicle screen. The screen blanking feature consists of Scanner Control Panel Options and a customer supplied cable connected to one of the COM ports on the VX7. Properly configured, the display is visible only when the cable provides a signal that the vehicle has stopped.

The customer must supply their own cable. The cable specifications are detail in "Technical Specifications – Screen Blanking Cable" in Chapter 2, Physical Description and Layout".

The cable can be hooked to either the COM1 or COM3 port. The COM port used must be selected in the **Scanner** control panel.

Screen blanking is configured on the **Main** tab of the **Scanner** control panel.



Scanner Control

Port 1
○ disabled ○ Bluetooth
○ COM1 ○ COM3
● COM1 ScrCtl ○ COM3 ScrCtl
□ Output Enable

Port 2
● disabled
○ COM1 ○ COM3
○ COM1 ScrCtl ○ COM3 ScrCtl
□ Output Enable

□ Power Port 1 while asleep
☑ Send Key Messages (WEDGE)
☑ Enable Internal Scanner Sound
3000 On Delay Ms

Figure 4-25 Enable Screen Blanking

S	If the COM1/COM3 screen blanking and On Delay choices are not shown, the system load must be updated.
Warning ⚠	Do not select **COM1 ScrCtl** or **COM3 ScrCtl** unless you have already attached the cable described in "Technical Specifications – Screen Blanking Cable" in Chapter 2, Physical Description and Layout". Failure to attach the cable before selecting a screen blanking option will cause the screen to go blank (and remain blank) until an appropriate cable is attached to the specified COM port.

Set the desired COM port (COM1 ScrCtl or COM3 ScrCtl) and On Delay. Press **OK**. The On Delay can be used to specify the time (in milliseconds) before the display turns on. For example, use the On Delay if the switch end of the cable is attached to the vehicle's accelerator pedal. Release of the accelerator may mean the truck is coasting to a stop rather than stationary. Configure the delay to allow time for the vehicle to coast to a stop.

To disable screen blanking, select COM1 or COM3 to return the selected COM port to normal operation.

Operation

To prevent a general user from disabling the screen blanking feature, at least one of the two following actions must be taken:

- Password protection can be set via the Password icon in the Windows Control Panel. Without this password, general users are unable to access the Control Panel to disable the screen blanking feature. For more information on the Password feature, please refer "Password", earlier in this chapter.
- AppLock can be used to restrict the general user's access to only a certain program. Since the user under AppLock cannot access the Control Panel, the user cannot disable the screen blanking feature. For more information on AppLock, please refer to Chapter 6, "AppLock".

Operation of the VX7 is unchanged except for the blank display. The keypad and touchscreen are still enabled, however any input from they keypad, touchscreen or other device **DOES NOT** wake up the display.

Chapter 5 Wireless Network Configuration

Introduction

The VX7 computer may have a Summit, Cisco or Symbol radio. The Summit radio is an 802.11g radio. The Cisco and Symbol radios are 802.11b radios. The radio can be configured for no encryption, WEP encryption or WPA security (N/A with Symbol radio).

Note: *Cisco and Symbol are only supported on devices with a Windows CE .NET operating system. Summit is supported for Windows CE .NET and CE 5.0 operating systems.*

Certificates are necessary for many of the WPA authentications. Please refer to the "Certificates" section at the end of this chapter for more information on generating and installing certificates.

Please refer to the table below for the security options supported for each radio type.

Security Options Supported	**Radio Type**		
	Summit	**Cisco**	**Symbol**
None	Yes	Yes	Yes
WEP	Yes	Yes	Yes
LEAP	Yes	Yes	Yes
WPA-PSK	Yes	Yes	No
WPA/LEAP	Yes	Yes	No
PEAP-MSCHAP	Yes	Yes	No
PEAP-GTC	Yes	Yes	No
EAP-TLS	No	Yes	No
EAP-FAST	Yes	No	No

Summit Radio

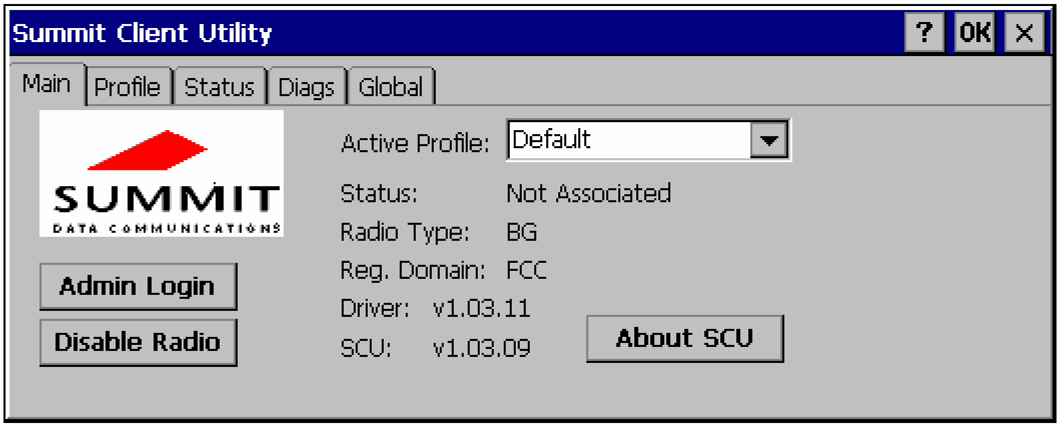
S	The Summit radio requires software revision 2BT or greater. All VX7's with a Summit radio ship with this software revision or greater. To identify the software revision, please click on the "About" icon in the Windows CE Control Panel.
📖	Please refer to the "LXE Security Primer" to prepare the Authentication Server and Access Point for VX7 communication.
Date/Time	It is important that all dates are correct on CE computers when using any type of certificate. Certificates are date sensitive and if the date is not correct authentication will fail.
⚠	It may be necessary to upgrade radio drivers to in order to use certain Summit Client Utility (SCU) features described in this chapter. Please contact your LXE representative for details.

The Summit radio is an 802.11g radio, capable of both 802.11b and 802.11g data rates. This radio supports no encryption, WEP, LEAP or WPA (PEAP-MSCHAP, PEAP-GTC, WPA/LEAP, EAP-FAST and WPA-PSK).

Summit Client Utility

Note: When making changes to profile or global parameters, the VX7 should be warmbooted afterwards.

Access: Start | Programs | Summit | SCU *or* SCU Icon on Desktop



Active Profile: Default

Status: Not Associated

Radio Type: BG

Reg. Domain: FCC

Driver: v1.03.11

SCU: v1.03.09

Figure 5-1 Summit Client Utility

The **Main** tab provides information, admin login and active profile selection.

Profile specific parameters are found on the **Profile** tab. The parameters on this tab can be set to unique values for each profile. This tab was labeled **Config** in early versions of the SCU.

The **Status** tab contains information on the current connection.

The **Diags** tab provides utilities to troubleshoot the radio.

Global parameters are found on the **Global** tab. The values for these parameters apply to all profiles. This tab was labeled **Global Settings** in early versions of the SCU.

Help

Help is available by clicking the **?** icon in the title bar on most SCU screens.

The SCU help may also be accessed by selecting **Start | Help** and tapping the **Summit Client Utility** link. The SCU *does not* have to be accessed to view the help information using this option.

Summit Tray Icon

The Summit tray icon 📶 provides access to the SCU and a visual indicator of radio status.

The Summit tray icon is displayed when:

- The Summit radio is installed and active
- The Windows Zero Config utility is not active
- The Tray Icon setting is On

Click the icon to launch the SCU.

Use the tray icon to view the radio status:

✖ The radio is not currently associated or authenticated to an Access Point

📶 The signal strength for the currently associated/authenticated Access Point is -80 dBm or weaker

📶 The signal strength for the currently associated/authenticated Access Point is stronger than -80dBm but not stronger than -60 dBm

📶 The signal strength for the currently associated/authenticated Access Point is stronger than -60 dBm but not stronger than -40 dBm

📶 The signal strength for the currently associated/authenticated Access Point is stronger than -40 dBm

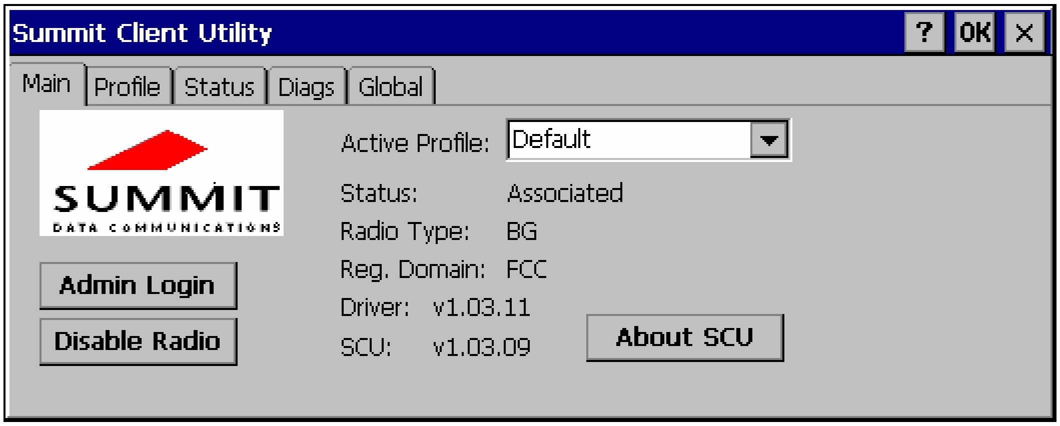
Wireless Zero Config Utility and the Summit Radio

- The WZC utility has an icon in the toolbar that looks like networked computers with a red X through them, indicating that Wireless Zero Config application is enabled but the connection is inactive at this time (the VX7 is not connected to a network).
- You can use either the Wireless Zero Configuration Utility or the Summit Client Utility to connect to your network. LXE recommends using the Summit Client Utility to connect to your network. The Wireless Zero Configuration Utility cannot control the complete set of security features of the radio.

Select **ThirdPartyConfig** in the Active Profile drop down list as the active profile. Warmboot the VX7. The Summit Client Utility passes control to Wireless Zero Config and the WZC Wireless Information control panel. Using the options in the Wireless Zero Config panels, setup radio and security settings.

To switch back to Summit Client radio control, select any other profile in the SCU Active Config drop down list, except ThirdPartyConfig. Warmboot the VX7. Radio control is passed to the SCU.

Main Tab



Active Profile: Default

Status: Associated

Radio Type: BG

Reg. Domain: FCC

Driver: v1.03.11

SCU: v1.03.09

Figure 5-2 SCU – Main Tab

The Main tab displays information about the radio including:

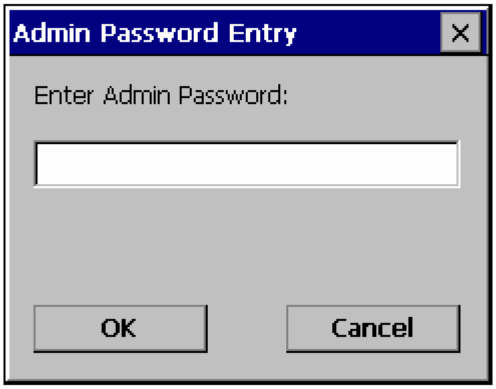
- SCU (Summit Client Utility) version
- Driver version
- Radio Type (the radio is an 802.11b/g radio)
- Regulatory Domain
- Copyright Info may be accessed by clicking the About SCU button
- Active Profile – Select from the profiles created using the Config tab.
- Status of the radio (Down, Associated, Authenticated, etc).

The **Disable Radio** button can be used to disable the radio card. Once disabled, the button label changes to **Enable Radio**. By default, the radio is enabled.

The **Admin Login** button provides access to editing radio parameters as well as adding, renaming and deleting profiles. Profile and Global parameters may only be edited after entering the Admin Login password. The Active Config may be changed without logging in. Once logged in, the button label changes to **Admin Logout**. The admin is also automatically logged out when the SCU is exited.

Admin Login

To login to Admin mode, click the Admin login button.



Admin Password Entry

Enter Admin Password:

Figure 5-3 Admin Password Entry

Enter the Admin password and press **OK**. If the password is incorrect, an error message is displayed. The default password is SUMMIT.

Note: The password is case sensitive!

The Admin password can be changed on the Global tab.

The end user can:

- Turn radio On/Off on the Main tab
- Select active Profile on the Main tab
- View the current parameter settings for the profiles on the Profile tab
- View the global parameter settings on the Global tab.
- View the current connection details on the Status tab
- View the radio status, software versions and regulatory domain on the Main tab
- Access additional troubleshooting features on the Diags tab.

After Admin login, the use can also:

- Create, edit, rename and delete profiles on the Profile tab
- Edit global parameters on the Global tab.

Profile Tab

Notes: If the Admin password is not entered, the user can view the Profile parameter settings but cannot make any changes. The buttons on this tab are grayed out if the user is not logged in.

The Profile tab was previously labeled Config.

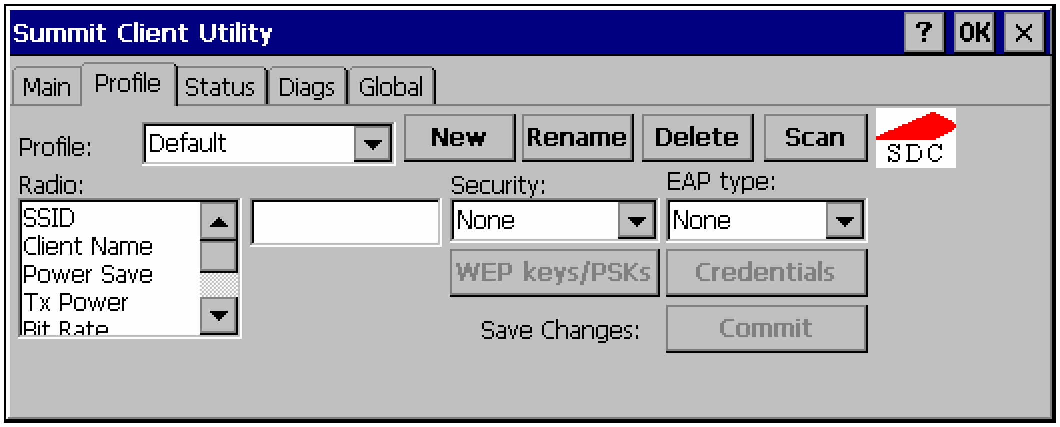


Figure 5-4 SCU – Profile Tab

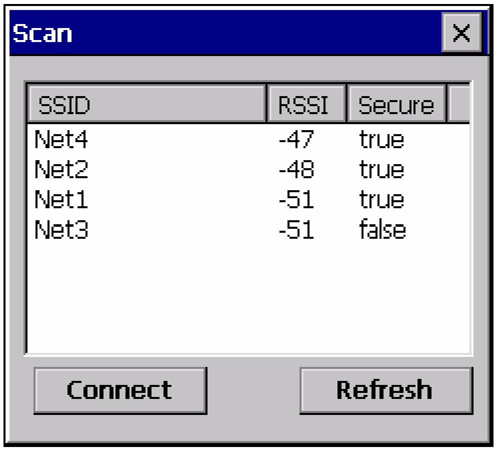
When logged in as an Admin (see the Main tab), use the Profile tab to manage profiles:

- **Rename** – Gives the profile a new, unique name. If the new name is not unique, an error message is displayed and the profile is not renamed.
- **Delete** – Deletes the profile. The current active profile cannot be deleted. In that case, an error message is displayed and the profile is not deleted.
- **New** – Creates a new profile with the default settings (see the list below) and prompts for a name. The name must be unique. If not, an error message is displayed and the profile is not created.
- **Scan** – Scans for and displays a list of available APs. Can be used to create a profile from the APs listed.
- **Commit** – Ensures that the profile settings made on this screen are saved in the profile.

When not logged in, the parameters can be viewed, but cannot be changed.

Using the Scan Feature

Clicking the **Scan** button opens a pop up window displaying any APs found during the scan.



SSID	RSSI	Secure
Net4	-47	true
Net2	-48	true
Net1	-51	true
Net3	-51	false

Figure 5-5 Scan

The scan displays information on the available APs:

- **SSID** – Lists the SSID of the network
- **RSSI** – Displays the Received Signal Strength Indication (RSSI) of the AP.
- **Secure** – Displays True if the data encryption is used by the AP, false is data encryption is not used.

Notes: The APs can be sorted by clicking on any of the column headings.

If there is more than one AP with the same SSID, the listing displays the AP with the strongest signal and least security.

If you are logged in as an administrator, you can use the **Connect** button to create a new profile. The button is grayed out is an administrator is not logged in.

- Highlight the desired network in the listing and click the **Connect** button.
- The new profile is named based on the SSID of the selected AP. If a profile already exists with that name, the new profile name contains an incremental number to avoid duplicate names.
- The SSID parameter is assigned the value of the SSID of the AP. Other profile entries must be completed manually.

Click the **Refresh** button to update the display.

Parameters

IMPORTANT *– Remember to click the* ***Commit*** *button after making changes to ensure the changes are saved. Newer versions of the SCU display a reminder if the Commit button is not clicked before an attempt it made to close or browse away from the Config tab if there are unsaved changes.*

Config

A string of 1 to 32 alphanumeric characters, name of the Profile

Default: Default

SSID

A string of up to 32 alphanumeric characters, the Service Set Identifier (SSID) of the WLAN to which the radio connects

Default: Blank

Client Name

A string of up to 16 characters – Name assigned to the radio and the device using the radio. The client name may be passed to networking radio devices, e.g. Access Points.

Default: Blank

Power Save

Power save mode.

Options: CAM = Constantly Awake Mode, power save off
Maximum = Maximum power saving mode
Fast = Fast power saving mode

Default: Fast

Tx Power

Desired transmit power.

Options: Maximum = Max power for current regulatory domain
50, 30, 10 or 1 mW

Default: Maximum

Bit Rate

Options: Auto = Rate negotiated automatically with the AP
1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48 or 54 Mbit

Default: Auto

Radio Mode

Specify 802.11g and/or 802.11b when communicating with AP.

Options: B rates only
BG Rates Full
G rates only
BG optimized

Default: BG optimized

Note: Some versions may have the default set as BG Rates Full.

Auth Type

802.11 authentication type used when associating with AP

Options: Open
Shared key
LEAP

Default: Open

Note: Set the Auth Type radio parameter is set to "Open" for all configurations unless using LEAP (not WPA) and the AP is configured for network EAP only. In this case, set the Auth Type radio parameter to "LEAP".

EAP Type

Extensible Authentication Protocol (EAP) type used for 802.1x authentication to AP

Options: None
LEAP
EAP-FAST
PEAP-MSCHAP
PEAP-GTC
EAP-TLS

Default: None

Note: The EAP type chosen determines if the ***Credentials*** *button is active. Available entries on the Credentials pop up window vary by EAP type chosen.*

Security

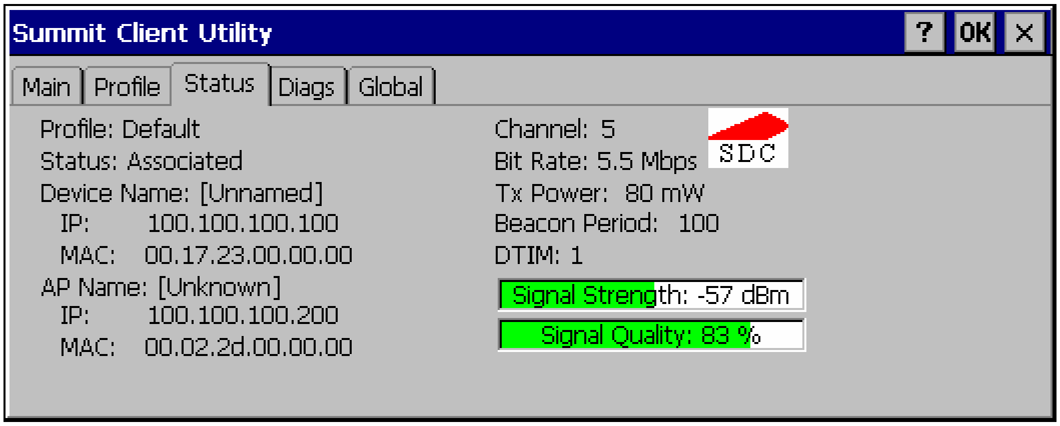
Type of encryption used to protect transmitted data. This parameter was labeled as Encryption in some versions of the SCU.

Options:	None Manual WEP Auto WEP WPA PSK WPA TKIP WPA2 PSK WPA2 AES CCKM TKIP CKIP Manual CKIP Auto
Default:	None

Note: The Encryption type chosen determines if the ***WEP/PSK Keys*** *button is active. Available entries on the pop up window vary by encryption type chosen.*

IMPORTANT – The settings for Auth Type, EAP Type and Encryption depend on the security type chosen. Please refer to "Summit Wireless Security", later in this chapter, to determine the proper settings for the security type implemented on the wireless LAN.

Status Tab



Profile: Default
Status: Associated
Device Name: [Unnamed]
IP: 100.100.100.100
MAC: 00.17.23.00.00.00
AP Name: [Unknown]
IP: 100.100.100.200
MAC: 00.02.2d.00.00.00

Channel: 5
Bit Rate: 5.5 Mbps
Tx Power: 80 mW
Beacon Period: 100
DTIM: 1
Signal Strength: -57 dBm
Signal Quality: 83 %

Figure 5-6 SCU – Status Tab

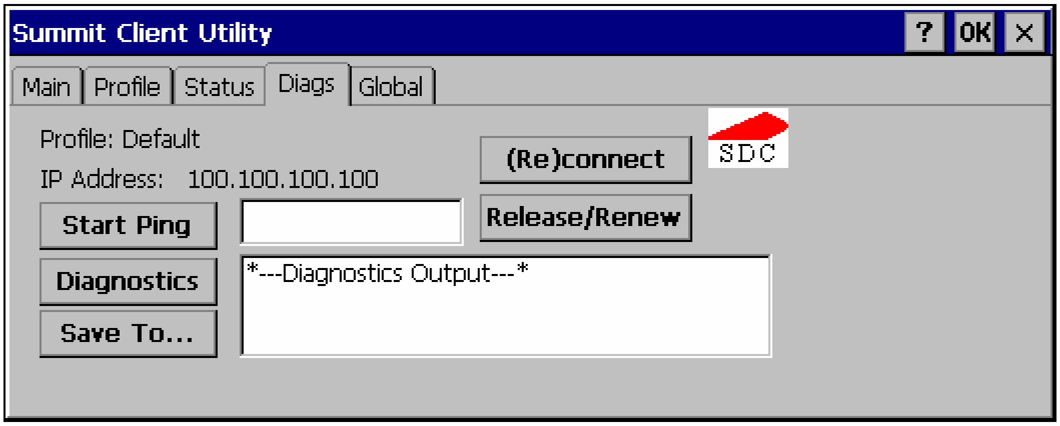
This screen provides information on the radio:

- The profile being used
- The status of the radio card (down, associated, authenticated, etc.)
- Client information including device name, IP address and MAC address.
- Information about the Access Point (AP) maintaining the connection to the network including AP name, IP address and MAC address.
- Channel currently being used for wireless traffic
- Bit rate in Mbit.
- Current transmit power in mW
- Beacon period – the time between AP beacons in kilomircoseconds. (one kilomicrosecond = 1,024 microseconds)
- DTIM interval – A multiple of the beacon period that specifies how often the beacon contains a delivery traffic indication message (DTIM). The DTIM tells power saving devices a packet is waiting for them. For example, if DTIM = 3, then every third beacon contains a DTIM.
- Signal strength (RSSI) displayed in dBm and graphically
- Signal quality, a measure of the clarity of the signal displayed in percentage and graphically.

There are no user entries on this screen.

Note: After completing radio configuration, it is a good idea to review this screen to verify the radio has associated (no encryption, WEP) or authenticated (LEAP, any WPA), as indicated above.

Diags Tab



Profile: Default

IP Address: 100.100.100.100

---Diagnostics Output---

Figure 5-7 SCU – Diags Tab

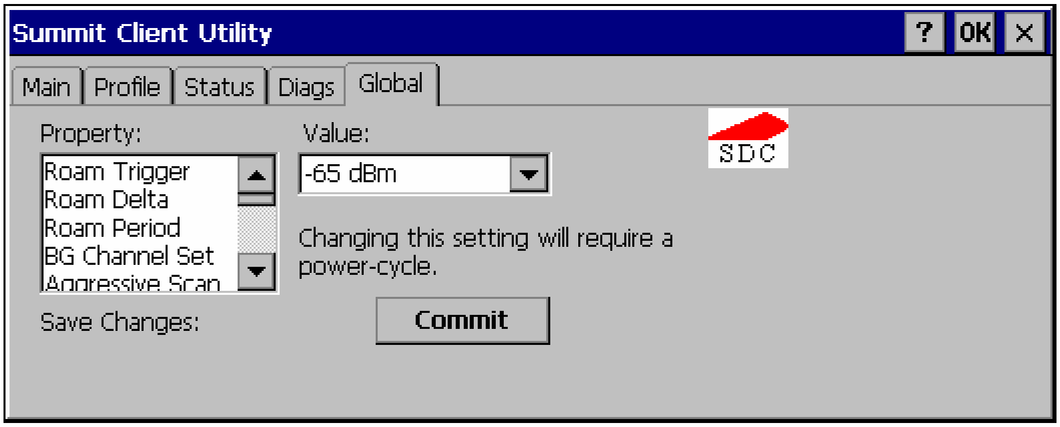
The Diags screen can be used for troubleshooting network traffic and radio connectivity issues.

- **(Re)connect** – Use this button to apply (or reapply) the current profile and attempt to associate or authenticate to the wireless LAN. All activity is logged in the Diagnostic Output box on the lower part of the screen.
- **Release/Renew** – Obtain a new IP address through release and renew. All activity is logged in the Diagnostic Output box. If a fixed IP address has been assigned to the radio, this is also noted in the Diagnostic Output box. Note that the current IP address is displayed above this button.
- **Start Ping** – Start a continuous ping to the IP address specified in the text box to the right of this button. Once the button is clicked, the ping begins and the button label changes to **Stop Ping**. Clicking the button ends the ping. The ping also ends when any other button on this screen is clicked or the user browses away from the Diags tab. The results of the ping are displayed in the Diagnostic Output box.
- **Diagnostics** – Also attempts to (re)connect to the wireless LAN. However, this option provides more data in the Diagnostic Output box than the (Re)connect option. This data dump includes radio state, profile settings, global settings, and a list of broadcast SSID APs.
- **Save To…** – Use this save the results of the diagnostics to a text file. Use the explorer window to specify the name and location for the diagnostic file. The text file can viewed using an application such as WordPad.

Global Tab

Note: The Global tab was previously labeled Global Settings.

The parameters on the global settings tab can be changed when an Admin is logged on. Without the admin login, the current values for the parameters can be viewed, but they cannot be edited.



Property:
Roam Trigger
Roam Delta
Roam Period
BG Channel Set
Aggressive Scan

Value: -65 dBm

Changing this setting will require a power-cycle.

Save Changes:

Figure 5-8 SCU – Global Tab

Parameters

IMPORTANT *– Remember to click the* ***Commit*** *button after making changes to ensure the changes are saved. Many versions of the SCU display a reminder if the Commit button is not clicked before an attempt it made to close or browse away from the Global tab if there are unsaved changes.*

Note: ***Custom*** *parameter options: Some parameters contain an option for custom. The parameter's value is displayed as "Custom" when the operating system registry has been used to set the parameter to a value not available from the Global settings parameter options. Selecting Custom for a parameter has no effect as the parameter value returns to the previously selected value when you press Commit.*

Roam Trigger

If signal strength is less than this trigger value, the radio looks for a different AP with a stronger signal.

Options:	-50, -55, -60, -65, -70, -75 dBm, Custom (see Note above)
Default:	-65 dBm

Roam Delta

Amount by which the new AP’s signal strength must exceed the current AP’s signal strength before roaming is attempted.

Options: 5, 10, 15, 20, 25, 30, 35 dBm,
Custom (see Note above)

Default: 10 dBm

Roam Period

The amount of time, after association or a roam scan with no roam, that the radio collects Received Signal Strength Indication (RSSI) scan data before a roaming decision is made.

Options: 5, 10, 15, 20, 25, 30, 35, 40, 45, 50, 55, 60 sec,
Custom (see Note above)

Default: 10 seconds

BG Channel Set

Defines the 2.4GHz channels to be scanned for an AP when the radio is contemplating roaming. By specifying the channels to search roaming time may be reduced over scanning all channels.

Options: Full (all channels)
1, 6, 11 (the most commonly used channels)
1, 7, 13 (For ETSI and TELEC radios only)
Custom (see Note above)

Default: Full

Aggressive Scan

When set to On and the current connection to an AP becomes weak, the radio scans for available APs more aggressively. Aggressive scanning work with standard scanning (set through Roam Trigger, Roam Delta and Roam Period). Aggressive scanning should b set to On unless there is significant co-channel interference because of overlapping APs on the same channel.

Options: On, Off

Default: On

CCX Features

Use of Cisco Compatible Extensions (CCX) radio management and AP specified maximum transmit power features.

Options: On, Off

Default: Off

WMM

Use of Wi-Fi Multimedia extensions.

Options: On, Off

Default: Off

TX Diversity

How to handle antenna diversity when transmitting packets to AP.

Options:	Main only = Main antenna only Aux only = Aux antenna only On = Use diversity
Default:	On

⚠	For a VX7 with a single external antenna use **Main Only**. For a VX7 with dual external antennas or an internal antenna use **On**.

RX Diversity

How to handle antennas diversity when receiving packets from AP.

Options:	Main Only = use main antenna only Aux Only = use aux. antenna only On-start on Main = On startup use main antenna On-start on Aux = On startup use aux antenna
Default:	On-start on Main

⚠	For a VX7 with a single external antenna use **Main Only**. For a VX7 with dual external antennas or an internal antenna use **On-start on main**.

Frag Thresh

If the packet size (in bytes) exceeds the specified number of bytes set in the fragment threshold, the packet is fragmented (sent as several pieces instead of as one block). Use a low setting in areas where communication is poor or where there is a great deal of radio interference.

Options:	256 to 2346
Default:	2346

RTS Thresh

If the packet size exceeds the specified number of bytes set in the Request to Send (RTS) threshold, an RTS is sent before sending the packet. A low RTS threshold setting can be useful in areas where many client devices are associating with the Access Point.

Options:	0 to 2347
Default:	2347

LED

The LED on the radio card is not visible to the user when the radio card is installed in a sealed mobile device.

Options:	On, Off
Default:	Off

Tray Icon

Determines if the Summit icon is displayed in the system tray.

Options:	On, Off
Default:	On

Hide Password

If On, the Summit Client Utility masks passwords as they are typed and when they are viewed.

Options:	On, Off
Default:	Off

Admin Password

A string of up to 64 alphanumeric characters that must be entered when the Admin Login button is tapped. If Hide Password is On, the password is masked when typed in the Admin Password Entry text box. The password is Case Sensitive.

Default: SUMMIT

Note: Password is case sensitive.

Auth Timeout

Specifies the number of seconds the Summit software waits for an EAP authentication request to succeed or fail.

If the authentication credentials are stored in the active profile and the authentication times out, the association fails. No error message or prompting for corrected credentials is displayed.

If the authentication credentials are not stored in the active profile and the authentication times out, the user is again prompted to enter the credentials.

Options:	An integer from 3 to 60
Default:	8

Certs Path

A valid directory path, of up to 64 characters, where Root CA certificates for EAP authentication (PEAP/MSCHAP, PEAP/GTC, EAP-TLS) and manual PACs for EAP-TLS are stored.

The Windows certificate store can also be used to store Root CA certificates. User certificates (EAP-TLS) must be stored in the Windows certificate store.

LXE suggests ensuring the directory path currently exists before assigning the path in this parameter. For example, if the certificate is stored in My Computer/System/mycertificate.cer, enter **System** in the Certs Path text box as the directory path.

Default: System

Ping Payload

Maximum amount of data to be transmitted on a ping.

Options:	32, 64, 128, 256, 512, 1024 bytes
Default:	32

Ping Timeout ms

The amount of time, in milliseconds, that a device will be continuously pinged. The Stop Ping button can be tapped to end the ping process ahead of the ping timeout.

Options:	0 to 30,000 ms
Default:	5000

Ping Delay ms

The amount of time, specified in milliseconds, between each ping.

Options:	0 to 30,000 ms
Default:	1000

Sign-On vs. Stored Credentials

When using wireless security that requires a user name and password to be entered, the Summit Client Utility offers two choices:

- The Username and Password may be entered on the Credentials screen. If this method is selected, anyone using the device can access the network.
- The Username and Password are left blank on the Credentials screen. When the device attempts to connect to the network, a sign on screen is displayed. The user must enter the Username and Password at that time to authenticate.

How to: Use Stored Credentials

8. After completing the other entries in the profile, click on the **Credentials** button.
9. Enter the **Username** and **Password** on the Credentials screen and click the **OK** button.
10. Click the **Commit** button.
11. For LEAP and WPA/LEAP, configuration is complete.
12. For PEAP-MSCHAP, PEAP-GTC and EAP-TLS import the CA certificate into the Windows certificate store.
13. For EAP-TLS, also import the User Certificate into the Windows certificate store.
14. Access the Credentials screen again. Make sure the **Validate server** and **Use MS store** checkboxes are checked.
15. The default is to use the entire certificate store for the CA certificate. Alternatively, use the **Browse** button next to the **CA Cert** (CA Certificate Filename) on the Credentials screen to select an individual certificate.
16. For EAP-TLS, also enter the **User Cert** (User Certificate filename) on the credentials screen by using the **Browse** button.
17. Click the **OK** button then the **Commit** button.
18. Verify the device is authenticated by reviewing the Status tab. When the device is property configured, the Status tab indicates the device is Authenticated and the method used.

Notes: More details are provided in the appropriate Summit Wireless Security section following in this chapter.

If invalid credentials are entered into the stored credentials, the authentication will fail. No error message is displayed and the user is not prompted to enter valid credentials.

How to: Use Sign On Screen

1. After completing the other entries in the profile, click on the **Credentials** button. Leave the Username and Password blank. No entries are necessary on the Credentials screen for LEAP or WPA/LEAP.
2. For PEAP-MSCHAP, PEAP-GTC and EAP-TLS import the CA certificate into the Windows certificate store.
3. For EAP-TLS, also import the User Certificate into the Windows certificate store.
4. Access the Credentials screen again. Make sure the **Validate server** and **Use MS store** checkboxes are checked.
5. The default is to use the entire certificate store for the CA certificate. Alternatively, use the **Browse** button next to the **CA Cert** (CA Certificate Filename) on the Credentials screen to select an individual certificate.
6. For EAP-TLS, also enter the **User Cert** (User Certificate filename) on the credentials screen by using the **Browse** button.
7. Click the **OK** button then the **Commit** button.
8. When the device attempts to connect to the network, a sign-on screen is displayed.
9. Enter the **Username** and **Password**. Click the **OK** button.

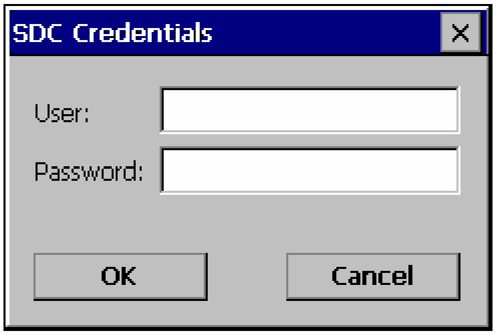


Figure 5-9 Sign-On Screen

10. Verify the device is authenticated by reviewing the **Status** tab. When the device is property configured, the Status tab indicates the device is Authenticated and the method used.
11. The sign-on screen is displayed after a reboot for each of the listed protocols.

Note: *Complete details are provided in the appropriate Summit Wireless Security section following in this chapter.*

If a user enters invalid credentials and clicks **OK**, *the device associates but does not authenticate. The user is again prompted to enter credentials.*

If the user clicks the **Cancel** *button, the device does not associate. The user is not prompted again for credentials until the device is rebooted, the radio is disabled then enabled, the* **Reconnect** *button on the Diags tag is clicked or the profile is modified and the* **Commit** *button is clicked.*

Windows Certificate Store vs. Certs Path

User Certificates

EAP-TLS authentication requires a user certificate. The user certificate must be stored in the Windows certificate store.

- To generate the user certificate, follow the instructions in “Generating a User Certificate for the Mobile Device”, later in this chapter.
- Import the user certificate into the Windows certificate store by following the instructions in “Installing a User Certificate on the Mobile Device”, later in this chapter.
- A Root CA certificate is also needed for EAP-TLS. Refer to the section below.

Root CA Certificates

Root CA certificates are required for PEAP/MSCHAP, PEAP/GTC, and EAP-TLS. Two options are offered for storing these certificates. They may be imported into the Windows certificate store or copied into the Certs Path directory.

How To: Use the Certs Path

1. Follow the instructions later in this chapter for “Downloading a Root CA Certificate to a PC”.
2. Copy the certificate to specified directory on the mobile device. The default location for Certs Path is \System. A different location may be specified by using the **Certs Path** global variable. Please note the location chosen for certificate storage should persist after warmboot.
3. When completing the Credentials screen for the desired authentication, do not check the **Use MS store** checkbox after checking the **Validate server** checkbox.
4. Enter the certificate name in the **CA Cert** textbox.
5. Click **OK** to exit the Credentials screen and then **Commit** to save the profile changes.

How To: Use Windows Certificate Store

1. Follow the instructions later in this chapter for "Downloading a Root CA Certificate to a PC".
2. To import the certificate into the Windows store, follow the instructions for "Installing a Root CA Certificate on the Mobile Device" later in this chapter.
3. When completing the Credentials screen for the desired authentication, be sure to check the **Use MS store** checkbox after checking the **Validate server** checkbox.
4. The default is to use all certificates in the store. If this is OK, skip to Step #8.
5. Otherwise, to select a specific certificate click on the **Browse** (…) button.

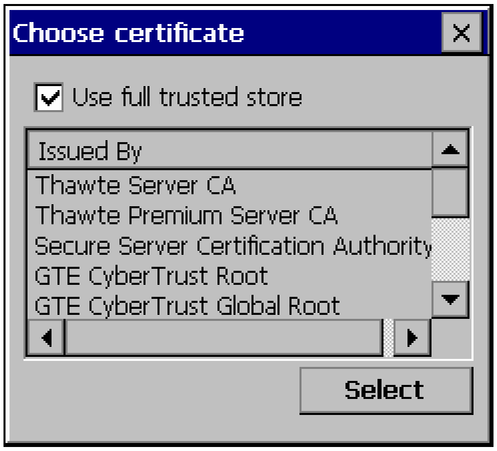


Figure 5-10 Choose Certificate

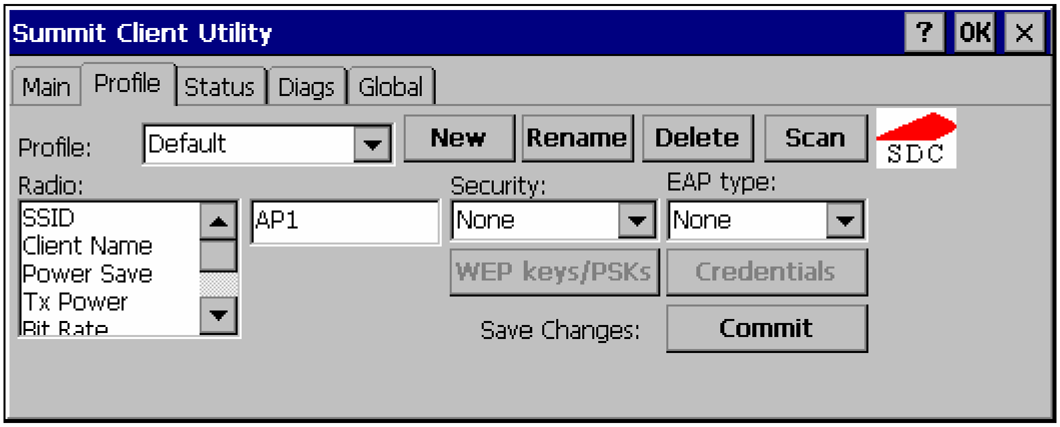
6. Uncheck the **Use full trusted store** checkbox.
7. Select the desired certificate and click the **Select** button to return the selected certificate to the **CA Cert** textbox.
8. Click **OK** to exit the Credentials screen and then **Commit** to save the profile changes.

Summit Wireless Security

Use the instructions in this section to complete the entries on the **Profile** tab according to the type of wireless security used by the network. The instructions that follow are the minimum required to successfully connect to a network. Your system may require more parameters than are listed in these instructions. Please see your system administrator for complete information about your network and its wireless security requirements.

To begin the configuration process:

- On the Main tab, click the **Admin Login** button and enter the password.
- LXE recommends editing the default profile with the parameters for your network. Select the Default profile from the pull down menu.


Summit Client Utility

Profile: Default

Radio:
SSID
Client Name
Power Save
Tx Power
Bit Rate

AP1

Security: None

EAP type: None

Save Changes: Commit

Figure 5-11 Default Profile

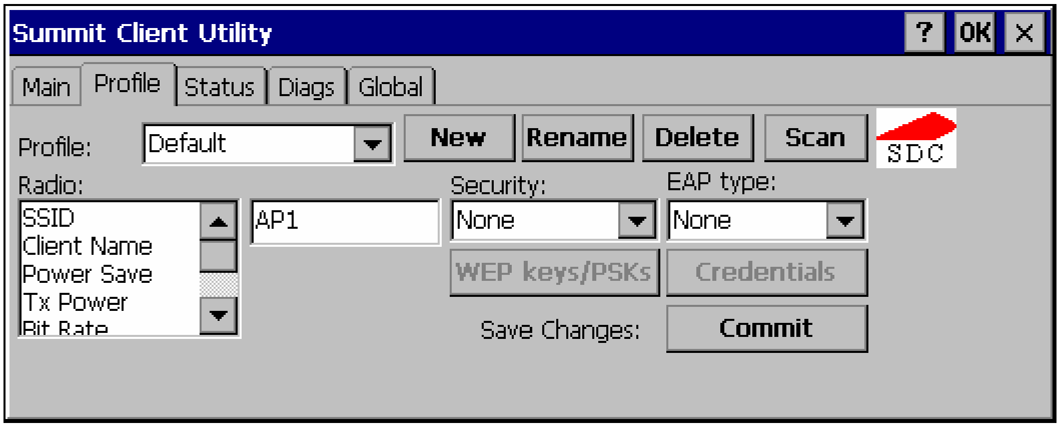
- Make any desired parameter changes as described in the applicable following section determined by network security type and click the **Commit** button to save the changes.

Be sure to click the **Commit** button after all changes have been made.

No Security

To connect to a wireless network with no security, make sure the following profile options are used:

- Enter the SSID of the Access Point assigned to this profile
- Set EAP Type to None
- Set Encryption to None
- Set Auth Type to Open



Profile: Default

Radio:
SSID
Client Name
Power Save
Tx Power
Bit Rate

AP1

Security: None

EAP type: None

Save Changes:

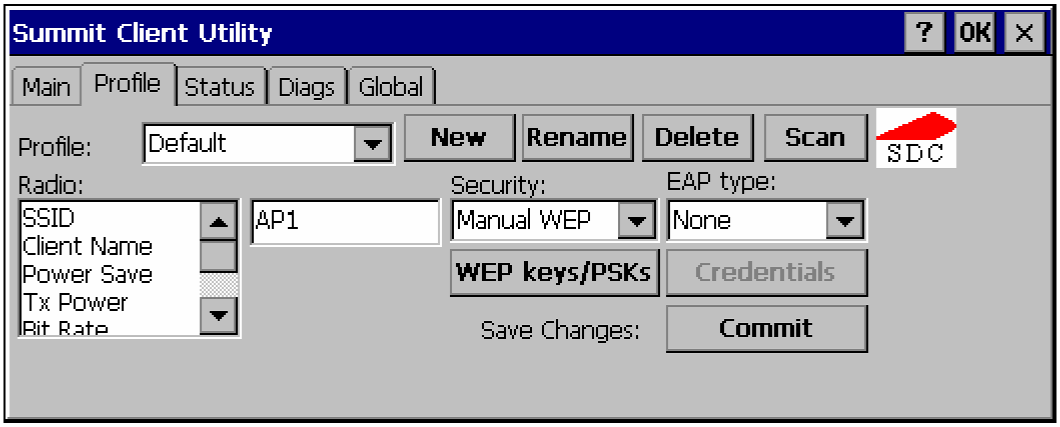
Figure 5-12 No Security

Once configured, click the **Commit** button. Ensure the correct Active Profile is selected on the Main tab and warmboot. The SCU Main tab shows the device is associated after the radio connects to the network.

WEP

To connect using WEP, make sure the following profile options are used.

- Enter the SSID of the Access Point assigned to this profile
- Set EAP Type to None
- Set Encryption to Manual WEP
- Set Auth Type to Open



Profile: Default

Radio:
SSID
Client Name
Power Save
Tx Power
Bit Rate

AP1

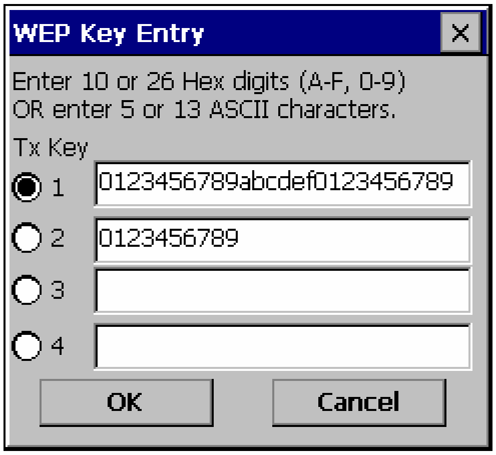
Security: Manual WEP

EAP type: None

Save Changes:

Figure 5-13 WEP Encryption

Click the **WEP keys/PSKs** button.



Enter 10 or 26 Hex digits (A-F, 0-9)
OR enter 5 or 13 ASCII characters.

Tx Key

● 1 0123456789abcdef0123456789

○ 2 0123456789

○ 3

○ 4

Figure 5-14 WEP Keys

Valid keys are 10 (for 40 bit encryption) or 26 (for 128 bit encryption) hexadecimal characters. Enter the key(s) and click **OK**.

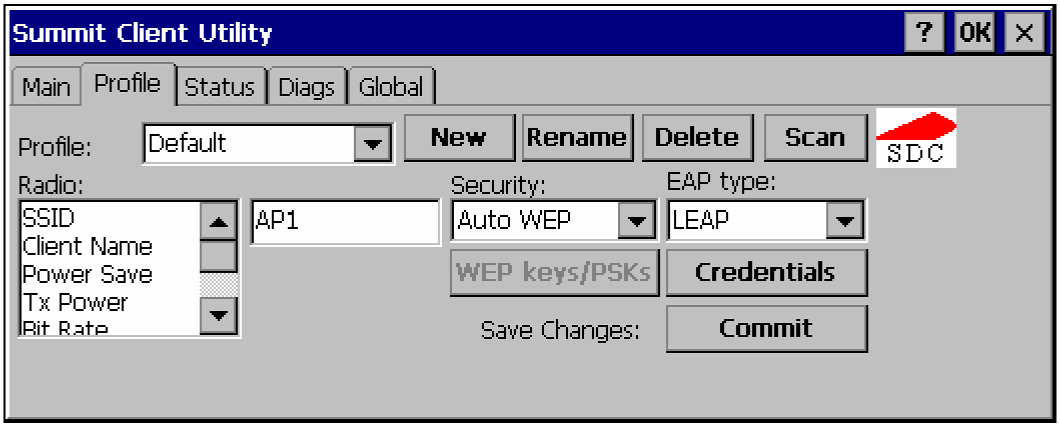
Once configured, click the **Commit** button. Ensure the correct Active Profile is selected on the Main tab and warmboot. The SCU Main tab shows the device is associated after the radio connects to the network.

LEAP without WPA Authentication

To use LEAP (without WPA) make sure the following profile options are used:

- Enter the SSID of the Access Point assigned to this profile
- Set EAP Type to LEAP
- Set Encryption to Auto WEP
- Set Auth Type as follows:
  - If the Cisco/CCX certified AP is configured for open authentication, set the Auth Type radio parameter to Open.
  - If the AP is configured for network EAP only, set the Auth Type radio parameter to LEAP.

Please see "WPA/LEAP" later in this section to configure the radio for WPA LEAP.



Profile: Default

Radio: SSID, Client Name, Power Save, Tx Power, Bit Rate

AP1

Security: Auto WEP

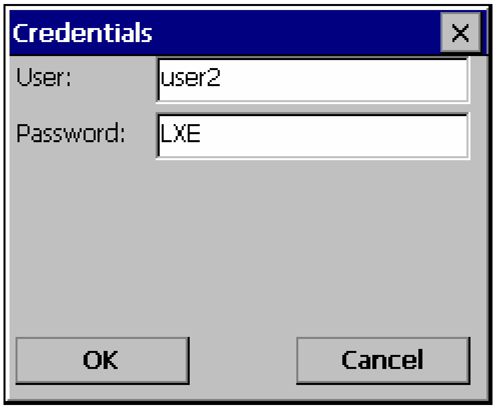
EAP type: LEAP

Save Changes:

Figure 5-15 LEAP Configuration

Please review "Sign-On vs. Stored Credentials", earlier in this chapter.

To use Stored Credentials, click on the **Credentials** button. No entries are necessary for Sign-On Credentials as the user will be prompted for the Username and Password when connecting to the network.



User: user2

Password: LXE

Figure 5-16 LEAP Credentials

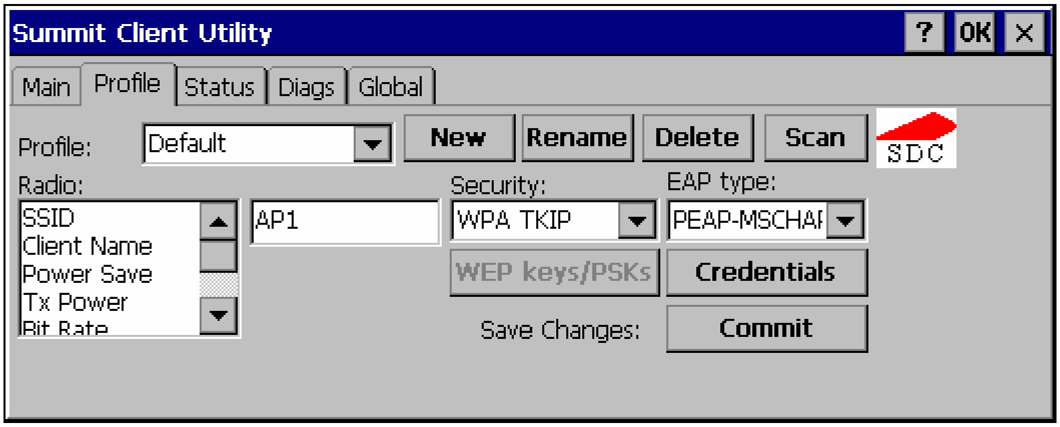
Enter the Domain\Username (if the Doman is required), otherwise enter the Username. Enter the password and click **OK**.

Once configured, click the **Commit** button. Ensure the correct Active Profile is selected on the Main tab and warmboot. The SCU Main tab shows the device is associated after the radio connects to the network.

PEAP/MSCHAP

To use PEAP/MSCHAP, make sure the following profile options are used.

- Enter the SSID of the Access Point assigned to this profile
- Set EAP Type to PEAP-MSCHAP
- Set Encryption to WPA TKIP
- Set Auth Type to Open



Profile: Default

Radio:

SSID
Client Name
Power Save
Tx Power
Bit Rate

AP1

Security: WPA TKIP

EAP type: PEAP-MSCHAP

Save Changes:

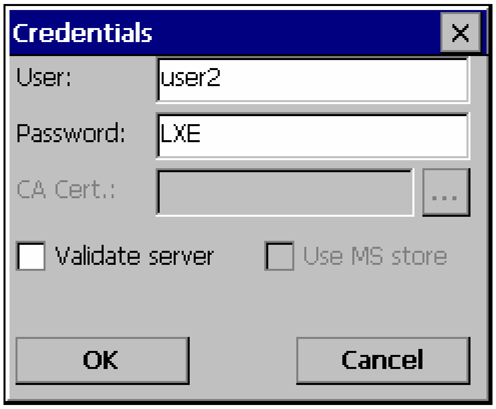
Figure 5-17 PEAP/MSCHAP

Please review “Sign-On vs. Stored Credentials” earlier in this chapter.

Click the **Credentials** button.

- No entries except the CA Certificate Filename are necessary for Sign-On Credentials as the user will be prompted for the User Name and Password when connecting to the network.
- For Stored Credentials, User, Password and the CA Certificate Filename must be entered.

Enter these items as directed below.



User: user2

Password: LXE

CA Cert.:

☐ Validate server ☐ Use MS store

Figure 5-18 PEAP/MSCHAP Credentials

Enter the Domain\Username (if the Doman is required), otherwise enter the Username.

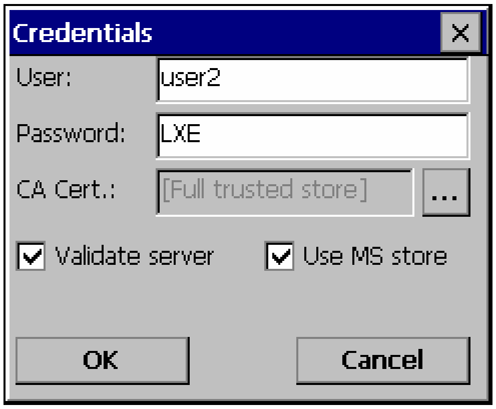
Enter the password.

Leave the CA Certificate File Name blank for now.

Click **OK** then click **Commit**. Ensure the correct Active profile is selected on the Main tab.

Please review “Windows Certificates Store vs. Certs Path” earlier in this chapter.

Once successfully authenticated, import the CA certificate into the Windows certificate store. Return to the Credentials screen and check the **Validate server** checkbox.



Credentials

User: user2

Password: LXE

CA Cert.: [Full trusted store]

☑ Validate server ☑ Use MS store

Figure 5-19 PEAP/MSCHAP Certificate Filename

If using the Windows certificate store:

- Check the **Use MS store** checkbox. The default is to use the Full Trusted Store.
- To select an individual certificate, click on the Browse button.
- Uncheck the **Use full trusted store** checkbox.
- Select the desired certificate and click **Select**. You are returned to the Credentials screen.

If using the Certs Path option:

- Leave the Use MS store box unchecked.
- Enter the certificate filename in the **CA Cert t**extbox.

Click **OK** then click **Commit**.

The device should be authenticating the server certificate and using PEAP/MSCHAP for the user authentication.

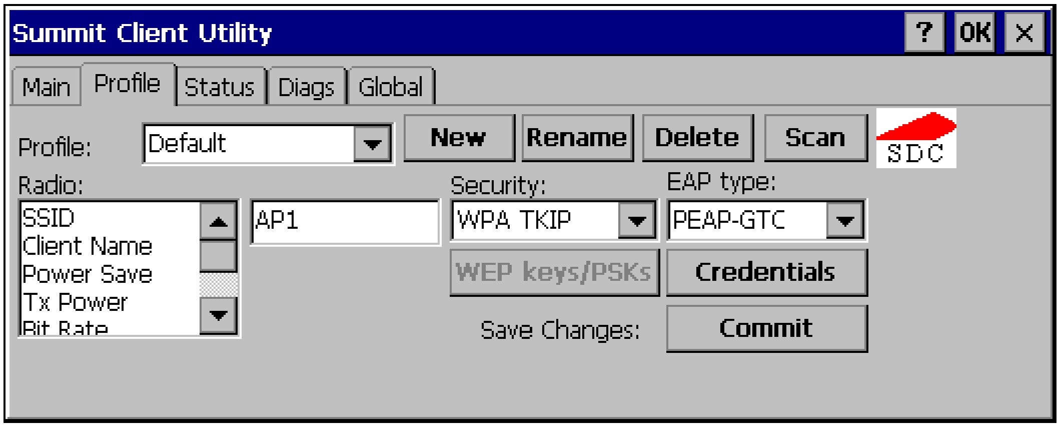
For information on generating a Root CA certificate, please see “Root CA Certificate” later in this chapter.

Note: The date must be properly set on the device to authenticate a certificate.

PEAP/GTC

To use PEAP/GTC, make sure the following profile options are used.

- Enter the SSID of the Access Point assigned to this profile
- Set EAP Type to PEAP-GTC
- Set Encryption to WPA TKIP
- Set Auth Type to Open



Profile: Default

Radio:
SSID
Client Name
Power Save
Tx Power
Bit Rate

AP1

Security: WPA TKIP

EAP type: PEAP-GTC

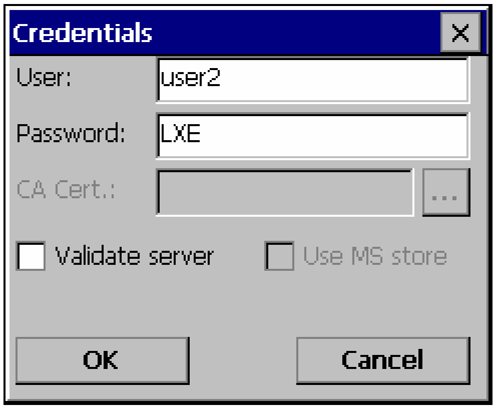
Figure 5-20 PEAP/GTC

Please review “Sign-On vs. Stored Credentials”, earlier in this chapter.

Click the **Credentials** button.

- No entries except the CA Certificate Filename are necessary for Sign-On Credentials as the user will be prompted for the User Name and Password when connecting to the network.
- For Stored Credentials, User, Password and the CA Certificate Filename must be entered.

Enter these items as directed below.



User: user2

Password: LXE

CA Cert.:

□ Validate server □ Use MS store

Figure 5-21 PEAP/GTC Credentials

Enter the Domain\Username (if the Doman is required), otherwise enter the Username.

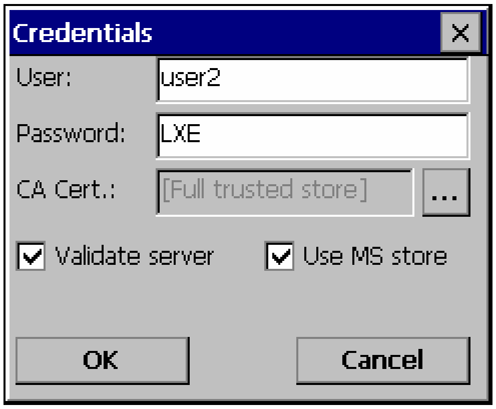
Enter the password.

Leave the CA Certificate File Name blank for now.

Click **OK** then click **Commit**. Ensure the correct Active Profile is selected on the Main tab.

Please review "Windows Certificates Store vs. Certs Path" earlier in this chapter.

Once successfully authenticated, import the CA certificate into the Windows certificate store. Return to the Credentials screen and check the **Validate server** checkbox.



Credentials

User: user2

Password: LXE

CA Cert.: [Full trusted store]

☑ Validate server ☑ Use MS store

Figure 5-22 PEAP/GTC Certificate Filename

If using the Windows certificate store:

- Check the **Use MS store** checkbox. The default is to use the Full Trusted Store.
- To select an individual certificate, click on the Browse button.
- Uncheck the **Use full trusted store** checkbox.
- Select the desired certificate and click **Select**. You are returned to the Credentials screen.

If using the Certs Path option:

- Leave the Use MS store box unchecked.
- Enter the certificate filename in the **CA Cert t**extbox.

Click **OK** then click **Commit**.

The device should be authenticating the server certificate and using PEAP/MSCHAP for the user authentication.

For information on generating a Root CA certificate, please see "Root CA Certificate" later in this chapter.

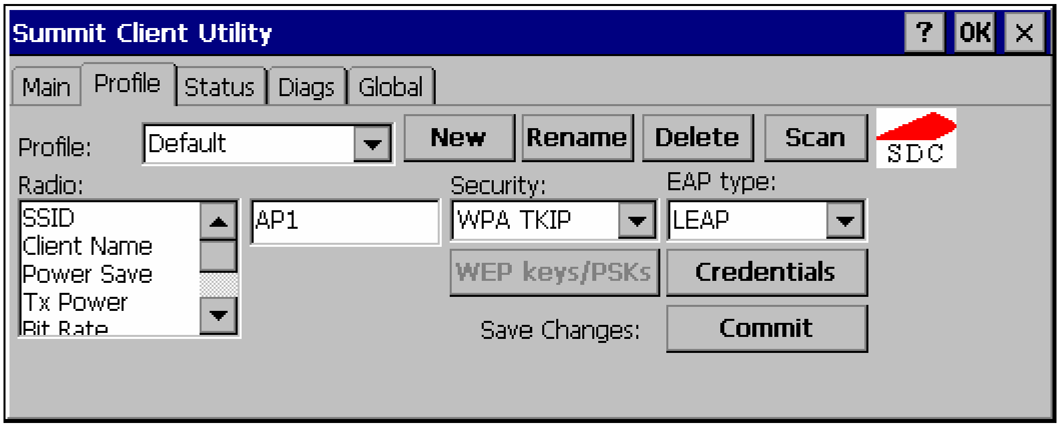
Note: The date must be properly set on the device to authenticate a certificate.

WPA/LEAP

To use WPA/LEAP, make sure the following profile options are used.

- Enter the SSID of the Access Point assigned to this profile
- Set EAP Type to LEAP
- Set Encryption to WPA TKIP
- Set Auth Type to Open

Please see “LEAP” earlier in this section to configure the radio for LEAP without WPA.



Summit Client Utility

Profile: Default

Radio: SSID, Client Name, Power Save, Tx Power, Bit Rate

SSID: AP1

Security: WPA TKIP

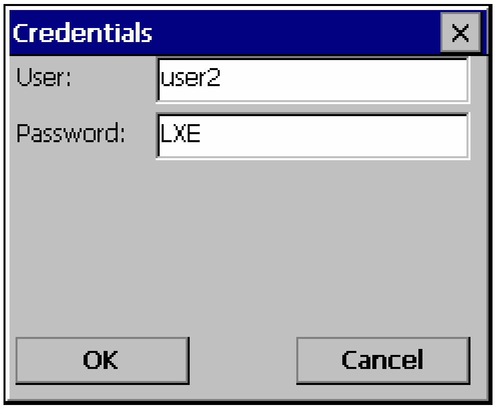
EAP type: LEAP

Save Changes: Commit

Figure 5-23 WPA/LEAP

Please review “Sign-On vs. Stored Credentials”, earlier in this chapter.

To use Stored Credentials, click on the **Credentials** button. No entries are necessary for Sign-On Credentials as the user will be prompted for the Username and Password when connecting to the network.



Credentials

User: user2

Password: LXE

Figure 5-24 WPA/LEAP Credentials

Enter the Domain\Username (if the Doman is required), otherwise enter the Username.

Enter the password.

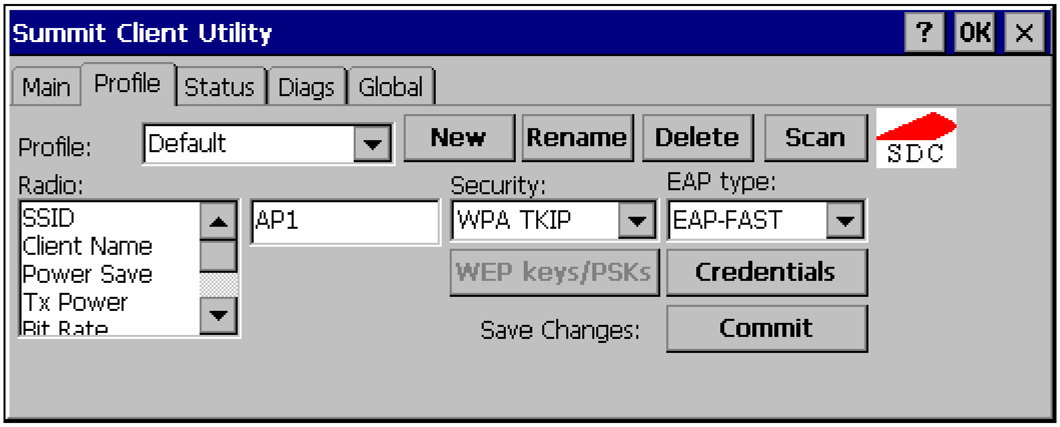
Click **OK** then click **Commit**. Ensure the correct Active Profile is selected on the Main tab and warmboot. The SCU Main tab shows the device is associated after the radio connects to the network.

EAP-FAST

To use EAP-FAST, make sure the following profile options are used.

- Enter the SSID of the Access Point assigned to this profile
- Set EAP Type to EAP-FAST
- Set Encryption to WPA TKIP
- Set Auth Type to Open

The SCU supports EAP-FAST with automatic or manual PAC provisioning. With automatic PAC provisioning, the user credentials, whether entered on the saved credentials screen or the sign on screen, are sent to the RADIUS server. The RADIUS server must have auto provisioning enabled to send the PAC provisioning credentials to the client device. Please refer to the "LXE Security Primer" for more information on the RADIUS server configuration.



Profile: Default

SSID: AP1

Security: WPA TKIP

EAP type: EAP-FAST

Figure 5-25 EAP-FAST Configuration

For automatic PAC provisioning, once a username/password is authenticated, the PAC information is stored on the computer. The same username/password must be used to authenticate each time. See the note on the next page for more details.

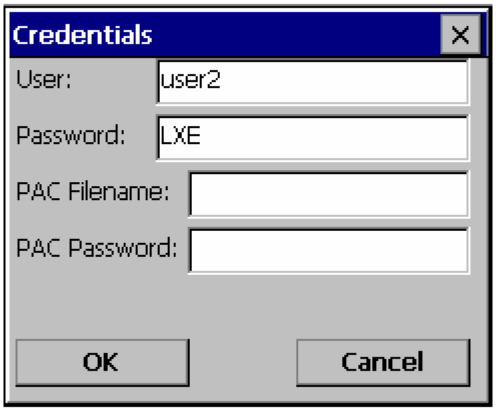
For manual PAC provisioning, the PAC filename and Password must be entered.

Please review "Sign-On vs. Stored Credentials", earlier in this chapter.

The entries on the Credentials screen are determined by the type of credentials (stored or sign on) and the type of PAC provisioning (automatic or manual).

Click on the **Credentials** button.

To use Stored Credentials, click on the **Credentials** button. No entries are necessary for Sign-On Credentials with automatic PAC provisioning as the user will be prompted for the Username and Password when connecting to the network.



User: user2

Password: LXE

PAC Filename:

PAC Password:

Figure 5-26 EAP-FAST Credentials

To use Sign-On credentials:

- Do not enter a User and Password as the user will be prompted for the Username and Password when connecting to the network.

To use Stored Credentials:

- Enter the Domain\Username (if the Doman is required), otherwise enter the Username.
- Enter the password.

To use Automatic PAC Provisioning:

- No additional entries are required.

To use manual PAC Provisioning:

- Enter the PAC Filename and PAC Password.
- The PAC file must be copied to the directory specified in the Certs Path global variable. The PAC file must not be read only.

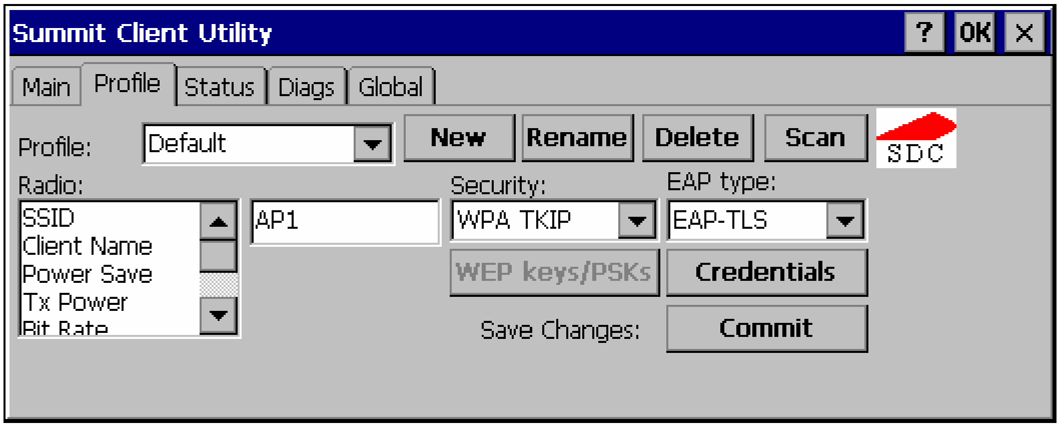
Tap **OK** then tap **Commit**. Ensure the correct Active Profile is selected on the Main tab and warmboot. The SCU Main tab shows the device is associated after the radio connects to the network.

*Note: When using Automatic PAC Provisioning, once authenticated, there is a file stored in the \System directory with the PAC credentials. If the username is changed, that file must be deleted. The filename is **autoP.00.pac**.*

EAP-TLS

To use EAP-TLS, make sure the following profile options are used.

- Enter the SSID of the Access Point assigned to this profile
- Set EAP Type to EAP-TLS
- Set Encryption to WPA TKIP
- Set Auth Type to Open



Summit Client Utility

Profile: Default

Radio:

SSID: AP1

Security: WPA TKIP

EAP type: EAP-TLS

Save Changes:

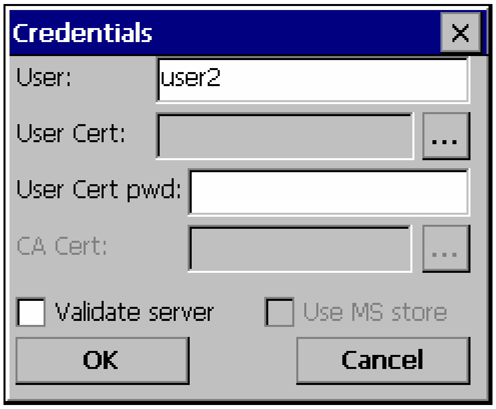
Figure 5-27 EAP-TLS

Please review “Sign-On vs. Stored Credentials”, earlier in this chapter.

Click the **Credentials** button.

- No entries except the User Certificate Filename and the CA Certificate Filename are necessary for Sign-On Credentials as the user will be prompted for the User Name and Password when connecting to the network.
- For Stored Credentials, User, Password and the CA Certificate Filename must be entered.

Enter these items as directed below.



Credentials

User: user2

User Cert:

User Cert pwd:

CA Cert:

□ Validate server

□ Use MS store

Figure 5-28 EAP-TLS Credentials

Enter the Domain\Username (if the Doman is required), otherwise enter the Username.

Leave the certificate file name entries blank for now.

Click **OK** then click **Commit**. Ensure the correct Active Profile is selected on the Main tab.

Once successfully authenticated, import the user certificate into the Windows certificate store.

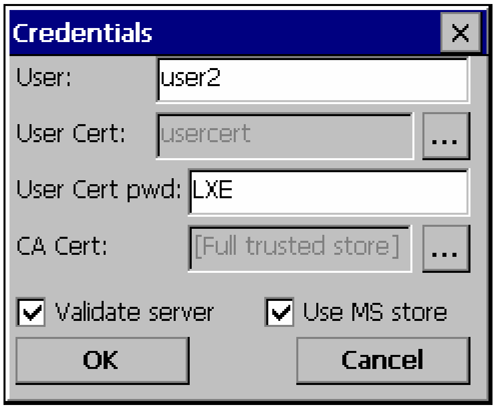
Return to the Credentials screen.

Use the **Browse** button to locate the User Cert from the certificate store. Highlight the desired certificate and press the **Select** button. The name of the certificate is displayed in the **User Cert** box.

Enter the password for the user certificate in the **User Cert pwd** box.

Please review "Windows Certificates Store vs. Certs Path" earlier in this chapter.

Check the **Validate server** a checkbox.



Credentials

User: user2

User Cert: usercert

User Cert pwd: LXE

CA Cert: [Full trusted store]

☑ Validate server ☑ Use MS store

Figure 5-29 EAP-TLS Credentials

If using the Windows certificate store:

- Check the **Use MS store** checkbox. The default is to use the Full Trusted Store.
- To select an individual certificate, click on the Browse button.
- Uncheck the **Use full trusted store** checkbox.
- Select the desired certificate and click **Select**. You are returned to the Credentials screen.

If using the Certs Path option:

- Leave the Use MS store box unchecked.
- Enter the certificate filename in the **CA Cert t**extbox.

Click **OK** then click **Commit**.

The device should be authenticating the server certificate and using EAP-TLS for the user authentication.

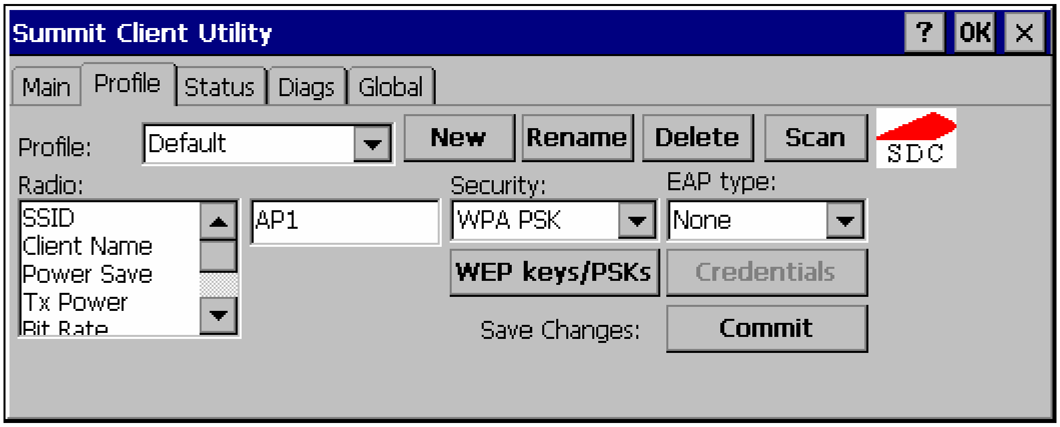
For information on generating a Root CA certificate, please see "Root CA Certificate" later in this chapter. For more information on generating a User certificate, see "User Certificate" later in this chapter.

Note: The date must be properly set on the device to authenticate a certificate.

WPA PSK

To connect using WPA/PSK, make sure the following profile options are used:

- Enter the SSID of the Access Point assigned to this profile
- Set EAP Type to None
- Set Encryption to WPA PSK
- Set Auth Type to Open



Summit Client Utility

Profile: Default

Radio:

SSID
Client Name
Power Save
Tx Power
Bit Rate

AP1

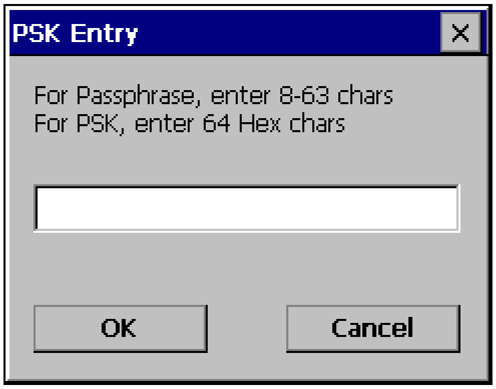
Security: WPA PSK

EAP type: None

Save Changes:

Figure 5-30 WPA/PSK Encryption

Click **WEP keys/PSKs** button.



PSK Entry

For Passphrase, enter 8-63 chars
For PSK, enter 64 Hex chars

Figure 5-31 PSK Entry

This value can be 64 hex characters or an 8 to 63 byte ASCII value. Enter the key and click **OK**.

Once configured, click the **Commit** button. Ensure the correct Active Profile is selected on the Main tab and warmboot. The SCU Main tab shows the device is associated after the radio connects to the network.

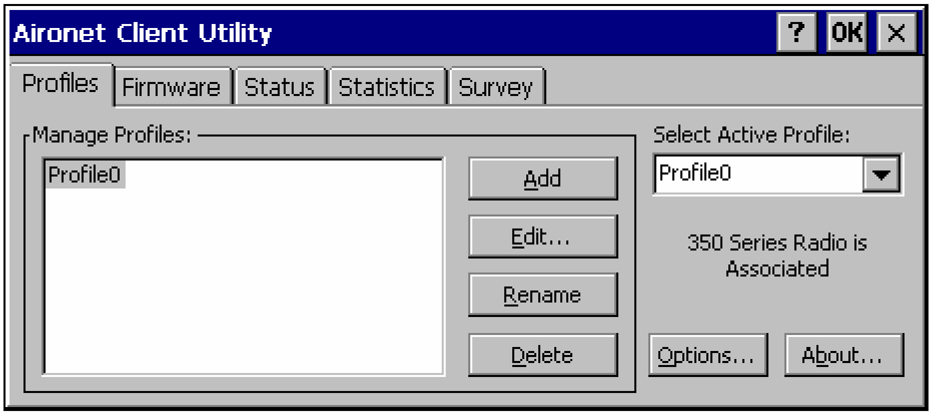
Cisco Radio

The Cisco radio is a 2.4GHz 802.11b radio. This radio supports no encryption, WEP, LEAP or WPA (PEAP-MSCHAP, PEAP-GTC, EAP-TLS, WPA/LEAP and WPA-PSK).Configuring without WPA

Cisco – Aironet Client Utility (ACU)

Note: When making changes to profile parameters, the VX7 should be warmbooted afterwards.

Access: Start | Programs | Cisco ACU *or* ACU Icon on Desktop



Select Active Profile: Profile0

Profile0

350 Series Radio is Associated

Figure 5-32 Cisco Aironet Client Utility

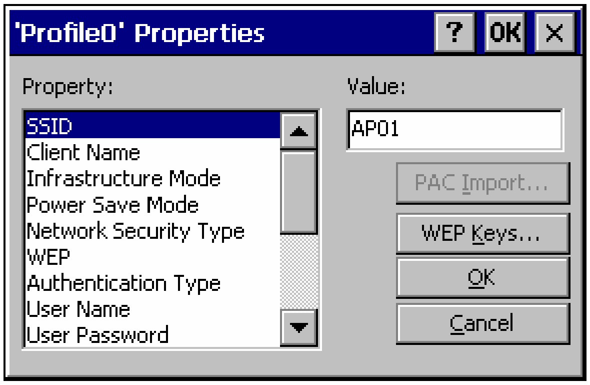
Note: To configure WPA, please see "Configuring for WPA", later in this section.

Profiles Tab

Use this option to manage profiles and review firmware information, status, statistics and wireless radio survey data.

Profile Parameter	Default
SSID	Blank
Client Name	Blank
Infrastructure Mode	Yes
Power Save Mode	Fast PSP
Network Security Type	None
WEP	No WEP
Authentication Types	Open
LEAP	Disabled
Mixed Mode	Disabled
World Mode	Disabled
Data Rates	Auto
Transmit Power	MAX
Offline Channel Scan	Enabled

Select an active profile to manage.



Value: AP01

Figure 5-33 Cisco Profile Properties Screen

No Security

Create a new profile or edit an exiting profile.

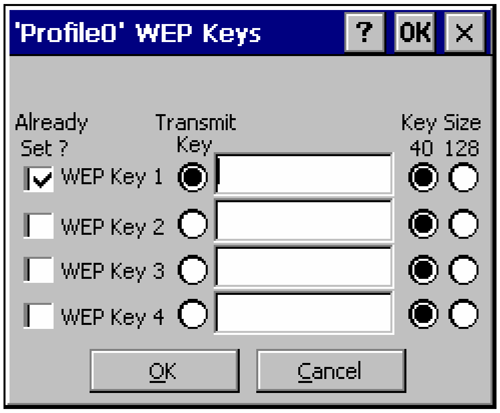
- If no security is used, the only entry necessary on the Profile Properties screen may be the SSID. If the SSID is left blank, the radio can associate to any available network.
- Network security must be set to None.
- WEP must be set to No WEP.

WEP

To use WEP, create a new profile or select an exiting profile.

- WEP must be set to either Static WEP keys or Dynamic WEP keys. When one of the WEP methods is selected, the WEP Keys button is active.
- Authentication must be set to Open
- The appropriate WEP keys must be entered:
  - 40-bit WEP keys consist of 10 hexadecimal characters of 5 ASCII characters
  - 128 bit WEP keys consist of 26 hexadecimal or 13 ASCII characters.
  - After a WEP key is entered, it will be hidden from view if you return to the screen. However, the "Already Set" indicates if a key has previously been entered.

Tap the WEP Keys button to enter WEP information. If a key is already entered, the Already set? Checkbox is checked. The previously entered key value is not displayed for security.



Already Set ?		Transmit Key		Key Size 40	128
☑	WEP Key 1	●		●	○
□	WEP Key 2	○		●	○
□	WEP Key 3	○		●	○
□	WEP Key 4	○		●	○

Figure 5-34 Cisco Profile WEP Keys

LEAP

Note: The instructions in this section are for LEAP without WPA. Please see WPA/LEAP later in this chapter for instructions on using LEAP with WPA.

Create a new profile or edit an exiting profile.

- Network security must be set to LEAP.
- The following parameters are accessible when LEAP is selected. Please enter the appropriate information.
  - User Name
  - User Password
  - User Domain (optional)

Firmware Tab

Displays the current firmware version and allows you to load new firmware. Tap the Browse button to locate the new firmware file.

Status Tab

Immediately runs status on : signal strength and signal quality.

Statistics Tab

Select the Receive Stats or Transmit Stats. The data is displayed on the screen.

Survey Tab

Immediately runs signal strength and quality and link speed. An option is available to Setup parameters for Active Mode reporting.

Configuring for WPA

💾	Wi-Fi Protected Access (WPA) is only available on VX7's equipped with the updated Cisco radio driver (release 2.60 or later).
S	WPA requires software revision 1ED or greater. To identify the software revision, please click on the "About" icon in the Windows CE Control Panel.
📖	Please refer to the "LXE Security Primer" to prepare the Authentication Server and Access Point for VX7 communication.
Date/Time	It is important that all dates are correct on CE computers when using any type of certificate. Certificates are date sensitive and if the date is not correct authentication will fail.

System Requirements

To support Wi-Fi Protected Access (WPA), the VX7 must be equipped as follows:

- Cisco 350 radio card with driver release 2.60 (or later).

The LXE VX7 supports WPA and all authentications. The Microsoft supplicant and Cisco supplicants are used separately or together to provide support for the different authentications.

Most of the configuration is done with the Microsoft Wireless Configuration tool WPA/LEAP requires the Cisco supplicant and configuration tool.

Installing Radio drivers

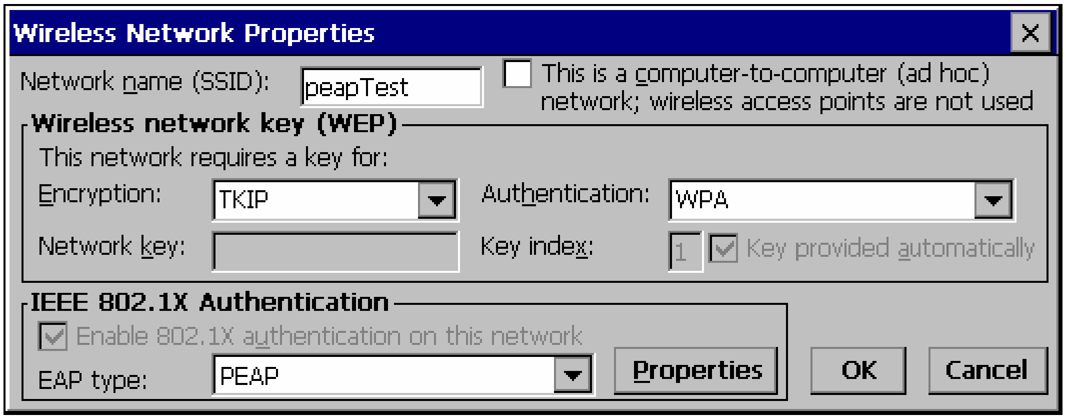
Which version of the Cisco driver should be installed depends on what authentication protocol is to be configured.

- Cisco PEAP should not be installed if using PEAP/MSCHAP.
- Cisco PEAP must be installed if using PEAP/GTC.
- For all other authentications (LEAP, EAP-TLS, WPA-PSK) it does not matter if Cisco PEAP is installed or not.

To determine if Cisco PEAP is installed or to change the installation, follow the instructions below.

Checking for the Cisco PEAP Supplicant

With a Cisco radio installed, open the Wireless network properties as described in "Wireless Network Configuration", later in this chapter. With the Authentication tab selected check the text in the EAP type drop down box. Refer to the following figures to determine if Cisco PEAP is installed.



Wireless Network Properties

Network name (SSID): peapTest

□ This is a computer-to-computer (ad hoc) network; wireless access points are not used

Wireless network key (WEP)

This network requires a key for:

Encryption: TKIP

Authentication: WPA

Network key:

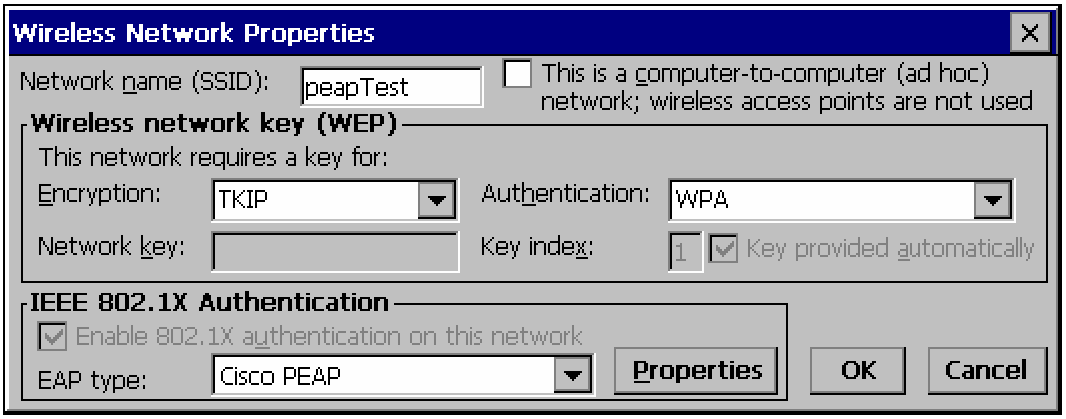
Key index: 1 ☑ Key provided automatically

IEEE 802.1X Authentication

☑ Enable 802.1X authentication on this network

EAP type: PEAP

Figure 5-35 No Cisco PEAP



Wireless Network Properties

Network name (SSID): peapTest

□ This is a computer-to-computer (ad hoc) network; wireless access points are not used

Wireless network key (WEP)

This network requires a key for:

Encryption: TKIP

Authentication: WPA

Network key:

Key index: 1 ☑ Key provided automatically

IEEE 802.1X Authentication

☑ Enable 802.1X authentication on this network

EAP type: Cisco PEAP

Figure 5-36 Cisco PEAP installed.

If the Cisco installation is correct continue, with the configuration. If it is not correct, follow the procedures below.

Note: Instructions are also included in the README file located in the \SYSTEM folder.

There are two Cisco CAB files in the \SYSTEM folder of the VX7. The default files are:

- CISCO.CAB
- CISCOPEAP.CAB

The default CISCO.CAB file provides for all authentications except Cisco PEAP. When the default CISCO.CAB file is loaded, the Wireless Network Properties screen looks like the figure labeled "No Cisco PEAP", above.

If Cisco PEAP is desired:

1. Rename the CISCO.CAB file to CISCOMSCHAP.CAB.
2. Rename the CISCOPEAP.CAB file to CISCO.CAB.
3. Coldboot the terminal to install the new driver with the registry.

The renamed CISCO.CAB file provides for Cisco PEAP and PEAP/GTC authentications. When the renamed CISCO.CAB file is loaded, the Wireless Network Properties screen looks like the figure labeled “Cisco PEAP Installed”, above.

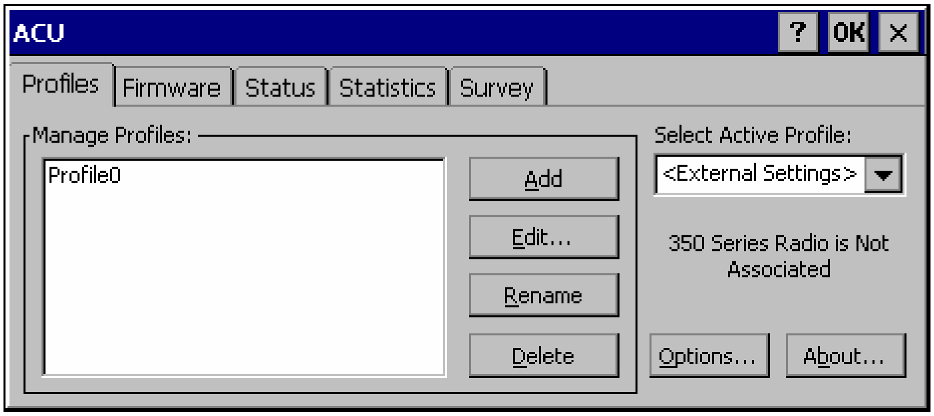
If it becomes necessary to switch to a different authentication than Cisco PEAP or PEAP/GTC,

1. Rename the CISCO.CAB file to CISCOPEAP.CAB.
2. Rename the CISCOMSCHAP.CAB file to CISCO.CAB
3. Coldboot the terminal to install the new driver with the registry.

Wireless Network Configuration

Use the following instructions for all authentication protocols to configure the Microsoft Wireless Network configuration utility unless WPA/LEAP is used. WPA/LEAP is configured with the Cisco ACU (see Section "WPA/LEAP Authentication Configuration").

Click the ACU icon on the desktop.



Manage Profiles: Profile0

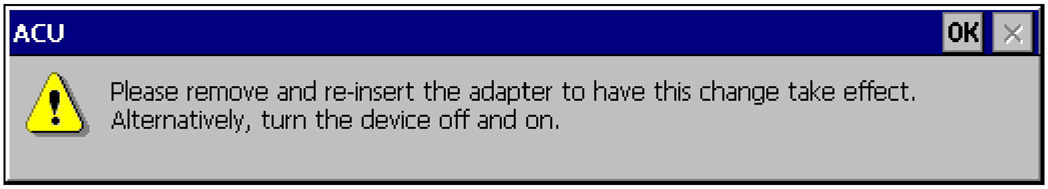
Select Active Profile: <External Settings>

350 Series Radio is Not Associated

Figure 5-37 Cisco ACU Profile Selection

From the "Select Active Profile" pull down list, select <External Settings>.

Click OK and warmboot.



Please remove and re-insert the adapter to have this change take effect. Alternatively, turn the device off and on.

Figure 5-38 Cisco ACU Reboot Message

After booting up, the Microsoft Zero Config tool should start. If it does not, start configuring the wireless connection by clicking on the icon on the task bar shown in below.

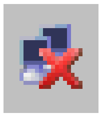
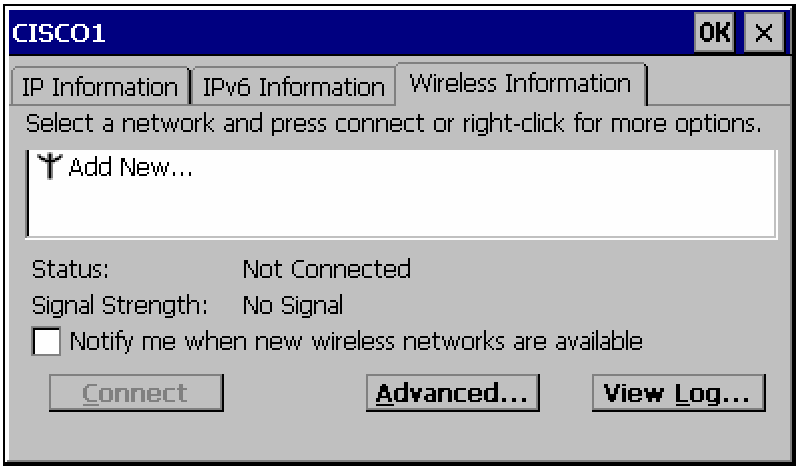


Figure 5-39 Microsoft Wireless Connection Icon

The Wireless Network Connection screen appears.



Select a network and press connect or right-click for more options.

Add New...

Status: Not Connected

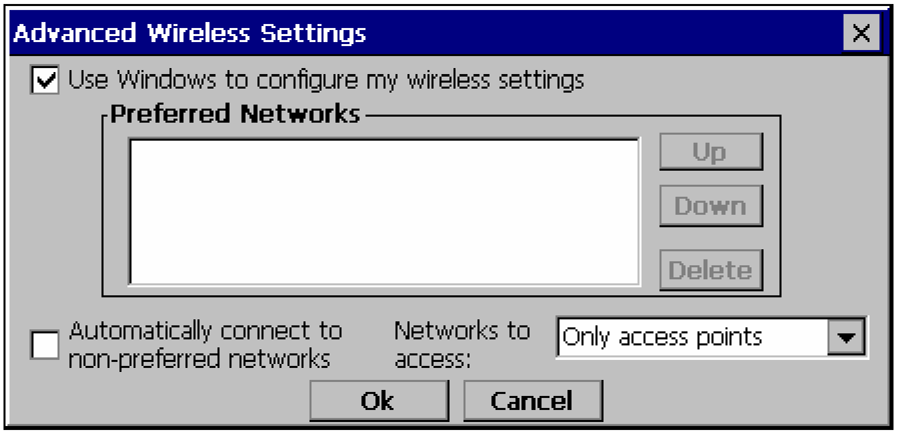
Signal Strength: No Signal

☐ Notify me when new wireless networks are available

Figure 5-40 Wireless Information Screen

Make sure the “Notify me when new wireless networks are available” box is not checked.

Click the Advanced… button.



☑ Use Windows to configure my wireless settings

☐ Automatically connect to non-preferred networks

Networks to access: Only access points

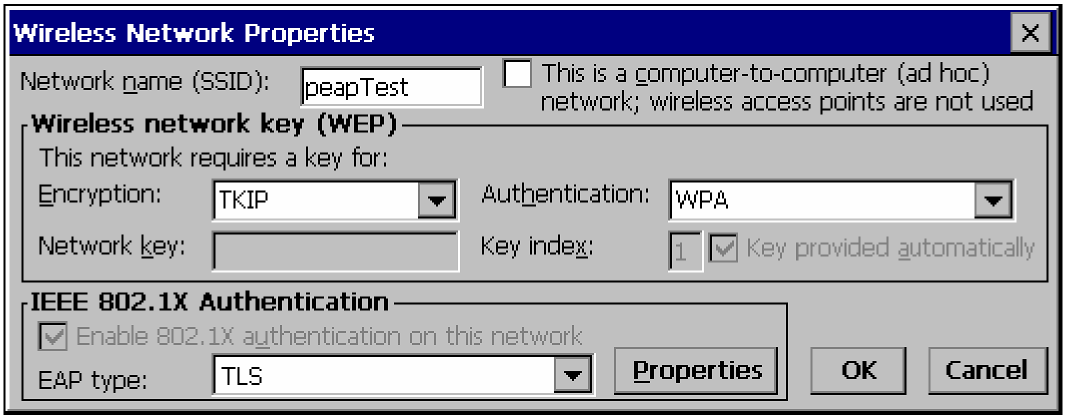
Figure 5-41 Advanced Wireless Settings

Make sure the “Use Windows to configure my wireless settings” box is checked.

Set the “Networks to access” drop down box to “Only access points”.

Click the OK button to return to the Wireless Information Screen.

Click the Add New … line.



Wireless Network Properties

Network name (SSID): peapTest

☐ This is a computer-to-computer (ad hoc) network; wireless access points are not used

Wireless network key (WEP)

This network requires a key for:

Encryption: TKIP

Authentication: WPA

Network key:

Key index: 1

☑ Key provided automatically

IEEE 802.1X Authentication

☑ Enable 802.1X authentication on this network

EAP type: TLS

Figure 5-42 Wireless Network Properties

Enter the Network name (SSID) into the text field.

For PEAP/MSCHAP and EAP/TLS, set Encryption to TKIP and Authentication to WPA.

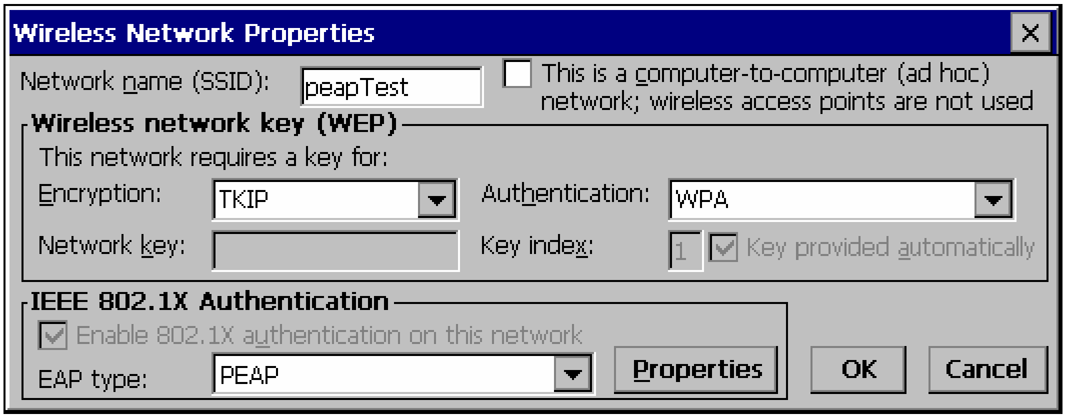
For WPA/PSK see “WPA/PSK Authentication Configuration”.

To configure the IEEE 802.1X Authentication box see the following sections for configuration of each authentication protocol.

PEAP/MS-CHAP Authentication Configuration

The Microsoft supplicant authenticates a user with the PEAP/MS-CHAP protocol. The Cisco CAB file without Cisco PEAP must be used with PEAP/MS-CHAP. See "Installing Radio Drivers", earlier in this chapter, for more information.

Configuring the PEAP/MS-CHAP Supplicant



Wireless Network Properties

Network name (SSID): peapTest

□ This is a computer-to-computer (ad hoc) network; wireless access points are not used

Wireless network key (WEP)

This network requires a key for:

Encryption: TKIP

Authentication: WPA

Network key:

Key index: 1

☑ Key provided automatically

IEEE 802.1X Authentication

☑ Enable 802.1X authentication on this network

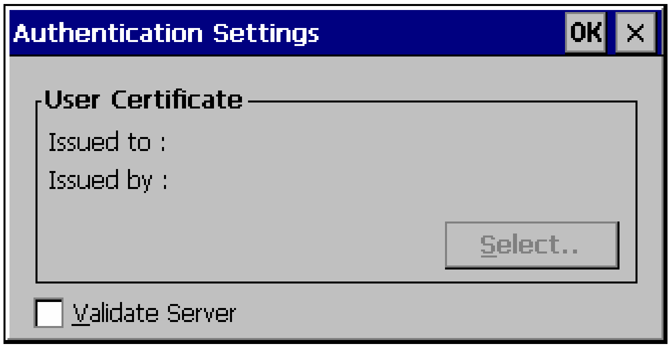
EAP type: PEAP

Figure 5-43 PEAP/MSCHAP Wireless Network Properties

With the radio parameters configured (see "Wireless Network Configuration", earlier in this chapter) set the EAP type to PEAP as shown above.

If the EAP type box text is not exactly as shown see "Installing Radio Drivers", earlier in this chapter, to change the radio cab file.

Click the Properties button.



Authentication Settings

User Certificate

Issued to :

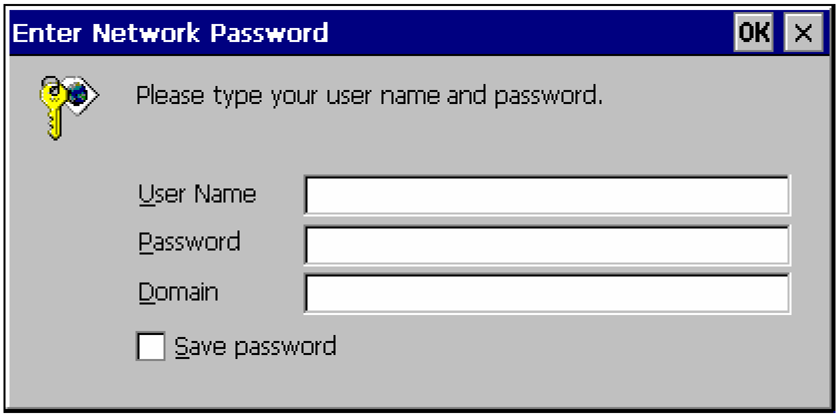
Issued by :

□ Validate Server

Figure 5-44 Authentication Settings

When first configuring and authenticating, do not validate the server certificate. This allows the user authentication to be tested. When that works, come back to this screen and validate the server certificate.

The login screen appears for logging into the wireless network.



Enter Network Password

Please type your user name and password.

User Name

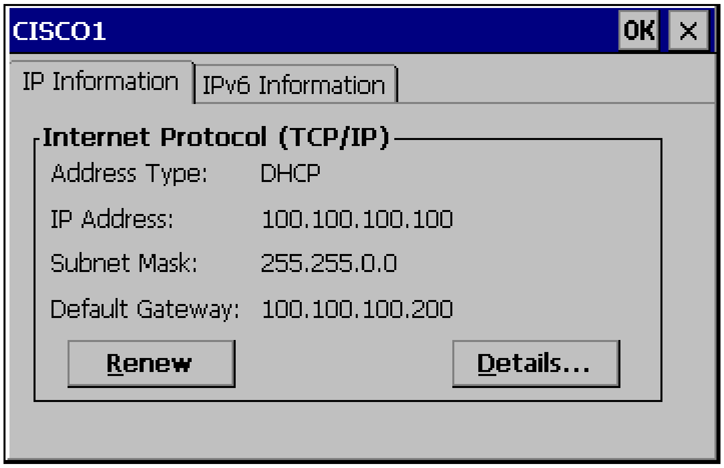
Password

Domain

□ Save password

Figure 5-45 Wireless Network Login

Once authenticated, click the IP Information tab.



CISCO1

Internet Protocol (TCP/IP)

Address Type: DHCP

IP Address: 100.100.100.100

Subnet Mask: 255.255.0.0

Default Gateway: 100.100.100.200

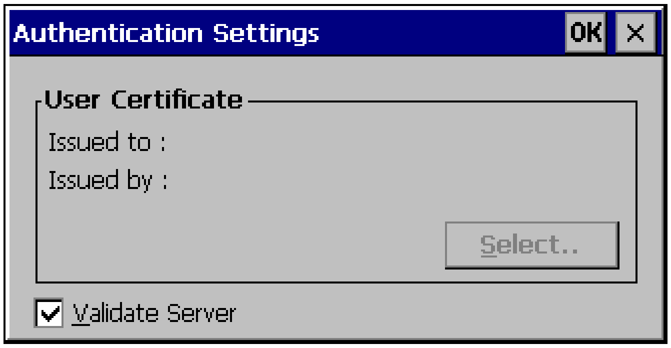
Figure 5-46 IP Information Tab

If the network is set to use DHCP, the VX7 displays the IP address given by the DHCP server.

Now go back and authenticate the server.

Server Authentication

To validate the server certificate install the root CA certificate. For instructions for installing, see "Root Certificates", later in this chapter.



Authentication Settings

User Certificate

Issued to :

Issued by :

☑ Validate Server

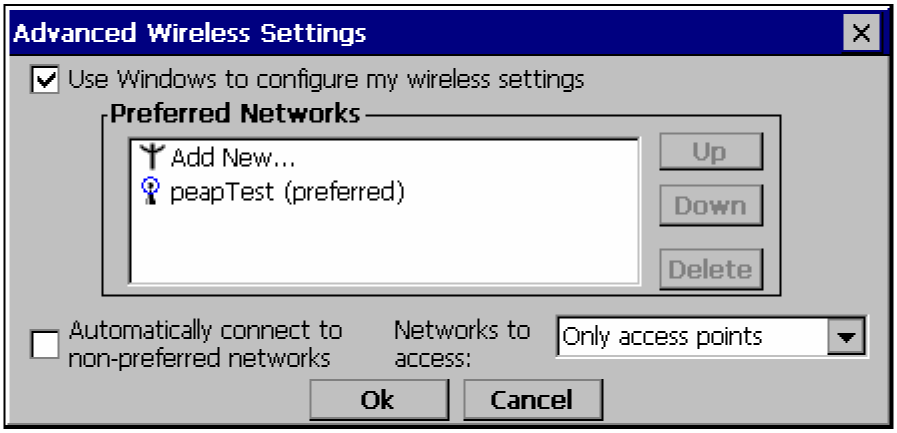
Figure 5-47 Authentication Settings, Validate Server

Navigate to the Wireless Network Properties configuration screen.

Click the Properties button.

Check the Validate server

Click OK to dismiss the configuration boxes.



Advanced Wireless Settings

☑ Use Windows to configure my wireless settings

Preferred Networks

Add New...

peapTest (preferred)

☐ Automatically connect to non-preferred networks

Networks to access: Only access points

Figure 5-48 Advanced Wireless Settings, Authenticated SSID

Once the authentication completes, the status changes to show the VX7 has authenticated to the <SSID>, as shown in the figure above.

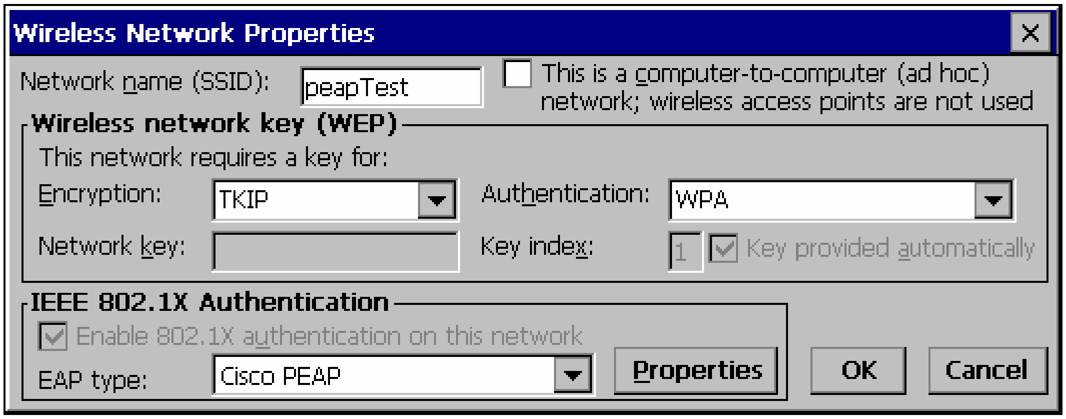
Click on the IP Information tab and make sure there is a valid IP address as shown in the figure labeled "IP Information Tab", earlier in this chapter.

PEAP/ GTC Authentication Configuration

The Microsoft supplicant authenticates a user with the PEAP/GTC protocol.

Configuring the PEAP / GTC Supplicant

With the radio parameters configured set the EAP type to Cisco PEAP as shown below.

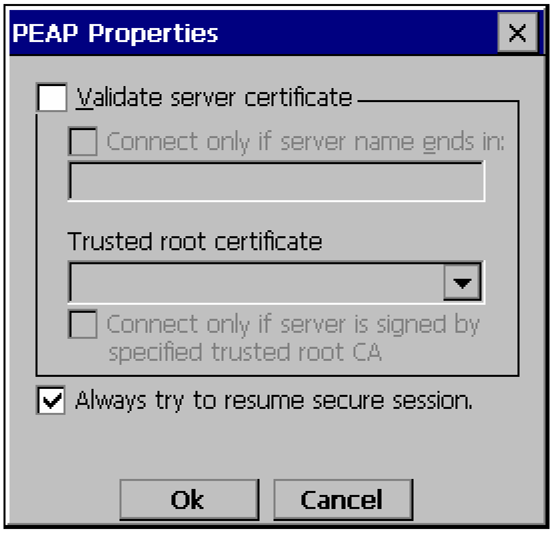


Wireless Network Properties
Network name (SSID): peapTest
□ This is a computer-to-computer (ad hoc) network; wireless access points are not used
Wireless network key (WEP)
This network requires a key for:
Encryption: TKIP
Authentication: WPA
Network key:
Key index: 1
☑ Key provided automatically
IEEE 802.1X Authentication
☑ Enable 802.1X authentication on this network
EAP type: Cisco PEAP
Properties
OK
Cancel

Figure 5-49 PEAP/GTC Wireless Network Properties

If the EAP type box text is not exactly as shown see “Installing Radio Drivers”, earlier in this chapter, to change the radio cab file.

Click the Properties button.



PEAP Properties
□ Validate server certificate
□ Connect only if server name ends in:
Trusted root certificate
□ Connect only if server is signed by specified trusted root CA
☑ Always try to resume secure session.
Ok
Cancel

Figure 5-50 PEAP Properties

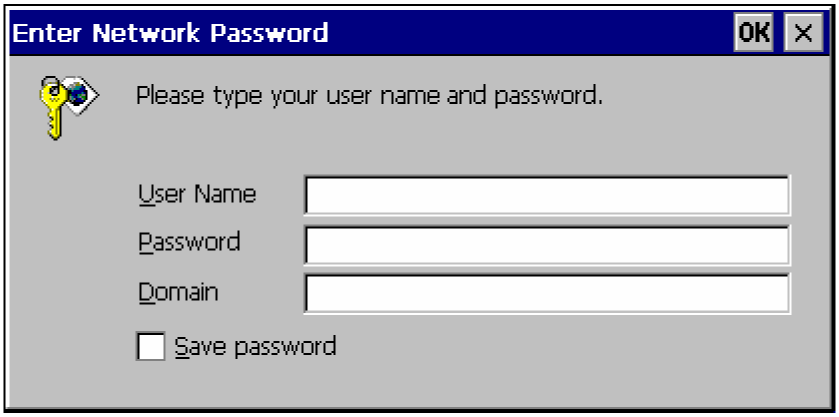
When first configuring and authenticating, do not validate the server certificate. This allows the user authentication to be tested. When user authentication is successful, return to this screen and validate the server certificate as shown later in this section.

Check the Always try to resume secure session box.

Note: This box must be checked for the LXE device to roam from one AP to another AP.

Click the OK button.

The login screen appears for logging into the wireless network.



Enter Network Password

Please type your user name and password.

User Name

Password

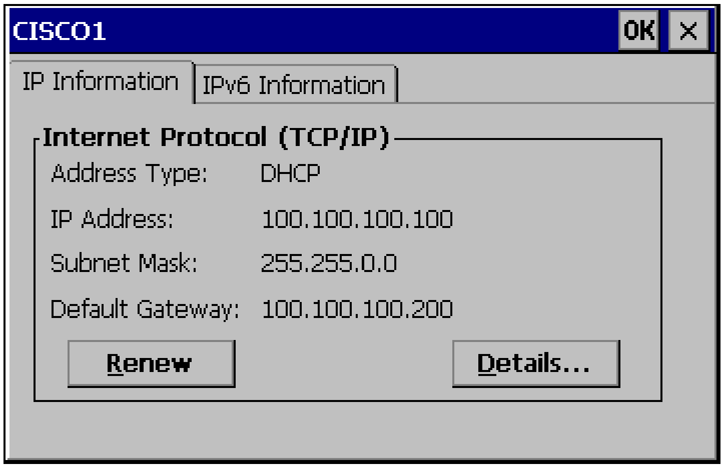
Domain

□ Save password

Figure 5-51 Login Screen

Enter valid user credentials.

Once authenticated click the IP Information tab



CISCO1

IP Information | IPv6 Information

Internet Protocol (TCP/IP)

Address Type: DHCP

IP Address: 100.100.100.100

Subnet Mask: 255.255.0.0

Default Gateway: 100.100.100.200

Figure 5-52 IP Information Tab

The device displays the IP address given by the DHCP server.

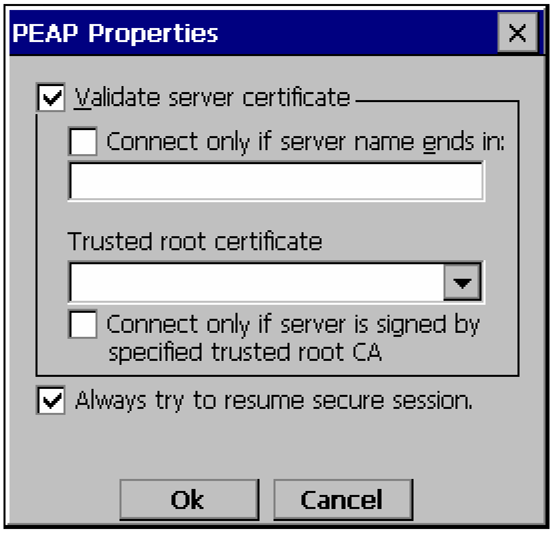
Now go back and authenticate the server.

Server Authentication

To validate the server certificate, the root CA certificate must be installed. For instructions for installing, see “Installing a Root CA Certificate” in this chapter. The RADIUS server certificate is not required, only the root CA which issued the server certificate.

Navigate to the Wireless Network Properties configuration screen.

Click the Properties button.



PEAP Properties

☑ Validate server certificate

□ Connect only if server name ends in:

Trusted root certificate

□ Connect only if server is signed by specified trusted root CA

☑ Always try to resume secure session.

Figure 5-53 PEAP Properties, Validate Server Certificate

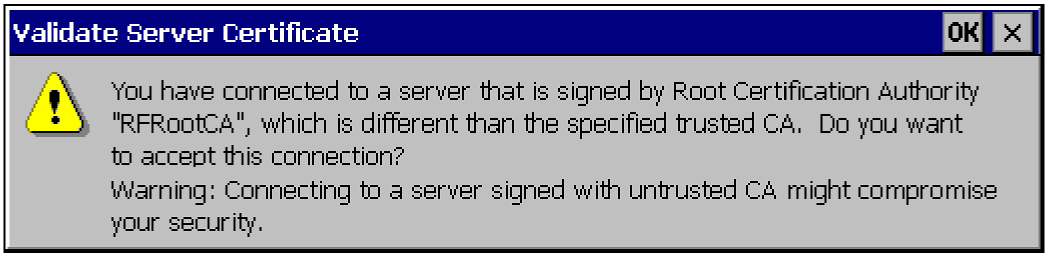
Check the Validate server certificate box.

Click OK to dismiss the configuration boxes.

When the login box appears enter valid user credentials.

It is possible for to be prompted to accept a Root CA certificate when using PEAP/GTC.

If the trusted root certificate box (as shown in the previous figure) is blank the user will be prompted to accept the Root CA certificate by name as shown below.



Validate Server Certificate

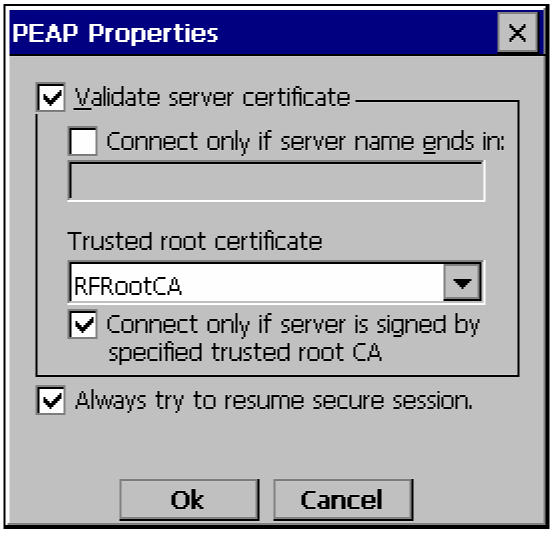
You have connected to a server that is signed by Root Certification Authority "RFRootCA", which is different than the specified trusted CA. Do you want to accept this connection?

Warning: Connecting to a server signed with untrusted CA might compromise your security.

Figure 5-54 Server Connection Warning

If this is the correct server certificate Root CA, click OK. If not, install the correct Root CA as described in “Installing a Root CA Certificate” in this chapter .

By clicking OK, the Trusted root certificate box is filled in on the properties window.


PEAP Properties

☑ Validate server certificate

□ Connect only if server name ends in:

Trusted root certificate

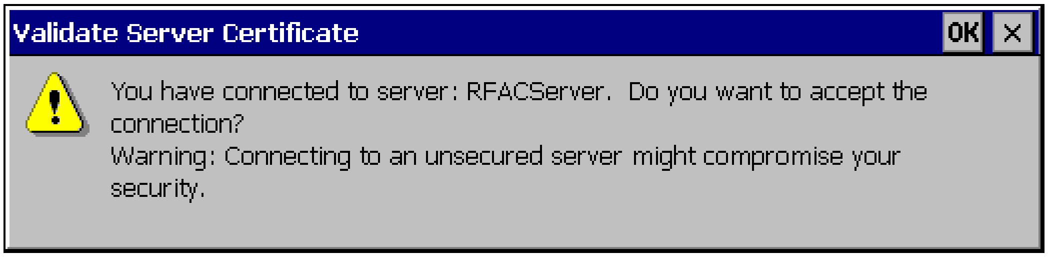
RFRootCA

☑ Connect only if server is signed by specified trusted root CA

☑ Always try to resume secure session.

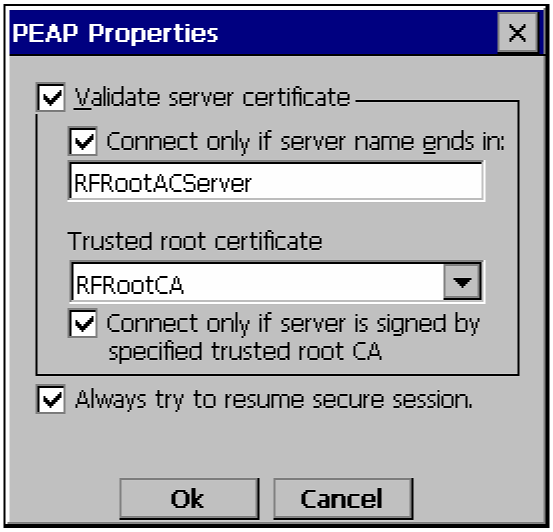
Figure 5-55 PEAP Properties, Trusted Root Certificate

The same thing can be done for the Connect only if server name ends in field. Check the box and leave the field blank. A prompt window will appear asking for confirmation of the correct server name.


Validate Server Certificate

You have connected to server: RFACServer. Do you want to accept the connection?
Warning: Connecting to an unsecured server might compromise your security.

Figure 5-56 Accept Server Connection Warning



☑ Validate server certificate

☑ Connect only if server name ends in:

RFRootACServer

Trusted root certificate

RFRootCA

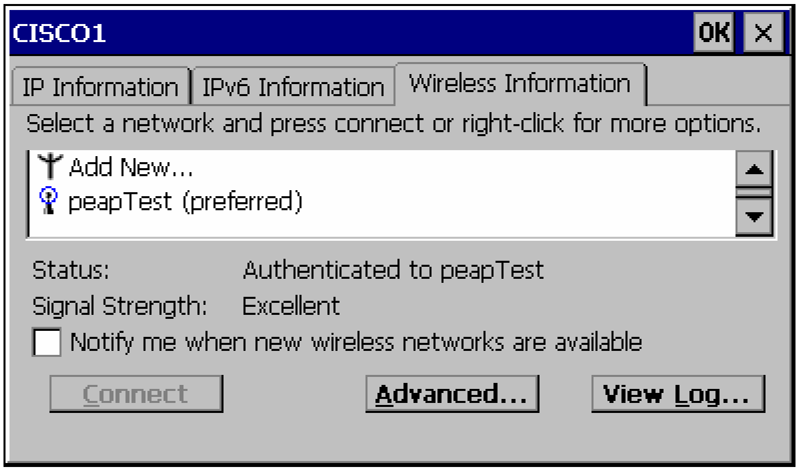
☑ Connect only if server is signed by specified trusted root CA

☑ Always try to resume secure session.

Figure 5-57 PEAP Properties, Connect Only If Server Name Ends In

If the ACS server name is correct, click the OK button and the server name field will be filled in with the correct server name.

The other option is to fill in the correct name



Select a network and press connect or right-click for more options.

Add New...
peapTest (preferred)

Status: Authenticated to peapTest

Signal Strength: Excellent

☐ Notify me when new wireless networks are available

Figure 5-58 Wireless Information, Authenticated

Once the authentication completes the status will change to Authenticated to <SSID> as shown.

Click on the IP Information tab and make sure there is a valid IP address as shown previously in this section.

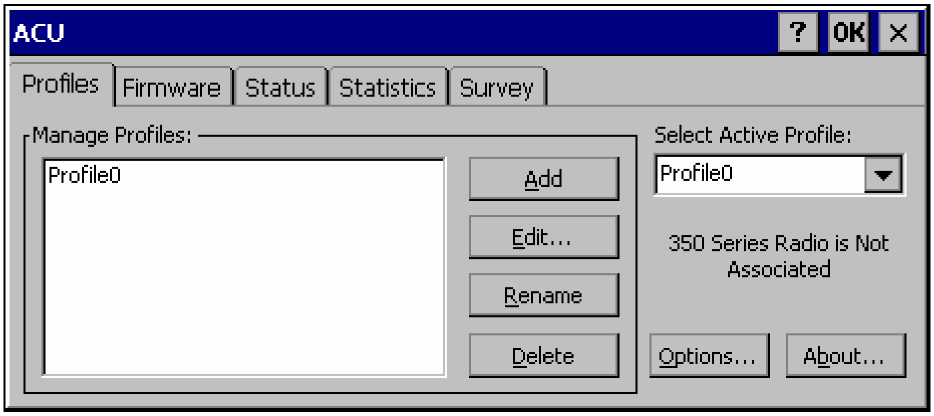
WPA/LEAP

LEAP is a Cisco proprietary authentication protocol and is not supported by the Microsoft supplicant. To configure the VX7 for WPA/LEAP, use the Cisco ACU installed during normal installation of the Cisco radio driver.

Cisco ACU

Start the Cisco ACU by clicking the icon on the desktop or navigate to **Start | Programs | Cisco | ACU**.

Click on the Profile tab.



Manage Profiles: Profile0

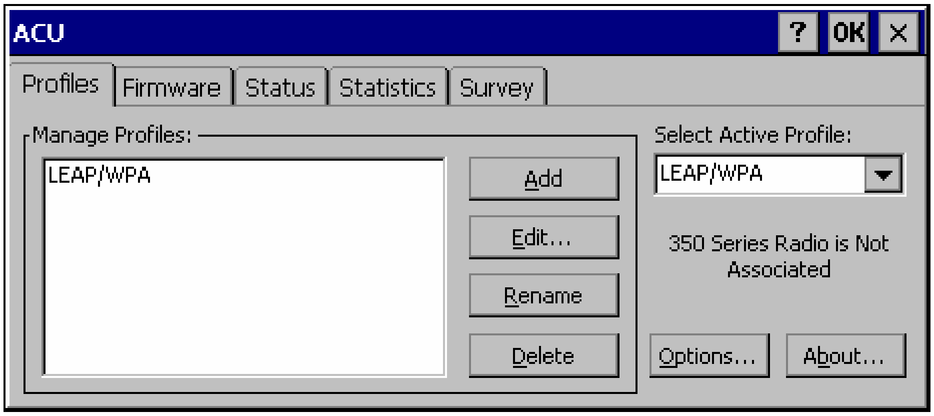
Select Active Profile: Profile0

350 Series Radio is Not Associated

Figure 5-59 ACU Profile Tab

Click the Rename button.

Name the profile



Manage Profiles: LEAP/WPA

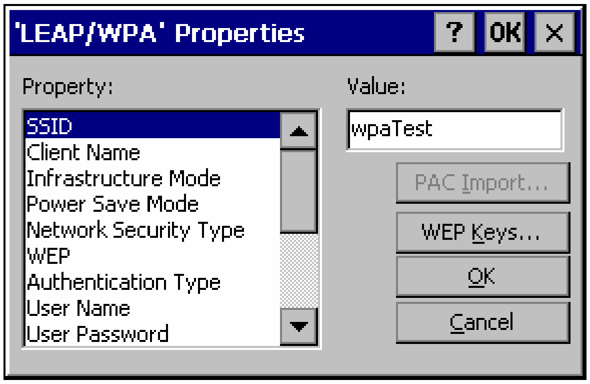
Select Active Profile: LEAP/WPA

350 Series Radio is Not Associated

Figure 5-60 Renaming Profile

Click the Edit button.

The profile properties screen is displayed.



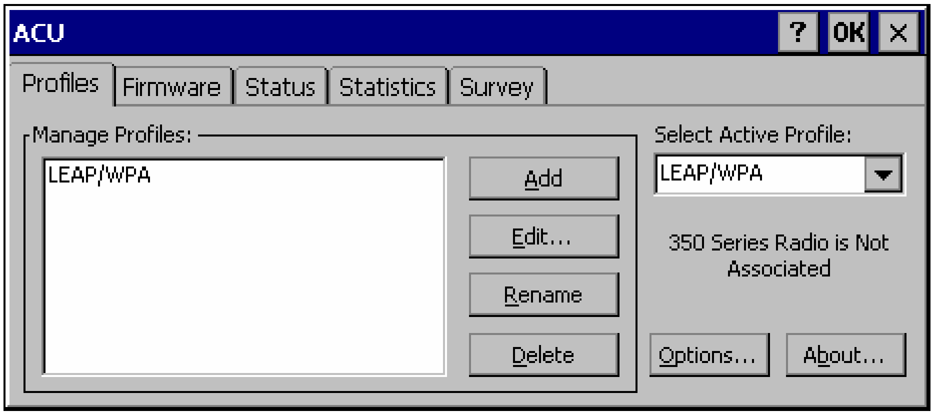
Value: wpaTest

Figure 5-61 Profile Properties Screen

Enter the SSID and Client Name in the correct fields.

Set the Network Security Type to LEAP(WPA).

Click the OK button.



Select Active Profile: LEAP/WPA

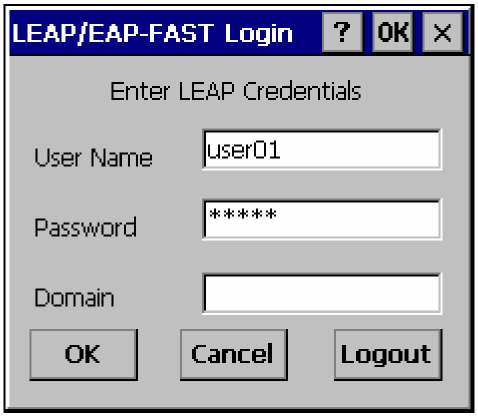
350 Series Radio is Not Associated

Figure 5-62 Select Profile

Use the drop down box to choose the profile just configured.

Click OK.

The VX7 associates and displays the sign on screen.



Enter LEAP Credentials

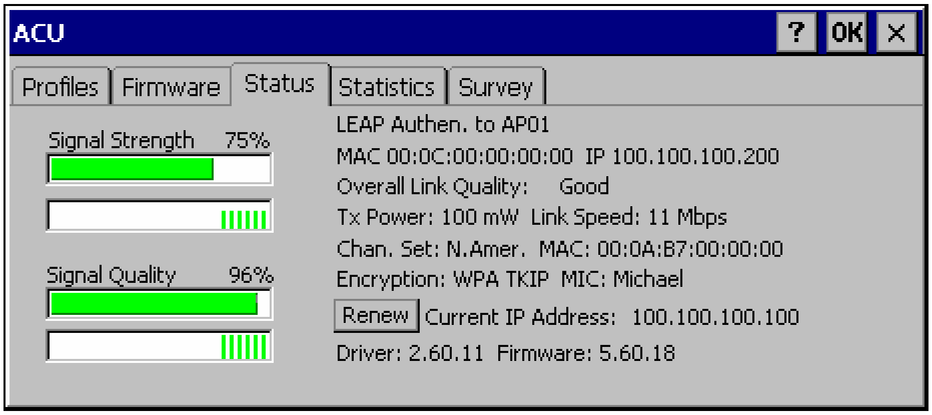
User Name: user01

Password: *****

Domain:

Figure 5-63 Login Screen

Click the Status tab to display status.



LEAP Authen. to AP01
MAC 00:0C:00:00:00:00 IP 100.100.100.200
Overall Link Quality: Good
Tx Power: 100 mW Link Speed: 11 Mbps
Chan. Set: N.Amer. MAC: 00:0A:B7:00:00:00
Encryption: WPA TKIP MIC: Michael
Current IP Address: 100.100.100.100
Driver: 2.60.11 Firmware: 5.60.18

Figure 5-64 ACU Status Tab

EAP-TLS Authentication Configuration

To authenticate using the EAP-TLS protocol you need a user certificate file and a private key file. Once you have the user certificate files run the certificate installer from the Microsoft control panel. For EAP-TLS it does not matter which Cisco cab file is installed.

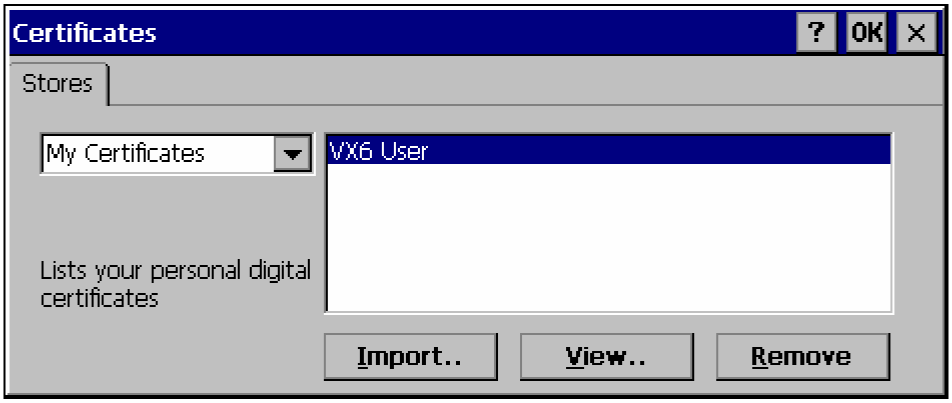
Note: It is important that the date is correct on the device when using any type of certificate. Certificates are date sensitive and if the date is not correct authentication will fail.

User Certificate

To check if a user certificate is installed navigate to **Start | Control Panel | Certificates**.

Set the drop down box to "My Certificates" as shown below.

The correct user certificate should be shown in the right pane.


Certificates

Stores

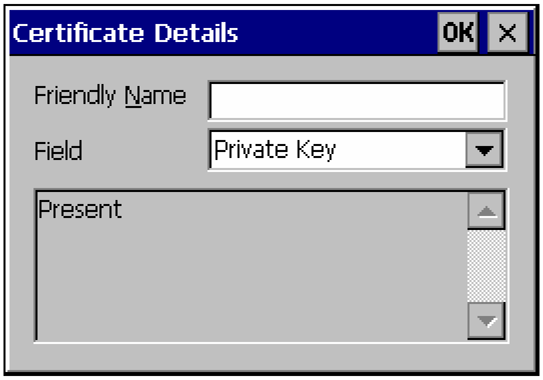
My Certificates

VX6 User

Lists your personal digital certificates

Figure 5-65 Certificate Stores

Click the View button.


Certificate Details

Friendly Name

Field: Private Key

Present

Figure 5-66 View Certificate Details

Set the Field to Private Key

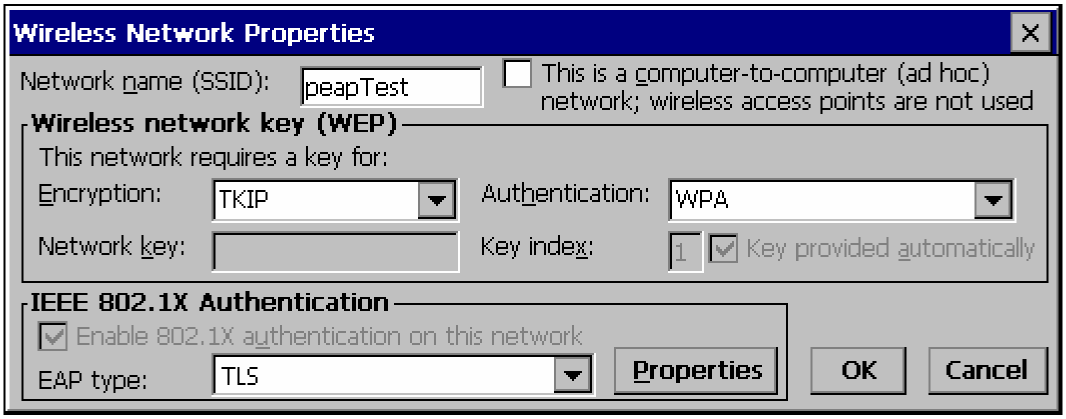
Make sure the private key is Present.

If it is not present, install the private key file.

If there is no user certificate refer to "User Certificates", earlier in this chapter, to acquire a user certificate and private key file.

Setting EAP/TLS Parameters

With the radio parameters configured (see "Wireless Network Configuration") set the EAP type to TLS as shown.



Wireless Network Properties

Network name (SSID): peapTest

□ This is a computer-to-computer (ad hoc) network; wireless access points are not used

Wireless network key (WEP)

This network requires a key for:

Encryption: TKIP

Authentication: WPA

Network key:

Key index: 1

☑ Key provided automatically

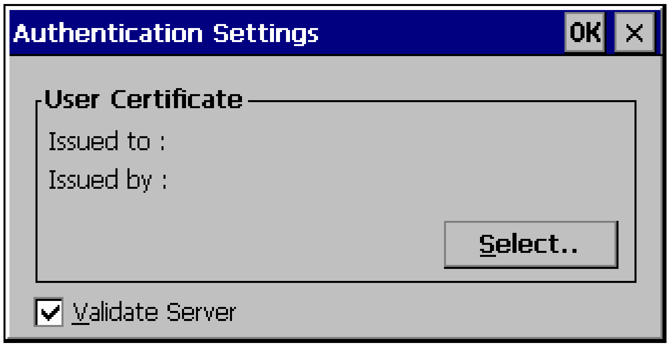
IEEE 802.1X Authentication

☑ Enable 802.1X authentication on this network

EAP type: TLS

Figure 5-67 EAP/TLS Configuration

Click the Properties button.



Authentication Settings

User Certificate

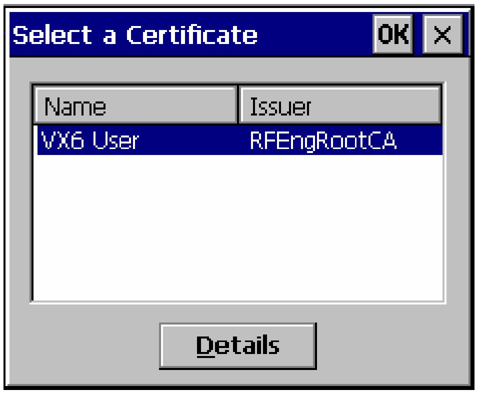
Issued to :

Issued by :

☑ Validate Server

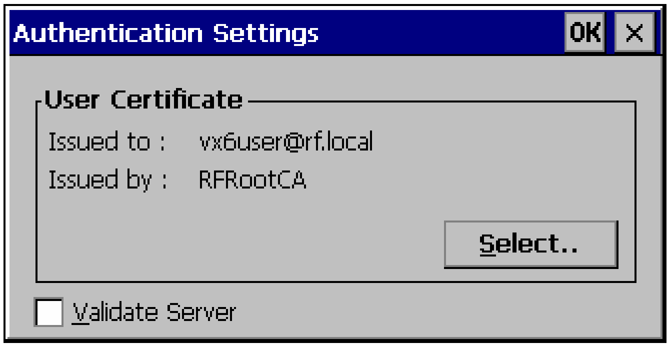
Figure 5-68 Authentication Settings

Click the Select button to choose the user certificate.



Name	Issuer
VX6 User	RFEngRootCA

Figure 5-69 Select Certificate



User Certificate

Issued to : vx6user@rf.local

Issued by : RFRootCA

□ Validate Server

Figure 5-70 Authentication Settings, Certificate Details

Do not check the Validate server certificate box. This allows the user to be authenticated as the first step.

When the user certificate successfully authenticates, come back to this screen and validate the server certificate as described in the next section.

Click the OK button to dismiss the configuration screens.

When the radio re-connects the user is authenticated with the user certificate.

If the user does not authenticate, recheck the user certificate and the date on the computer.

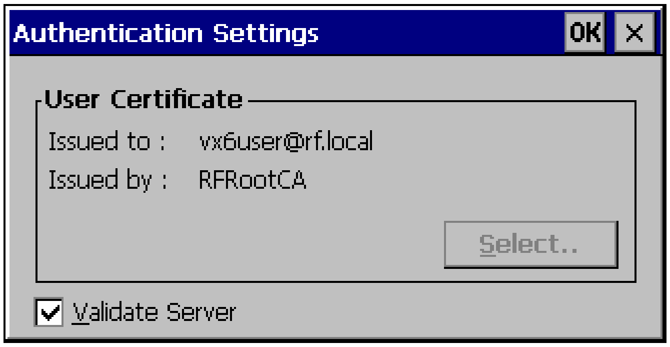
Validating the Server Certificate

Before validating the server certificate, make sure the Root CA certificate is installed on the VX7.

Navigate to the Wireless Network Properties configuration screen.

Click the Properties button.

Check the Validate server box as shown below.



Authentication Settings

User Certificate

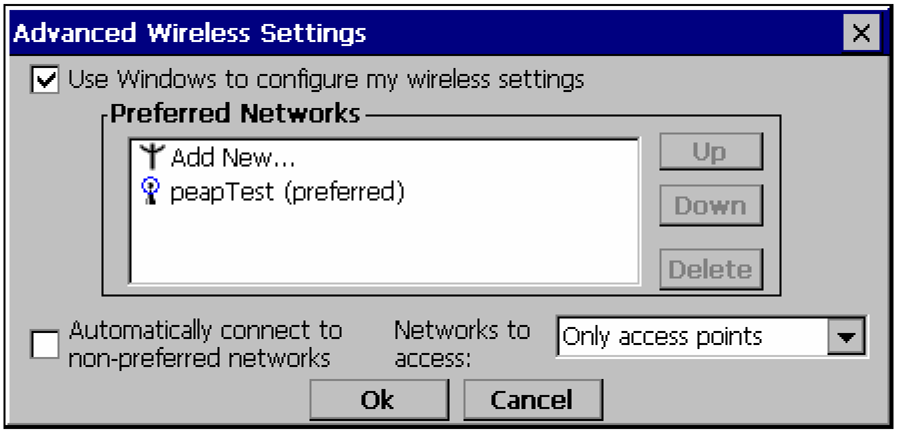
Issued to : vx6user@rf.local

Issued by : RFRootCA

☑ Validate Server

Figure 5-71 Validate Server

Click OK to dismiss the configuration boxes.



Advanced Wireless Settings

☑ Use Windows to configure my wireless settings

Preferred Networks

- Add New...
- peapTest (preferred)

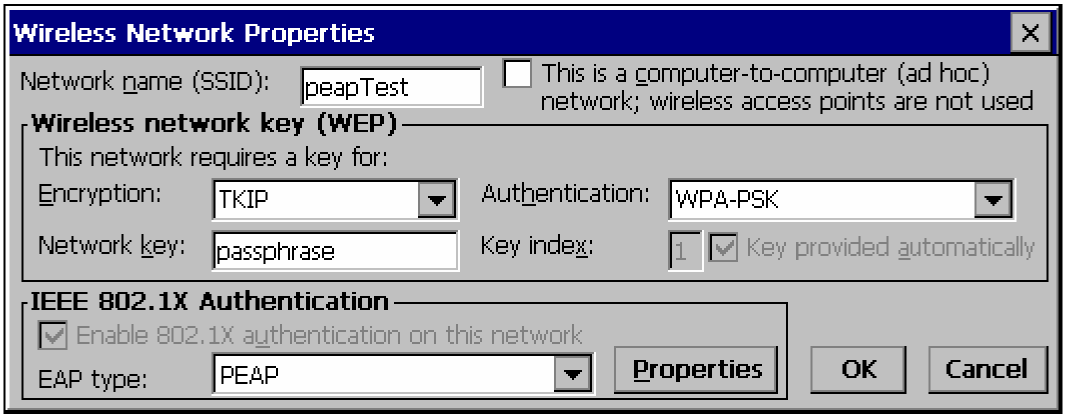
□ Automatically connect to non-preferred networks

Networks to access: Only access points

Figure 5-72 SSID Authenticated

Once the authentication completes the status changes to show the VX7 has authenticated to <SSID> as shown above.

WPA PSK Configuration



Wireless Network Properties

Network name (SSID): peapTest

□ This is a computer-to-computer (ad hoc) network; wireless access points are not used

Wireless network key (WEP)

This network requires a key for:

Encryption: TKIP

Authentication: WPA-PSK

Network key: passphrase

Key index: 1 ☑ Key provided automatically

IEEE 802.1X Authentication

☑ Enable 802.1X authentication on this network

EAP type: PEAP

Figure 5-73 WPA PSK Configuration

Configure the Wireless Network Settings as described in “Wireless Network Settings”, earlier in this chapter.

Change the Network Authentication to WPA-PSK.

Enter an ASCII network key in the text field. Hex keys do not work in the Microsoft Zero Config utility at this time.

There is no server authentication when using WPA-PSK.

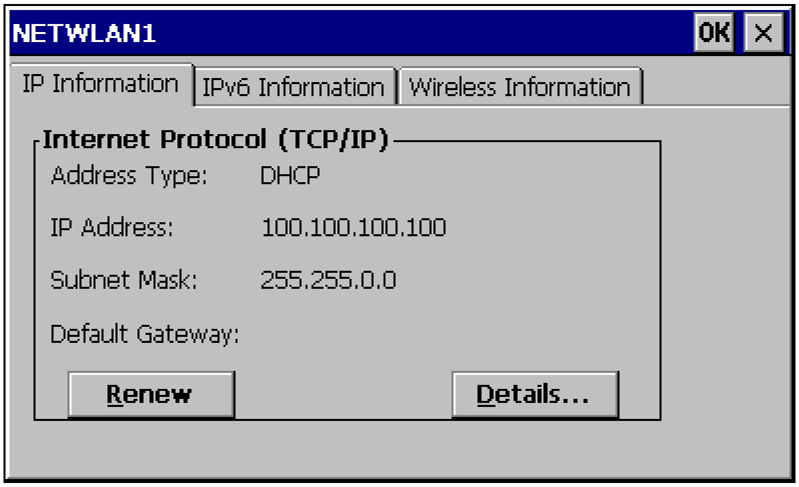
Click the OK button to complete configuration.

Symbol Radio

The Symbol radio is a 2.4GHz 802.11b radio. This radio supports no encryption and WEP.

Note: When making changes to profile parameters, the VX7 should be warmbooted afterwards.

Access: Double Tap the Network Connected Icon in the Status Bar



Internet Protocol (TCP/IP)

Address Type: DHCP

IP Address: 100.100.100.100

Subnet Mask: 255.255.0.0

Default Gateway:

Figure 5-74 Symbol NETWLAN Screen

IP Information Tab

After the IP Address has been assigned to the VX7, tap the Renew button to renew the IP address if necessary.

Tap the Details button to view the Network Connection details.

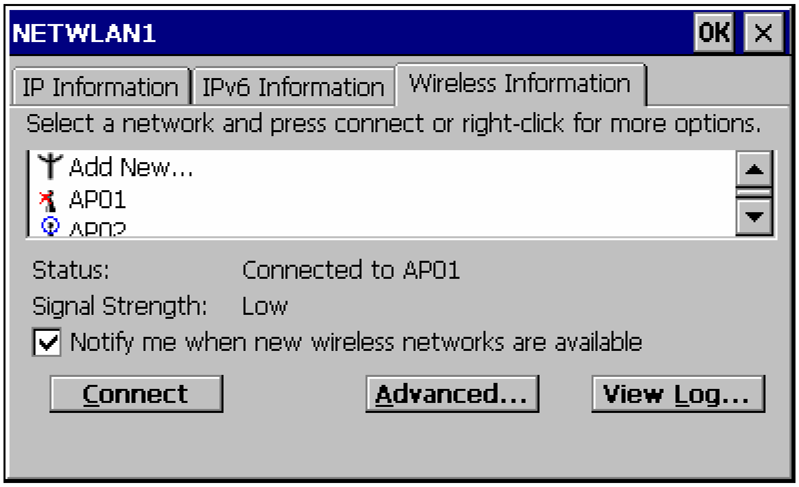
IPv6 Information Tab

This is the TCP/IPv6 information screen. The contents cannot be edited by the user.

Note: IPv6 can be disabled. Please see "Configuring IPv6 Broadcast Messages", earlier in this chapter.

Wireless Information Tab

Factory Default Settings	
Wireless Information tab	
Notify when new networks available	Enabled
Advanced Button	
Use Windows to configure wireless settings	Enabled
Automatically connect to non-preferred networks	Disabled
Networks to access (Only APs, Only comp-to-comp)	All available
Encryption (WEP, TKIP)	WEP
Authentication (WPA, Open, Shared, WPA-PSK)	WPA
Ad hoc network	Disabled
Key provided automatically	Enabled
Enable 802.1X authentication	Enabled
EAP Type (MDF-Challenge, PEAP, TLS)	TLS



Select a network and press connect or right-click for more options.

Status: Connected to AP01

Signal Strength: Low

☑ Notify me when new wireless networks are available

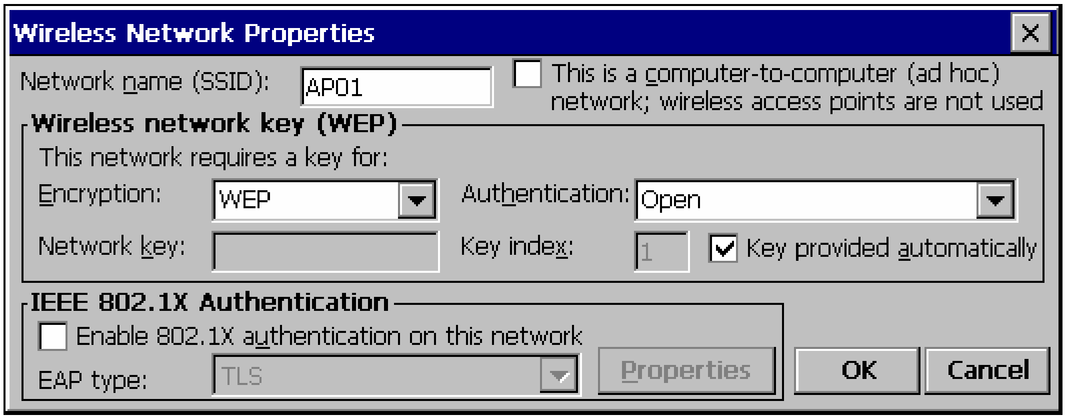
Figure 5-75 Symbol Wireless Information Tab

View Log

Displays the logon/connection data for the current network connection.

Add a new connection

Select **Add New**. Enter the SSID in the **Network Name** text box.



Network name (SSID): AP01

□ This is a computer-to-computer (ad hoc) network; wireless access points are not used

Wireless network key (WEP)

This network requires a key for:

Encryption: WEP

Authentication: Open

Network key:

Key index: 1

☑ Key provided automatically

IEEE 802.1X Authentication

□ Enable 802.1X authentication on this network

EAP type: TLS

Figure 5-76 Symbol Wireless Network Properties

Disable WEP

- If WEP is to be disabled, tap the down arrow in the **Authentication** drop down box. Select **Open**.
- Tap the down arrow in the **Encryption** drop down box. Tap **Disabled** and WEP is disabled.
- Tap the **OK** button to return to the **Wireless Information** tab.

Enable WEP

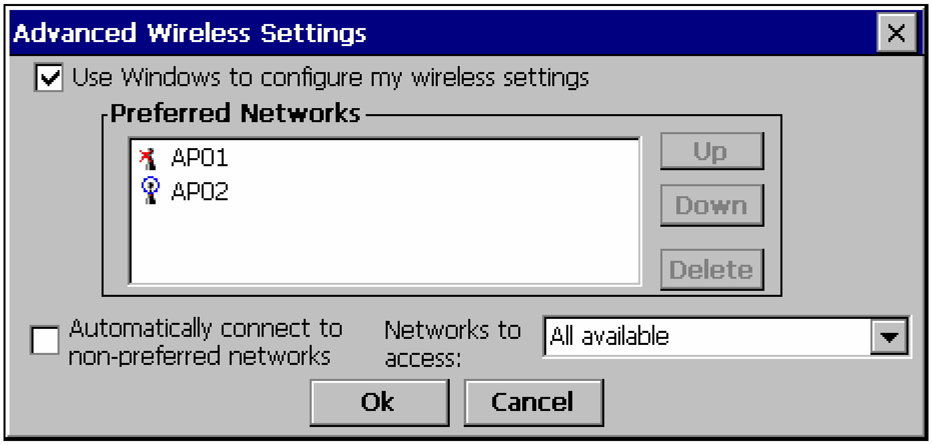
- Tap the down arrow in the **Authentication** drop down box.
- Tap the **WEP Authentication** protocol.
- If the key is provided automatically by your network, check the “**Key provided automatically**” checkbox.
- If you wish to enter your Authentication key, uncheck the “**Key provided automatically**” checkbox and enter the Network Key in the **Network Key** text box.
- Tap the **OK** button to return to the **Wireless Information** tab.

Continue

Tap the **Advanced** … button on the Wireless Information Tab. Make sure there is a checkmark in the "**Use Windows to configure my wireless settings**" checkbox. Make sure there is ***no*** checkmark in the "**Automatically connect to non-preferred networks**" checkbox.

Tap **OK** to return to the **Wireless Information** tab.

Tap the **Connect** button.



Advanced Wireless Settings

☑ Use Windows to configure my wireless settings

Preferred Networks

AP01
AP02

□ Automatically connect to non-preferred networks

Networks to access: All available

Figure 5-77 Symbol Advanced Wireless Settings

To access NETWLAN1 Properties again, double tap the **Network Connected icon** in the Toolbar.

Select a User Certificate

12. Select Wireless Information Tab
13. Select a network by double tapping the network name.
14. In the IEEE 802.1X Authentication box, enable 802.1X authentication
15. Select an EAP type
16. Tap the Properties button. Validate Server is enabled by default.
17. At the Authentication Settings display, tap the Select button to choose a User Certificate.

Certificates

Root Certificates

Generating a Root CA Certificate

📖	Please refer to the “LXE Security Primer” for more information on obtaining and installing root certificates.

The easiest way to get the root CA certificate is to use a browser on a PC to navigate to the CA. To request the root CA certificate, open a browser to

http://<CA IP address>/certsrv.

Sign into the CA with any valid username and password.

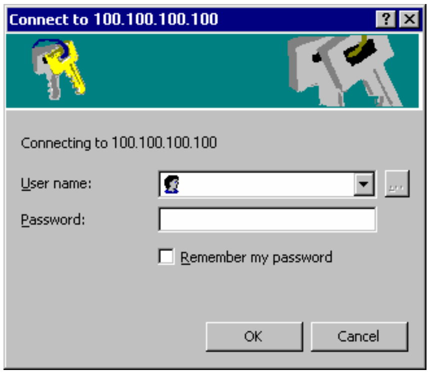
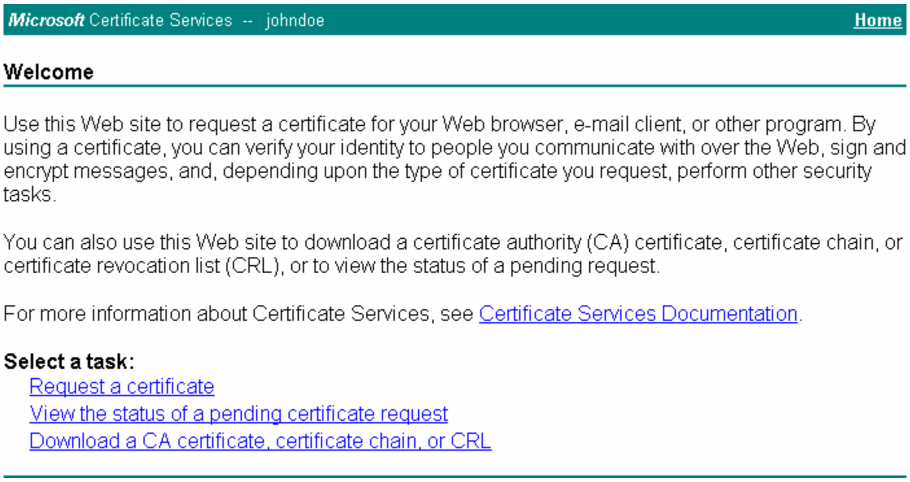


Figure 5-78 Logon to Certificate Authority



Microsoft Certificate Services -- johndoe **Home**

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Certificate Services, see Certificate Services Documentation.

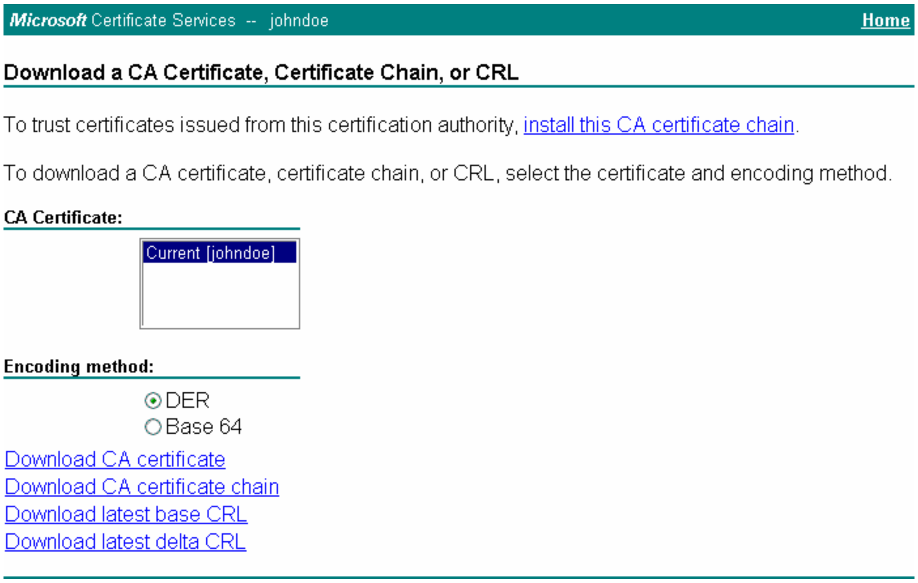
Select a task:

Request a certificate
View the status of a pending certificate request
Download a CA certificate, certificate chain, or CRL

Figure 5-79 Certificate Services Welcome Screen

Click the **Download a CA certificate, certificate chain or CRL** link.

Make sure the correct root CA certificate is selected in the list box.



Microsoft Certificate Services -- johndoe

Home

Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from this certification authority, install this CA certificate chain.

To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.

CA Certificate:

Current [johndoe]

Encoding method:

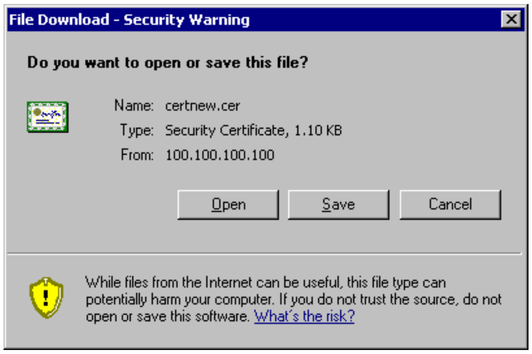
● DER
○ Base 64

Download CA certificate
Download CA certificate chain
Download latest base CRL
Download latest delta CRL

Figure 5-80 Download CA Certificate Screen

Click the DER button.

To download the CA certificate, click on the **Download CA certificate** link.



File Download - Security Warning

Do you want to open or save this file?

Name: certnew.cer
Type: Security Certificate, 1.10 KB
From: 100.100.100.100

While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not open or save this software. What's the risk?

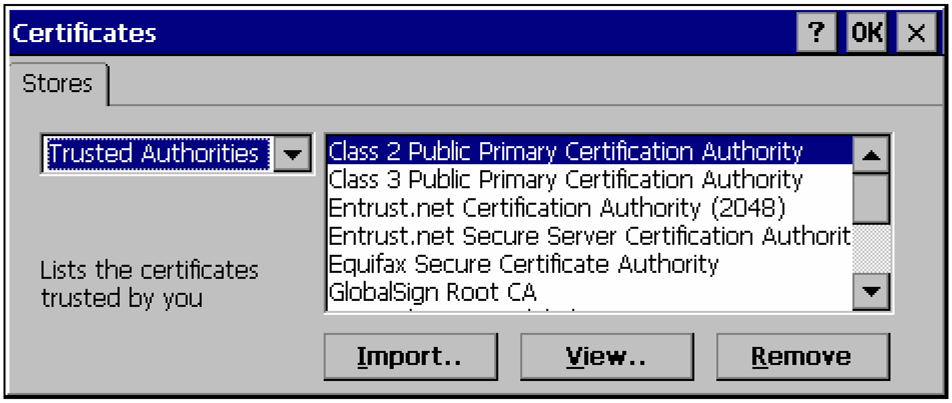
Figure 5-81 Download CA Certificate Screen

Click the Save button and save the certificate. Make sure to keep track of the name and location of the certificate.

Installing a Root CA Certificate

Note: This section is used for Cisco radios only. Summit radios do not use the Windows certificate store. Instead, copy the certificate to the \System folder for use with a Summit radio.

Copy the certificate file to the VX7. Import the certificate by navigating to **Start | Control Panel | Certificates**.



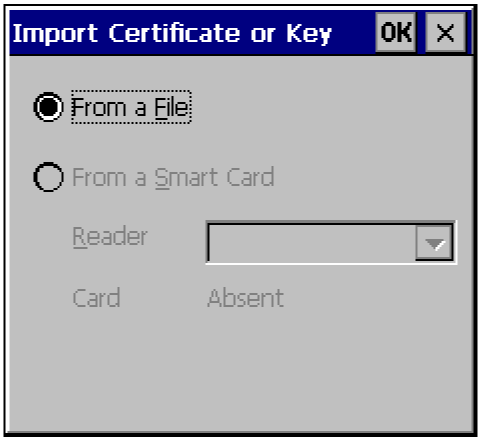
Trusted Authorities

Class 2 Public Primary Certification Authority
Class 3 Public Primary Certification Authority
Entrust.net Certification Authority (2048)
Entrust.net Secure Server Certification Authorit
Equifax Secure Certificate Authority
GlobalSign Root CA

Lists the certificates trusted by you

Figure 5-82 Certificates

Click the "Import" button.



● From a File

○ From a Smart Card

Reader

Card Absent

Figure 5-83 Import Certificate

Make sure "From a File" is selected and click OK.

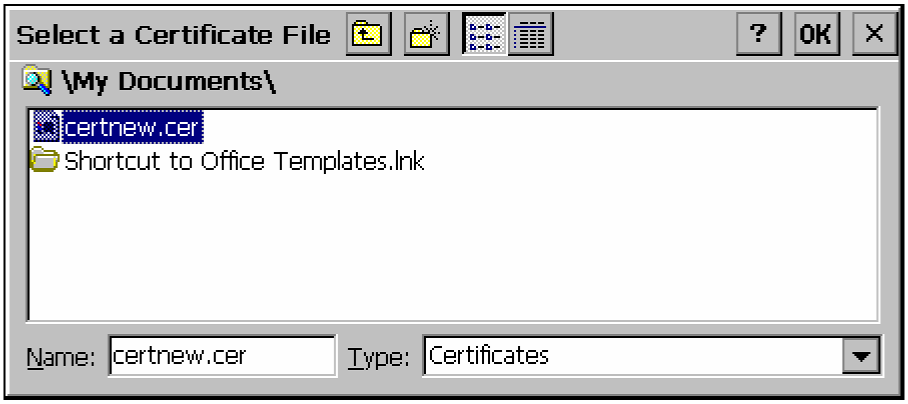
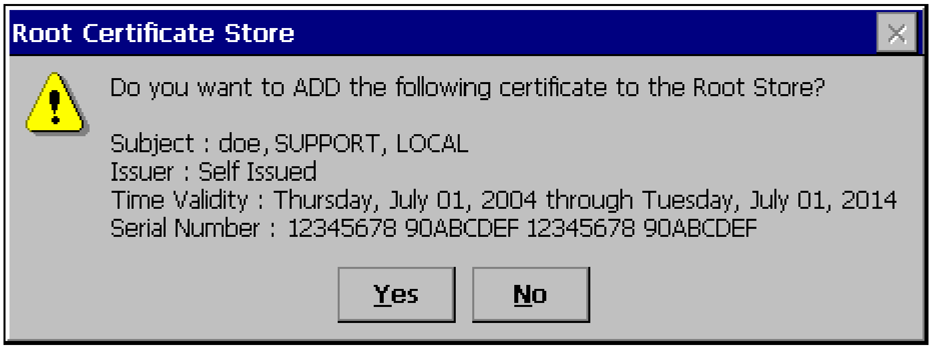


Figure 5-84 Browsing to Certificate Location

Using the explorer buttons, browse to the location where you copied the certificate, select the certificate desired and click OK.



Do you want to ADD the following certificate to the Root Store?

Subject : doe, SUPPORT, LOCAL
Issuer : Self Issued
Time Validity : Thursday, July 01, 2004 through Tuesday, July 01, 2014
Serial Number : 12345678 90ABCDEF 12345678 90ABCDEF

Figure 5-85 Certificate Import Confirmation

Click Yes to import the certificate.

Once the certificate is installed, return to the proper authentication section, earlier in this manual.

User Certificates

User certificates are only needed for EAP-TLS.

Generating a User Certificate

🕮	Please refer to the "LXE Security Primer" for more information on obtaining and installing user certificates.

The easiest way to get the user certificate is to use a browser on a PC to navigate to the CA. To request the user certificate, open a browser to

http://<CA IP address>/certsrv.

Sign into the CA with the username and password of the person who will be logging into the mobile device.

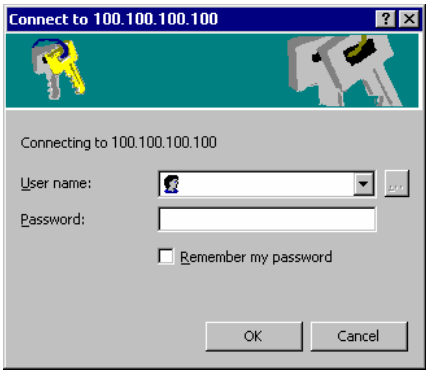
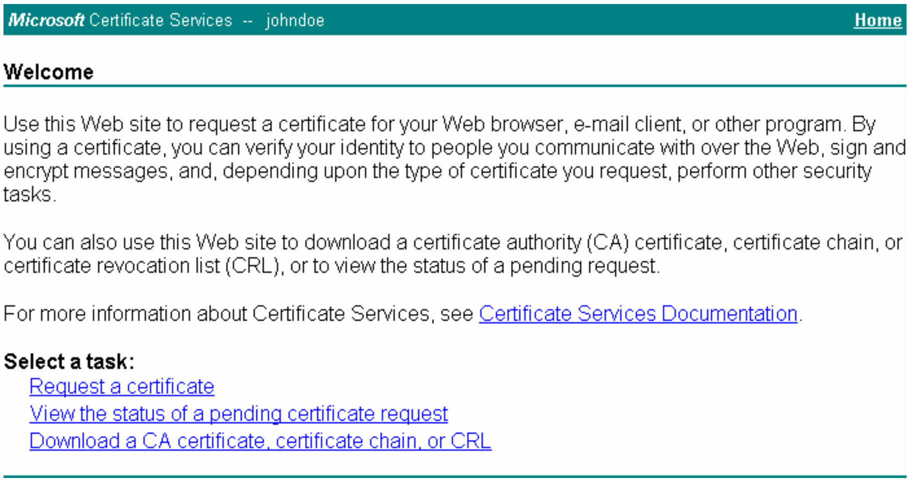


Figure 5-86 Logon to Certificate Authority

This process saves a user certificate and a separate private key file. Windows CE equipped devices such as the VX7 require the private key to be saved as a separate file rather than including the private key in the user certificate.



Microsoft Certificate Services -- johndoe **Home**

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

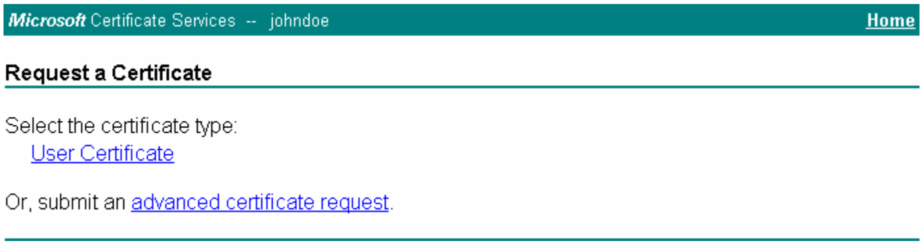
You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Certificate Services, see Certificate Services Documentation.

Select a task:
Request a certificate
View the status of a pending certificate request
Download a CA certificate, certificate chain, or CRL

Figure 5-87 Certificate Services Welcome Screen

Click the **Request a certificate** link.



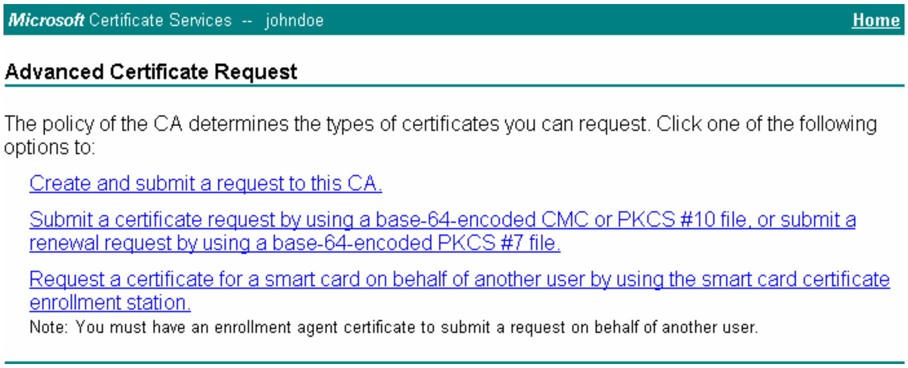
Request a Certificate

Select the certificate type:
User Certificate

Or, submit an advanced certificate request.

Figure 5-88 Request a Certificate Screen

Click on the **advanced certificate request** link.



Advanced Certificate Request

The policy of the CA determines the types of certificates you can request. Click one of the following options to:

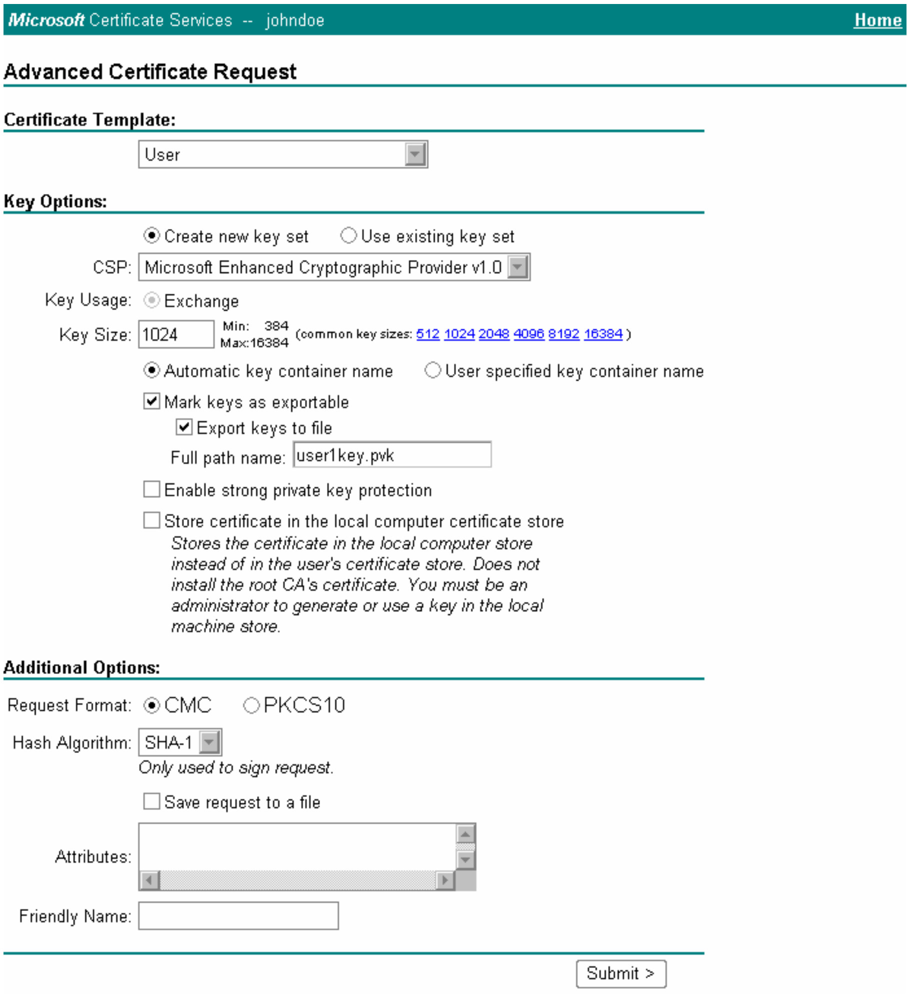
Create and submit a request to this CA.

Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.

Request a certificate for a smart card on behalf of another user by using the smart card certificate enrollment station.
Note: You must have an enrollment agent certificate to submit a request on behalf of another user.

Figure 5-89 Advanced Certificate Request Screen

Click on the **Create and submit a request to this CA** link.



Microsoft Certificate Services -- johndoe

Advanced Certificate Request

Certificate Template:

User

Key Options:

● Create new key set ○ Use existing key set

CSP: Microsoft Enhanced Cryptographic Provider v1.0

Key Usage: ● Exchange

Key Size: 1024 Min: 384 Max:16384 (common key sizes: 512 1024 2048 4096 8192 16384)

● Automatic key container name ○ User specified key container name

☑ Mark keys as exportable

☑ Export keys to file

Full path name: user1key.pvk

□ Enable strong private key protection

□ Store certificate in the local computer certificate store

Stores the certificate in the local computer store instead of in the user's certificate store. Does not install the root CA's certificate. You must be an administrator to generate or use a key in the local machine store.

Additional Options:

Request Format: ● CMC ○ PKCS10

Hash Algorithm: SHA-1

Only used to sign request.

□ Save request to a file

Attributes:

Friendly Name:

Figure 5-90 Advanced Certificate Details

For the Certificate Template, select “User”.

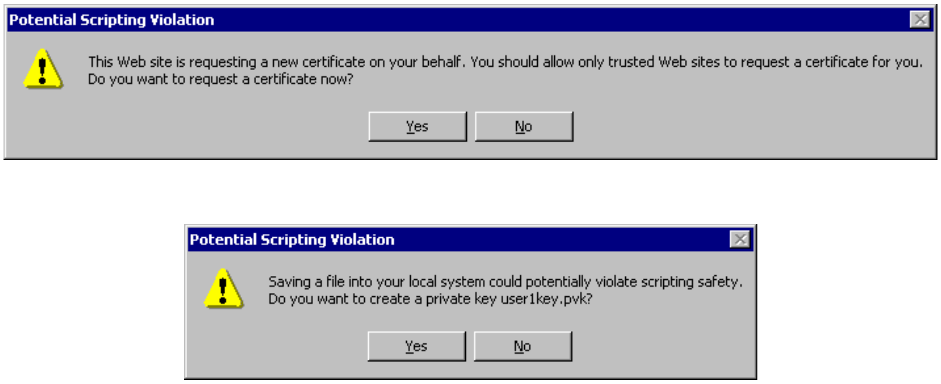
Check the “Mark keys as exportable” and the “Export keys to file” checkboxes.

Type the full path on the local PC where the private key is to be copied. Also specify the private key filename.

⚠	Be sure to note the name used for the private key file, for example VX7USER.PVK. The certificate file created later in this process must be given the same name, for example, VX7USER.CER.

DO NOT check to use strong private key protection.

Make any other desired changes and click the “Submit” button.



Potential Scripting Violation

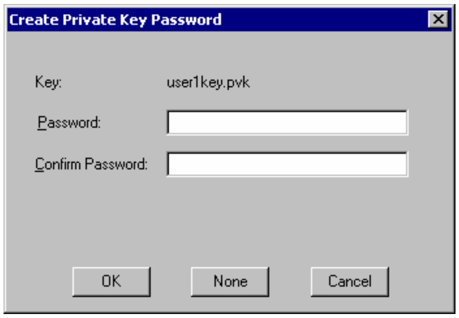
This Web site is requesting a new certificate on your behalf. You should allow only trusted Web sites to request a certificate for you. Do you want to request a certificate now?

Potential Scripting Violation

Saving a file into your local system could potentially violate scripting safety. Do you want to create a private key user1key.pvk?

Figure 5-91 Script Warnings

If any script notifications occur, click the “Yes” button to continue the certificate request.



Create Private Key Password

Key: user1key.pvk

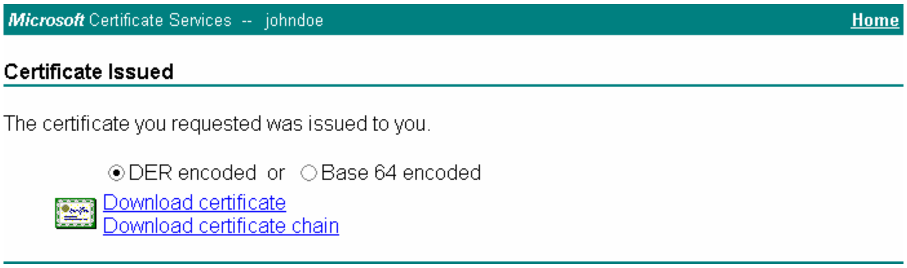
Password:

Confirm Password:

Figure 5-92 Script Warnings

When prompted for the private key password:

- Click “None” if you do not wish to use a password, *or*
- Enter and confirm your desired password then click “OK”.



Microsoft Certificate Services -- johndoe Home

Certificate Issued

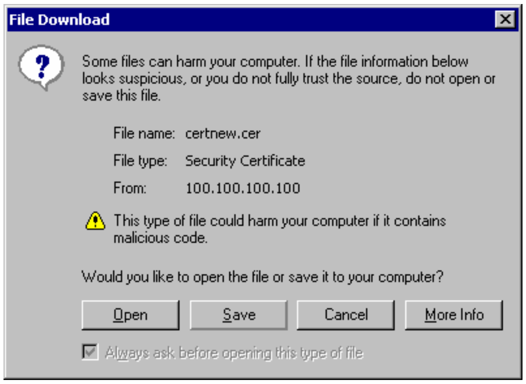
The certificate you requested was issued to you.

● DER encoded or ○ Base 64 encoded

Download certificate
Download certificate chain

Figure 5-93 Certificate Issued

Click the **Download certificate** link.



File Download

Some files can harm your computer. If the file information below looks suspicious, or you do not fully trust the source, do not open or save this file.

File name: certnew.cer
File type: Security Certificate
From: 100.100.100.100

This type of file could harm your computer if it contains malicious code.

Would you like to open the file or save it to your computer?

☑ Always ask before opening this type of file

Figure 5-94 Download Security Warning

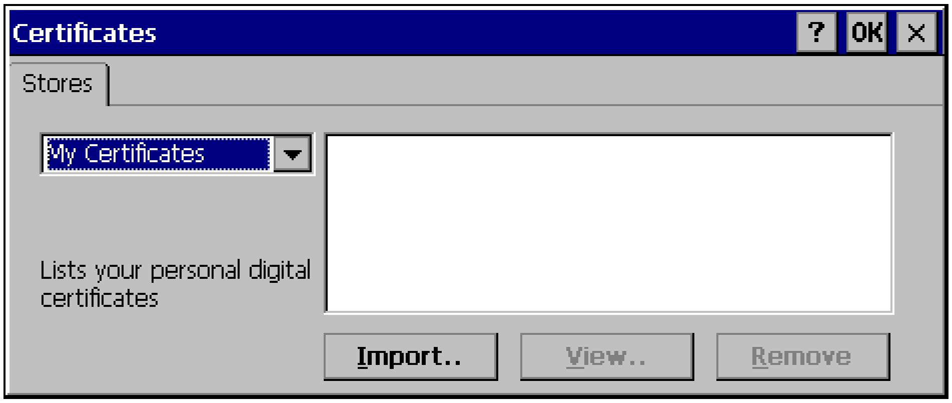
Click Save to download and store the user certificate to the PC. Make sure to keep track of the name and location of the certificate. The private key file is also downloaded and saved during this process.

⚠	Be sure use the same name for the certificate file as was used for the private key file. For example, it the private key was saved as VX7USER.PVK then the certificate file created must be given the same name, for example, VX7USER.CER.

Installing a User Certificate

Copy the certificate and private key files to the VX7. Import the certificate by navigating to **Start | Control Panel | Certificates**.

Select “My Certificates” from the pull down list.

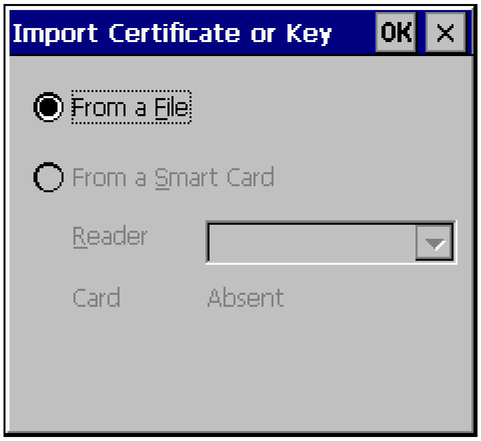


My Certificates

Lists your personal digital certificates

Figure 5-95 Certificates

Click the “Import” button.



● From a File

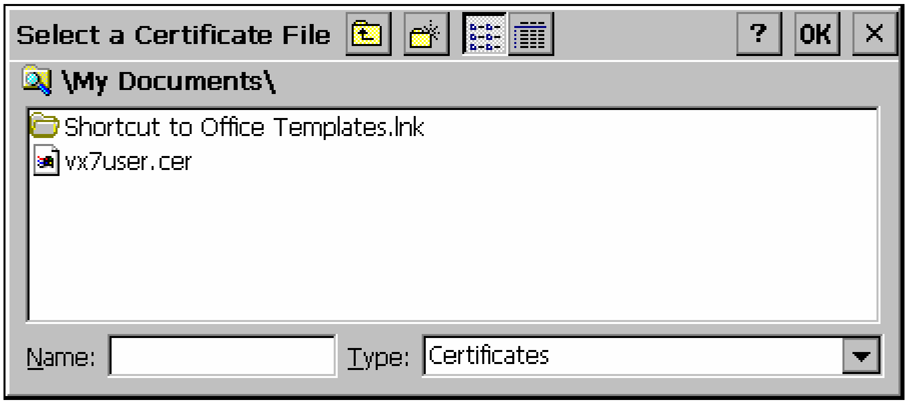
○ From a Smart Card

Reader

Card Absent

Figure 5-96 Import Certificate

Make sure “From a File” is selected and click OK.



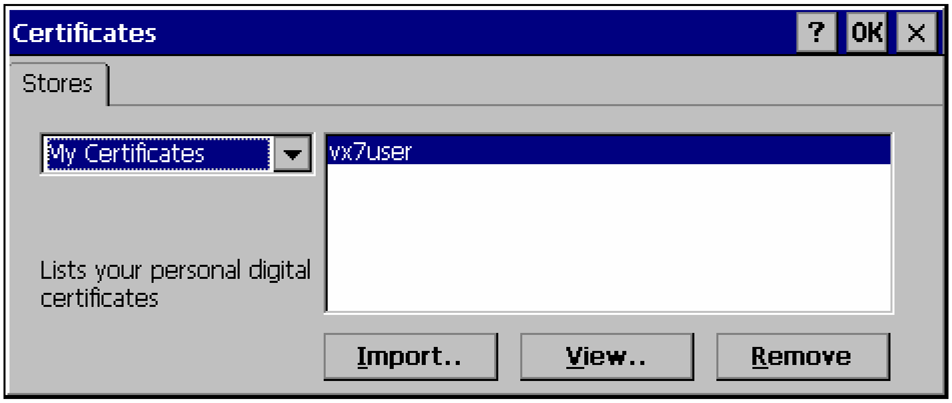
Name:

Type: Certificates

Figure 5-97 Browsing to Certificate Location

Using the explorer buttons, browse to the location where you copied the certificate, select the certificate desired and click OK.

The certificate is now shown in the list.



My Certificates

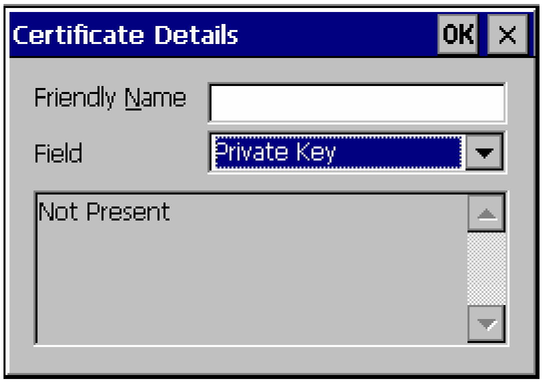
vx7user

Lists your personal digital certificates

Figure 5-98 Certificate Listing

With the certificate you just imported highlighted, click View.

From the Field pull down menu, select “Private Key.


Certificate Details

Friendly Name

Field: Private Key

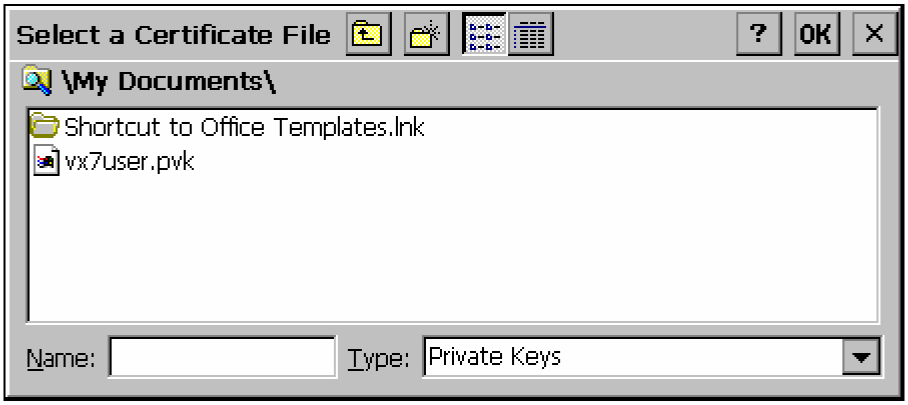
Not Present

Figure 5-99 Private Key Not Present

- If the private key is present, the process is complete.
- If the private key is not present, import the private key.

To import the private key, click OK to return to the Certificates screen.

Click import.


Select a Certificate File

\My Documents\

Shortcut to Office Templates.lnk
vx7user.pvk

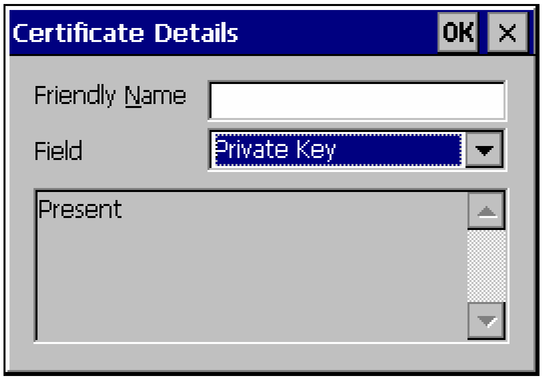
Name:

Type: Private Keys

Figure 5-100 Browsing to Private Key Location

Using the explorer buttons, browse to the location where you copied the private key file, change the Type pull down list to “Private Keys”, select the certificate desired and click OK. Enter the password for the certificate if appropriate.

Click on View to see the certificate details again.



Certificate Details

Friendly Name

Field: Private Key

Present

Figure 5-101 Private Key Present

The private key should now say present. If it does not, there is a problem. Possible items to check:

- Make sure the certificate was generated with a separate private key file, as shown earlier in this section. If the certificate was not generated with a separate private key file, generate a new certificate and follow the import process again.
- Make sure the certificate and private key file have the same name, for example vx7user.cer for the certificate and vx7user.pvk for the private key file. If the file names are not the same, rename the private key file and import it again.

Chapter 6 AppLock

Introduction

LXE's AppLock is designed to be run on LXE certified Windows CE based devices only. LXE loads the AppLock program as part of the LXE customer installation process.

Configuration parameters are specified by the AppLock Administrator for the mobile device end-user. AppLock is password protected by the Administrator.

End-user mode locks the end-user into the configured applications. The end user can still reboot the mobile device and respond to dialog boxes. The administrator-specified applications are automatically launched in the specified order and run in full screen mode when the device boots up.

When the mobile device is reset to factory default values, for example after a cold reset, the Administrator may need to reconfigure the AppLock parameters.

LXE has made the assumption, in this chapter, that the first user to power up a new mobile device is the system administrator.

Note: AppLock Administrator Control panel file Launch option does not inter-relate with similarly-named options contained in other LXE Control Panels.

*Note: A few applications do not follow normal procedures when closing. AppLock cannot prevent this type of application from closing, but is notified that the application has closed. For these applications, AppLock immediately restarts the application (see **Auto Re-Launch**) which causes the screen to flicker. If this type of application is being locked, the administrator should close all other applications before switching to end-user mode to minimize the screen flicker.*

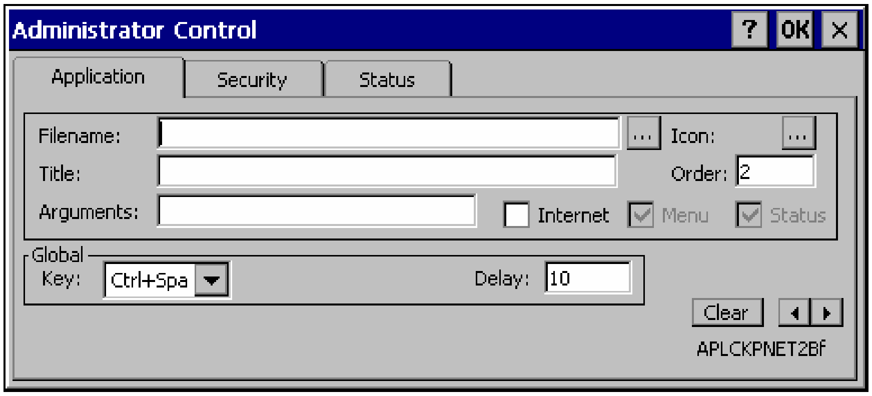
AppLock is updated periodically as new options become available. Contact your LXE representative for assistance, downloads and update availability.

Determining Your AppLock Version

Multi-Application AppLock

A mobile device running the Multi-Application version of AppLock becomes a dedicated, dual application device. Only the applications or features specified in the AppLock configuration by the Administrator are available to the end-user. This version offers a user-mode taskbar icon allowing the end-user to switch between user applications.

If your Administrator Control Panel has **Application**, **Security** and **Status** tabs, then the device has LXE Multi-Application AppLock installed. The Administrator can configure multiple applications to lock and the end user can swap between the applications.



Filename:
Icon:
Title:
Order: 2
Arguments:
☐ Internet ☑ Menu ☑ Status
Global
Key: Ctrl+Spa
Delay: 10
APLCKPNET2Bf

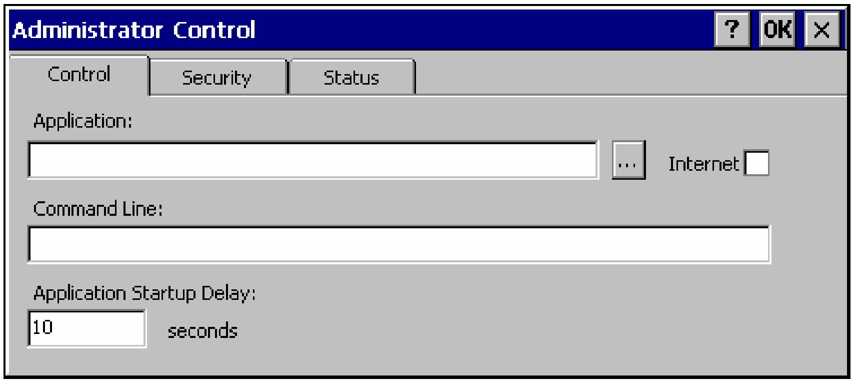
Figure 6-1 Multi-Application AppLock

The configuration instructions in this chapter are designed for users of Multi-Application AppLock.

Single Application AppLock

A mobile device running the Single Application version of AppLock becomes a dedicated, single application device. In other words, only the application or feature specified in the AppLock configuration by the Administrator is available to the user.

If your Administrator Control Panel has **Control**, **Security** and **Status** tabs, then the device has LXE's Single-Application AppLock installed. The Administrator can configure a single application to lock and the end user is limited to that application.



Application:

Internet □

Command Line:

Application Startup Delay:

10 seconds

Figure 6-2 Single-Application AppLock

Though this chapter is designed for users of the newer Multi-Application AppLock, the instructions may also be used to configure Single-Application AppLock with the following differences:

- The Control tab is used to specify the application to lock instead of the Application tab. While the Application tab contains provisions for multiple applications, the Control tab only allows the administrator to specify a single application.
- The section on End User Switching Technique does not apply to this version.
- Some configuration items may not be available.

Setup a New Device

LXE devices with the AppLock feature are shipped to boot in Administration mode with no default password, thus when the device is first booted, the user has full access to the device and no password prompt is displayed. After the administrator specifies the applications to lock, a password is assigned and the device is rebooted or the hotkey is pressed, the device switches to end-user mode.

Briefly, the process to configure a new device is as follows:

18. Connect an external power source to the device and press the Power button.
19. Adjust screen display, audio volume and other parameters if desired. Install accessories.
20. Tap **Start | Settings | Control Panel | Administration** icon.
21. Assign applications on the **Control** (single application) or **Application** (dual application) tab screen.
22. Assign a password on the Security tab screen.
23. Select a view level on the Status tab screen, if desired.
24. Tap OK
25. Press the hotkey sequence to launch AppLock and lock the configured application(s).
26. The device is now in end-user mode.

Administration Mode

Administration mode gives full access to the mobile device, hardware and software configuration options.

The administrator must enter a valid password (when a password has already been assigned) before access to Administration mode and configuration options are allowed. The administrator can configure the following options:

- Create/change the keystroke sequence to activate administrator access.
- Create/change the password for administrator access.
- Assign the name of the application, or applications, to lock.
- Select the command line of the application to lock.

In addition to these configuration options, the administrator can view and manage the status logs of AppLock sessions.

Administrator default values for this device:

Administrator Hotkey	**Shift+Ctrl+A**
Password	**none**
Application path and name	**none**
Application command line	**none**

End User Mode

End-user mode locks the end-user into the configured application or applications. The end user can still reboot and respond to dialog boxes. Each application is automatically launched and runs in full screen mode when the device boots up.

The user cannot unintentionally or intentionally exit the application nor can the end user execute any other applications. Normal application exit or switching methods and all Microsoft defined Windows CE key combinations, such as close (X) icon, File Exit, File Close, Alt-F4, Alt-Tab, etc. are disabled. The Windows CE desktop icons, menu bars, task bar and system trays are not visible or accessible. Task Manager is not available.

If the end-user selects File/Exit or Close from the applications menu bar, the menu is cleared and nothing else happens; the application remains active. Nothing happens when the end-user clicks on the Close icon on the application’s title bar and the application remains active.

Note: A few applications do not follow normal procedures when closing. AppLock cannot prevent this type of application from closing, but is notified that the application has closed. For these applications, AppLock immediately restarts the application which causes the screen to flicker. If this type of application is being locked, the administrator should close all other applications before switching to end user mode to minimize the screen flicker.

Windows accelerator keys such as Alt-F4 are disabled.

Passwords

A password must be configured. If the password is not configured, a new device switches into Administration mode without prompting for a password. In addition to the hotkey press, a mode switch occurs if inaccurate information has been configured or if mandatory information is missing in the configuration.

There are several situations that display a password prompt after a password has been configured.

If the configured hotkey is pressed, the password prompt is displayed. In this case the user has 30 seconds to enter a password. If a valid password is not entered within 30 seconds, the password prompt is dismissed and the device returns to end-user mode.

All other situations that present the password prompt do not dismiss the prompt -- this is because the other situations result in invalid end-user operation.

These conditions include:

- If inaccurate configuration information is entered by the administrator, i.e. an application is specified that does not exist.
- If the application name, which is mandatory for end-user mode, is missing in the configuration.
- Invalid installation of AppLock (e.g. missing DLLs).
- Corrupted registry settings.

To summarize, if an error occurs that prevents AppLock from switching to user mode, the password will not timeout and AppLock will wait until the correct password is entered.

Troubleshooting

Can’t locate the password that has been set by the administrator? Enter this LXE back door key sequence:

Ctrl+L Ctrl+X Ctrl+E

Or

Ctrl+5 Ctrl+9 Ctrl+3

End-User Switching Technique

Note: The touch screen must be enabled.

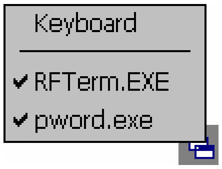


Figure 6-3 Switchpad Menu

A checkmark indicates applications currently active or available for Launching by the user. When Keyboard is selected, the VX7 default input method (Input Panel, Transcriber, or custom input method) is activated.

Using a Stylus Tap

When the mobile device enters end-user mode, a Switchpad icon (it looks like three tiny windows one above the other) is displayed in the taskbar. The taskbar is always visible on top of the application in focus.

When the user taps the Switchpad icon, a menu is displayed showing the applications available to the user. The user can tap an application name in the popup menu and the selected application is brought to the foreground. The previous application continues to run in the background. Stylus taps affect the application in focus only. When the user needs to use the Input Panel, they tap the Keyboard option. Input Panel taps affect the application in focus only.

The figure shown above is an example and is shown only to aid in describing how the user can switch between applications using a stylus. The switchpad lists user applications as well as the Keyboard option.

See Also: *Application Panel | Launch | Manual (Launch) and Allow Close*

Using the Switch Key Sequence

One switch key sequence (or hotkey) is defined by the administrator for the end-user to use when switching between locked applications. This is known as the **Activation key**. The Activation key is assigned by the Administrator using the Global Key parameter. When the switch key sequence is pressed on the keypad, the next application in the AppLock configuration is moved to the foreground and the previous application moves to the background. The previous application continues to run in the background. End-user key presses affect the application in focus only.

See Also: *Application Panel | Global Key*

Application Configuration

The default Administrator Hotkey sequence is **Shift+Ctrl+A.**

Administrator mode allows access to all features on the device. When the hotkey is pressed to switch into Administrator mode, a password prompt is displayed (if a password has been configured). A password must be entered within 30 seconds (and within three tries) or the password prompt is removed and the device remains in end-user mode with the focus returned to the locked application. Without entry of a valid password, the switch into Administrator mode will not occur.

Access: Settings | Control Panel | Administration icon

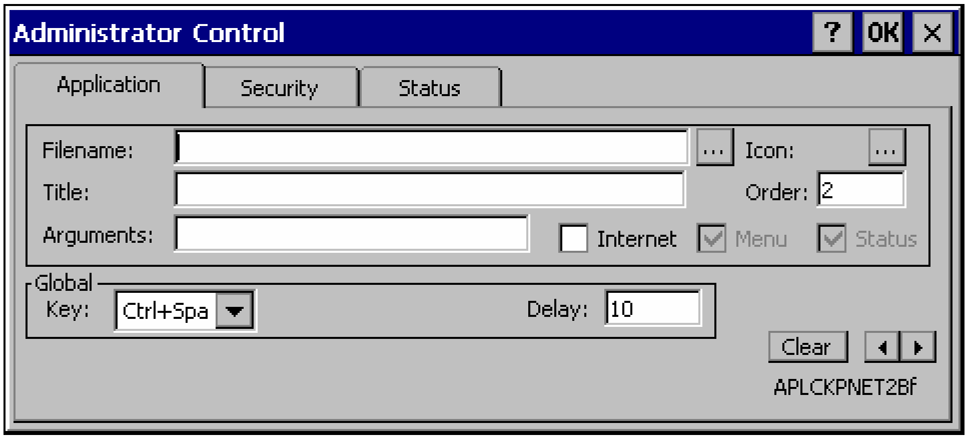
The password prompt is displayed if a password has been configured. When the valid password is entered, the Administration Control panel is displayed. When a valid password is not entered within 30 seconds, the user is returned to the System Control Panel.

If a password has not been configured, the Administrator Control panel is displayed.

Important: Before setting up multiple instances of the same application, make sure the targeted software application will allow two instances to run at the same time.

Application Panel

Note: Users of Single-Application AppLock have a Control tab instead of an Application tab. Some of the options in this section do not apply to the Control tab.



Order: 2

☐ Internet ☑ Menu ☑ Status

Key: Ctrl+Spa

Delay: 10

APLCKPNET2Bf

Figure 6-4 Application Panel

Note: If your Application Panel does not look like the figure shown above, you may have the Single Application version.

Single Application version.

Use the **Application** tab options to select the applications to launch when the device boots up in End-user Mode.

If no application is specified when the Administrator Control Panel is closed, the mobile device reboots into Administrator mode. If a password has been set, but an application has not been specified, the user will be prompted for the password before entering administration mode. The password prompt remains on the display until a valid password is entered.

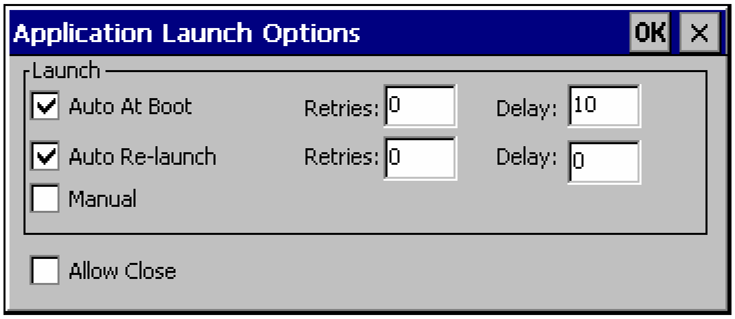
Option	**Explanation**
Filename	Default is blank. Move the cursor to the Filename text box and either type the application path or tap the Browse button (the … button). The standard Windows CE Browse dialog is displayed. After selecting the application from the Browse dialog, tap OK.
Title	Default is blank. Enter the Title to be associated with the application. The assumption is that multiple copies of the same application may need unique titles in order to differentiate them in the application switcher panel.
Arguments	Default is blank. Enter the command line parameters for the application in the Arguments text box.
Order	Default is 1. Enter the Order in which the application is to be loaded or presented to the end-user. Applications are launched in lowest to highest number order.
Internet	Default is Disabled. Enable the Internet checkbox to use the End-user Internet Explorer (EUIE.EXE) When the checkbox is enabled, the Internet Menu and Internet Status are available. See the section titled *End-user Internet Explorer (EUIE)* for more details.
Launch Button	See following section titled *Launch Button*. *Note: AppLock Administrator Control panel file Launch option does not inter-relate with similarly-named options contained in other LXE Control Panels.*
Global Key	Default is Ctrl+Spc. Select the Global Key key sequence the end-user is to press when switching between applications. The Global Key default key sequence must be defined by the AppLock Administrator. The Global key is presented to the end-user as the *Activation* key.
Global Delay	Default is 10 seconds. Enter the number of seconds that Applications must wait before starting to run after reboot. *Note: Delay (Global) may not be available in all versions of AppLock. You can simulate a Global Delay function by setting a delay for the first application (lowest Order) launched and setting the delay to 0 for all other applications. See Boot Options.*
Input Panel	Default is Disabled. Enable (check) to show the Keyboard option on the Switchpad menu. When enabled the input panel cannot be enabled or disabled for each individual application, and is available to the user for all configured applications.
Clear Button	Tap the **Clear** button to clear all currently displayed Filename or Application information. The Global settings are not cleared.

Option	**Explanation**
Scroll Buttons	Use the left and right **scroll buttons** to move from application setup screen to application setup screen. The left and right buttons update the information on the screen with the previous or next configured application respectively.

Launch Button

Note: The Launch button may not be available in all versions of Multi-AppLock. Contact your LXE representative for assistance, downloads and AppLock update availability.

When clicked, displays the Launch options panel for the Filename selected on the Administration panel.



Application Launch Options

Launch

☑ Auto At Boot Retries: 0 Delay: 10

☑ Auto Re-launch Retries: 0 Delay: 0

□ Manual

□ Allow Close

Figure 6-5 Application Launch Options

Note: Launch order is determined by the Order specified in the Application tab. The Order value does not have to be sequential.

Auto At Boot

Default is Enabled. Auto At Boot, when enabled, automatically launches (subject to the specified Delay in seconds) the application after the unit is rebooted. If a Delay in seconds is specified, AppLock waits for the specified period of time to expire before launching the application. The Delay default value is 10 seconds; valid values are between 0 “no delay” and a maximum of 999 seconds.

Auto At Boot **Retries** is the number of times the application launch will be retried if a failure occurs when the application is automatically launched at bootup. Valid values are between 0 (no tries) and 99 tries or -1 for infinite. Infinite tries ends when the application successfully launches. The default is 0 retries.

Auto At Boot **Delay** timer is the time that AppLock waits prior to the initial launch of the selected application when it is automatically launched at bootup. Delay default is 10 seconds. Valid values are between 0 seconds (no delay) and 999 seconds.

The Auto At Boot delay is associated for each application; it will be either a value specified by the Administrator or it will be the delay default value. At startup, when a delay has been assigned for each application, AppLock waits for the delay associated with the first application to expire before launching the first application then AppLock waits for the delay associated with the second application to expire before launching the second application. AppLock continues in this manner until all applications are launched.

Note: A “Global Delay” can be accomplished by setting a timed delay for the first application to be launched (by lowest Order number) and no delay (0 seconds) for all other applications.

Note: Launch order is determined by the Order specified in the Application tab. The Order value does not have to be sequential.

Auto Re-Launch

Default is Enabled. Auto Re-Launch, when enabled for a specific application. automatically re-launches it (subject to the specified Auto Re-Launch Delay in seconds) after it terminates. This option allows the Administrator to disable the re-launch operation. AppLock cannot prevent all applications from closing. When an application that AppLock cannot prevent from closing terminates, perhaps because of an error condition, AppLock re-launches the application when this option is enabled.

Note: If Allow Close is enabled and both Auto Re-launch and Manual (Launch) are disabled, the application cannot be restarted for the end-user or by the end-user after the application terminates.

Auto Re-Launch **Retries** default is 0 tries. Retries is the number of times AppLock will try to re-launch the application. The retry count is reset after an application is successfully launched and controlled by AppLock. Valid values are between 0 (no tries) and 99 tries or -1 for infinite. Infinite tries ends when the application successfully launches.

Auto Re-Launch **Delay** timer default is 0 seconds (no delay). Delay is the amount of time AppLock waits prior to re-launching an application that has terminated. The delay is specified in seconds. Valid values are between 0 (no delay) and 99 seconds.

AppLock must also be configured to automatically re-launch an application. To AppLock, application termination by the end-user is indistinguishable from application termination for any other reason.

Manual (Launch)

Default is Disabled. Enabling this option allows the end-user to launch the specified application(s). Upon bootup completion an application with Manual enabled is listed on the Switchpad accompanied by a checkmark that indicates the application is currently active or available for Launching. When an application name is tapped by the end-user, the application is launched (if inactive) and brought to the foreground.

Applications set up with Manual (Launch) enabled may or may not be launched at bootup. This function is based on the application’s Auto At Boot setting. The applications have been listed as approved applications for end-user manual launch using the Switchpad menu structure. The approved applications are listed on the Switchpad. A checkmark indicates the applications active status.

When Manual (Launch) is disabled for an application, and Allow Close is enabled for the application, when the end-user closes the specific application it is no longer available (shown) on the Switchpad.

When Auto At Boot and Manual (Launch) are both disabled for a specific application, the application is 1) not placed on the list of approved applications for end-user manual launch and 2) never launched, and 3) not displayed on the Switchpad.

Allow Close

Default is Disabled. When enabled, the associated application can be closed by the end-user.

This option allows the administrator to configure applications that consume system resources to be terminated if an error condition occurs or at the end-user's request. Error conditions may generate a topmost popup requiring an end-user response, memory resource issues requiring an end-user response, etc. Also at the administrator's discretion, these types of applications can be started manually (see Manual [Launch]) by the end-user.

End User Internet Explorer (EUIE)

AppLock supports applications that utilize Internet Explorer, such as .HTML pages and JAVA applications. The end user can run an application by entering the application name and path in Internet Explorer's address bar.

To prevent the end user from executing an application using this method, the address bar and Options settings dialog are restricted in Internet Explorer. This is accomplished by creating an Internet Explorer that is used in end user mode: End-user Internet Explorer (EUIE.EXE). The EUIE executes the Internet Explorer application in full screen mode which removes the address bar and status bar. The Options Dialog is also removed so the end user cannot re-enable the address bar.

The administrator specifies the EUIE by checking the **Internet** checkbox in the Application tab of the Administrator applet. The internet application should then be entered in the **Application** text box.

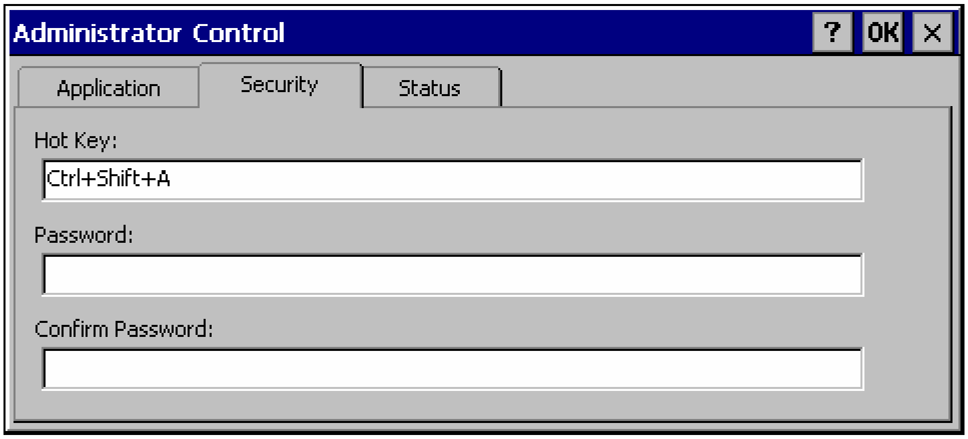
When the Internet checkbox is enabled, the **Menu** and **Status** check boxes are available.

Enabling the **Menu** checkbox displays the EUIE menu which contains navigation functions like Back, Forward, Home, Refresh, etc., functions that are familiar to most Internet Explorer users. When the Menu checkbox is blank, the EUIE menu is not displayed and Navigation functions are unavailable.

When the **Status** checkbox is enabled, the status bar displayed by EUIE gives feedback to the end-user when they are navigating the Internet.

If the standard Internet Explorer that is shipped with the mobile device is desired, it should be treated like any other application. This means that IEXPLORER.EXE should be specified in the Application text box and the internet application should be entered in the command line. In this case, do not check the Internet checkbox.

Security Panel



Administrator Control

Hot Key: Ctrl+Shift+A

Password:

Confirm Password:

Figure 6-6 Security Panel

Hotkey

Specify the hotkey sequence that triggers AppLock to switch between administrator and user modes and the password required to enter Administrator mode. The default hotkey sequence is **Shift+Ctrl+A**.

A 2nd key keypress is an invalid keypress for a hotkey sequence.

Move the cursor to the Hot Key text box. Enter the new hot key sequence by first pressing the Shift state key followed by a normal key. The hotkey selected must be a key sequence that the application being locked does not use. The hotkey sequence is intercepted by AppLock and is not passed to the application.

Input from the keyboard or Input Panel is accepted with the restriction that the normal key must be pressed from the keyboard when switching modes. The hotkey sequence is displayed in the Hot key text box with "Shift", "Alt", and "Ctrl" text strings representing the shift state keys. The normal keyboard key completes the hotkey sequence. The hotkey must be entered via the keypad. Some hotkeys cannot be entered via the Input Panel. Also, hotkeys entered via the SIP are not guaranteed to work properly when switching operational modes.

For example, if the 'Ctrl' key is pressed followed by 'A', "Ctrl+A" is entered in the text box. If another key is pressed after a normal key press, the hotkey sequence is cleared and a new hotkey sequence is started.

A normal key is required for the hotkey sequence and is unlike pressing the normal key during a mode switch; this key can be entered from the SIP when configuring the key. However, when the hotkey is pressed to switch modes, the normal key must be entered from the keypad; it cannot be entered from the SIP.

Password

Move the cursor to the Password text box. The passwords entered in the Password and Confirm Password fields must match. Passwords are case sensitive.

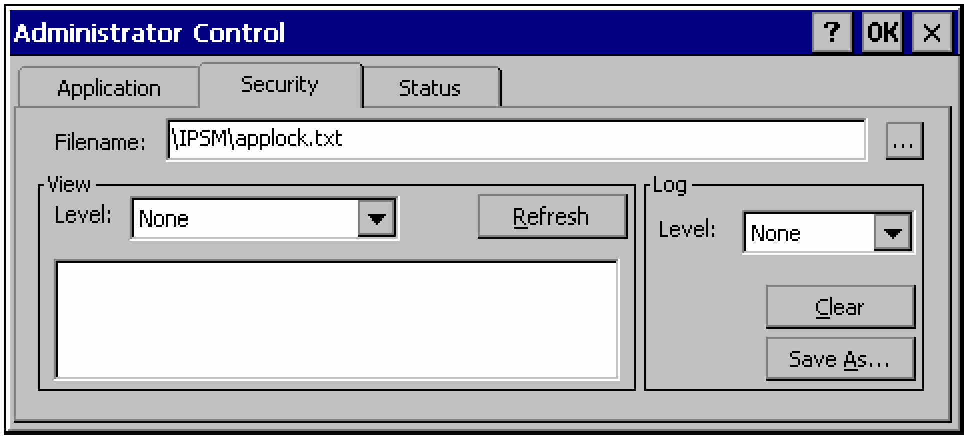
When the user exits the Administrator Control panel, the two passwords are compared to verify that they match. If they do not match, a dialog box is displayed notifying the user of the error. After the user closes the dialog box, the Security Panel is displayed and the password can then be entered and confirmed again. If the passwords match, the password is encrypted and saved.

See Also: *Passwords* and *Troubleshooting Multi-Application AppLock*

Status Panel

Use the Status panel to view the log of previous AppLock operations and to configure which messages are to be recorded during AppLock operation.

Status information is stored in a specific location on the storage device and in a specific logfile specified by the Administrator. For this reason, the administrator can configure the type of status information that is logged, as well as clear the status information.



Filename: \IPSM\applock.txt

View Level: None

Log Level: None

Figure 6-7 Status Panel

Move the cursor to the **Filename** text box and either type the logfile path or tap the Browse button (the … button). The standard Windows CE Browse dialog is displayed. After selecting the logfile from the Browse dialog, tap OK.

Note: If your Status Panel does not look like the figure shown above, you may have the Single Application version which does not have as many options.

View

Error	Error status messages are logged when an error occurs and is intended to be used by the administrator to determine why the specified application cannot be locked.
Process	Processing status shows the flow control of AppLock components and is mainly intended for LXE Customer Service when helping users troubleshoot problems with their AppLock program.
Extended	Extended status provides more detailed information than that logged by Process Logging.
All	All messages are displayed.

Tap the Refresh button after changing from one view level to another. The filtered records are displayed, all others are not displayed.

Log

Note: ***If a level higher than Error is selected, the status should be cleared frequently by the administrator.***

In addition to the three view levels the administrator can select that all status information be logged or turn off all status information logging completely. The system default is ‘None’; however to reduce registry use, the administrator may want to select ‘None’ after verifying the configuration. Tap the Clear button to clear the status information from the registry.

- None
- Error
- Processing
- Extended
- All

Save As

When the 'Save As'… button is selected, a standard 'Save As' dialog screen is displayed. Specify the path and filename. If the filename exists, the user is prompted whether the file should be overwritten. If the file does not exist, it is created.

See Also: *Error Messages*

Appendix A Key Maps

95-key Keypad with Pointing Device

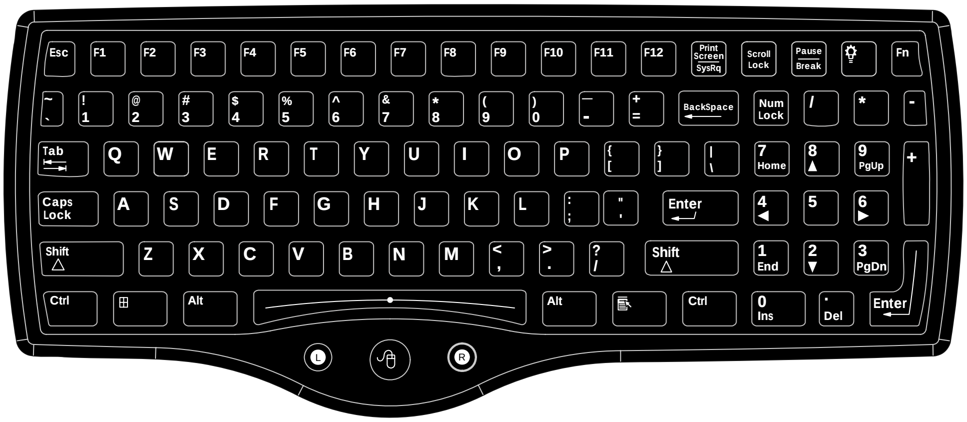


Figure A-1 95-Key VMT QWERTY Keyboard

The key map table that follows lists the commands used for the VX7. Note that since the VX7 uses a Microsoft Windows CE operating system, no DOS Terminal Emulation keypress sequences are provided.

Key Map 101-Key Equivalencies

There are ten hidden keys on the 95-key keyboard. Each of these hidden keys is accessed by pressing the <Fn> key plus another key.

To get this key	Press These Keys and Then
Insert	Fn + 0 on the number pad
Home	Fn + 7 on the number pad
Page Up	Fn + 9 on the number pad
Delete	Fn + . on the number pad
End	Fn + 1 on the number pad
Page Down	Fn + 3 on the number pad
Up Arrow	Fn + 8 on the number pad
Left Arrow	Fn + 4 on the number pad
Down Arrow	Fn + 2 on the number pad
Right Arrow	Fn + 6 on the number pad

Note: *The 95-key keyboard does not have a 2nd key function.*

60-key Standard Keypad

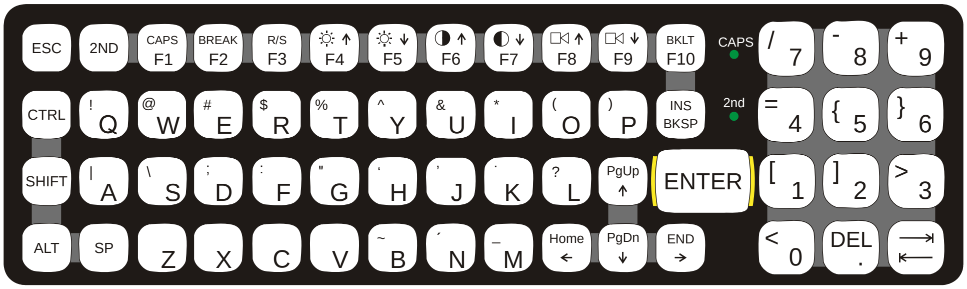


Figure A-2 60-Key VMT QWERTY Keyboard

The key map table that follows lists the commands used when running LXE's VX7.

Key Map 101-Key Equivalencies

When using a sequence of keys that includes the 2nd key, press the 2nd key first then the rest of the key sequence.

Note: This keyboard does not have a NumLock indicator. By default, NumLock is enabled when the VX7 reboots. The warmboot behavior of NumLock can be configured. Please refer to Chapter 3, "System Configuration".

The default condition of Caps (or CapsLock) is Off. The Caps (or CapsLock) condition can be set toggled with a <2nd>+<F1> key sequence. The CAPS LED on the VMT keyboard is illuminated when CapsLock is On.

To get this key	Press These Keys and Then					Press this key
	2nd	Shift	Ctrl	Alt	CapsLock	
Increase Brightness [4]	x					F4
Decrease Brightness [4]	x					F5
Increase Contrast [5]	x					F6
Decrease Contrast [5]	x					F7
Increase Volume [6]	x					F8
Decrease Volume [6]	x					F9

[4] The Brightness Adjustment keys have no function. Brightness is adjusted via the buttons on the VX7 control panel.

[5] The Contrast Adjustment keys have no function because the VX7 is equipped with a TFT display that has no provision for these adjustments.

[6] The Volume Control keys have no function as the volume control is adjusted via the Windows System Tray Volume icon.

To get this key	Press These Keys and Then					Press this key
	2nd	Shift	Ctrl	Alt	CapsLock	
Keyboard Backlight [7]	x		x			F10
Suspend/Resume [8]	x					F3
2nd						2nd
Shift						Shift
Alt						Alt
Ctrl						Ctrl
Esc						Esc
Space						Sp
Enter						Enter
Enter (numeric)	x					Enter
CapsLock (Toggle)	x					F1
Back Space						Ins/BkSp
Tab						Tab
BackTab	x					Tab
Ctrl-Break [9]	x		x			F2
Pause	x					F2
Up Arrow						Up Arrow
Down Arrow						Down Arrow
Right Arrow						Right Arrow
Left Arrow						Left Arrow
Insert	x					Ins/BkSp
Delete (numeric)	x					DOT
Home	x					Left Arrow
End	x					Right Arrow
Page Up	x					Up Arrow
Page Down	x					Down Arrow
Right Shift	x	x				F7
Right Alt	x	x				F8
Right Ctrl	x	x				F9
ScrollLock	x	x				F4
NumLock	x	x				F10
F1						F1
F2						F2
F3						F3

[7] The Keyboard Backlight key is used in <2nd> + <CTRL> + <F10> key sequence. Refer to "VMT Keyboard Backlighting" in Chapter 4, "System Configuration".

[8] The Suspend/Resume key has no function as Windows Power Management controls all power management modes on the VX7.

[9] Press <Ctrl> then <2nd> then <F2> to produce Ctrl-Break.

To get this key	Press These Keys and Then					Press this key
	2nd	Shift	Ctrl	Alt	CapsLock	
F4						F4
F5						F5
F6						F6
F7						F7
F8						F8
F9						F9
F10						F10
F11	x	x				F1
F12	x	x				F2
a						A
b						B
c						C
d						D
e						E
F						F
g						G
h						H
I						I
j						J
k						K
l						L
m						M
n						N
o						O
p						P
q						Q
r						R
s						S
t						T
u						U
v						V
w						W
x						X
y						Y
z						Z
A					x	A
B					x	B
C					x	C
D					x	D
E					x	E

To get this key	Press These Keys and Then					Press this key
	2nd	Shift	Ctrl	Alt	CapsLock	
F					x	F
G					x	G
H					x	H
I					x	I
J					x	J
K					x	K
L					x	L
M					x	M
N					x	N
O					x	O
P					x	P
Q					x	Q
R					x	R
S					x	S
T					x	T
U					x	U
V					x	V
W					x	W
X					x	X
Y					x	Y
Z					x	Z
1 (alpha)	x	x				1
2 (alpha)	x	x				2
3 (alpha)	x	x				3
4 (alpha)	x	x				4
5 (alpha)	x	x				5
6 (alpha)	x	x				6
7 (alpha)	x	x				7
8 (alpha)	x	x				8
9 (alpha)	x	x				9
0 (alpha)	x	x				0
DOT (alpha)	x					K
1 (numeric)						1
2 (numeric)						2
3 (numeric)						3
4 (numeric)						4
5 (numeric)						5
6 (numeric)						6
7 (numeric)						7
8 (numeric)						8

To get this key	Press These Keys and Then					Press this key
	2nd	Shift	Ctrl	Alt	CapsLock	
9 (numeric)						9
0 (numeric)						0
DOT (numeric)						DOT
<	x					0
[	x					1
]	x					2
>	x					3
=	x					4
{	x					5
}	x					6
/ (numeric)	x		x			7
/ (alpha)	x					7
- (numeric)	x		x			8
- (alpha)	x					8
+ (numeric)	x		x			9
+ (alpha)	x					9
* (numeric)	x					I
* (alpha)	x		x			I
: (colon)	x					D
; (semicolon)	x					F
?	x					L
`	x					N
_ (underscore)	x					M
, (comma)	x					J
‘ (apostrophe)	x					H
~ (tilde)	x					B
\	x					S
|	x					A
“	x					G
!	x					Q
@	x					W
#	x					E
$	x					R
%	x					T
^	x					Y
&	x					U
(	x					O
)	x					P

IBM 3270 Keypad Ovelay

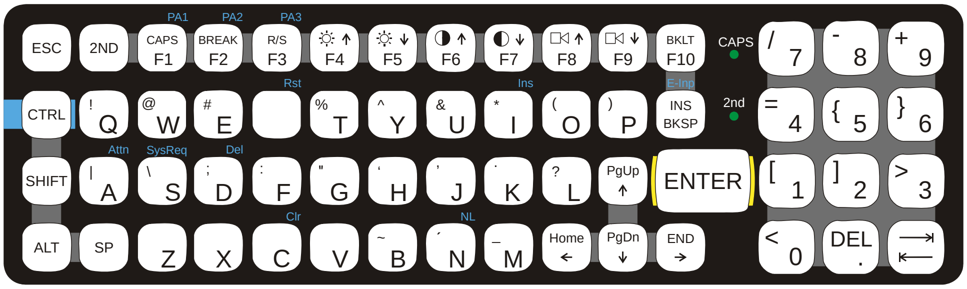


Figure A-3 IBM 3270 Specific Keypad

The 60-key keypad is available with an IBM 3270 overlay designed to allow the user to enter terminal emulator commands when running LXE's RFTerm™ program. When running this program please refer to the following reference guide for equivalent keys and keypress sequences:

- RFTerm™ Reference Guide

IBM 5250 Keypad Overlay

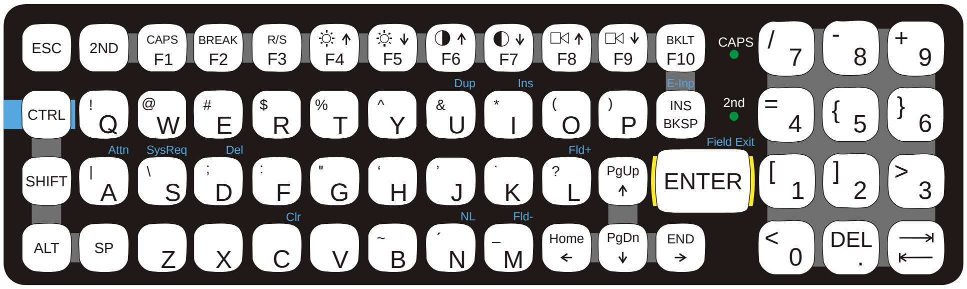


Figure A-4 IBM 5250 Specific Keypad

The 60-key keypad is available with an IBM 5250 overlay designed to allow the user to enter terminal emulator commands when running LXE's RFTerm™ program. When running this program please refer to the following reference guide for equivalent keys and keypress sequences:

- RFTerm™ Reference Guide

Appendix B Technical Specifications

Physical Specifications

Features		Specification	Comments
CPU		400MHz Intel® PXA255	
Memory	ROM	128 MB Flash [10]	
	RAM	128MB of SDRAM [10]	System Memory
Display	Controller	SVGA compatible controller	
	Type	TFT	
Mass Storage	Compact Flash	Various sizes supported. Compact Flash supported via PCMCIA adapter.	
	PCMCIA		
	Secure Digital		
PCMCIA/CardBus Interface		Two (2) PCMCIA: Accepts Type I and II PCMCIA cards.	
External Connectors/ Interfaces		Two (2) external RS-232C serial ports: COM1 and COM3 [11]	9-pin "D" (male) connectors
		One USB Host and one USB Client Port One (1) Ethernet Port	Via Adapter Cable
Power Connector		12-80V DC input power	5-pin connector
Power Switch		Sealed power switch	
Beeper		Minimum loudness greater than 95dBm at 10 cm in front of unit	
Dimensions		Length: 12.2 in (30.98 cm) Width: 9.6 in (24.38 cm) Depth: 3.7 in (9.39 cm)	
Battery for CMOS		Internal lithium Battery	
External Power Supply	AC Adapter	120-240VAC to 12VDC	

[10] 64MB Flash and 64MB RAM options have been discontinued.

[11] COM3 is labeled "COM2/3".

Environmental Specifications

The VX7 will withstand the following environmental characteristics and has been tested in accordance with applicable sections of MIL-STD-810E.

Feature	Specification
Altitude	Operational to 10,000 ft. (3048 meters)
Operating Temperature	Standard version: -4°F to 122°F (-20°C to 50°C) [non-condensing] Extended temperature version: -22º to 122º F (-30ºC to 50ºC [condensing]
Storage Temperature	Standard version: -22°F to 140°F (-30°C to 60°C) [non-condensing] Extended temperature version: -22°F to 140°F (-30°C to 60°C) [condensing]
Water, Sand and Dust	IP66 per IEC60529
Humidity	Standard version: Up to 90% Non-condensing at 40°C (104°F) Extended temperature version: 100%
Vibration	Bounce loose cargo for 0.5 hour duration. Common carrier transportation, transit face.
ESD	15 kV
Shock	75G, 5msec duration, 100 shock impacts

Display Specifications

Characteristic		Specification
Type	TFT	SVGA
Resolution		Default: 800 X 600 pixels (25 lines x 80 characters) Optional: 640x480 pixels on Platform 2 VX7s.
Cell Size		8 x 16 pixels (8 x 8 also supported – 25 lines x 80 chars)
Dot Dimensions		.30mm x .30mm
Display Dimensions		280mm x 218mm x 11mm (11.0” x 8.6” x 0.4”)
Viewing Area		249mm x 187.5mm (9.8” x 7.38”)
Active Display Area		246mm x 184.5mm (9.7” x 7.26”)

UPS Battery Pack Specifications

Feature	Specification
Altitude	Operational to 10,000 ft. (3048 meters)
Operating Temperature	-30 °C to +50 °C (-22 °F to +122 °F)
Storage Temperature	-40 °C to +70 °C (-40 °F to +158 °F)
Water, Sand and Dust	IP66 per IEC60529
Humidity	10-90% Non-condensing at 40°C (104°F)
Vibration	Bounce loose cargo for 0.5 hour duration. Common carrier transportation, transit face.
ESD	15 kV

Radio Specifications

Summit CF 2.4GHz

Bus Interface:	Compact Flash via a PCMCIA adapter
Radio Frequencies:	2.4 - 2.4897 GHz IEEE 802.11b 802.11g DSSS OFDM
RF Data Rates:	1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps
RF Power Level:	64 mW (18 dBm)
Channels	11 US, 13 Europe, 13 Japan
Operating Temperature	see VX7 Environmental Specifications
Storage Temperature	see VX7 Environmental Specifications
Connectivity:	Novell, TCP/IP, Ethernet, ODI

PCMCIA Cisco 2.4GHz Type II

Bus Interface:	PCMCIA 2.0, Type II slot
Radio Frequencies:	2.4 - 2.4835 GHz IEEE 802.11b DS SS
RF Data Rates:	11 Mbps
RF Power Level:	100 mW
Channels	11 US, 13 Europe, 4 France, 1 Japan
Operating Temperature	see VX7 Environmental Specifications
Storage Temperature	see VX7 Environmental Specifications
Connectivity:	Novell, TCP/IP, Ethernet, ODI

PCMCIA Symbol 11Mb 2.4GHz Type II

Bus Interface:	PCMCIA 2.0, Type II slot
Radio Frequencies:	2.4 - 2.5 GHz IEEE 802.11b DS SS
RF Data Rates:	11 Mbps maximum
RF Power Level:	100 mW
Channels	11 US, 13 Europe, 4 France, 1 Japan
Operating Temperature	see VX7 Environmental Specifications
Storage Temperature	see VX7 Environmental Specifications
Connectivity:	Novell, TCP/IP, Ethernet, ODI

Bluetooth

Bus Interface	SD card via a PCMCIA interface
Enhanced Data Rate	Up to 3.0 Mbit/s over the air
Connection	No less than 32.80 ft (10 meters) line of sight
Bluetooth Version	2.0 + EFR
Operating Frequency:	2.402 - 2.480 GHz
Operating Temperature	see VX7 Environmental Specifications
Storage Temperature	see VX7 Environmental Specifications

Appendix C Reference Material

Introduction

Contents of this Appendix include:

- AppLock Error Messages and Registry Settings
- Revision History

and the following charts:

- Valid VK Codes for CE
- ASCII Control Codes
- Hat Encoding
- Decimal-Hexadecimal Chart

AppLock Error Messages

Any messages whose first word is an ‘ing’ word is output prior to the action described in the message. For example, “Switching to admin-hotkey press” is logged after the administrator has pressed the hotkey but prior to starting the switch process.

For all operations that can result in an error, an Error level message is displayed when a failure occurs. These messages contain the word “failure”. These messages have a partner Extended level message that is logged which contains the word “OK” if the action completed successfully rather than with an error.

For processing level messages, “Enter…” is logged at the beginning of the function specified in the message and “Exit…” is logged at the end (just before the return) of the function specified in the message.

Message	Explanation and/or corrective action	Level
Error reading hotkey	The hotkey is read but not required by AppLock.	LOG_EX
Error reading hotkey; using default	A hotkey is required. If there is a failure reading the hotkey, the internal factory default is used.	LOG_ERROR
App Command Line= <Command line>	Command line of the application being locked	LOG_PROCESSING
App= <Application name>	Name of the application being locked	LOG_PROCESSING
dwProcessID= <#>	Device ID of the application being locked	LOG_EX
Encrypt exported key len <#>	Size of encrypt export key	LOG_EX
Encrypt password length= <#>	The length of the encrypted password.	LOG_EX
Encrypted data len <#>	Length of the encrypted password	LOG_EX
hProcess= <#>	Handle of the application being locked	LOG_EX
Key pressed = <#>	A key has been pressed and trapped by the hotkey processing.	LOG_EX
****************	The status information is being saved to a file and the file has been opened successfully.	LOG_EX
Address of keyboard hook procedure failure	AppLock found the kbdhook.dll, but was unable to get the address of the initialization procedure. For some reason the dll is corrupted. Look in the \Windows directory for kbdhook.dll. If it exists, delete it. Also delete AppLock.exe from the \Windows directory and reboot the unit. Deleting AppLock.exe triggers the AppLock system to reload.	LOG_ERROR
Address of keyboard hook procedure OK	AppLock successfully retrieved the address of the keyboard filter initialization procedure.	LOG_EX

Message	Explanation and/or corrective action	Level
Alt pressed	The Alt key has been pressed and trapped by the HotKey processing.	LOG_EX
Alt	Processing the hotkey and backdoor entry	LOG_EX
Application handle search failure	The application being locked did not complete initialization.	LOG_ERROR
Application handle search OK	The application initialized itself successfully	LOG_ERROR
Application load failure	The application could not be launched by AppLock; the application could not be found or is corrupted.	LOG_ERROR
Backdoor message received	The backdoor keys have been pressed. The backdoor hotkeys provide a method for customer service to get a user back into their system without editing the registry or reloading the device.	LOG_PROCESSING
Cannot find kbdhook.dll	The load of the keyboard filter failed. This occurs when the dll is missing or is corrupted. Look in the \Windows directory for kbdhook.dll. If it exists, delete it. Also delete AppLock.exe from the \Windows directory and reboot the unit. Deleting AppLock.exe triggers the AppLock system to reload.	LOG_ERROR
Converted Pwd	Converted password from wide to mbs.	LOG_EX
Could not create event EVT_HOTKEYCHG	The keyboard filter uses this event at the Administrator Control panel. The event could not be created.	LOG_ERROR
Could not hook keyboard	If the keyboard cannot be controlled, AppLock cannot process the hotkey. This failure prevents a mode switch into user mode.	LOG_ERROR
Could not start thread HotKeyMon	The keyboard filter must watch for hot key changes. The watch process could not be initiated.	LOG_ERROR
Ctrl after L or X	Processing the backdoor entry.	LOG_EX
Ctrl pressed	The Ctrl key has been pressed and trapped by the HotKey processing.	LOG_EX
Ctrl	Processing the hotkey and backdoor entry.	LOG_EX
Decrypt acquire context failure	Unable to decrypt password.	LOG_ERROR
Decrypt acquired context OK	Decryption process ok.	LOG_EX
Decrypt create hash failure	Unable to decrypt password.	LOG_ERROR
Decrypt created hash OK	Decryption process ok.	LOG_EX
Decrypt failure	Unable to decrypt password.	LOG_ERROR

Message	Explanation and/or corrective action	Level
Decrypt import key failure	Unable to decrypt password.	LOG_ERROR
Decrypt imported key OK	Decryption process ok.	LOG_EX
Encrypt acquire context failure	Unable to encrypt password.	LOG_ERROR
Encrypt acquire encrypt context failure	Unable to encrypt password.	LOG_ERROR
Encrypt acquired encrypt context OK	Encrypt password process successful.	LOG_EX
Encrypt create hash failure	Unable to encrypt password.	LOG_ERROR
Encrypt create key failure	Unable to encrypt password.	LOG_ERROR
Encrypt created encrypt hash OK	Encrypt password process successful.	LOG_EX
Encrypt export key failure	Unable to encrypt password.	LOG_ERROR
Encrypt export key length failure	Unable to encrypt password.	LOG_ERROR
Encrypt exported key OK	Encrypt password process successful.	LOG_EX
Encrypt failure	The password encryption failed.	LOG_ERROR
Encrypt gen key failure	Unable to encrypt password.	LOG_ERROR
Encrypt generate key failure	Unable to encrypt password.	LOG_ERROR
Encrypt get user key failure	Unable to encrypt password.	LOG_ERROR
Encrypt get user key ok	Encrypt password process successful.	LOG_EX
Encrypt hash data failure	Unable to encrypt password.	LOG_ERROR
Encrypt hash data from pwd OK	Encrypt password process successful.	LOG_EX
Encrypt length failure	Unable to encrypt password.	LOG_ERROR
Encrypt out of memory for key	Unable to encrypt password.	LOG_ERROR
Encrypted data OK	The password has been successfully encrypted.	LOG_EX
Enter AppLockEnumWindows	In order for AppLock to control the application being locked so it can prevent the application from exiting, AppLock launches the application and has to wait until it has created and initialized its main window. This message is logged when the function that waits for the application initialization is entered.	LOG_EX
Enter DecryptPwd	Entering the password decryption process.	LOG_PROCESSING

Message	Explanation and/or corrective action	Level
Enter EncryptPwd	Entering the password encryption processing.	LOG_PROCESSING
Enter FullScreenMode	Entering the function that switches the screen mode. In full screen mode, the taskbar is hidden and disabled.	LOG_PROCESSING
Enter GetAppInfo	Processing is at the beginning of the function that retrieves the application information from the registry.	LOG_PROCESSING
Enter password dialog	Entering the password dialog processing.	LOG_PROCESSING
Enter password timeout	Entering the password timeout processing.	LOG_PROCESSING
Enter restart app timer	Some application shut down before AppLock can stop it. In these cases, AppLock gets notification of the exit. When the notification is received, AppLock starts a timer to restart the application. This message logs that the timer has expired and the processing is at the beginning of the timer function.	LOG_PROCESSING
Enter TaskbarScreenMode	Entering the function that switches the screen to non-full screen mode and enable the taskbar.	LOG_PROCESSING
Enter ToAdmin	Entering the function that handles a mode switch into admin mode.	LOG_PROCESSING
Enter ToUser	Entering the function that handles the mode switch to user mode	LOG_PROCESSING
Enter verify password	Entering the password verification processing.	LOG_PROCESSING
Exit AppLockEnumWindows-Found	There are two exit paths from the enumeration function. This message denotes the enumeration function found the application.	LOG_PROCESSING
Exit AppLockEnumWindows-Not found	There are two exit paths from the enumeration function. This message denotes the enumeration function did not find the application.	LOG_PROCESSING
Exit DecryptPwd	Exiting password decryption processing.	LOG_PROCESSING
Exit EncryptPwd	Exiting password encryption processing.	LOG_PROCESSING
Exit FullScreenMode	Exiting the function that switches the screen to full screen.	LOG_PROCESSING
Exit GetAppInfo	Processing is at the end of the function that retrieved the application information from the registry.	LOG_PROCESSING
Exit password dialog	Exiting password prompt processing.	LOG_PROCESSING
Exit password dialog-cancel	Exiting password prompt w/cancel.	LOG_PROCESSING
Exit password dialog-OK	Exiting password prompt successfully.	LOG_PROCESSING

Message	Explanation and/or corrective action	Level
Exit password timeout	Exiting password timeout processing.	LOG_PROCESSING
Exit restart app timer	Processing is at the end of the timer function	LOG_PROCESSING
Exit TaskbarScreenMode	Exiting the function that switches the screen mode back to normal operation for the administrator.	LOG_PROCESSING
Exit ToAdmin	Exiting the function that handles the mode switch into admin mode.	LOG_PROCESSING
Exit ToUser	Exiting the user mode switch function.	LOG_PROCESSING
Exit ToUser-Registry read failure	The AppName value does not exist in the registry so user mode cannot be entered.	LOG_PROCESSING
Exit verify password-no pwd set	Exiting password verification.	LOG_PROCESSING
Exit verify password-response from dialog	Exiting password verification.	LOG_PROCESSING
Found taskbar	The handle to the taskbar has been found so that AppLock can disable it in user mode.	LOG_PROCESSING
Getting address of keyboard hook init procedure	AppLock is retrieving the address of the keyboard hook.	LOG_PROCESSING
Getting configuration from registry	The AppLock configuration is being read from the registry. This occurs at initialization and also at entry into user mode. The registry must be re-read at entry into user mode in case the administration changed the settings of the application being controlled.	LOG_PROCESSING
Getting encrypt pwd length	The length of the encrypted password is being calculated.	LOG_EX
Hook wndproc failure	AppLock is unable to lock the application. This could happen if the application being locked encountered an error after performing its initialization and shut itself down prior to being locked by AppLock.	LOG_ERROR
Hook wndproc of open app failure	The application is open, but AppLock cannot lock it.	LOG_ERROR
Hot key event creation failure	The Admin applet is unable to create the hotkey notification.	LOG_ERROR
Hot key pressed	Processing the hotkey and backdoor entry	LOG_EX
Hot key pressed	Processing the hotkey and backdoor entry	LOG_EX
Hot key set event failure	When the administrator changes the hotkey configuration the hotkey controller must be notified. This notification failed.	LOG_ERROR
Hotkey press message received	The user just pressed the configured hotkey.	LOG_PROCESSING

Message	Explanation and/or corrective action	Level
In app hook:WM_SIZE	In addition to preventing the locked application from exiting, AppLock must also prevent the application from enabling the taskbar and resizing the application's window. This message traps a change in the window size and corrects it.	LOG_EX
In app hook:WM_WINDOWPOSCHANGED	In addition to preventing the locked application from exiting, AppLock must also prevent the application from enabling the taskbar and resizing the application's window. This message traps a change in the window position and corrects it.	LOG_EX
Initializing keyboard hook procedure	AppLock is calling the keyboard hook initialization.	LOG_PROCESSING
Keyboard hook initialization failure	The keyboard filter initialization failed.	LOG_ERROR
Keyboard hook loaded OK	The keyboard hook dll exists and loaded successfully.	LOG_EX
L after Ctrl	Processing the backdoor entry.	LOG_EX
Loading keyboard hook	When AppLock first loads, it loads a dll that contains the keyboard hook processing. This message is logged prior to the load attempt.	LOG_PROCESSING
Open failure	The status information is being saved to a file and the file open has failed. This could occur if the file is write protected. If the file does not exist, it is created.	LOG_ERROR
Open registry failure	If the Administration registry key does not exist, the switch to user mode fails because the AppName value in the Administration key is not available.	LOG_ERROR
Opened status file	The status information is being saved to a file and the file has been opened successfully.	LOG_EX
Out of memory for encrypted pwd	Not enough memory to encrypt the password.	LOG_ERROR
pRealTaskbarWndProc already set	The taskbar control has already been installed.	LOG_EX
Pwd cancelled or invalid-remain in user mode	The password prompt was cancelled by the user or the maximum number of failed attempts to enter a password was exceeded.	LOG_EX
Read registry error-hot key	The hotkey registry entry is missing or empty. This is not considered an error. The keyboard hook uses an embedded default if the value is not set in the registry.	LOG_ERROR
Read registry failure-app name	AppName registry value does not exist or is empty. This constitutes a failure for switching into user mode.	LOG_ERROR

Message	Explanation and/or corrective action	Level
Read registry failure-Cmd Line	AppCommandLine registry entry is missing or empty. This is not considered an error since command line information is not necessary to launch and lock the application.	LOG_ERROR
Read registry failure-Internet	The Internet registry entry is missing or empty. This is not considered an error since the Internet value is not necessary to launch and lock the application.	LOG_ERROR
Registering Backdoor MSG	The AppLock system communicates with the keyboard hook via a user defined message. Both AppLock.exe and Kbdhook.dll register the message at initialization.	LOG_PROCESSING
Registering Hotkey MSG	The AppLock system communicates with the keyboard hook via a user defined message. Both Applock.exe and Kbdhook.dll register the message at initialization.	LOG_PROCESSING
Registry read failure at reenter user mode	The registry has to be read when entering user mode is the AppName is missing. This user mode entry is attempted at boot and after a hotkey switch when the administrator has closed the application being locked or has changed the application name or command line.	LOG_ERROR
Registry read failure at reenter user mode	The registry has to be read when switching into user mode. This is because the administrator can change the settings during administration mode. The read of the registry failed which means the Administration key was not found or the AppName value was missing or empty.	LOG_ERROR
Registry read failure	The registry read failed. The registry information read when this message is logged is the application information. It the Administration key cannot be opened or if the AppName value is missing or empty, this error is logged. The other application information is not required. If the AppName value is not available, AppLock cannot switch into user mode.	LOG_ERROR
Reset system work area failure	The system work area is adjusted when in user mode to cover the taskbar area. The system work area has to be adjusted to exclude the taskbar area in administration mode. AppLock was unable to adjust this area.	LOG_ERROR
Shift pressed	The Shift key has been pressed and trapped by the HotKey processing.	LOG_EX
Shift	Processing the hotkey and backdoor entry	LOG_EX
Show taskbar	The taskbar is now being made visible and enabled.	LOG_PROCESSING
Switching to admin-backdoor	The system is currently in user mode and is now switching to admin mode. The switch occurred because of the backdoor key presses were entered by the administrator.	LOG_PROCESSING

Message	Explanation and/or corrective action	Level
Switching to admin-hotkey press	The system is currently in user mode and is now switching to admin mode. The switch occurred because of a hotkey press by the administrator.	LOG_PROCESSING
Switching to admin-kbdhook.dll not found	The keyboard hook load failed, so AppLock switches to admin mode. If a password is specified, the password prompt is displayed and remains until a valid password is entered.	LOG_PROCESSING
Switching to admin-keyboard hook initialization failure	If the keyboard hook initialization fails, AppLock switches to admin mode. If a password is specified, the password prompt is displayed and remains until a valid password is entered.	LOG_PROCESSING
Switching to admin-registry read failure	See the explanation of the “Registry read failure” above. AppLock is switching into Admin mode. If a password has been configured, the prompt will be displayed and will not be dismissed until a valid password is entered.	LOG_PROCESSING
Switching to TaskbarScreenMode	In administration mode, the taskbar is visible and enabled.	LOG_EX
Switching to user mode	The registry was successfully read and AppLock is starting the process to switch to user mode.	LOG_PROCESSING
Switching to user-hotkey press	The system is currently in admin mode and is now switching to user mode. The switch occurred because of a hotkey press by the administrator.	LOG_PROCESSING
Taskbar hook failure	AppLock is unable to control the taskbar to prevent the locked application from re-enabling it.	LOG_ERROR
Taskbar hook OK	AppLock successfully installed control of the taskbar.	LOG_EX
Timeout looking for app window	After the application is launched, AppLock must wait until the application has initialized itself before proceeding. The application did not start successfully and AppLock has timed out.	LOG_ERROR
ToUser after admin, not at boot	The user mode switch is attempted when the device boots and after the administrator presses the hotkey. The mode switch is being attempted after a hotkey press.	LOG_EX
ToUser after admin-app still open	The switch to user mode is being made via a hotkey press and the administrator has left the application open and has not made any changes in the configuration.	LOG_EX
ToUser after admin-no app or cmd line change	If user mode is being entered via a hotkey press, the administrator may have left the configured application open. If so, AppLock does not launch the application again unless a new application or command line has been specified; otherwise, it just locks it.	LOG_EX

Message	Explanation and/or corrective action	Level
Unable to move desktop	The desktop is moved when switching into user mode. This prevents them from being visible if the application is exited and restarted by the timer. This error does not affect the screen mode switch; processing continues.	LOG_ERROR
Unable to move taskbar	The taskbar is moved when switching into user mode. This prevents them from being visible if the application is exited and restarted by the timer. This error does not affect the screen mode switch; processing continues.	LOG_ERROR
Unhook taskbar wndproc failure	AppLock could not remove its control of the taskbar. This error does not affect AppLock processing	LOG_ERROR
Unhook wndproc failure	AppLock could not remove the hook that allows monitoring of the application.	LOG_ERROR
Unhooking taskbar	In administration mode, the taskbar should return to normal operation, so AppLock's control of the taskbar should be removed.	LOG_EX
Unhooking wndproc	When the administrator leaves user mode, the device is fully operational; therefore, AppLock must stop monitoring the locked application.	LOG_EX
WM_SIZE adjusted	This message denotes that AppLock has readjusted the window size.	LOG_EX
X after Ctrl+L	Processing the backdoor entry.	LOG_EX
Ret from password <#>	Return value from password dialog.	LOG_EX
Decrypt data len <#>	Length of decrypted password.	LOG_EX
Window handle to enumwindows=%x	The window handle that is passed to the enumeration function. This message can be used by engineering with other development tools to trouble shoot application lock failures.	LOG_EX
WM_WINDOWPOSCHG adjusted=%x	Output the window size after it has been adjusted by AppLock	LOG_EX

AppLock Registry Settings

This system application runs at startup via the "launch" feature of LXE Windows CE devices. When the launch feature is installed on the device, the following registry settings are created. The launch feature registry settings are embedded in the mobile device OS image:

```
HKEY_LOCAL_MACHINE\\Software\\LXE\\Persist\\Filename=AppLock.exe
HKEY_LOCAL_MACHINE\\Software\\LXE\\Persist\\Installed=
HKEY_LOCAL_MACHINE\\Software\\LXE\\Persist\\FileCheck=
```

AppLock registry settings identify the application that is going to be locked and any parameters that are needed by the application. These registry settings are as follows:

```
HKEY_LOCAL_MACHINE\\Software\\LXE\\Administration\\AppName
HKEY_LOCAL_MACHINE\\Software\\LXE\\AppCommandLine=
```

In addition to the registry settings needed to specify the application, additional registry settings are needed to store the configuration options for AppLock. These options include, among others, the administrator's password and hotkey.

```
HKEY_LOCAL_MACHINE\\Software\\LXE\\AppLock\\Administration\\HotKey=
HKEY_LOCAL_MACHINE\\Software\\LXE\\AppLock\\Administration\\EP=
```

Valid VK Codes for CE

This is the list of codes parsed by KEYCOMP compiler. Refer to Microsoft Windows documentation for further clarification of the meaning of these key codes. Any VK keys not defined here are not valid for use under Windows CE .

VK_ADD	VK_F3	VK_NUMPAD9
VK_APOSTROPHE	VK_F4	VK_OEM_CLEAR
VK_APPS	VK_F5	VK_OFF
VK_ATTN	VK_F6	VK_PA1
VK_BACK	VK_F7	VK_PAUSE
VK_BACKQUOTE	VK_F8	VK_PERIOD
VK_BACKSLASH	VK_F9	VK_PLAY
VK_BROWSER_BACK	VK_FINAL	VK_PRINT
VK_BROWSER_FAVORITES	VK_HANGUL	VK_PRIOR
VK_BROWSER_FORWARD	VK_HANJA	VK_RBRACKET
VK_BROWSER_HOME	VK_HELP	VK_RBUTTON
VK_BROWSER_REFRESH	VK_HOME	VK_RCONTROL
VK_BROWSER_SEARCH	VK_HYPHEN	VK_RETURN
VK_BROWSER_STOP	VK_INSERT	VK_RIGHT
VK_CANCEL	VK_JUNJA	VK_RMENU
VK_CAPITAL	VK_KANA	VK_RSHIFT
VK_CLEAR	VK_KANJI	VK_RWIN
VK_COMMA	VK_LAUNCH_APP1	VK_SCROLL
VK_CONTROL	VK_LAUNCH_APP2	VK_SELECT
VK_CONVERT	VK_LAUNCH_MAIL	VK_SEMICOLON
VK_CRSEL	VK_LAUNCH_MEDIA_SELECT	VK_SEPARATOR
VK_DECIMAL	VK_LBRACKET	VK_SHIFT
VK_DELETE	VK_LBUTTON	VK_SLASH
VK_DIVIDE	VK_LCONTROL	VK_SLEEP
VK_DOWN	VK_LEFT	VK_SNAPSHOT
VK_END	VK_LMENU	VK_SPACE
VK_EQUAL	VK_LSHIFT	VK_SUBTRACT
VK_EREOF	VK_LWIN	VK_TAB
VK_ESCAPE	VK_MBUTTON	VK_UP
VK_EXECUTE	VK_MEDIA_NEXT_TRACK	VK_VOLUME_DOWN
VK_EXSEL	VK_MEDIA_PLAY_PAUSE	VK_VOLUME_MUTE
VK_F1	VK_MEDIA_PREV_TRACK	VK_VOLUME_UP
VK_F10	VK_MEDIA_STOP	VK_ZOOM
VK_F11	VK_MENU	
VK_F12	VK_MULTIPLY	
VK_F13	VK_NEXT	
VK_F14	VK_NOCONVERT	
VK_F15	VK_NONAME	
VK_F16	VK_NUMLOCK	
VK_F17	VK_NUMPAD0	
VK_F18	VK_NUMPAD1	
VK_F19	VK_NUMPAD2	
VK_F2	VK_NUMPAD3	
VK_F20	VK_NUMPAD4	
VK_F21	VK_NUMPAD5	
VK_F22	VK_NUMPAD6	
VK_F23	VK_NUMPAD7	
VK_F24	VK_NUMPAD8	

ASCII Control Codes

The following table lists ASCII Control codes in hexadecimal and their corresponding Control-key combinations.

Char	Hex	Control-Key	Control Action	
NUL	0	^@	NULL character	Ctrl-Shift-`
SOH	1	^A	Start Of Heading	VK_CONTROL (0x11) down VK_A (0x41) down WM_CHAR (0x1) VK_A (0x41) up VK_CONTROL (0x11) up
STX	2	^B	Start of TeXt	Ctrl-b
ETX	3	^C	End of TeXt	Ctrl-c
EOT	4	^D	End Of Transmission	Ctrl-d
ENQ	5	^E	ENQuiry	Ctrl-e
ACK	6	^F	ACKnowledge	Ctrl-f
BEL	7	^G	BELl, rings terminal bell	Ctrl-g
BS	8	^H	BackSpace (non-destructive)	Ctrl-h
HT	9	^I	Horizontal Tab (move to next tab position)	Ctrl-i
LF	a	^J	Line Feed	Ctrl-j
VT	b	^K	Vertical Tab	Ctrl-k
FF	c	^L	Form Feed	Ctrl-l
CR	d	^M	Carriage Return	Ctrl-m
SO	e	^N	Shift Out	Ctrl-n
SI	f	^O	Shift In	Ctrl-o
DLE	10	^P	Data Link Escape	Ctrl-p
DC1	11	^Q	Device Control 1, normally XON	Ctrl-q
DC2	12	^R	Device Control 2	Ctrl-r
DC3	13	^S	Device Control 3, normally XOFF	Ctrl-s
DC4	14	^T	Device Control 4	Ctrl-t
NAK	15	^U	Negative AcKnowledge	Ctrl-u
SYN	16	^V	SYNchronous idle	Ctrl-v
ETB	17	^W	End Transmission Block	Ctrl-w

Char	Hex	Control-Key	Control Action	
CAN	17	^X	CANcel line	Ctrl-x
EM	19	^Y	End of Medium	Ctrl-y
SUB	1a	^Z	SUBstitute	Ctrl-z
ESC	1b	^[	ESCape	VK_CONTROL (0x11)down VK_PACKET (0xe7) down WM_CHAR 0x1b VK_PACKET up VK_CONTROL up
FS	1c	^\	File Separator	VK_CONTROL (0x11)down VK_PACKET (0xe7) down WM_CHAR 0x1c VK_PACKET up VK_CONTROL up
GS	1d	^]	Group Separator	VK_CONTROL (0x11)down VK_PACKET (0xe7) down WM_CHAR 0x1d down WM_CHAR (0x1d) up VK_PACKET up VK_CONTROL up
RS	1e	^^	Record Separator	VK_CONTROL (0x11)down VK_SHIFT (0x10) down WM_CHAR 0x36 down WM_CHAR 0x36 up VK_SHIFT up VK_CONTROL up
US	1f	^_	Unit Separator	VK_CONTROL (0x11) down VK_SHIFT (0x10) down VK_PACKET (0xe7) down WM_CHAR 0x1f VK_PACKET (0xe7) up VK_SHIFT (0x10) up VK_CONTROL (0x11) up

Hat Encoding

The VX7 supports only 7-bit hat encoding which means only ^@ through ^_ (underscore) are supported.

Desired ASCII	Hex Value	Hat Encoded
NUL	0X00	^@
SOH	0X01	^A
STX	0X02	^B
ETX	0X03	^C
EOT	0X04	^D
ENQ	0X05	^E
ACK	0X06	^F
BEL	0X07	^G
BS	0X08	^H
HT	0X09	^I
LF	0X0A	^J
VT	0X0B	^K
FF	0X0C	^L
CR	0X0D	^M
SO	0X0E	^N
SI	0X0F	^O
DLE	0X10	^P
DC1 (XON)	0X11	^Q
DC2	0X12	^R
DC3 (XOFF)	0X13	^S
DC4	0X14	^T
NAK	0X15	^U
SYN	0X16	^V
ETB	0X17	^W
CAN	0X18	^X
EM	0X19	^Y
SUB	0X1A	^Z
ESC	0X1B	^[
FS	0X1C	^\\
GS	0X1D	^]
RS	0X1E	^^
US	0X1F	^_ (Underscore)
	0X7F	^?
	80	~^@
	81	~^A
	82	~^B
	83	~^C
IND	84	~^D
NEL	85	~^E
SSA	86	~^F
®	AE	~. (Period)
¯	AF	~/
°	B0	~0 (Zero)
±	B1	~1
ESA	87	~^G
HTS	88	~^H
HTJ	89	~^I
VTS	8A	~^J
PLD	8B	~^K
PLU	8C	~^L
RI	8D	~^M
SS2	8E	~^N
SS3	8F	~^O
DCS	90	~^P
PU1	91	~^Q
PU2	92	~^R
STS	93	~^S
CCH	94	~^T
MW	95	~^U
SPA	96	~^V
EPA	97	~^W
	98	~^X
	99	~^Y
	9A	~^Z
CSI	9B	~^[
ST	9C	~^\\
OSC	9D	~^]
PM	9E	~^^
APC	9F	~^_ (Underscore)
(no-break space)	A0	~ (Tilde and Space)
¡	A1	~!
¢	A2	~”
£	A3	~#
¤	A4	~$
¥	A5	~%
¦	A6	~&
§	A7	~’
¨	A8	~(
©	A9	~)
ª	AA	~*
«	AB	~+
¬	AC	~,
(soft hyphen)	AD	~- (Dash)
×	D7	~W
Ø	D8	~X
Ù	D9	~Y
Ú	DA	~Z

Desired ASCII	Hex Value	Hat Encoded
²	B2	~2
³	B3	~3
´	B4	~4
µ	B5	~5
¶	B6	~6
·	B7	~7
¸	B8	~8
¹	B9	~9
º	BA	~:
»	BB	~;
¼	BC	~<
½	BD	~=
¾	BE	~>
¿	BF	~?
À	C0	~@
Á	C1	~A
Â	C2	~B
Ã	C3	~C
Ä	C4	~D
Å	C5	~E
Æ	C6	~F
Ç	C7	~G
È	C8	~H
É	C9	~I
Ê	CA	~J
Ë	CB	~K
Ì	CC	~L
Í	CD	~M
Î	CE	~N
Ï	CF	~O
Ð	D0	~P
Ñ	D1	~Q
Ò	D2	~R
Ó	D3	~S
Ô	D4	~T
Õ	D5	~U
Ö	D6	~V

Desired ASCII	Hex Value	Hat Encoded
Û	DB	~[
Ü	DC	~\\
Ý	DD	~]
Þ	DE	~\^
ß	DF	~_ (Underscore)
à	E0	~`
á	E1	~a
â	E2	~b
ã	E3	~c
ä	E4	~d
å	E5	~e
æ	E6	~f
ç	E7	~g
è	E8	~h
é	E9	~i
ê	EA	~j
ë	EB	~k
ì	EC	~l
í	ED	~m
î	EE	~n
ï	EF	~o
ð	F0	~p
ñ	F1	~q
ò	F2	~r
ó	F3	~s
ô	F4	~t
õ	F5	~u
ö	F6	~v
÷	F7	~w
ø	F8	~x
ù	F9	~y
ú	FA	~z
û	FB	~{
ü	FC	~|
ý	FD	~}
þ	FE	~~
ÿ	FF	~^?

Decimal - Hexadecimal Chart

0	0x00	40	0x28	80	0x50	120	0x78
1	0x01	41	0x29	81	0x51	121	0x79
2	0x02	42	0x2A	82	0x52	122	0x7A
3	0x03	43	0x2B	83	0x53	123	0x7B
4	0x04	44	0x2C	84	0x54	124	0x7C
5	0x05	45	0x2D	85	0x55	125	0x7D
6	0x06	46	0x2E	86	0x56	126	0x7E
7	0x07	47	0x2F	87	0x57	127	0x7F
8	0x08	48	0x30	88	0x58	128	0x80
9	0x09	49	0x31	89	0x59	129	0x81
10	0x0A	50	0x32	90	0x5A	130	0x82
11	0x0B	51	0x33	91	0x5B	131	0x83
12	0x0C	52	0x34	92	0x5C	132	0x84
13	0x0D	53	0x35	93	0x5D	133	0x85
14	0x0E	54	0x36	94	0x5E	134	0x86
15	0x0F	55	0x37	95	0x5F	135	0x87
16	0x10	56	0x38	96	0x60	136	0x88
17	0x11	57	0x39	97	0x61	137	0x89
18	0x12	58	0x3A	98	0x62	138	0x8A
19	0x13	59	0x3B	99	0x63	139	0x8B
20	0x14	60	0x3C	100	0x64	140	0x8C
21	0x15	61	0x3D	101	0x65	141	0x8D
22	0x16	62	0x3E	102	0x66	142	0x8E
23	0x17	63	0x3F	103	0x67	143	0x8F
24	0x18	64	0x40	104	0x68	144	0x90
25	0x19	65	0x41	105	0x69	145	0x91
26	0x1A	66	0x42	106	0x6A	146	0x92
27	0x1B	67	0x43	107	0x6B	147	0x93
28	0x1C	68	0x44	108	0x6C	148	0x94
29	0x1D	69	0x45	109	0x6D	149	0x95
30	0x1E	70	0x46	110	0x6E	150	0x96
31	0x1F	71	0x47	111	0x6F	151	0x97
32	0x20	72	0x48	112	0x70	152	0x98
33	0x21	73	0x49	113	0x71	153	0x99
34	0x22	74	0x4A	114	0x72	154	0x9A
35	0x23	75	0x4B	115	0x73	155	0x9B
36	0x24	76	0x4C	116	0x74	156	0x9C
37	0x25	77	0x4D	117	0x75	157	0x9D
38	0x26	78	0x4E	118	0x76	158	0x9E
39	0x27	79	0x4F	119	0x77	159	0x9F

Figure C-1 Decimal - Hexadecimal Chart (0 to 159 Decimal)

160	0xA0	200	0xC8	240	0xF0
161	0xA1	201	0xC9	241	0xF1
162	0xA2	202	0xCA	242	0xF2
163	0xA3	203	0xCB	243	0xF3
164	0xA4	204	0xCC	244	0xF4
165	0xA5	205	0xCD	245	0xF5
166	0xA6	206	0xCE	246	0xF6
167	0xA7	207	0xCF	247	0xF7
168	0xA8	208	0xD0	248	0xF8
169	0xA9	209	0xD1	249	0xF9
170	0xAA	210	0xD2	250	0xFA
171	0xAB	211	0xD3	251	0xFB
172	0xAC	212	0xD4	252	0xFC
173	0xAD	213	0xD5	253	0xFD
174	0xAE	214	0xD6	254	0xFE
175	0xAF	215	0xD7	255	0xFF
176	0xB0	216	0xD8		
177	0xB1	217	0xD9		
178	0xB2	218	0xDA		
179	0xB3	219	0xDB		
180	0xB4	220	0xDC		
181	0xB5	221	0xDD		
182	0xB6	222	0xDE		
183	0xB7	223	0xDF		
184	0xB8	224	0xE0		
185	0xB9	225	0xE1		
186	0xBA	226	0xE2		
187	0xBB	227	0xE3		
188	0xBC	228	0xE4		
189	0xBD	229	0xE5		
190	0xBE	230	0xE6		
191	0xBF	231	0xE7		
192	0xC0	232	0xE8		
193	0xC1	233	0xE9		
194	0xC2	234	0xEA		
195	0xC3	235	0xEB		
196	0xC4	236	0xEC		
197	0xC5	237	0xED		
198	0xC6	238	0xEE		
199	0xC7	239	0xEF		

Figure C-2 Decimal - Hexadecimal Chart (160 to 255 Decimal)

Revision History

Revision A, Initial Release: November 2004

Revision B: August 2005

Section	Explanation
Chapter 1 – Introduction	Revised “Document Conventions”, “When To Use This Guide”, “Touchscreen and Mouse” and “Accessories” sections. Specified the proper USB adapter cable to use in “Connect” section.
Chapter 2 – Physical Description and Layout	Added “Identifying Your VX7”, “USB Keyboard/Mouse” and “Touchscreen Heater” sections. Updated “Video Subsystem”, “Antenna Connections”, “The Keyboards”, “On/Off Switch”, “General Windows CE .NET Keyboard Shortcuts” and “CAPS LED” sections. Replaced “CapsLock, Scroll Lock and the VX7” section with “CapsLock and the VX7” and “Scroll Lock and the VX7” sections. Replaced “Antenna Connector” section with “Antenna Connections” section.
Chapter 4 – System Configuration	Revised “About”, “Administrator Control”, “LAUNCH.EXE”, “Reflash the VX7”, “Accessibility” and Date/Time” sections. Added “2.4GHz Radio Configuration”, “Changing the Display Resolution”, “Disabling the Touchscreen Heater”, “Configuring CapsLock Behavior” and “Configuring IPv6 Broadcast Messages” sections. Removed “Cisco – Aironet Configuration Utility (ACU)” and “Symbol” sections. This information is now included in Chapter 5.
Chapter 5 – Wireless Network Configuration	Added new chapter containing sections removed from Chapter 4.

Revision C: October 2005

Section	Explanation
Chapter 1 – Introduction	Updated “When To Use This Guide”. Updated “Accessories” list.
Chapter 4 – System Configuration	Renamed “Configuring IPv6 Broadcast Messages” section to “Configuring IPv6” and revised section.
Chapter 5 – Wireless Network Configuration	Revised “Introduction” and “Cisco – Aironet Client Utility (ACU)” section. Renamed “Configuring VX7 Radio” to “Configuring VX7 Radio Without WPA”. Added “WPA for the VX7” section.

Revision D: August 2006

Section	**Explanation**
Entire Manual	Updated all images with the new LXE logo.
Notices	Updated copyrights and trademarks.
Chapter 1 – Introduction	Revised “Accessories” listing.
Chapter 2 – Physical Description and Layout	Revised “On/Off Switch”, “Scanner Serial Connector (COM1)”, “Printer/PC Serial Connector (COM3)”, “Install the 2.4GHz Type II PCMCIA Radio”, “Input Panel (Virtual Keyboard)”, “Video Subsystem” and “The Display” . Added new section: “Technical Specifications – Screen Blanking Cable”.
Chapter 3 – Power Supply	Revised “VX7 Input Power Specifications”.
Chapter 4 – System Configuration	Revised “Installed Software”, “Start Menu Program Options”, “Network and Dialup Connections”, “Control Panel Options”, “About”, “Date/Time”, “Keyboard”, “Password”, “Regional Settings”, “Remote Desktop Connection”, “Scanner”, “Storage Manager”, “LAUNCH.EXE” and “Reflash the VX7” sections. Added new sections: “Folders Copies at Startup” and “Enabling GrabTime”. Removed section: “Bluetooth Manager”. Renamed “VX7 Command Line Utility” to “VX7 Command Line Utilities” and updated section.
Chapter 5 – Wireless Network Configuration	Revised “Profiles Tab” section. Split radio configuration section into two sections “Cisco Radio” and “Symbol radio”. Added a new section, “Summit Radio”. Each section contains the manufacturer specific configuration information. Moved all certificate generating and installation instructions to a new “Certificates” section.
Chapter 6 – AppLock	New chapter. Information previously included in Appendix B is now referred to as “Single Application”. Added Multi Application AppLock to chapter.
Appendix B – Technical Specifications	Added “Revision History” to appendix. Added Summit Radio Technical Specifications.
Appendix C – AppLock	Deleted appendix. Information is now included in Chapter 6, AppLock.

Revision E: November 2006

Section	Explanation
Notices	Added Wavelink trademark information.
Chapter 1 – Introduction	Revised “When to Use this Guide”.
Chapter 2 – Physical Description and Layout	Added information that was previously included in Chapter 3, “Power Supply”.
Chapter 3 – Power Supply	Deleted chapter. This information is now included in Chapter 2, “Physical Description and Layout”.
Chapter 4 – System Configuration	Renamed to Chapter 3, “System Configuration”. Revised “Software Load”, “LAUNCH.EXE”, Control Panel Options” and “Scanner” section. Scanner information is now included in Chapter 6, “Scanner”. Added new section “Wavelink Avalanche Enabler Configuration”.
Chapter 4 – Scanner	Created new chapter with scanner information removed from Chapter 4, “System Configuration” and updated as necessary.
Chapter 5 – Wireless Network Configuration	Revised “Summit Radio” section to include new Sign-On screen and support for PEAP-GTC.
Chapter 6 – AppLock	Revised “Setup A New Device”.

Revision F: November 2007

Section	Explanation
Entire Manual	Added CE 5.0 information and instruction where applicable.
Chapter 1 – Introduction	Added Bluetooth information. Revised Accessories listing.
Chapter 2 – Physical Description and Layout	Added Bluetooth information. Revised “Vehicle 12-80VDC Power Connection” with updated graphic.
Chapter 3 – System Configuration	Added Bluetooth information. Revised “Mixer” and “Step 3: Check Barcode Length” sections. Revised “Enabling GrabTime”. Revised “Wavelink Avalanche Enabler Configuration” for Avalanche Mobility Center.
Chapter 5 – Wireless Network Configuration	Updated chapter for EAP-FAST support, tray icon, help feature, etc. included in latest version of SCU. Revised section: “Admin login”.

Index