Honeywell

THE POWER OF **CONNECTED**

Thor VM2

Vehicle-Mounted Computer

with Microsoft® Windows® Embedded Standard 2009
with Microsoft® Windows® Embedded Standard 7
with Microsoft® Windows® 7 Professional

User Guide

Disclaimer

Honeywell International Inc. ("HII") reserves the right to make changes in specifications and other information contained in this

document without prior notice, and the reader should in all cases consult HII to determine whether any such changes have been made. The information in this publication does not represent a commitment on the part of HII.

HII shall not be liable for technical or editorial errors or omissions contained herein; nor for incidental or consequential damages resulting from the furnishing, performance, or use of this material. HII disclaims all responsibility for the selection and use of soft-ware and/or hardware to achieve intended results.

This document contains proprietary information that is protected by copyright. All rights are reserved. No part of this document may be photocopied, reproduced, or translated into another language without the prior written consent of HII.
Copyright ©2012 – 2018 Honeywell International Inc. All rights reserved.

Web Address: www.honeywellaidc.com

Trademarks

RFTerm is a trademark or registered trademark of EMS Technologies, Inc. in the United States and/or other countries.

Microsoft®, Windows®, ActiveSync®, MSN, Outlook®, Windows Mobile®, the Windows logo, and Windows Media are registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Intel® and Atom™ are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Laird Technologies, the Laird logo, Summit Data Communications, the Summit logo, and "Connected. No Matter What" are trade-marks of Laird Technologies, Inc.

Wi-Fi®, WMM®, Wi-Fi Mutlimedia™, Wi-Fi Protected Access®, WPA™, WPA2™ and the Wi-Fi CERTIFIED™ logo are trademarks or regis-tered trademarks of Wi-Fi Alliance.

The Bluetooth® word mark and logos are owned by the Bluetooth SIG, Inc.

Symbol® is a registered trademark of Symbol Technologies. MOTOROLA, MOTO, MOTOROLA SOLUTIONS and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license.

Freefloat, Link*One, Key*One and Access*One are trademarks of Freefloat, Mölndalsvägen 30B, SE-412 63Gothenburg, Sweden.

RAM® and RAM Mount™ are both trademarks of National Products Inc., 1205 S. Orr Street, Seattle, WA 98108.

Qualcomm® is a registered trademark of Qualcomm Incorporated. Gobi is a trademark of Qualcomm Incorporated.

Verizon® is a registered trademark of Verizon Trademark Services LLC.

T-MOBILE® is a registered trademark of Deutsche Telekom AG.

AT&T® is a registered trademark of AT&T Intellectual Property.

Google and the Google Logo are registered trademarks of Google LLC.

SD and SDHC are trademarks or registered trademarks of SD-3C, LLC in the United States and/or other countries.

SanDisk® and CompactFlash® are trademarks of SanDisk Corporation, registered in the United States and other countries.

ATP is a trademark of ATP Electronics, Inc.

FreeDos is a trademark of Jim Hall. FreeDOS is distributed under the GNU General Public License Version 2 (GPLv2) and GNU General Public License Version 3 (GLPv3). Source code is available by contacting Technical Assistance or by writing Honeywell Scanning and Mobility, 9680 Old Bailes Road, Fort Mill, SC 29707 USA and requesting software package **VM2PFDOS11SRC1AB**.

Other product names or marks mentioned in this document may be trademarks or registered trademarks of other companies and are the property of their respective owners.

Patents

For patent information, refer to www.hsmpats.com.

TABLE OF CONTENTS

CHAPTER

1 CUSTOMER SUPPORT

Technical Assistance

To search our knowledge base for a solution or to log in to the Technical Support portal and report a problem, go to www.hsmcontactsupport.com.

For our latest contact information, see www.honeywellaidc.com/locations.

Product Service and Repair

Honeywell International Inc. provides service for all of its products through service centers throughout the world. To obtain warranty or non-warranty service, return your product to Honeywell (postage paid) with a copy of the dated purchase record. To learn more, go to www.honeywellaidc.com and select **Service & Repair** at the bottom of the page.

Limited Warranty

For warranty information, go to www.honeywellaidc.com and click **Get Resources** > **Product Warranty**.

Send Feedback

Your feedback is crucial to the continual improvement of our documentation. To provide feedback about this manual, contact the Honeywell Technical Communications department at ACSHSMTechnicalCommunications@honeywell.com.

GETTING STARTED

Overview

The Thor VM2 Vehicle Mount Computer (VMC) is a rugged, vehicle mounted computer running a Microsoft® Windows® Embedded Standard 2009, Windows® 7 Professional or Windows® Embedded Standard 7 operating system and capable of wireless data communications from a fork-lift truck or any properly configured vehicle. Wireless communications are supported over a 802.11 WLAN network and, optionally, over a WWAN network. The Bluetooth® module supports Bluetooth printers and scanners.

> ⚠ **Caution: Before shipping the Thor VM2, be sure to** Disconnect UPS Battery

The Thor VM2 is designed for use with a vehicle dock. Two models of docks are supported, a Standard Dock and an Enhanced Dock. The dock installs in the vehicle and connects to vehicle power. The dock provides conditioned input power for the Thor VM2. Peripheral connections are on the dock. The Thor VM2 is designed to easily be removed from the dock with a latch on the lower rear of the Thor VM2 housing. Since the dock remains attached to the vehicle, the Thor VM2 computer can easily be moved from one vehicle equipped with a dock to another vehicle equipped with a dock.

The Thor VM2 contains a UPS battery which, when fully charged, can power the Thor VM2 for a minimum of 30 minutes. This can be when the Thor VM2 is not attached to a dock or when the Thor VM2 is attached to a dock but the vehicle power is interrupted, such as when the vehicle battery is being changed.

The Thor VM2 can be used with or without an external keyboard. There are 5 programmable keys (P1-P5) on the front bezel and, when used with the Orange modifier key, provide 5 additional programmable keys (P6-P10).

Contact Technical Assistance for information on the latest upgrades for your Thor VM2.
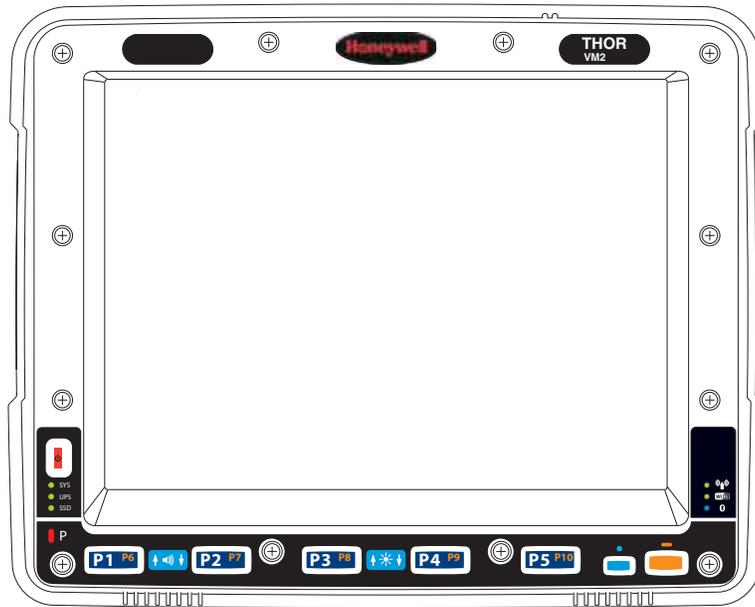
About this Guide

This user's guide has been developed for a Thor VM2 with a Microsoft® Windows® Embedded Standard 2009, Windows® 7 Professional or Windows® Embedded Standard 7 operating system.

Out of the Box

The following items may be packaged separately:

- Thor VM2
- Standard or Enhanced Dock (includes 10–60VDC power cable)
- RAM or U-Bracket vehicle mount kit

If you ordered additional accessories for the Thor VM2, verify they are also included with the order. Keep the original packaging material in the event the Thor VM2 should need to be returned for service. For details, see Technical Assistance.

Initial Setup for Thor VM2

This page lists a quick outline of the steps you might take when setting up a new Thor VM2. More instruction for each step is listed later in this guide.

Contact Technical Assistance if you need additional help.

Hardware Setup

⚠ **Caution: If the Thor VM2 has connectors for external antennas, do not power up the Thor VM2 without the external antennas connected. Damage to the WLAN radio may result.**

1. Install RAM Mount or Install U Bracket Mount to the vehicle.
2. Place Thor VM2 in the Dock.
3. Secure the optional external keyboard to either an integrated or remote mounting bracket.
4. Connect Cables for any peripherals.
5. Connect Power.
6. Secure all cables in Strain Relief Cable Clamps.
7. Press the Power Switch on the dock to the on position.
8. Press the Power Button on the Thor VM2.

Note: After the initial power on, the Thor VM2 can be configured to automatically power on, either when power is attached or the vehicle ignition is turned on.

Software

This section only applies if the Thor VM2 was ordered with an operating system. For a Thor VM2 ordered without an operating system, see Thor VM2 with no Operating System.

Languages

The language selection and installation process varies by operating system:

- The Thor VM2 with a Windows Embedded Standard 2009 operating system may be shipped with an English only operating system. Contact Technical Assistance to order a Thor VM2 Recovery DVD in a different language. The language installed is identified on the **Software** tab of the About control panel.
- The Thor VM2 with a Windows Embedded Standard 7 operating is delivered with an English operating system. Additional Language Packs are available for installation using the Region and Language control panel. The language installed is identified on the **Software** tab of the About control panel.
- The Thor VM2 with a Windows 7 Professional operating system provides a choice between English or Simplified Chinese upon initial configuration. Once selected, the

operating system language cannot be changed without reinstallation using a recovery DVD. Recovery DVDs may also be available for additional languages. Contact Technical Assistance to order a Thor VM2 Recovery DVD. The language installed is identified on the **Software** tab of the About control panel.

First Boot

The first boot (also known as the Out of Box Experience) provides initial configuration of the Thor VM2. When a Thor VM2 is ordered with a Windows 7 Professional or Windows Embedded 7 operating system, the product key is printed on a decal on the rear of the Thor VM2. It may be necessary to remove the Thor VM2 from the dock to view the product key decal. Under normal circumstances, it is not necessary to re-enter the product key as it was entered during the manufacturing process. If the Thor VM2 was ordered without an operating system, a product key must be provided by the customer to activate Windows.

When a new Thor VM2 starts up a EULA (End User License Agreement) may be displayed on the touch screen. It remains on the screen until the **Accept** or **Decline** button is tapped with a stylus.

Tap the **Accept** button to accept the EULA terms and the Thor VM2 continues the startup process. The EULA is not presented to the user again.

Tap the **Decline** button to decline the EULA and the Thor VM2 reboots. It will continue to reboot until the **Accept** button is tapped with the stylus.

Software Setup

Hardware setup should be completed before starting software setup.

1. If prompted, perform Touch Screen Calibration.
2. Select a Power Scheme or Power Plan and set timers.
3. Adjust Speaker Volume.
4. Pair Bluetooth devices
5. Set wireless client parameters using the Summit Client Utility.
6. Set terminal emulation parameters.

Dock

The Thor VM2 assembly consists of two parts, the Thor VM2 computer and the dock. The Thor VM2 contains an internal UPS battery that, once fully charged, powers the Thor VM2 for a minimum of 30 minutes when the unit is not mounted in the dock.

There are three available vehicle-mount docks for the Thor VM2:

- VM1D Standard Dock
- VM3D Enhanced Dock
- VMXD Enhanced Dock

Additionally an off-vehicle dock is available for the Thor VM2 for use in environment such as an office where AC power is available:

- VMXD Enhanced Dock for Off-Vehicle Use

All docks provide:

- A mount for the Thor VM2 computer. The dock attaches to a vehicle via a RAM or U-bracket mount or to a RAM table stand for use in an office environment.
- Conditioned power for the Thor VM2. The vehicle-mount docks accept 10-60VDC power input directly or 50-150VDC power input with a DC/DC converter. The off-vehicle dock requires an AC/DC power supply.
- Mobility of the Thor VM2, since the dock remains attached to the vehicle the Thor VM2 computer can easily be moved from one vehicle equipped with a dock to another.
- I/O ports as described in the below.
- Strain relief provisions for cables.
- Headset connection via an adapter cable. When a headset is not attached, the microphone and speakers on the Thor VM2 are active.

Features of the docks are described in the following sections.

VM1D Standard Dock

⚠ **Caution: This dock is designed for DC power vehicle–mounted applications only.**

SKUs	VM1001VMCRADLE (with RAM ball) VM1002VMCRADLE VM1003VMCRADLE
Power Connection	Direct or DC/DC power supply
Serial Ports	COM1 and COM2
USB Ports	USB port provides host connection via an adapter cable. This port also supports Honeywell external keyboards.
Ethernet	N/A
CANbus	CANbus connection via an adapter cable
Audio	Headset connection via an adapter cable
Screen Blanking	Supported via COM1 and COM2 connectors.
Ignition Control	Supported

VM3D Enhanced Dock

Caution: This dock is designed for DC power vehicle-mounted applications only.

SKU	VM3001VMCRADLE
Power Connection	Direct or DC/DC power supply
Serial Ports	COM1 and COM2
USB Ports	USB1 port provides host connection via an adapter cable. This port also supports Honeywell external keyboards. USB2 port provides two USB host ports via an adapter cable. Direct USB host connection on top of dock.
Ethernet	RJ-45 Ethernet connection on top of dock. *Note:* *For Windows 7 and Windows Embedded Standard 7: An upgrade is necessary to support the Ethernet port on this dock. See Thor VM2 and Enhanced Dock Support.* *Note:* *For Windows Embedded Standard 2009: The Ethernet port is not supported.*
CANbus	CANbus connection via an adapter cable
Audio	Headset connection via an adapter cable
Screen Blanking	Supported via COM1 and COM2 connectors.
Ignition Control	Supported

VMXD Enhanced Dock

⚠ **Caution: This dock is designed for DC power vehicle–mounted applications only.**

This dock is designed for use when the Thor VM2 is replacing a Thor VX8 or Thor VX9. This dock utilizes the existing vehicle wiring from the earlier computer and supports screen blanking through that wiring.

SKUs	VMX004VMCRADLE
Power Connection	Designed to connect to existing Thor VX8 or Thor VX9 power cable only, using existing DC/DC power supply
Serial Ports	COM1 and COM2 (see note below)
USB Ports	USB1 port provides host connection via an adapter cable. This port also supports Honeywell external keyboards. USB2 port provides two USB host ports via an adapter cable. Direct USB host connection on top of dock.
Ethernet	RJ-45 Ethernet connection on top of dock. *Note:* *For Windows 7 and Windows Embedded Standard 7: An upgrade is necessary to support the Ethernet port on this dock. See Thor VM2 and Enhanced Dock Support.* *Note:* *For Windows Embedded Standard 2009: The Ethernet port is not supported.*
CANbus	CANbus connection via an adapter cable
Audio	Headset connection via an adapter cable
Screen Blanking	Supported via power cable connector. (see note below)
Ignition Control	Not supported

Note: *For the VMX Enhanced Dock: COM1 is used for screen blanking (via the power cable connector) and is unavailable when the screen blanking box is attached. When a screen blanking box is attached, any external serial device such as a scanner, must be connected to the COM2 port on the dock. If a screen blanking box is not connected via the power cable, the COM1 port on the dock is available for a serial device.*

VMXD Enhanced Dock for Off-Vehicle Use

⚠️ **Caution: This dock is designed for AC power (non vehicle-mounted) applications only.**

SKU	VMX005VMCRADLE
Power Connection	AC/DC Adapter
Serial Ports	COM1 and COM2
USB Ports	USB1 port provides host connection via an adapter cable. This port also supports Honeywell external keyboards. USB2 port provides two USB host ports via an adapter cable. Direct USB host connection on top of dock.
Ethernet	RJ-45 Ethernet connection on top of dock. *Note:* *For Windows 7 and Windows Embedded Standard 7: An upgrade is necessary to support the Ethernet port on this dock. See Thor VM2 and Enhanced Dock Support.* *Note:* *For Windows Embedded Standard 2009: The Ethernet port is not supported.*
CANbus	CANbus connection via an adapter cable
Audio	Headset connection via an adapter cable
Screen Blanking	Supported via COM1 and COM2 connectors.
Ignition Control	Not supported

Thor VM2 and Enhanced Dock Support

The Thor VM2 with a Windows 7 Professional or Windows Embedded Standard 7 operating system supports the enhanced dock models. To support the Ethernet port:

- A BIOS and software upgrade is necessary.
- A MAC address must be assigned to the Ethernet port.

Contact Customer Support for information.

The Thor VM2 with a Windows Embedded Standard 2009 operating system supports the enhanced dock models. However the Ethernet port is not supported.

Additional Connectors

External antenna connectors may be present on the back of the Thor VM2. The connectors may include:

- 802.11 WLAN antenna connectors, used when the Thor VM2 is not equipped with internal antennas.

- External GPS antenna connector, when the Thor VM2 is equipped with GPS.

- External WWAN antenna connectors, when the Thor VM2 is equipped with WWAN. Optional WWAN radio (available in North America, Europe, New Zealand, and Australia only).

⚠ **Caution: If the Thor VM2 has connectors for external antennas, do not power up the Thor VM2 without the external antennas connected. Damage to the WLAN radio may result.**

Scanners

The Thor VM2 supports external scanners. These scanners may be:

- A tethered scanner attached to a serial port. See Connect a Tethered Scanner for details on connecting a serial scanner. See Scanner Wedge for information on processing scanned bar code data.

- A tethered scanner attached to a USB port. See USB Scanner for details on connecting a USB scanner. See Scanner Wedge for information on processing scanned bar code data.

- A Bluetooth scanner. See Bluetooth for details on connecting a Bluetooth scanner. See Scanner Wedge for information on processing scanned bar code data.

Components

Front View – Thor VM2

Microphone

Power
Button

Speakers

Back View - Thor VM2

Antenna Connectors

SD Card
Access
Panel

SIM Card
Access
Panel

Dock
Contact
Pads

Provision for
Laptop Security
Cable

Provision for Padlock   Quick Release Handle
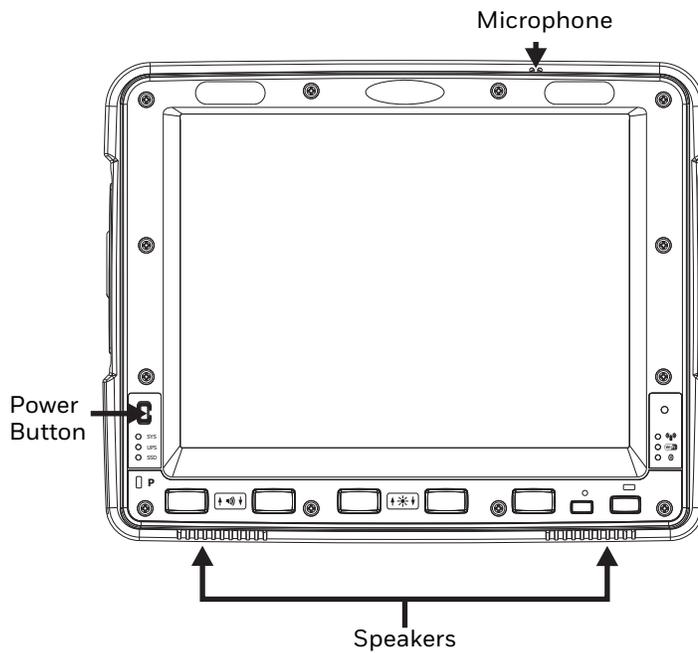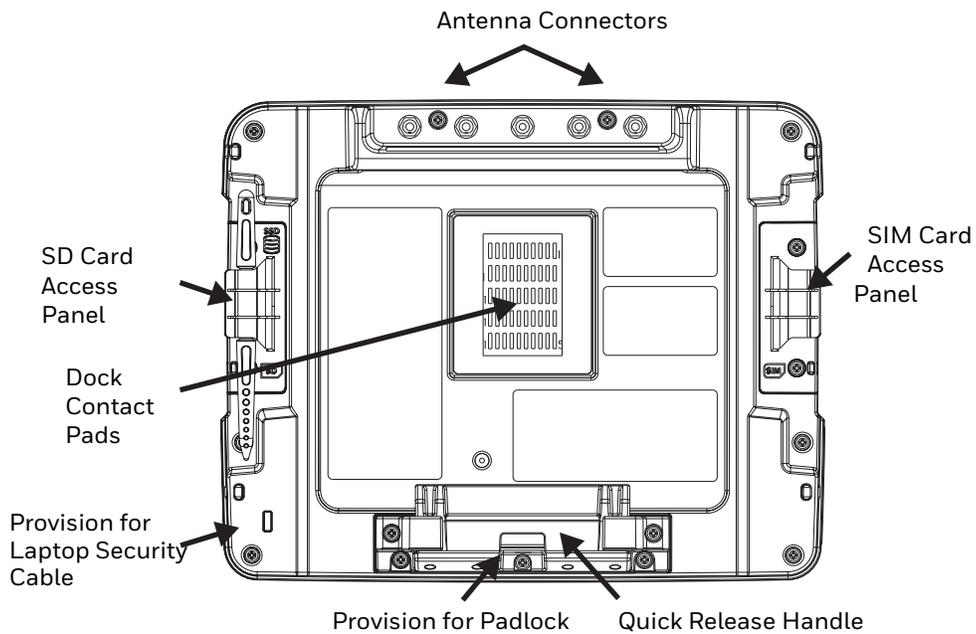
Access Panels – Thor VM2

SD Card Access Panel with door removed
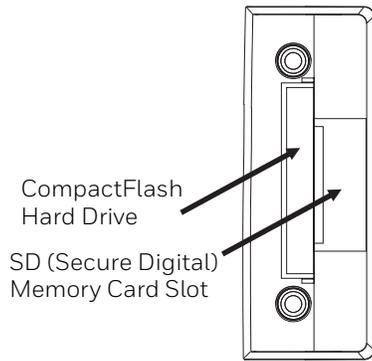
SIM Card Access Panel with door removed

CompactFlash
Hard Drive

SD (Secure Digital)
Memory Card Slot

Card Slot
for WWAN Radio

UPS Battery
Disconnect

Access Panel Door is labeled with **SSD** and **SD** .
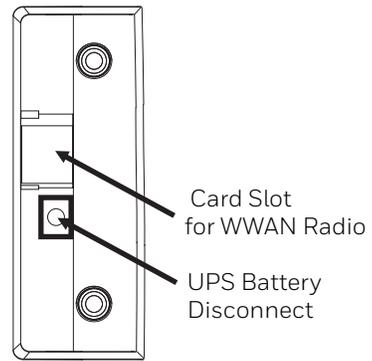
Access Panel Door is labeled with **SIM** .

Front View – Dock

Standard Dock
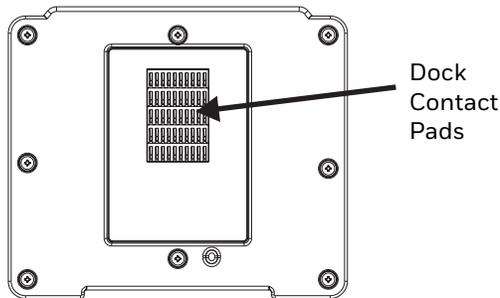
Dock
Contact
Pads

Enhanced Dock

The Enhanced Dock has a foam surround around the dock contact pad.

Dock
Contact
Pads

Foam
Surround
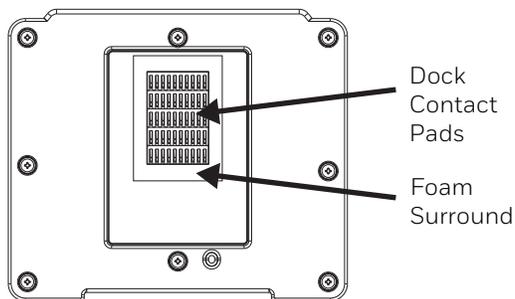
Back View - Dock

The connectors on the back of the dock vary by dock model.

Standard Dock
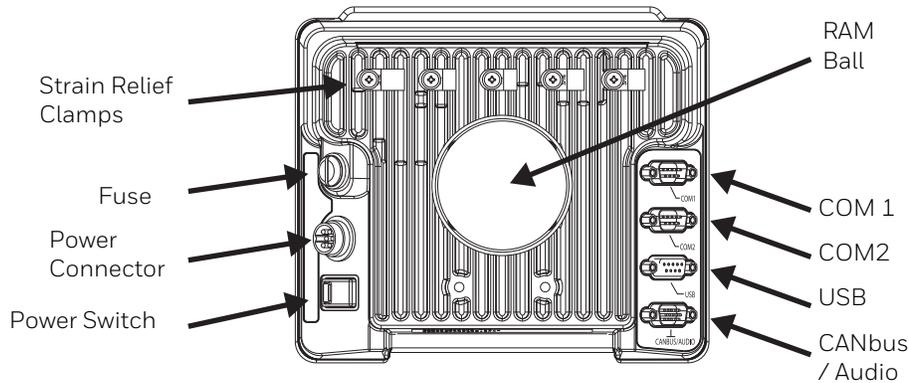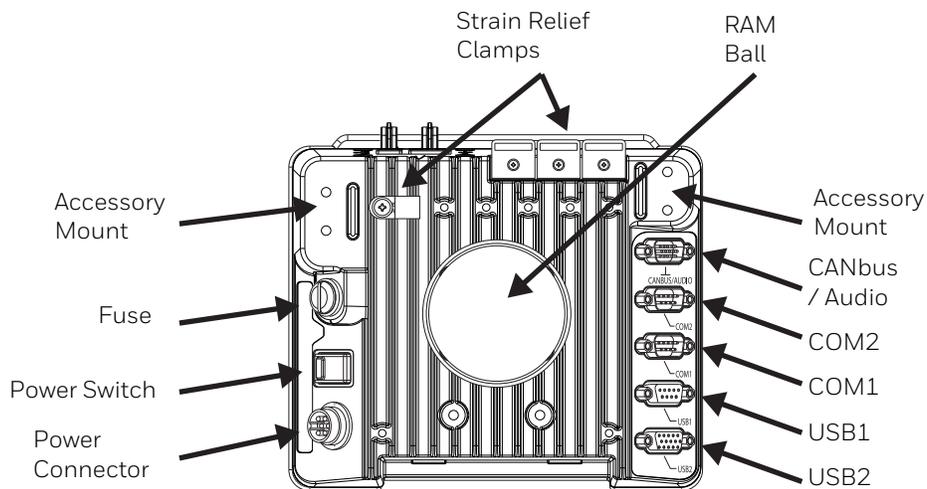
Strain Relief Clamps

RAM Ball

Fuse

Power Connector

Power Switch

COM 1

COM2

USB

CANbus / Audio

Enhanced Dock

Strain Relief Clamps

RAM Ball

Accessory Mount

Accessory Mount

Fuse

Power Switch

Power Connector

CANbus / Audio

COM2

COM1

USB1

USB2

Note: *For the VMX Enhanced Dock: COM1 is used for screen blanking (via the power cable connector) and is unavailable when the screen blanking box is attached. When a screen blanking box is attached, any external serial device such as a scanner, must be connected to the COM2 port on the dock. If a screen blanking box is not connected via the power cable, the COM1 port on the dock is available for a serial device*

Top View – Enhanced Dock

Only the Enhanced Dock has these connectors on the top. The connectors are located behind water tight plugs.
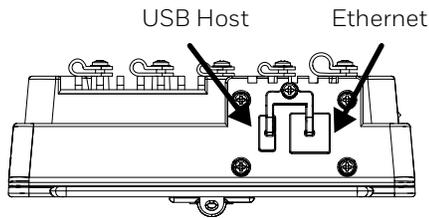
USB Host   Ethernet

Note: *A BIOS and operating system upgrade is necessary to support the Ethernet port with the Windows 7 or Windows Embedded Standard 7 operating systems. Contact Thor VM2 and Enhanced Dock Support for information.*

Backlights and Indicators

Display Backlight

There are several configuration options for the Thor VM2 display backlight:

Power Management

The display backlight is controlled by power management. When the user activity timer expires, the display backlight is turned off. Timeouts can be set for the available power management schemes.

See Power Options for configuration options.

Backlight Brightness

The intensity of the display backlight can be manually configured:

1. Press the **Blue** key to enter Blue mode
2. Press the **P3** key to increase backlight brightness or the **P4** key to decrease backlight brightness.
3. Press the **Blue** key to exit Blue mode.

Refer to the Screen Control panel for the current display brightness level.

Screen Blanking

The Thor VM2 can be configured to blank (blackout) the display while the vehicle is in motion.

Refer to the Screen Control panel for information.

Keypad Backlight

By default, the integrated keypad backlight follows the display backlight. The integrated keypad backlight can be disabled.

To change this behavior, see the Options control panel.

The external USB keyboard backlight is manually controlled.

Speaker Volume

The speaker volume can be adjusted via the Thor VM2 keypad:

1. Press the **Blue** key to enter Blue mode
2. Press the **P1** key to increase speaker volume or the **P2** key to decrease speaker volume.
3. Press the **Blue** key to exit Blue mode.

The current volume level can be viewed on the Sounds control panel or via the system tray speaker icon. These items can also be used to adjust speaker volume.

Power Up

⚠️ If a USB drive, such as a thumb drive is attached to the Thor VM2, the device attempt to boot from the USB drive and cannot. Remove the USB drive and power up the Thor VM2 again.

The dock has a power switch on the back.
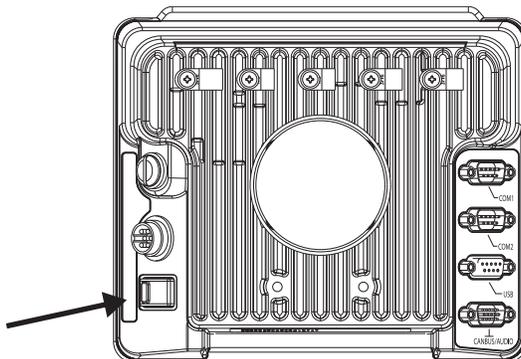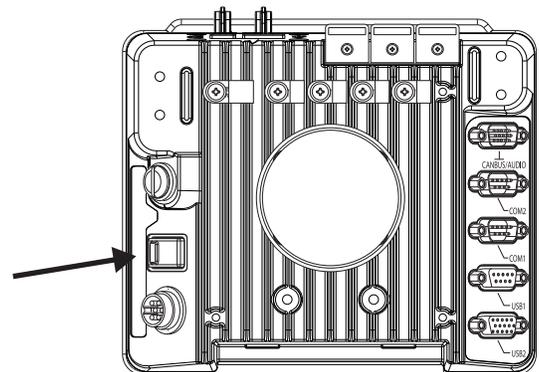
Standard Dock   Enhanced Dock

The "On" side of this rocker switch has a raised bump to allow the state of the switch to be determined when the switch may not be easily viewed, for example, after the dock is mounted in a vehicle.

After external power has been connected and the Thor VM2 has been mounted in the dock, press the side of the power switch with the raised bump to pass power from the dock to the Thor VM2.

Next locate the power button on the front of the Thor VM2.
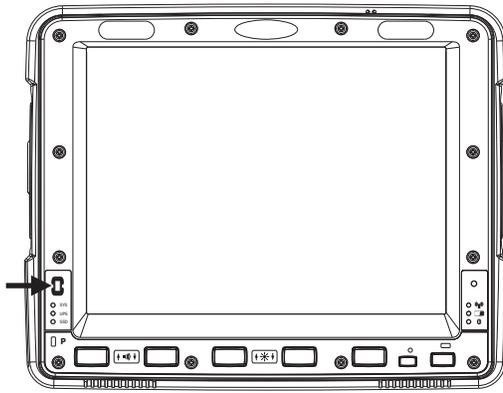
Press the power button to turn the Thor VM2 on. When the Windows desktop is displayed or an application begins, the power up sequence is complete.

After initial power on, the Thor VM2 can be configured to automatically power on. See Power Controls for more information.

Rebooting the Thor VM2

⚠️ If a USB drive, such as a thumb drive is attached to the Thor VM2, the device attempts to boot from the USB drive:

- If the USB drive contains a bootable sector, the Thor VM2 boots from the USB drive.
- If the USB drive does not contain a bootable sector, the Thor VM2 does not boot. Remove the USB drive and boot the Thor VM2 again.

Restart

Restart performs a controlled shutdown of the Thor VM2 and then restarts the device.

- If an optional keyboard is attached, use the **Ctrl** + **Alt** + **Del** keypress sequence to start the task manager. Tap the **Shut Down** button and select **Restart** from the pull-down list. Tap the **OK** button to restart the Thor VM2.
- Select **Start** > **Shut Down** > **Restart** and tap **OK** to restart the Thor VM2.
- Use the **P1 + P5 + Orange** key press sequence to reboot the Thor VM2. The keys must be pressed in sequence; they do not need to be held down simultaneously.

Tapping the Touch Screen with a Stylus

Note: *Always use the point of the stylus for tapping or making strokes on the touch screen.*

Never use an actual pen, pencil, or sharp/abrasive object to write on the touch screen.

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.

Firmly press the stylus into the stylus holder when the stylus is not in use.

Using a stylus is similar to moving the mouse pointer then left-clicking icons on a desktop computer screen.

Using the stylus to tap icons on the touch screen is the basic action that can:

- Open applications
- Choose menu commands
- Select options in dialog boxes or drop-down boxes
- Drag the slider in a scroll bar
- Select text by dragging the stylus across the text
- Place the cursor in a text box prior to typing in data
- Place the cursor in a text box prior to retrieving data using a scanner/imager.

 A right click is generated by tapping the mouse icon, usually located in the upper right hand corner of the screen. After tapping, the mouse icon highlights the right button. The next touch screen tap is treated as a right click. The mouse icon returns to the left button highlighted so subsequent taps are treated as left clicks.

Note: *If the mouse icon is not displayed, this feature can be enabled by tapping the PenMount icon* *in the System Tray. From the menu that pops up, tap the Right Button to enable the mouse icon. When this option is enabled, a check mark is displayed in the menu.*

A stylus replacement kit is available.

When a dialog box is too large for the display, tap and drag the dialog box up or down or from side to side to view the remainder of the dialog box.

Setup Terminal Emulation Parameters

Note: *The instructions below are for Honeywell RFTerm. If a different terminal emulation software is installed on your Thor VM2 refer to the documentation for that software.*

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 (802.11*x*), make sure your mobile client is communicating with the Access Point.

2. From **Start** > **Programs,** run 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 Tool Bar. Upon a successful connection, you should see the host application screen displayed.

To change options such as Display, Colors, Cursor, Bar Code, etc., refer to these sections in the *RFTerm Reference Guide* for complete descriptions of these and other features.

Cleaning

Cleaning the Thor VM2 and the Dock

Dampen a cloth with the cleaner and then wipe the surface. Do not spray the cleaner directly onto the Thor VM2 or the dock. Avoid harsh chemicals. The following cleaners are recommended:

- Windex® Glass Cleaner
- Formula 409® All-Purpose Cleaner or Glass and Surface Cleaner
- Fantastik® All Purpose Cleaner
- Liquid hand soap

Cleaning the Touch Screen

Note: *These instructions are for components made of glass. If there is a removable protective film sheet on the display, remove the film sheet before cleaning the screen.*

Keep rough or sharp objects away from the Thor VM2 touch screen and, if installed, the bar code reader scanning aperture.

If the glass becomes soiled or smudged, clean only with a standard household cleaner such as Windex® without vinegar or use isopropyl alcohol. Dampen the cloth with the cleaner and then wipe the surface.

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 and particulates can be removed with clean, filtered canned air.

Startup Help

Contact Technical Assistance if you need more help.

Touch screen is not accepting stylus taps or needs recalibration.	Press **Ctrl+Esc** to force the Start Menu to appear. Use the tab, backtab and arrow keys to move the cursor from element to element. See Touch Screen Calibration.

Thor VM2 seems to lockup as soon as it is rebooted.	There may be slight delays while the wireless client connects to the network, authorization for voice-enabled applications complete, and Bluetooth relationships establish or re-establish. When an application begins, the Thor VM2 is ready for use.

CHAPTER
3

HARDWARE OVERVIEW

System Hardware

802.11a/b/g/n Wireless Client

The Thor VM2 has an 802.11a/b/g/n network card that supports diversity with two internal or external antennas. Power management for the network card is configured with the Summit Client Utility or Laird Connection Manager.

Central Processing Unit

The CPU is a 1.6 GHz Intel Atom processor.

The operating system is Microsoft Windows Embedded Standard 2009, Windows Embedded Standard 7 or Windows 7 Professional.

The OS image is stored on an internal CompactFlash memory card and is loaded into DRAM for execution.

Input/Output Components

The Thor VM2 supports the following I/O components of the core logic:

- Two 9-pin RS-232 serial ports, COM1 and COM2, on dock.
- One slot for CompactFlash (CF) card for operating system storage.
- One slot for SD memory card for storage expansion.
- Integrated keyboard with programmable keys.
- Ports available via adapter cables on dock: USB host port, CANbus, Audio. USB client port is not supported with Windows Embedded Standard 2009, Windows Embedded Standard 7 or Windows 7 Professional. Multiple USB host ports are available when using the Enhanced Dock.
- Direct connections on Enhanced Dock: Ethernet and USB host. A BIOS and operating system upgrade is necessary for other operating systems. See *Thor VM2 and Enhanced Dock Support* for more information.

System Memory

Main system memory is 2GB SDRAM.

Video Subsystem

The Thor VM2 video subsystem consists of a color TFT display. The video subsystem complies with the VESA VL bus standard. The resolution of this display is 1024x768 pixels. This resolution complies with the SVGA graphics industry standard.

The display supports screen blanking to eliminate driver distraction when the vehicle is in motion.

Audio Interface

Speakers are located on the bottom front of the Thor VM2. A headset adapter cable provides a connection for headset operation. When a headset is plugged into the adapter cable, the main speakers are disabled.

A microphone is located at the upper right of the Thor VM2 display, near the Thor VM2 emblem. When a headset is plugged into the adapter cable, the internal microphone is disabled.

Card Slots

CompactFlash (CF) Slot

The CF ATA slot is not hot swappable. The Thor VM2 must be powered down to insert or remove an ATA card. Since the operating system is stored on the CF ATA card, the Thor VM2 cannot operate without the ATA card.

Secure Digital (SD) Slot

The SD slot accepts an SD memory card. The SD card is hot swappable.

Bluetooth EZPair

The Thor VM2 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 cannot select PIN authentication or encryption on connections from the Thor VM2. However, the Thor VM2 supports authentication requests from pairing devices. If a pairing device requests authentication or encryption, the Thor VM2 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 simultaneously supports one printer as a slave Bluetooth device and one scanner, either as a slave or as a master Bluetooth device.

- The LED on the Bluetooth scanner illuminates during a scanning operation.

- Bar code data captured by the Bluetooth scanner can be manipulated by the settings in the optional Freefloat Link*One application.

- Multiple beeps may be heard during a bar code scan using a mobile Bluetooth scanner. The mobile Bluetooth scanner may beep as the bar code data is accepted/ rejected and the Thor VM2 may beep during final bar code data manipulation.

WWAN

WWAN (Wireless Wide Area Networking) is available on the Thor VM2. A slot is provided for a SIM card.

GPS

GPS (Global Positioning System) is available on the Thor VM2.

Power

Vehicle DC Power Supply

> ⚠ **Caution: Vehicle DC power supply connections require a DC–compatible Dock.**

Vehicle power input for the Thor VM2 dock is 10V to 60V DC and is accepted without the need to perform any manual operation within the Thor VM2 dock, see 12-48 VDC Vehicles (10-60 VDC Direct Connection). The dock provides a conditioned power output for the Thor VM2. By using a specified DC/DC power supply, input voltage of 50-150V DC can be accepted, see 60-144 VDC Vehicles (50-150 VDC Power Supply, Screws on Top of Lid) or 60-144 VDC Vehicles (50-150 VDC Power Supply, Screws on Top of Lid).

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

External AC Power Supply

If 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. AC to DC power input for the Thor VM2 is delivered to the dock via an optional external power supply and adapter cable. See External AC/DC Power Supply.

Uninterruptible Power Supply

The Thor VM2 contains an internal UPS battery.

The UPS battery is automatically charged when the Thor VM2 is placed in a powered dock, provided the safe charging temperature conditions below are met.

When external power is removed, the UPS automatically powers the Thor VM2 with no user intervention. When running on UPS power, the power management timeouts may be different than when vehicle power is applied.

The UPS allows the Thor VM2 to continue operation when not mounted in a dock or when the vehicle battery is being swapped. When fully charged the UPS battery is designed to power the Thor VM2 for a minimum of 30 minutes at temperatures of -20ºC (-4ºF) or greater.

If operating on UPS power and the UPS battery becomes critically low, the Thor VM2 performs a controlled shutdown.

If there is no external power available, there must be 10% or greater power in the UPS battery or the Thor VM2 does not power on.

The UPS status LED and the Battery Control Panel can be used to monitor the state of the UPS battery.

> Safety requirements restrict the temperature at which the Li-Ion UPS battery can be charged. Charging is disabled if the temperature is outside of the 0ºC to 35ºC safe charging range. In order to maintain UPS charge the Thor VM2 should have power applied while the unit is within the safe charging range for at least an hour each day.

Safe Charging Temperature Range

The internal temperature of the Thor VM2 is the trigger for UPS battery charging.

- The UPS battery is not charged when the internal Thor VM2 temperature is below 0ºC (32ºF). This corresponds to an ambient (room) temperature of approximately -10ºC (-14ºF).

- The UPS battery is not charged when the internal Thor VM2 temperature is above 45ºC (113ºF). This corresponds to an ambient (room) temperature of approximately 35ºC (95ºF).

- If the UPS battery cannot be charged due to a temperature extreme, the UPS Status LED is amber. Move the Thor VM2 to a different location to charge the UPS battery.

When the Thor VM2 is operated in an environment where the UPS battery is not able to charge due to temperature extremes, the Thor VM2 should be removed to a location within the safe charging temperature range during off hours. A discharged UPS battery cannot protect against data loss in the event vehicle power is interrupted.

Charging Timeout

- A fully discharged UPS battery normally recharges in less than 4 hours when the Thor VM2 is in a powered dock and within the safe charging temperature range.

- If the UPS battery is not charged before an 8 hour (or 4 hours for some earlier software revisions) timeout period expires, the UPS Status LED is amber.

- The charge timeout is reset if charging resumes upon application of external power.

- The charge timeout is reset if charging resumes when the Thor VM2 enters the permissible temperature range for charging.

- If the charge timeout occurs, remove the Thor VM2 from the dock and Disconnect UPS Battery. Reinstall the Thor VM2 in the dock and power on.

Charging and Power Management

- Charging does not occur when either Ignition Mode power scheme/plan is selected and the ignition is inactive.

Backup Battery

The Thor VM2 has a permanent Lithium battery installed to maintain time, date and CMOS setup information for a minimum of 90 days. The lithium battery is not user serviceable and should last four years with normal use before it requires replacement.

Warning: **Improper replacement or repair could damage the battery, cause overheating, risk of explosion, and result in injury. The battery should be disposed of properly. The battery should not be disassembled or crushed. The battery should not be heated above 212˚F (100˚C) or incinerated. The battery must be recycled or disposed of separately from household waste.**

Note: *The backup battery should only be changed by authorized service personnel.*

Fuse
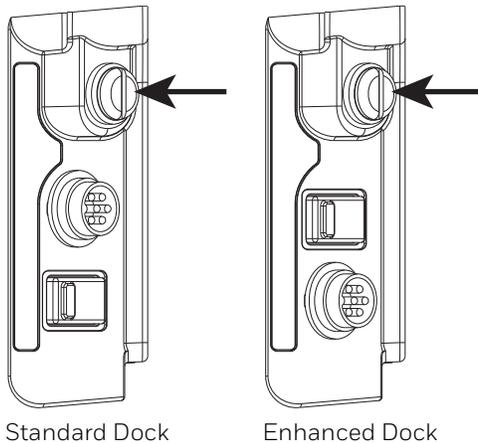
The Thor VM2 uses an 8A time delay (slow blow) fuse that is externally accessible and user replaceable. The fuse is located on the back of the dock. The fuse is accessed by unscrewing the cap as indicated.

Should it need replacement, replace with same size, rating and type of fuse:

Standard Dock   Enhanced Dock

• **Littelfuse 0215008.MXP**

• **Cooper Bussmann BK1/S506-8-R**

• **Bel Fuse 5HT 8-R**

or equivalent.

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

Power Management Modes

The Thor VM2 has four power modes: Full On, Standby/Sleep, Hibernate and Off.

Full On Mode

When the Thor VM2 is attached to either vehicle power or an external power supply or is operating from the UPS battery and the power button is pressed, the Thor VM2 is in the On mode. In this mode, the keypad, touch screen and any attached peripherals such as a scanner function normally. The display remains on until the display, standby or hibernate timer (if enabled) expires.

When in Full On mode, the status LED is solid green.

If the Thor VM2 is Full On, a press of the power button can be configured to put the unit in Standby. See the Advanced tab of the Power control panel or Choose What the Power Button Does, depending on the operating system installed.

Standby/Sleep Mode

This mode is called Standby in Windows Embedded Standard 2009. This mode is called Sleep in Windows Embedded Standard 7 and Windows 7 Professional.

When the standby/sleep timer expires without a primary event occurring, the Thor VM2 transitions to Standby/Sleep mode. Pressing the power button exits Standby/Sleep mode and transitions the Thor VM2 to Full On.

When in Standby/Sleep mode, the status LED:

- blinks green very slowly if external power is attached.
- is off if external power is not attached.

By default, power is turned off to the USB port when the Thor VM2 is in Standby/Sleep mode.

The Thor VM2 can be configured to provide power to the USB port in Standby/Sleep using the Options control panel.

Note: *Because the Thor VM2 with Windows Embedded Standard 7 or Windows 7 Professional cannot transition from Sleep to Hibernate due to an operating system limitation, Sleep is disabled by default in the predefined power plans. Power savings are significantly greater using Hibernate.*

System Standby/Sleep Wakeup Events

The following events transition the Thor VM2 from Standby/Sleep to Full On Mode:

- Pressing and releasing the power button
- Pressing or releasing any key on the integrated keypad
- Tapping the touch screen.

Hibernate Mode

When the Thor VM2 enters hibernate mode, all LEDs are off. Pressing the power button returns the Thor VM2 to Full On.

When in Hibernate Mode, the status LED:

- blinks green very slowly if external power is attached.
- is off if external power is not attached.

Power is turned off to the USB port when the Thor VM2 is in Hibernate.

System Hibernate Wakeup Events

The following event transitions the Thor VM2 from Hibernate to Full On Mode:

- Pressing and releasing the power button.

Off Mode

By default, pressing the power button shuts down the Thor VM2. This behavior can be modified. See Choose What the Power Button Does.

The Thor VM2 is also off when it is not connected to a power source and the UPS battery is depleted. However, an internal Real Time Clock (RTC) powered by an internal battery maintains the date and time while the Thor VM2 is off.

Power Controls

Power Switch
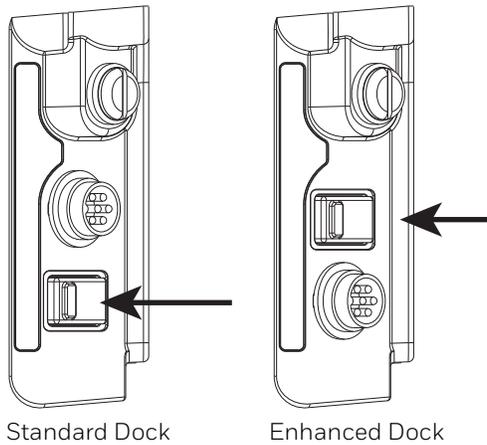
After all cables are connected, the Thor VM2 can be powered on.

There is a power switch located on the back of the dock. The power switch is a rocker switch.

The power switch has a raised bump to identify the switch position even when it is hidden from view. When the side of the switch with the raised bump is pressed, the power switch is On. If the dock is connected to external power, the dock delivers power to the Thor VM2.

Standard Dock   Enhanced Dock

Generally, once the dock is powered On, there is no need to power it off. The dock power can remain On even when the Thor VM2 is not attached.

Power Button
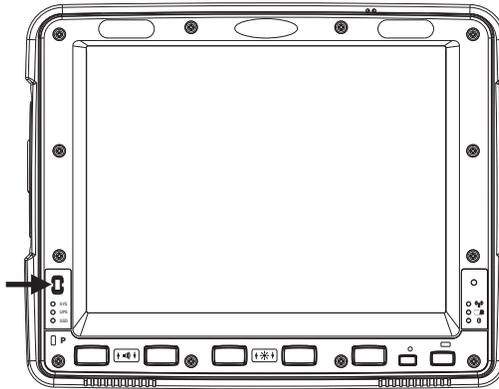
The power button is located at the lower left of the Thor VM2.

If the Thor VM2 is Off, pressing the power button starts the power up sequence.

Note: *This assumes that the Thor VM2 is docked in a powered dock or that the internal UPS battery has a sufficient charge to power the Thor VM2. If no external power is available and the UPS battery does not have a charge, pressing the power button causes no action.*

If the Thor VM2 is On, pressing the power button performs the option selected in the **Advanced** tab of the Power control panel (options may vary by OS type):

• Ignore power button press

• Prompt the user to select action

• Shut down (default, an orderly shutdown is performed)

• Standby/Sleep

• Hibernate

Power Configuration

Use the Power Options control panel to select the desired power scheme/plan.

For information on the Ignition input signal see Vehicle 10-60VDC Direct Power Connection and Auto-On Control Wiring Diagram.

AC/DC

The Thor VM2 is designed to power on whenever external power is attached. When external power is present, the "Plugged In" power management timeouts are used,

Ignition Control

The Thor VM2 is configured to power on when the vehicle ignition is switched on. When either Ignition Control/Ignition On or Ignition Control/Ignition Off is selected and external power is present, the Thor VM2 uses the "Pugged In" power management plan/ scheme settings which corresponds to the state of the vehicle ignition.

Auto-On

The Thor VM2 is designed to power on whenever external power is present. When external power is present, the "Plugged In" power management timeouts are used.

UPS

The Thor VM2 uses the UPS mode whenever external power is not available. When external power is not present, the "Running on Batteries" or "On battery" power management timeouts from the selected power scheme/plan are used.

External Connectors

Power the Thor VM2 off before attaching a cable to any port (serial, USB, Audio/CAN, etc.).

The external I/O connectors for the Thor VM2 are located on the right side of the dock (when viewed from the back).

The Power Supply Connector is on the left side of the dock (when viewed from the back).

Antenna connectors are located on the top rear of the Thor VM2.

Serial Connector (COM1 and COM2)

Standard Dock

Enhanced Dock
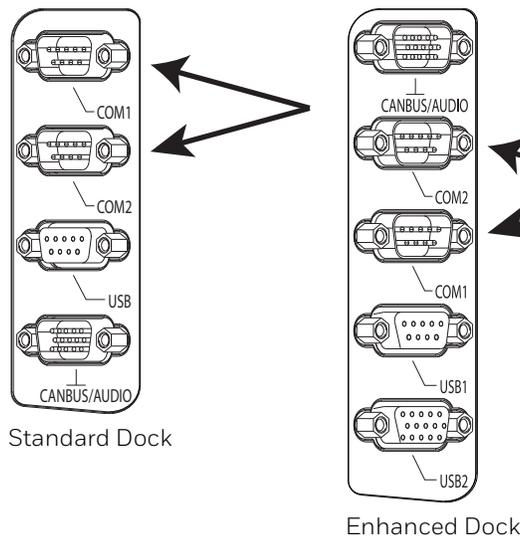
The COM1 and COM2 connectors are D-9 male connectors located on the back of the dock.

Power the Thor VM2 off before attaching a cable to any port (serial, USB, Audio/CAN, etc.).

The serial connectors are industry-standard RS-232, PC/AT standard 9–pin "D" male connector. See COM1 and COM2 Connector for connector pinout detail.

By default, Pin 9 is configured to provide +5V for an external bar code scanner. Pin 9 of COM1 or COM2 may also be configured to provide RI.

See Connect Serial Device for more information.

If a COM port is not being used for a scanner, it can be used for Screen Blanking when the vehicle is in motion.

Screen Blanking

The screen blanking signal can be provided either by a Honeywell Screen Blanking Box or a user supplied switch or relay. See Screen Blanking for information on connecting screen blanking accessories.

USB Connector(s)
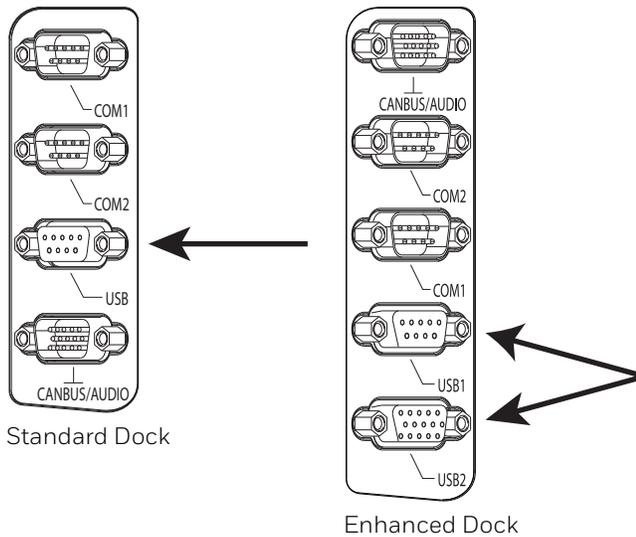
The USB or USB1 connector is a D-9 female connector located on the back of the dock. See USB and USB1 Connector for connector pin-out detail.

The USB client port is not supported with Windows Embedded Standard 2009, Windows Embedded Standard 7 or Windows 7 Professional operating systems.

See Connect USB Host for more information.

The USB-2 connector is a D-15 female connector located on the back of the dock. See USB2 Connector for connector pinout detail.

Power the Thor VM2 off before attaching a cable to any port (serial, USB, Audio/CAN, etc.).

Standard Dock

Enhanced Dock

An additional USB host port is located on the top of the Enhanced Dock. Lift the cover to access the USB port.
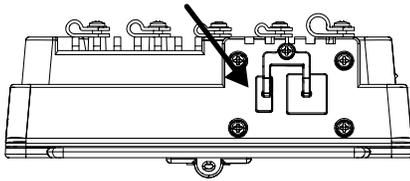
Ethernet Connector

An Ethernet port is located on the top of the Enhanced Dock. Lift the cover to access the Ethernet port.
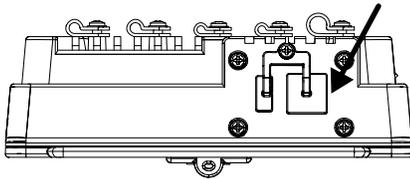
Note: *A BIOS and operating system upgrade is necessary to support the Ethernet port with the Windows 7 or Windows Embedded Standard 7 operating systems. See Thor VM2 and Enhanced Dock Support for information.*

CANbus / Audio Connector

Standard Dock

Enhanced Dock
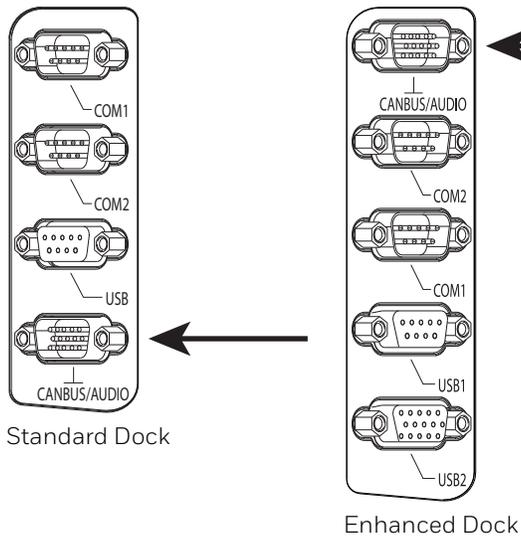
The CANbus/Audio connector is a D-15 male connector located on the back of the dock.

The connector supports a headset adapter cable or a CANbus cable. The Thor VM2 does not support connecting audio and CANbus simultaneously.

See CANbus / Audio Connector for connector pinout detail.

A headset cable attaches to the CANbus / Audio connector and provides a quick connect connection for a headset. See Connect Headset Cable for more information.

The CANbus Y cable has a 9 pin F SAE J1939 (Deutsch) and 9 pin M SAE J1939 (Deutsch) connector. See Connect CANbus Cable for more information.

The CANbus interface is a virtual COM4 port. This port can be accessed using standard Windows API calls.

Power Supply Connector

Standard Dock   Enhanced Dock
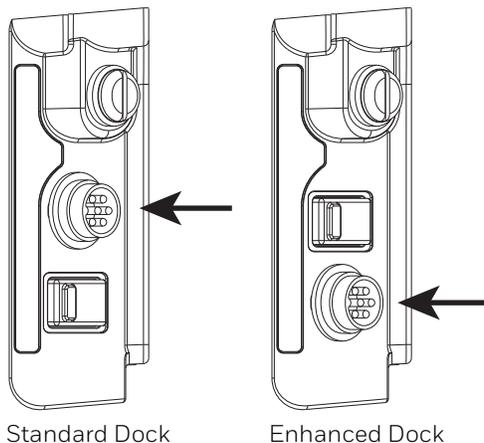
Power is supplied to the Thor VM2 through the power connector. Additionally this assembly provides a connection point for the vehicle's chassis ground to be connected internally to the conductive chassis of the computer.

The Thor VM2 internal power supply can accept DC input voltages in the range of 10 to 60 Volts DC when using the VM1D standard dock or VM3D enhanced docks. Other docks have different power requirements. See Dock for details.

See Power Supply Connector for connector pinout detail. See Connect Power for more information on connecting power to the Thor VM2.

Antenna Connections

① ② ③ ④	The Thor VM2 is equipped with an 802.11 radio and can be ordered with internal antennas, external antennas or external remote mount antennas. When the Thor VM2 is ordered with internal antennas, the external antenna connectors are not used. GPS and WWAN are optional on the Thor VM2 and require external remote mount antennas. 1. WI-FI (MAIN) (Red label) 802.11 Main External Antenna Connector 2. GPS (Green label) GPS Antenna Connector 3. MOBILE NET (Blue label) WWAN Antenna Connector 4. WI-FI (AUX) (Yellow label) 802.11 Auxiliary External Antenna Connector

External Antenna Connector

When the Thor VM2 is ordered with the internal antenna option, the 802.11 antenna connectors on the back are not connected to the 802.11 radio. Instead the internal antenna connector is connected to the 802.11 radio.

Remove the rubber cap, if present, from the antenna connector before connecting an external antenna.

Internal 802.11 Antenna

If the internal 802.11 antenna option is ordered, antennas are mounted inside the Thor VM2. The internal antennas are not user accessible.

External 802.11 Antenna

An external whip antenna can be connected to the Wi-Fi antenna connections on the back of the Thor VM2 for the 802.11 radio. Two external antennas are used for radio diversity.

See Install External Antenna for instructions.

Vehicle Remote Antenna

The external antennas can be remotely mounted on the vehicle. See Install Remote Antenna for instructions. External antenna kits are available for the 802.11 Wi-Fi radio, GPS and WWAN.

Keyboard Options

Integrated Keypad

The integrated keypad contains five programmable keys, a blue modifier key and an orange modifier key.

The **P1** though **P5** keys are user programmable.

- When used with no modifier key, **P1** through **P5** can be configured for a user programmable function.

- When used with the **Orange** modifier key, **P1** through **P5** provide secondary programmable keys, **P6** through **P10**, and can be configured for a user programmable function.

- The programmable keys can be remapped to provide a single keypress, a string of keypresses or to execute an application or command. Key remapping is configured via the Programmable Key option in the Control Panel.

- Programmable keys persist across a warmboot or power cycle.

- When used with the **Blue** modifier key, **P1** through **P4** keys are used to adjust speaker volume and display brightness.

The **P1** through **P5** keys provide limited functionality before the operating system loads, such as during BIOS configuration. See Integrated Keypad and BIOS for available keystrokes.

The Thor VM2 integrated keypad is backlit.

- By default, the integrated keypad backlight follows the display backlight. When the display backlight is on, the integrated keypad backlight is on.

- If the display backlight brightness is increased (or decreased) the integrated keypad backlight brightness is increased (or decreased).

- The integrated keypad backlight and the display share the same timer, which is configured in the Power Options control panel.

- The integrated keypad backlight can be disabled via the About control panel.

Keypad LEDs

See Keyboard LEDs for details.

USB Keyboards

Two Honeywell ruggedized USB keyboards are available, 95-key alphanumeric and 21-key numeric.

95-Key USB Keyboard

The 95-key USB keyboard may have any of the following markings on the decal on the back of the keyboard:

- **164288-0001**
- **95 KEY USB**
- **9000160KEYBRD**

If the keyboard looks similar but has a different part number refer to 95-key PS/2 Keyboard.

If the keyboard is labeled as **164288-0001 Revision B** (or greater) the keyboard has sticky keys for Alt, Ctrl and Shift. These keys will remain active for the next keypress. Earlier versions of this keyboard (Revision A) do not have sticky keys implemented.

The Thor VM2 uses an optional rugged QWERTY 95 key keyboard, designed for ease of use with the Windows operating system. The USB keyboard connects directly to the D9 USB connector (Standard Dock) or USB1 connector (Enhanced Dock).

- The 95 key keyboard supports all 104 keyboard functions (101 standard keyboard 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 keyboard supports what is called hidden keys - keys that are accessible but not visible on the keyboard.

- The 95 key keyboard keys are backlit. The keyboard backlight is manually controlled.

Keyboard Backlight

The keyboard backlight key in the top right hand corner has a light bulb icon.

The keyboard keys are backlit. 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, Low intensity, Medium intensity, Maximum intensity, Off, etc. When the Thor VM2 is powered on, the keyboard backlight defaults to Off.

Since the keyboard is a USB device, by default the external keyboard backlight is turned off when the Thor VM2 enters Standby/Sleep. This behavior can be changed by enabling USB power in Standby/Sleep on the Options control panel.

21-key Numeric Keypad

A numeric keypad is available for the Thor VM2 in applications where a full keyboard may not be needed. The USB keyboard connects directly to the D9 USB connector (Standard Dock) or USB1 connector (Enhanced Dock).

Keyboard Backlight

The keyboard backlight key has a light bulb icon.

The keyboard keys are backlit. 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, Low intensity, Medium intensity, Maximum intensity, Off, etc. When the Thor VM2 is powered on, the keyboard backlight defaults to Off.

Since the keyboard is a USB device, by default the external keyboard backlight is turned off when the Thor VM2 enters Standby/Sleep. This behavior can be changed by enabling USB power in Standby/Sleep on the Options control panel.

PS/2 Keyboards

Legacy PS/2 keyboards can be used with the Thor VM2 via a USB to PS/2 adapter cable. PS/2 keyboards are available in 60-key and 95-key versions and were used with the VX6, VX7, Thor VX8 or Thor VX9.

95-key PS/2 Keyboard

The 95-key PS/2 keyboard may have any of the following markings on the decal on the back of the keyboard:

- **160491-0001**
- **95 KEY PS-2**
- **9000154KEYBRD** (also available as **VX89154KEYBRD**)

If the keyboard looks similar but has a different part number refer to 95-Key USB Keyboard.

An adapter cable is required to attach this keyboard to the Thor VM2. See Connect PS/2 Keyboard for details.

Note: *If the keyboard was previously used with Thor VX8 or Thor VX9, the adapter cable for the Thor VX8/VX9 is not used. The new PS/2 to USB adapter cable must be used.*

This keyboard is visually similar to the USB external keyboard.

⚠️ The mouse pointer function on the PS/2 keyboard is not available when connected via an adapter cable to the Thor VM2.

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 Thor VM2 keyboard supports what is called hidden keys -- keys that are accessible but not visible on the keyboard. Refer to External 95-Key Keyboard for keymaps.

NumLock

For the 95-key PS/2 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.

CapsLock and Scroll Lock

For the 95-key PS/2 keyboard, the **CapsLock** key is backlit green when CapsLock is off. When CapsLock is on, the backlight for the CapsLock key is amber.

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 keyboard keys are backlit. 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, Low intensity, Medium intensity, Maximum intensity, Off, etc.

60-key PS/2 Keyboard

The 60-key PS/2 keyboard is part number **160068-0001** (see decal on back of keyboard).

An adapter cable is required to attach this keyboard to the Thor VM2. See Connect PS/2 Keyboard for details.
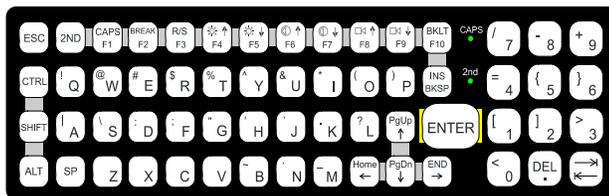
The 60-key keyboard has 101 keyboard functions, including a numeric keyboard pad.

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 Thor VM2 keyboard supports what is called hidden keys - keys that are accessible but not visible on the keyboard.

On standard keyboards many keys are found in the Alphanumeric section as well as on the Numeric keypad (i.e. the 1 key is found on the numeric keypad and above the alpha characters on standard keyboards). However these keys send distinctly different scan codes when the keys are pressed. The default codes for the Thor VM2 number keys correspond to the numeric keypad on standard keyboards. In order to duplicate the codes sent when the alphanumeric key is pressed, the hidden keystroke must be used.

Refer to External 60-Key Keyboard for keymaps.

NumLock

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.

Keyboard Backlight

The keyboard keys are backlit with LEDs. The backlight is manually controlled using the **2nd + CTRL + F10** keypress sequence. The keyboard backlight is off when the Thor VM2 is powered up. The backlight must be manually turned on with the **2nd + CTRL + F10** key sequence.

Control Keys

The VMT keyboard has several control keys. Because of the construction of the Thor VM2 and the Microsoft Windows operating system, many of the Control Keys are not used on the Thor VM2.

- The **2nd** functions of the **F4** and **F5** keys are not used as the display brightness is adjusted via the buttons on the Thor VM2.
- The **2nd** functions of the **F6** and **F7** keys are not used as the Thor VM2 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 Thor VM2 is controlled with the Sound icon in the Microsoft Windows System Tray.
- 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.

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.

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

The default value of CapsLock is Off.

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.

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.

- Press **2nd** and **F1** to turn CapsLock on and off.
- Press **2nd** and ? (up arrow) to initiate the PgUp command.
- Press **2nd** and **Q** to type the "!" key.
- Press **2nd** and **BkSp** to enter the Insert (Ins) mode.

USB Keyboard / Mouse

A standard USB keyboard or mouse can be attached to the Thor VM2 using the appropriate adapter cable.

The Y cable attaches to the Thor VM2 and provides a USB connector. Please refer to documentation provided with the USB keyboard or mouse for more information on their operation.

LED Functions

System LEDs

Connection LEDs

Programmable LED

Blue LED   Orange LED
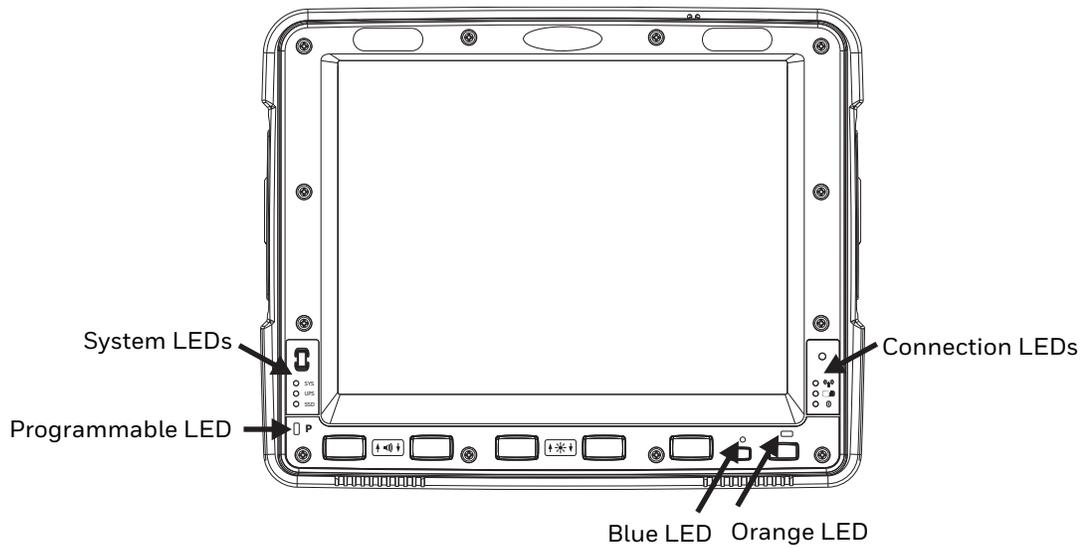
System LEDs

SYS (System Status) LED ⟶ ◯ SYS

UPS (Uninterruptible Power Supply) LED ⟶ ◯ UPS

SSD (Solid State Drive) LED ⟶ ◯ SSD
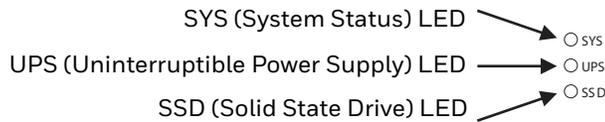
SYS (System Status) LED

LED Behavior	System State
Solid Green	• On • On but Display Off
Green blinking very slowly External power present (1/2 sec. on, 4 1/2 sec. off)	• Standby/Sleep
Off External power present	• Hibernate • Off
Off External power not present	• Hibernate • Standby/Sleep • Off
Off External power not present	• Hibernate • Standby/Sleep • Off
Green blinking slowly External power present (1/2 sec. on, 1 1/2 sec. off)	CPU temperature less than –20ºC, Heater warming CPU for 30 sec.

LED Behavior	System State
Green blinking slowly External power not present (1/2 sec. on, 1 1/2 sec. off)	CPU temperature less than –20ºC, Need to move unit to warmer environment

UPS Status LED

The color of the UPS LED identifies the charge level, while the behavior of the LED identifies the charging state.

Charge Level

LED Color	Status
Green	Fully charged (>90%)
Amber	• Less than fully charged, but more than 2 minutes runtime remaining • Out of Safe Charging Temperature Range. Charging only occurs between approximately –10ºC and 35ºC ambient temperature • No UPS present • Charging Timeout Not fully charged after 4 or 8 hours depending on software revision.
Red	Low battery, less than 2 minutes runtime until shutdown

Charging State

LED Behavior	Status
Slow Blink (1 sec. on, 3 sec. off)	Charging
Fast Blink (1/2 sec. on, 1/2 sec. off)	UPS supplying power and discharging
On	Neither charging or discharging
Off	Unit is off or is in Hibernate

SSD (Solid State Drive) LED

LED Behavior	Status
Flashing Green	SSD read or write activity
Off	No SSD read or write activity

Connection LEDs

WWAN LED

Wi-Fi LED

Bluetooth LED
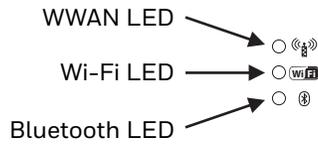
WWAN LED

LED Behavior	Status
Solid Green	Indicates a WWAN connection to a network
Off	Indicates no WWAN connection

Wi-Fi LED

LED Behavior	Status
Solid Green	Indicates a connection with an IP address to an Access Point
Off	Indicates no connection to an Access Point

Bluetooth LED

LED Behavior	Status
Blue Blinking Slowly	Bluetooth is paired but not connected to a device
Blue Blinking Medium	Bluetooth is paired and connected to a device
Blue Blinking Fast	Bluetooth is discovering Bluetooth devices
Off	Bluetooth hardware has been turned off

The Bluetooth LED blinks once every 6 seconds when the Bluetooth client is paired but not connected. It blinks once for a very short time every 2 seconds when paired and connected. It blinks every second when in discovery. The LED is off when the Bluetooth client is off.

Keyboard LEDs

The keyboard LEDs are located near the specified key.

Blue LED

LED Behavior	Status
Solid Blue	• Indicates the **Blue** modifier key is active • Pressing the **Blue** key a second time exits this modifier mode and turns off the LED • Pressing the **Orange** key exits the Blue mode and turns off the Blue LED • If no key other key is pressed within five seconds, the **Blue** key times out and turns off the LED • When Blue mode is active, keys **P1** through **P4** provide volume and brightness adjustment functions •
Off	Blue mode is not invoked

Orange LED

LED Behavior	Status
Solid Orange	• Indicates the **Orange** modifier key is active. Orange mode is invoked for the next keypress only • Pressing the **Orange** key a second time exits this modifier mode and turns off the LED • Pressing the **Blue** key exits the Orange mode and turns off the Orange LED
Off	Orange mode is not invoked.

Programmable LED

The Programmable LED is available for user applications. The LED defaults to Off unless activated by user application.

LED Behavior	Status
Controlled by application	Refer to application developer for LED behavior details.
Off	Default mode. Refer to application developer for LED behavior details.

Display

The display is a thin-film transistor display capable of supporting SVGA graphics modes. Display size is 1024x768 pixels. The display covering is designed to resist stains. The touch screen allows signature capture and touch input. The display supports screen blanking to eliminate driver distraction when the vehicle is in motion.

Touch Screen

The touch screen 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.

When a dialog box is too large for the display, tap and drag the dialog box up or down or from side to side to view the remainder of the dialog box.

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

An extra or replacement stylus may be ordered.

A replaceable touch screen protective film is available when the Thor VM2 is used in an abrasive environment. Contact Technical Assistance for availability.

Note: *If the touch screen is disabled or loses calibration on a Thor VM2, you must use a USB mouse or keyboard attached to the Thor VM2 to access the control panel to re-enable or recalibrate the touch screen unless a programmable key has been assigned to that function.*

Screen Blanking

Screen blanking (blackout) can be enabled when the vehicle is in motion. See Screen Blanking for hardware setup and Screen Control for software setup to enable screen blanking. Once screen blanking is enabled, the display is blanked out any time when the cable sends the signal that the vehicle is in motion. If the cable is removed, screen blanking is disabled and the display remains on.

Display Backlight Control

The display brightness can be adjusted manually, via the keypad:

1. Press the **Blue** key to enter Blue mode.
2. Press **P3** to increase brightness or **P4** to decrease brightness.
3. Press the **Blue** key to exit Blue mode.

VEHICLE MOUNTING AND ACCESSORY INSTALLATION

Introduction

⚠️ **Warning: The correct dock must be selected for the installation:**

- For a vehicle installation with 10-60 VDC direct connection: Use either a VM1D standard dock or a VM3D enhanced dock.

- For a vehicle installation with 60-144 VDC connection: Use a DC/DC power supply with either a VM1D standard dock or a VM3D enhanced dock.

- To replace a Thor VX8 or Thor VX9: Use the existing power supply and wiring with a VMXD enhanced dock.

- To replace a VX6, VX7 or CV61: Use the appropriate adapter cable and either a VM1D standard dock or a VM3D enhanced dock. Voltage must be 10-60 VDC.

- For an AC powered application: Use an AC/DC power supply and the VMXD off-vehicle enhanced dock.

The Thor VM2 is designed to be mounted to a dock in a vehicle with either a RAM mount or U Bracket system. A power cable is provided with the Thor VM2 dock. An optional 21 key numeric or 95 key laptop-style USB keyboard and keyboard mounts are available. An integrated scanner mount is also offered. Optional communication cables are available.

Vehicle mounting brackets are specifically designed for vehicle mount applications. The vehicle mounted assembly restrains the Thor VM2 and isolates it from shock and vibration. A RAM metal table stand is available to secure the Thor VM2 and dock when in an office environment, for example.

The vehicle mount holds the dock and the Thor VM2 attaches to the dock. The dock remains attached to the vehicle, however, the Thor VM2 has a quick release located on the lower rear side that allows the Thor VM2 to easily be removed from the dock. The Thor VM2 can be operated for a minimum of 30 minutes from an internal UPS battery when not attached to a dock. The Thor VM2 can be transferred from one dock equipped vehicle to another for easy portability. The dock provides accessory attachment and conditioned power for the Thor VM2.

Overhead, dash and roof support pillar mounting is via a RAM Mount or U-bracket accessory which includes all the hardware required for vehicle mounting.

Never put the Thor VM2 into the vehicle mounted assembly until the assembly is securely fastened to the vehicle.

Prepare for Vehicle Mounting

The Thor VM2 should be secured to an area in the vehicle where it:

- Does not obstruct the driver's vision or safe vehicle operation.
- Will be protected from rain or inclement weather.
- Will be protected from extremely high concentrations of dust or wind–blown debris.
- Can be easily accessed by a user seated in the driver's seat while the vehicle is not in operation.

Quick Start

The following list outlines, in a general way, the process to follow when mounting the Thor VM2 in a vehicle. Refer to the following sections in this document for more details.

1. Install RAM Mount or Install U Bracket Mount to the vehicle.
2. Place Thor VM2 in the Dock.
3. Secure accessories such as an optional external keyboard or a scanner holder to either an integrated or remote mounting bracket.
4. Adjust the Thor VM2 to the best viewing angle.
5. Install Remote Antenna or Install External Antenna if necessary.
6. Connect Cables for any peripherals.
7. Connect vehicle power:
    - 12-48 VDC Vehicles (10-60 VDC Direct Connection)
    - 60-144 VDC Vehicles (50-150 VDC Power Supply, Screws on Top of Lid)
    - 60-144 VDC Vehicles (50-150 VDC Power Supply, Screws on Side of Lid).
    - Thor VX8 / Thor VX9 Adapter Cable
    - VX6 / VX7 Adapter Cable
8. Secure all cables in Strain Relief Cable Clamps.

The Thor VM2 is ready for use.

Maintenance – Vehicle Mounted Devices

Check the vehicle mounting hardware frequently and re-tighten if necessary.

If the vehicle mounting hardware and connections become broken, loose or cracked, the assembly must be taken out of service and replaced. Contact Technical Assistance for help.

Cleaning

If it becomes necessary to clean the Thor VM2, dock, peripherals or mounting hardware see:

- Cleaning the Thor VM2 and the Dock
- Cleaning the Touch Screen

Place Thor VM2 in the Dock

Back of Thor VM2

Front of Dock

Upper Lip on Dock

Notch on
Thor VM2

Lower Lip on Dock

Release Lever
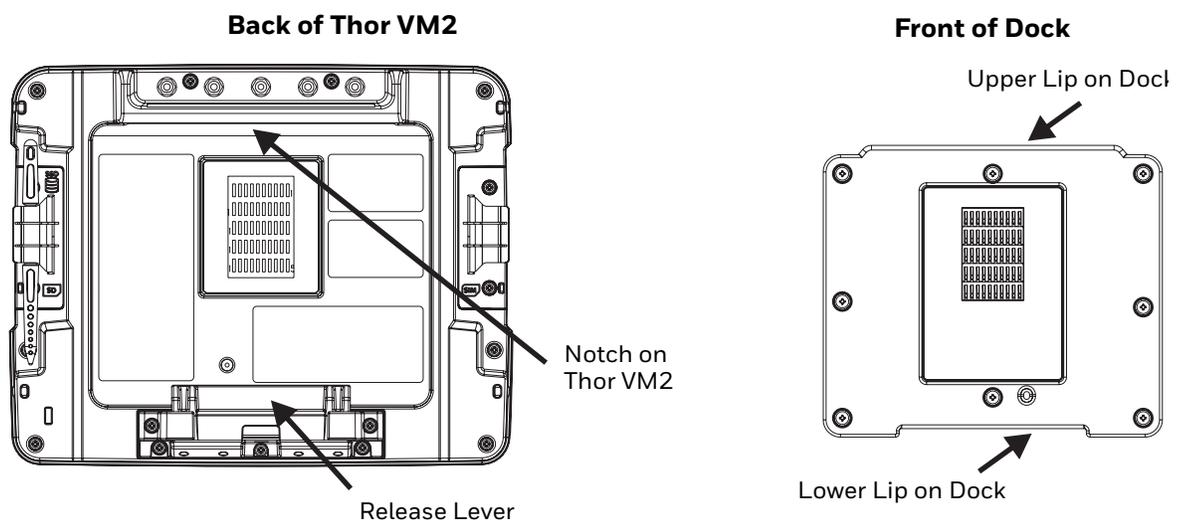
1. Locate the notch on the upper rear of the Thor VM2.
2. Slide this notch over the top lip of the dock. Slide the Thor VM2 from side to side on the dock to make sure it fully engages on the lip of the dock. If the Thor VM2 cannot be slid side to side, the lip is engaged.
3. Pull the quick release lever on the Thor VM2 down and push the Thor VM2 against the dock.
4. Release the quick release lever. The quick release lever catches the lower lip on the dock and secures the Thor VM2 to the dock. Be sure the red quick release lever is pushed all the way in to secure the Thor VM2 to the dock.
5. If necessary, adjust the viewing angle of the Thor VM2.

When the Thor VM2 is placed in the dock, the following may happen:

- If the Thor VM2 is off and power is connected to the dock, the Thor VM2 may boot when placed in the dock. The behavior depends on the Power Scheme selected. See Ignition Control/Ignition On and Auto-On.

- If the Thor VM2 is on and power is connected to the dock, the Thor VM2 power management timers may change when the Thor VM2 is placed in the dock. See Select a Power Scheme or Power Plan.

When the Thor VM2 is removed from the dock, the following may happen:

- If the Thor VM2 is on and power is connected to the dock, the Thor VM2 power management timers may change when the Thor VM2 is placed in the dock. See Select a Power Scheme or Power Plan.

Dock I/O Pin Cover.
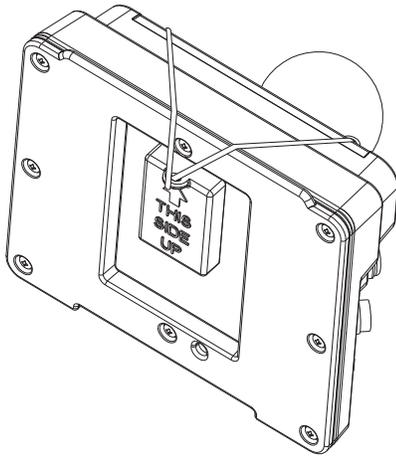
The dock contains a tethered I/O Pin Cover to protect the I/O pins on the dock when a Thor VM2 is not mounted in the dock.

- When the Thor VM2 is not installed in the dock, use the I/O Pin Cover to protect the pins on the dock as shown.

- When a Thor VM2 is installed in the dock, the I/O Pin Cover can be placed out of the way behind the dock.

Padlock
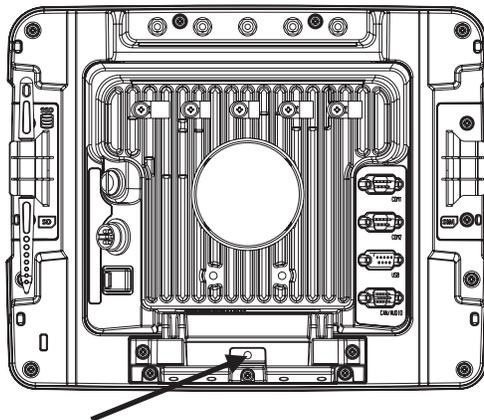
It may be desirable to secure the Thor VM2 in the dock so it cannot be removed from the dock. The quick release handle on the Thor VM2 is notched to allow a user supplied standard padlock to be placed through a hole in the bracket on the back of the Thor VM2 in the location shown below. Once the padlock is installed, the release handle cannot be moved so the Thor VM2 cannot be removed from the dock. The padlock shackle must be smaller than 3/16" (4.76mm).

A cable tie wrap can be used instead of a padlock if desired.

Laptop Security Cable
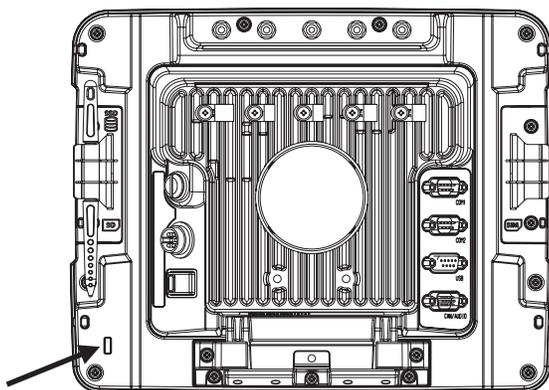
The Thor VM2 can be secured with a standard laptop security cable using the slot on the back of the Thor VM2.

Install RAM Mount

⚠	**Caution:** **This device is intended to transmit RF energy. For protection against RF exposure to humans and in accordance with FCC rules and Industry Canada rules, this transmitter should be installed such that a minimum separation distance of at least 20 cm (7.8 in.) is maintained between the antenna and the general population. This device is not to be co-located with other transmitters.**

Before installation begins, verify you have the applicable vehicle mounting bracket assembly components necessary, as shown in the following figures.

Components - RAM Mounting Kits

Mounting kits that do not include an external keyboard are shown below.

Mounting kits that include a provision for an external keyboard include the parts on this page plus the parts on the next page.

In addition to the kits below, individual RAM mounting components are also available.

Mounting Kits without Keyboards

Each mounting kit contains:

- RAM Ball (Size D) for back of Thor VM2 dock with hardware (screws and washers) to attach RAM ball to dock

- RAM Arm (Size D), length varies by kit selected

- One of three mounting options:
  - RAM Ball mount (Size D, may include 3 cone washers), or
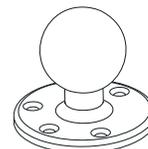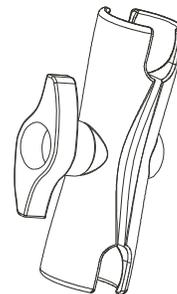
- ○ RAM Clamp mount (Size D), or
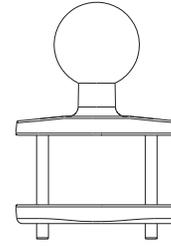
- ○ RAM Plate mount with RAM Ball (Size D) with Hardware (cone washers and nuts) to attach Ball to Plate
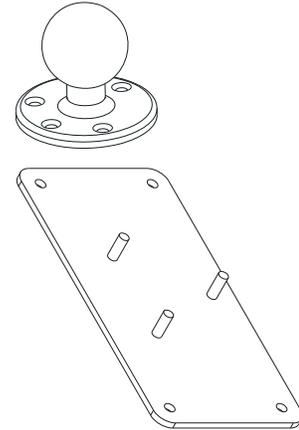
Mounting Kits with Integrated Keyboard Mounting

Additionally, the kits for the Thor VM2 with an integrated 95 key keyboard mount include:

- • Thor VM2 Keyboard Mounting Bracket
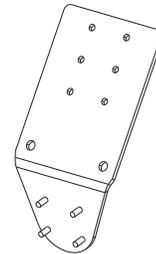
- • RAM Ball (Size C) with hardware (nuts) to attach RAM ball to Keyboard Mounting Bracket

- • RAM Arm (Size C)

- • Keyboard Mounting Plate with RAM Ball (Size C) and hardware (screws and washers) to attack Keyboard to Mounting Plate
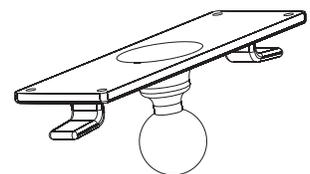
Accessory Mounting Kits

An accessory mounting kit is also available. This kit mounts the 21 key numeric key–board or the Thor scanner holder to the Enhanced Dock.

Note: *This accessory mount kit is only for use with the Enhanced Dock.*

- Accessory RAM Ball
  This accessory RAM ball mounts to the back of the Enhanced Dock.
- RAM Ball (Size C) to attach RAM ball to 21key numeric keyboard or scanner holder.

- RAM Arm (Size C)
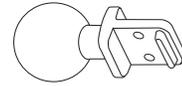
Procedure - RAM Mount Assembly

Equipment Needed: Sockets, screwdriver and a Torque wrench capable of measuring to 50 inch pounds (5.64±.56 N/m).

Note: *Torquing tool is not supplied by Honeywell. Tools needed to attach the RAM Clamp Mount to the vehicle are not supplied by Honeywell.*

Torque Measurement

You will need a torquing tool capable of torquing to 20 inch pounds (1.10 N/m). Torque all screws and bolts according to the following table:

For these nuts...	Torque to
10-32 lock nuts	17 - 20 in/lb (0-95 - 1.10 N/m)

Step 1a – Attach RAM Ball to Vehicle

Note: *If you are using the RAM clamp mount, please go to Step 1b – Mount RAM Clamp to Vehicle. If you are using the RAM plate mount, please go to Step 1c – Attach RAM Plate to Vehicle and Attach RAM Ball.*

1. Determine the position for mounting the RAM ball base. Be sure to position the RAM bracket to allow access to the switches and ports on the bottom of the Thor VM2.

2. Attach the RAM ball base to the vehicle mounting surface using three or four 1/4 bolts (not included) or equivalent fasteners. If the mounting kit includes cone washers, use those as illustrated below.

   IMPORTANT: Mount to the most rigid surface available.
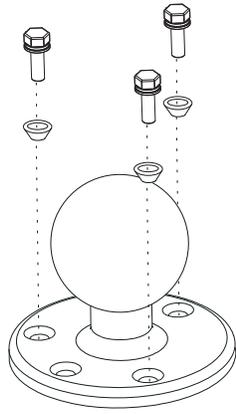
Mounting Dimensions

Note: Drill and tap holes for three 1/4 bolts. Drawing not to scale.

3.69" / 93.73 mm

2.75" / 69.85 mm

60°   60°

120°   120°
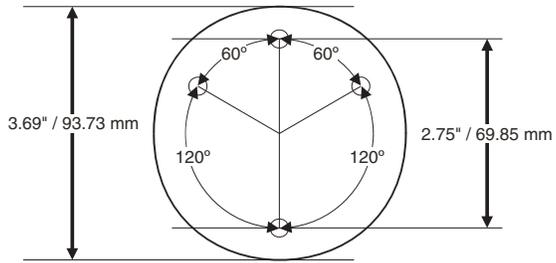
Step 1b – Mount RAM Clamp to Vehicle

Note: *If you are using the RAM ball mount, please go to Step 1a – Attach RAM Ball to Vehicle. If you are using the RAM plate mount, please go to Step 1c – Attach RAM Plate to Vehicle and Attach RAM Ball.*

1. Determine the position for mounting the RAM clamp mount. The clamp mount can be used on a beam (such as on a fork lift truck) up to 2.5" (63.5 mm) wide and approximately 2" (50.8 mm) thick. The clamp may be attached to a thicker beam by substituting longer bolts (not included). Be sure to position the RAM clamp mount to allow access to the switches and ports on the bottom of the Thor VM2.
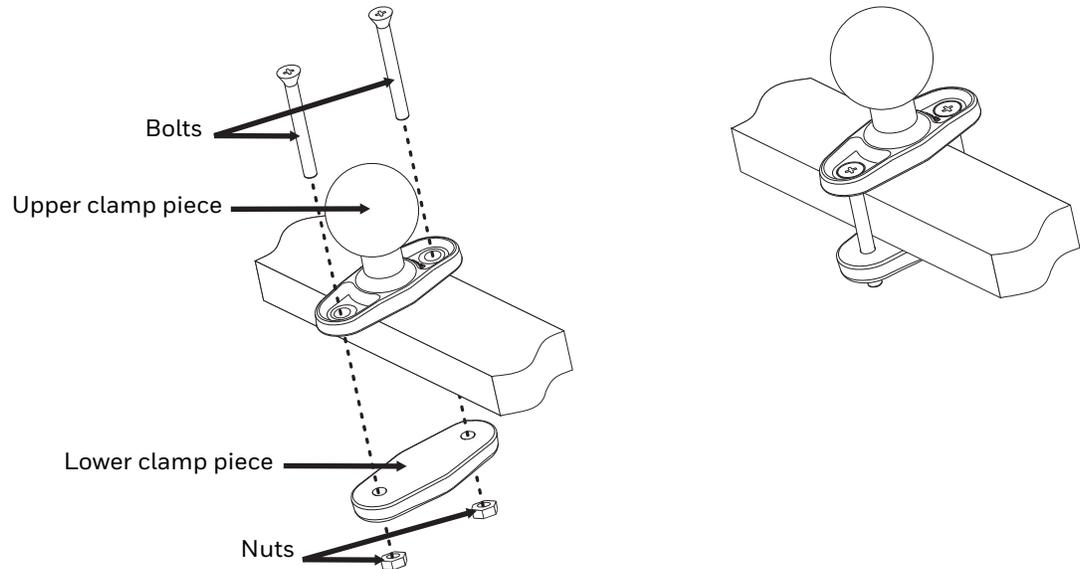
Position the upper clamp piece with ball on the beam. Place the bolts through the holes in the upper clamp piece.

2. Position the lower clamp piece below the beam. Align the bolts with the holes in the lower clamp piece.

3. Place the nylon locking nuts on the bolts and tighten the bolts.

Mounting Dimensions

Note: *Drawing not to scale.*
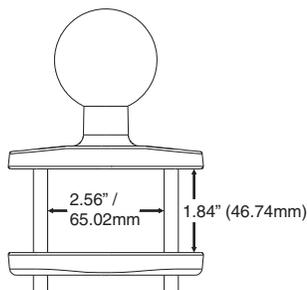
Step 1c – Attach RAM Plate to Vehicle and Attach RAM Ball

Note: *If you are using the RAM ball mount, please go to Step 1a – Attach RAM Ball to Vehicle If you are using the RAM clamp mount, please go to Step 1b – Mount RAM Clamp to Vehicle.*

1. Determine the position for mounting the RAM ball plate. Be sure to position the RAM plate to allow access to the switches and ports on the bottom of the Thor VM2.

2. Attach the RAM ball plate to the vehicle mounting surface using four 1/4 bolts (not included) or equivalent fasteners.

3. If not already attached, attach the RAM ball to the RAM ball plate using three M6 nuts and washers.

   IMPORTANT: Mount to the most rigid surface available.
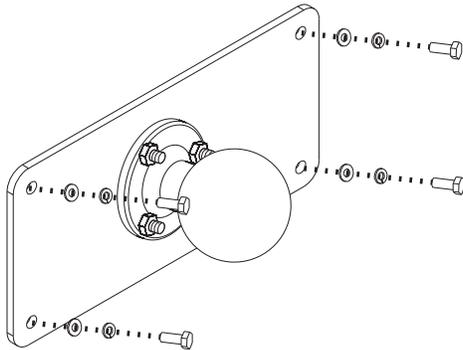
Mounting Dimensions

There are 4 mounting holes in the plate. Use four 1/4 bolts to secure the plate to the vehicle.

Note: *Drawing not to scale.*
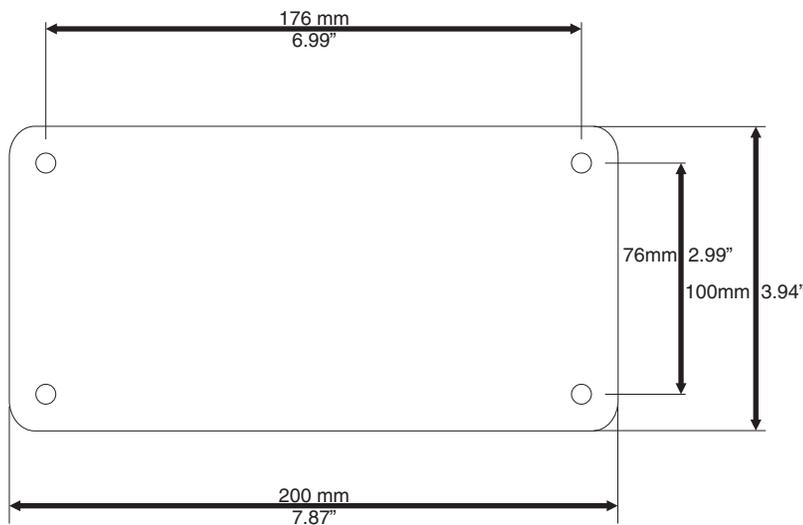
Step 2 – Attach RAM Mount Ball to the Thor VM2 Dock

1. Turn the Thor VM2 off before attaching the RAM mount ball.

2. Place the Thor VM2 face down on a stable surface.

3. If using the external keyboard mount, position the Keyboard Bracket and the Size D RAM ball on the rear of the Thor VM2 dock, aligning the holes on the back of the Thor VM2 dock with the holes on the bracket and the RAM ball base.

4. If not using the external keyboard mount, position the RAM ball on the rear of the Thor VM2 dock, aligning the holes on the back of the Thor VM2 dock with the holes on the RAM ball base. Attach with four M5 screws, flat washers and lock washers.

5. If using the external keyboard mount, attach the Size C RAM ball to the Thor VM2 Keyboard bracket with four M5 nuts, flat washers and lock washers.
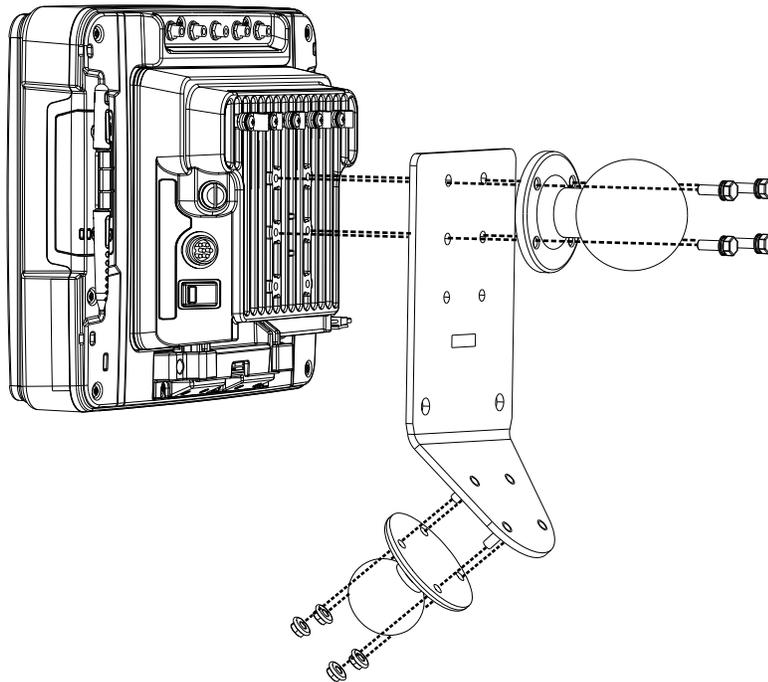
Step 3 – Attach Thor VM2 Assembly to RAM Mount

1. Slip the Size D RAM arm over the ball on the vehicle RAM mount (RAM Ball mount shown).

2. Insert the ball on the dock into the RAM arm and tighten the knob on the RAM arm using the supplied RAM wrench.
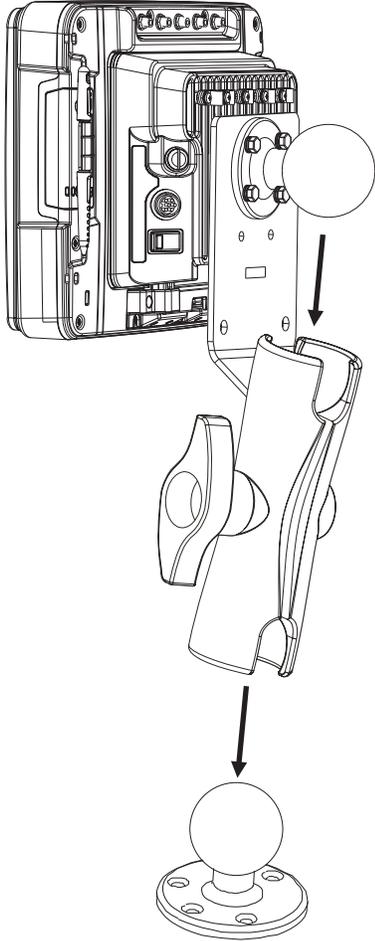
Step 4 – Place the Thor VM2 into the Dock

If the Thor VM2 is not already mounted to the dock, Place Thor VM2 in the Dock

If the optional external keyboard is not used, the mounting process is complete.

Step 5 – Attach Alphanumeric Keyboard to Mounting Plate (Optional)

Note: *This step is only for a Thor VM2 with the optional external keyboard.*

If using the optional integrated keyboard mount, attach the keyboard to keyboard mounting plate, using four #8 screws, flat washers and lock washers.
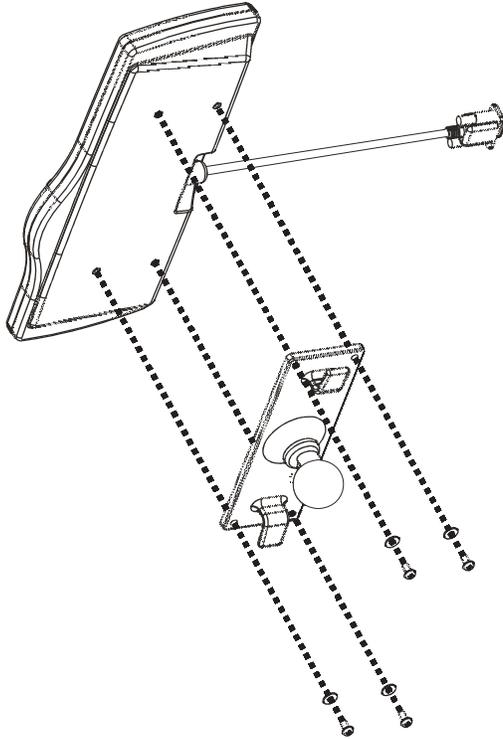
Note: *Excess keyboard cable length can be looped around the hooks on the bottom of the keyboard mounting plate.*

Step 6 – Attach Keyboard Assembly to Thor VM2 Assembly (Optional)

Note: This step is only for a Thor VM2 with the optional external keyboard.

1. Slip the Size C RAM arm over the ball on the Thor VM2 Keyboard Bracket.
2. Slip the ball on the Keyboard Mounting Plate into the other end of the Size C RAM arm.
3. Tighten the knob on the RAM arm using the supplied RAM wrench.
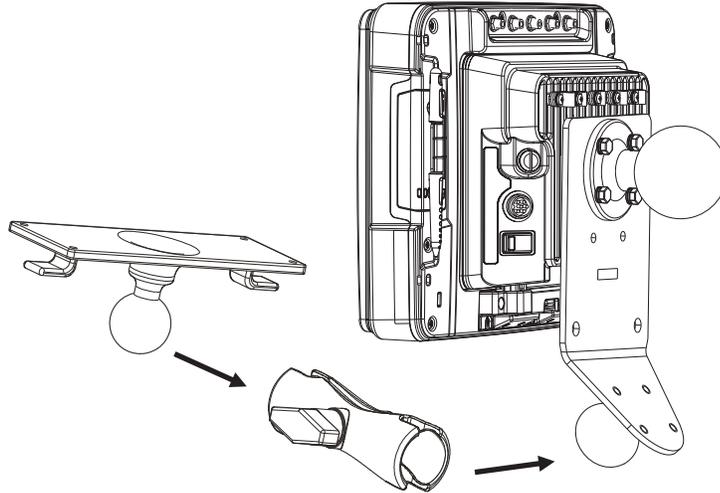
Note: Some components omitted for detail clarity.

Step 7 – Attach Numeric Keypad (Optional)

This step is only for use with the Enhanced Dock.

1. Attach the accessory RAM ball to the Enhanced Dock. There are two mounting pro-visions, one on either side of the Enhanced Dock and either can be used to mount the numeric keypad.
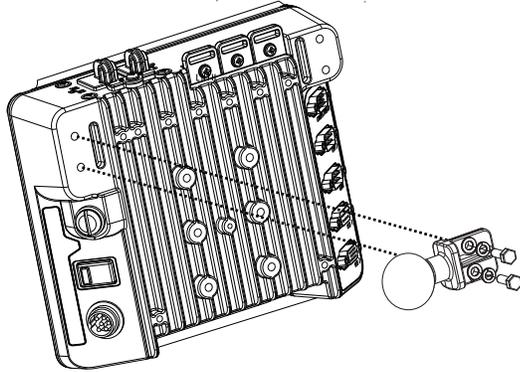
Note: *Some components omitted for detail clarity.*

2. Attach the RAM ball to the back of the keypad.
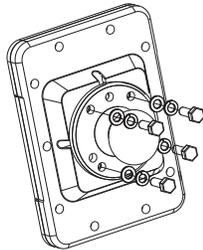
3. Slip the RAM arm over the accessory RAM ball.
4. Slip the RAM ball on the keyboard into the RAM arm.
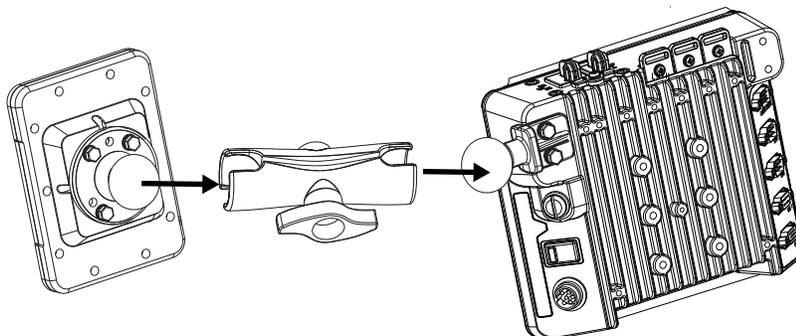
5. Tighten the knob on the RAM arm while adjusting to the desired angle.

Step 8 – Attach Scanner Holder (Optional)

This step is only for use with the Enhanced Dock.

1. Attach the accessory RAM ball to the Enhanced Dock. There are two mounting provisions, one on either side of the Enhanced dock and either can be used to mount the scanner holder.
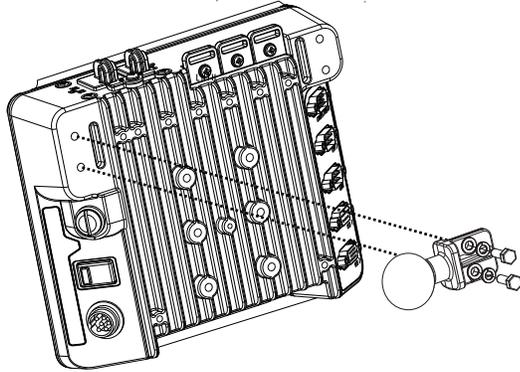
Note: *Some components omitted for detail clarity.*

2. Attach the RAM ball to the back of the scanner holder.
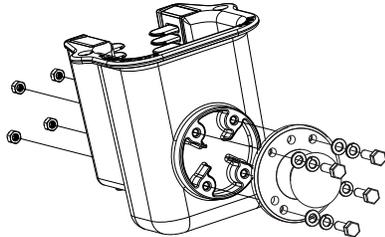
3. Slip the RAM arm over the accessory RAM ball.
4. Slip the RAM ball on the scanner holder into the RAM arm.
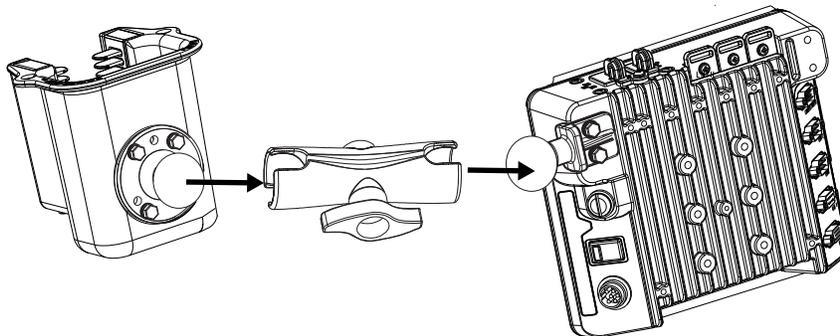
5. Tighten the knob on the RAM arm while adjusting to the desired angle.

Install U Bracket Mount

Note: *This mounting system does not have provision for an integrated external keyboard mount or scanner holder. These accessories can be mounted remotely if desired. Contact* Technical Assistance *for details.*

⚠	**Caution:** **This device is intended to transmit RF energy. For protection against RF exposure to humans and in accordance with FCC rules and Industry Canada rules, this transmitter should be installed such that a minimum separation distance of at least 20 cm (7.8 in.) is maintained between the antenna and the general population. This device is not to be co-located with other transmitters.**

Before installation begins, verify you have the applicable vehicle mounting bracket assembly components necessary, as shown in the following figures.

Components - U Bracket Mounting Assembly

The U bracket kit is available in two configurations:

- With a U Bracket included for new vehicle installations
- Without a U Bracket for installing the Thor VM2 in place of a previous Honeywell vehicle mounted computer, such as a VX6 or VX7.
  - ○ U Bracket (only necessary for new installations)
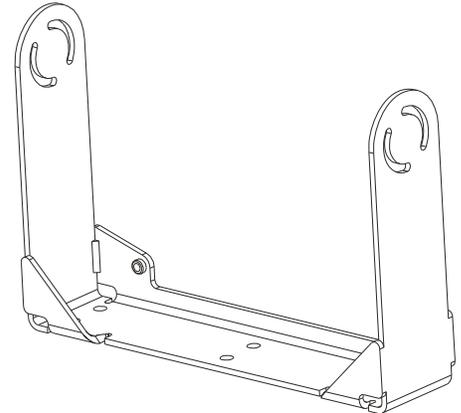
  - ○ Adapter Bracket (includes screws, flat washers and lock washers to attach Adapter Bracket to Thor VM2 and to U Bracket). The U bracket may already be installed on the vehicle where a VX1, VX2, VX4, VX5, VX6 or VX7 was previously installed.
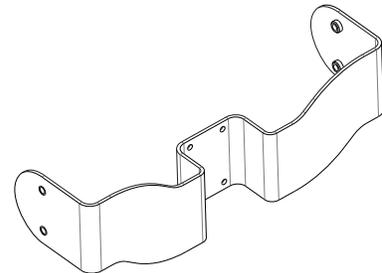
Procedure – U Bracket Assembly

Equipment Needed: Sockets and a Torque wrench capable of measuring to 50 inch pounds (5.64±.56 N/m).

Note: *Torquing tool is not supplied by Honeywell.*

Torque Measurement

You will need a torquing tool capable of torquing to 35-50 inch pounds (1.10 N/m). Torque all screws and bolts according to the following table:

For these bolts...	Torque to
1/4-20x5/8 Bolts	50 in/lb (5.6 N/m)
M5x16mm Bolts	35 in/lb (4.0 N/m)
1/4 Bolts (user supplied)	50.0±5 in/lb (5.64±.56 N/m)

Mounting Positions

The adapter bracket can be mounted in a high or low position, depending on viewing position, as shown below.
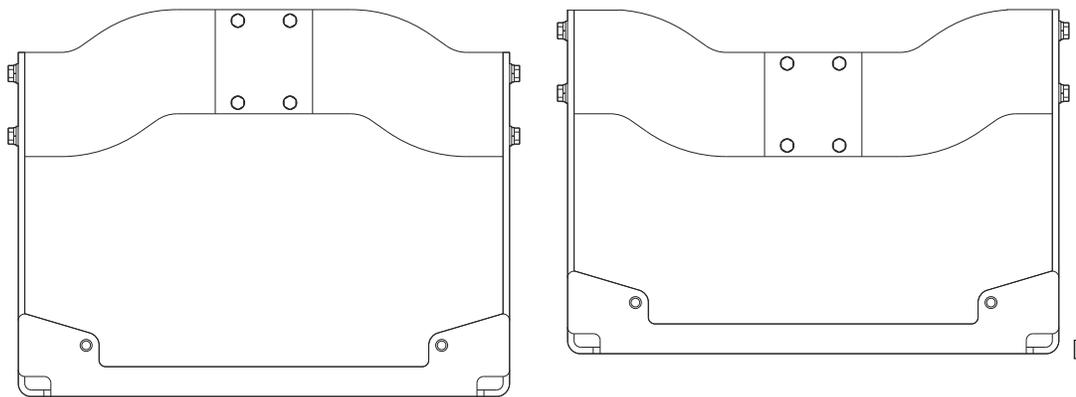
Additionally, the slotted U bracket allows the Thor VM2 to be mounted vertically or tilted forward or backward for best viewing angle.
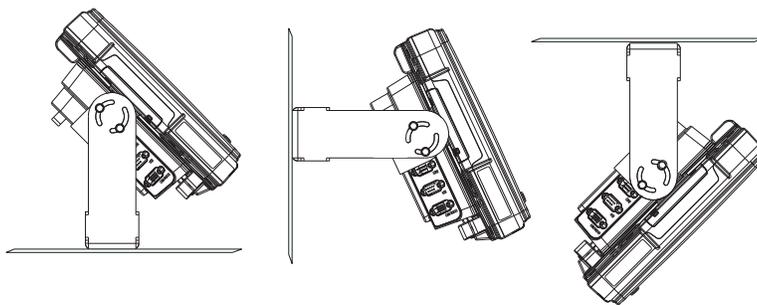
Step 1 – Install U Bracket to Vehicle

1. Position the bracket to allow access to the switches and ports on the bottom of the Thor VM2.

2. Attach the bottom mounting bracket to the vehicle mounting surface using a minimum of four 1/4 bolts (or equivalent) fasteners.

Note: *1/4 bolts and washers not included. It is recommended to use lock washers and flat washers on the fasteners.*

IMPORTANT: Mount to the most rigid surface available.
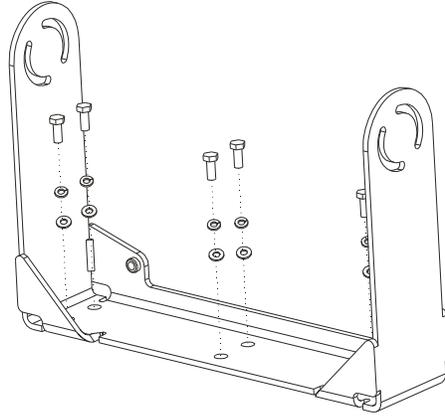
After the bottom bracket has been attached to a rigid surface, you are ready to assemble the Thor VM2 bracket configuration.

Mounting Dimensions

Note: *Drawing not to scale.*
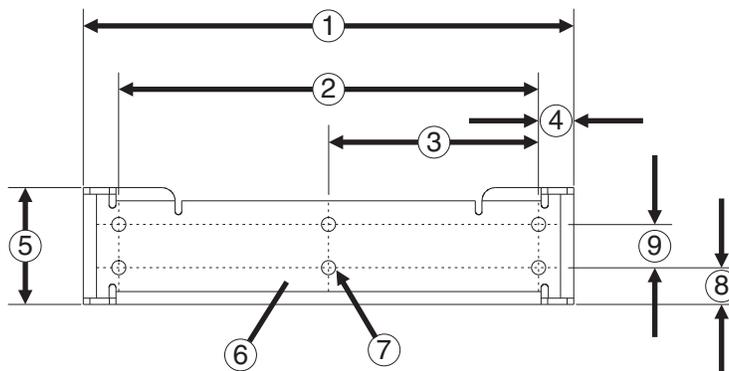
1. 14.40 in / 359.2 mm
2. 12.10 in / 307.3 mm
3. 6.05 in / 153.6 mm
4. 1.02 in / 25.9 mm
5. 3.38 in / 85.85 mm
6. Vehicle Mount Footprint
7. 0.406 in / 10.312 mm
8. 0.88 in / 22.3 mm
9. 1.25 in / 31.75 mm

Step 2 – Remove RAM Ball

If the Thor VM2 dock has a RAM ball attached, the RAM ball must be removed from the dock to use the U Bracket mount.

Remove the RAM ball. The hardware used to attach the RAM ball to the dock is not reused for the U bracket mount.

Step 3 – Attach Adapter Bracket
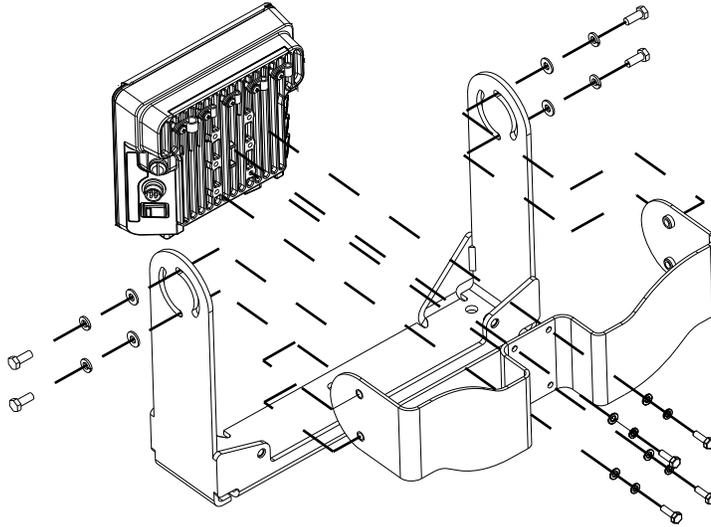
Note: *For the steps below, always place the lock washer on the bolt before the flat washer.*

1. Attach the Adapter Bracket to the Thor VM2 dock using four each M5x16mm bolt, M5 lock washer and M5 flat washer. Torque to 35 in/lbs (4.0 N/m).
2. Attach the Thor VM2/Adapter Bracket assembly to the U Bracket using 4 each 1/4–20x5/8 bolt, 1/4 lock washer and 1/4 flat washer.
3. If the Thor VM2 is not already mounted to the dock, Place Thor VM2 in the Dock.
4. Adjust the Thor VM2 to the desired viewing angle.
5. Torque the 14–20 bolts to 50 in/lbs (5.6 N/m).

Connect Cables

There are many cables available for the Thor VM2 including power cables, and data/ communication cables.

Strain Relief Cable Clamps

Equipment Required: Phillips screwdriver (not supplied by Honeywell)

There are five strain relief cable clamps secured to the Standard Dock.

There is one strain relief cable clamp and three strain relief brackets for securing cables to the Enhanced Dock.

Use the strain relief clamps to secure audio, power, and I/O cables attached to the Thor VM2 dock.

Use the left-most strain relief clamp for the power cable.
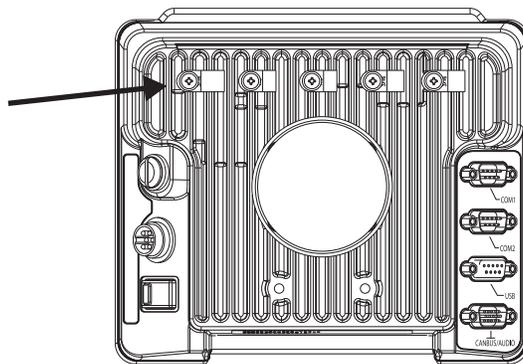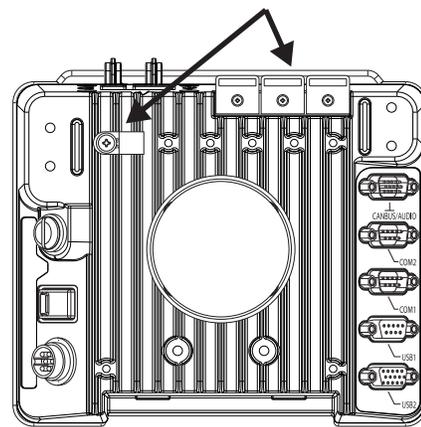
Standard Dock   Enhanced Dock

To use the strain relief clamp(s):

1. Determine the proper strain relief cable clamp. There are three sizes of cable clamps on the Standard Dock which should be matched to the cable to be secured. For example, the largest clamp (on the left when viewing the back of the dock) is designed to secure the power cable. For the Enhanced Dock there is a single cable clamp. Use this clamp for the power cable, Use the brackets for all other cables.

2. Remove the strain relief clamp from the Thor VM2 by turning the screw counterclockwise. Put the screw aside in a safe location.

3. Slide the strain relief clamp over the cable.

4. Using a Phillips screwdriver and the screw that was removed, refasten the clamp holding the cable to the Dock. Do not stretch the cable. Leave enough slack in the cable to allow it to be connected and disconnected easily when needed.

5. Continue in this manner until all cables are secured to the dock.

To use the stradin relief brackets (Enhanced Dock only):

1. Secure the cable to the bracket with plastic tie straps (cable ties).
2. If necessary, the cable ties can be trimmed to length after installation. Cut the excess tie length off flush and not at an angle to prevent sharp edges that may cause cuts.

Connect Power

See Power Supply Connector for connector pinout

For the **VM1D Standard Dock** and **VM3D Enhanced Dock**, power options include:

- 12-48 VDC Vehicles (10-60 VDC Direct Connection) – Direct connection to vehicle power.
- 60-144 VDC Vehicles (50-150 VDC Power Supply, Screws on Side of Lid) – Requires the use of a DC/DC power supply.
- 60-144 VDC Vehicles (50-150 VDC Power Supply, Screws on Top of Lid) – Requires the use of a DC/DC power supply.
- VX6 / VX7 Adapter Cable – For applications where the Thor VM2 replaces a previously installed VX6 or VX7.
- Thor VX8 / Thor VX9 Adapter Cable – For applications where the Thor VM2 (with a VM1D Standard Dock or VM3D Enhanced dock (replaces a previously installed Thor VX8 or Thor VX9.
- CV61 Adapter Cable – For applications where the Thor VM2 replaces a previously installed CV61.
- Screen Blanking – Optional connection to blank the Thor VM2 display while the vehicle is in motion.

For the **VMXD Enhanced Dock**, power options include:

- VMXD Enhanced Dock with Thor VX8/Thor VX9 Power Cable – For applications where a Thor VM2 (with a VMXD Enhanced Dock) replaces a previously installed Thor VX8 or Thor VX9.

When using the Thor VM2 with AC power, use the **VMXD Enhanced Dock for Off-Vehicle Use** and:

- External AC/DC Power Supply – For use when DC power is not available to power the Thor VM2, such as in an office environment.

Power Cable Cautions

⚠️ **Caution: When routing the power cable:**

- Route power cable away from the outside of the fork truck.
- Choose a mounting location so that the power cable does not extend outside the vehicle and that provides sufficient clearance so that the power cable (especially the dock connector end) is not pressed against part of the vehicle.
- Use the proper Strain Relief Cable Clamps to secure cable.
- The power cable is less flexible in low temperature environments. Avoid sharp bends.

⚠️ **Caution: Regularly inspect power cable for damage, especially in low temperature environments. Contact** Technical Assistance **for replacement cable options.**

Power Cable Routing

Power cable with right–angle connector	Power cable with straight connector

Avoid sharp bends in this area of the power cable
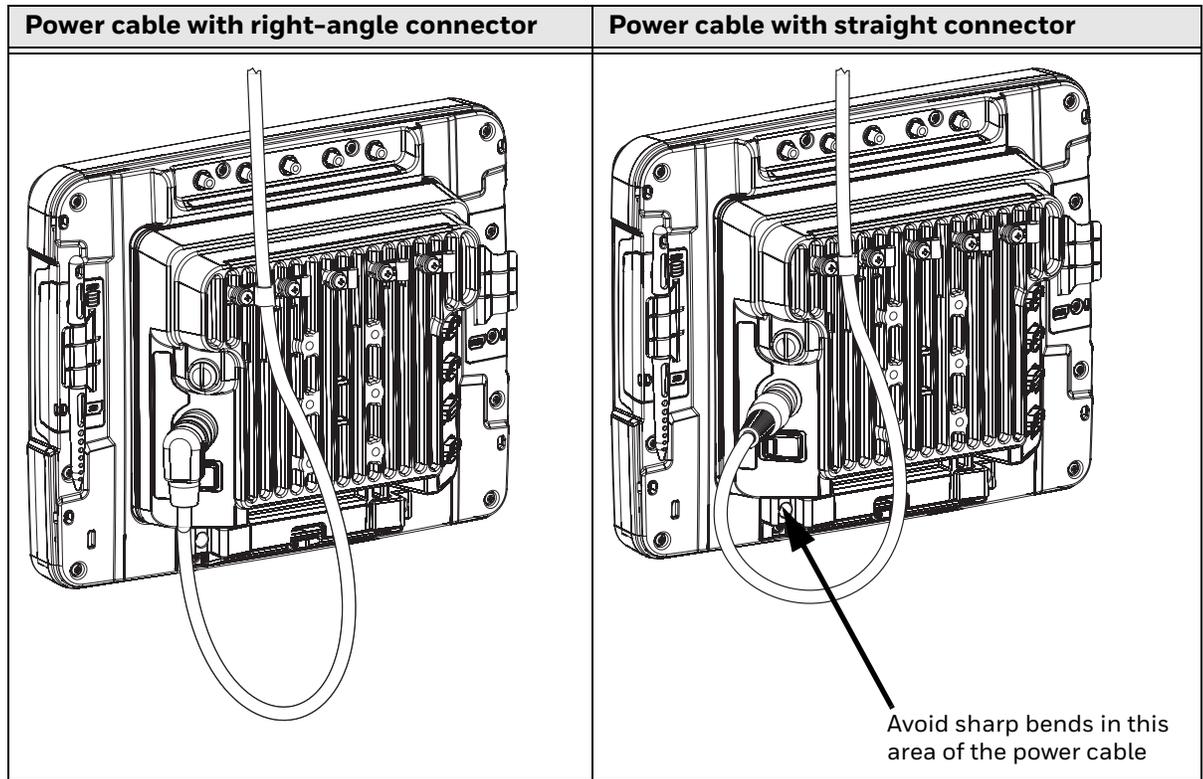
12-48 VDC Vehicles (10-60 VDC Direct Connection)

⚠ **Caution:** **For installation by trained service personnel only.**

⚠ **Caution:** **Use caution when routing the power cable. See** Power Cable Cautions**.**

⚠ **Caution:** These instructions for use with VM1D Standard Dock and VM3D Enhanced Dock only.

Fuse Requirements

⚠ **Warning:** **For proper and safe installation, the input power cable must be connected to a fused circuit on the vehicle. If the supply connection is made directly to the battery, the fuse should be installed in the positive lead within 5 inches of the battery's positive (+) terminal. Use VM3055FUSE (or equivalent) to install the fuse as shown below:**

• For **12VDC** input, use the 10A fuse from the kit or a slow blow fuse that has a DC voltage rating greater than 12VDC.

• For **24VDC** input, use the 6A fuse from the kit or a slow blow fuse that has a DC voltage rating greater than 24VDC.

- For **36VDC** input, use the 4A fuse from the kit or a slow blow fuse that has a DC voltage rating greater than 36VDC.

- For **48VDC** input, use the 3A fuse from the kit or a slow blow fuse that has a DC voltage rating greater than 48VDC.

Note: *For North America, a UL Listed fuse is to be used.*

Power Cable Identification

The DC power cable is included with the dock and is one of the two styles below:

Power cable with right angle connector and 6 wires:

Wire Color	Connection
Red	DC + (10-60 VDC)
Red/White	DC + (10-60 VDC)
Black	DC –
Black/White	DC –
Green	Ground
Blue	Ignition Input (optional)

⚠️ ***Twist the red and red/white wires together and twist the black and black/white wires together before connecting to vehicle power.***

Power cable with straight connector and 4 wires:

Wire Color	Connection
Red	DC + (10-60 VDC)
Black	DC –
Green	Ground
Blue	Ignition Input (optional)

Note: *Correct electrical polarity is required for safe and proper installation. See the figures below for additional wire color-coding specifics.*

The Thor VM2 DC input wires (Red, Red/White DC+ and Black, Black/White DC–) and the Blue ignition input wire are galvanically isolated. The Green ground input is used for electrostatic discharge (ESD) protection.

Vehicle 10-60VDC Direct Power Connection

1. The Thor VM2 must not be mounted in the dock. The power switch on the dock must be turned *Off*. The power cable must be UNPLUGGED from the dock.

2. While observing the Fuse Requirements, connect the power cable as close as possible to the actual battery terminals of the vehicle (if using unswitched power).

3. Use proper electrical and mechanical fastening means for terminating the cable. Properly sized "crimp" type electrical terminals are an accepted method of termination. Please select electrical connectors sized for use with 20AWG (0.81mm2) conductors.

4. Refer to the wiring diagrams following this section for wire colors and connections:

- Ignition Control Wiring Diagram
- Auto-On Control Wiring Diagram
- Manual Control Wiring Diagram

5. Route the power cable the shortest way possible removing any left-over cable. The cable is rated for a maximum temperature of 105°C (221°F). Therefore, when routing this cable it should be protected from physical damage and from surfaces that might exceed this temperature. Cable should be protected from physical damage from moving parts. Do not expose the cable to chemicals or oil that may cause the wiring insulation to deteriorate. Always route the cable so that it does not interfere with safe operation and maintenance of the vehicle.

6. Provide mechanical support for the cable by securing it to the vehicle structure at approximately one foot intervals, taking care not to over tighten and pinch conductors or penetrate outer cable jacket.

7. Connect the watertight connector end of the power cable to the Thor VM2 dock power connector by aligning the connector pins to the power connector; push down on the watertight connector and twist it to fasten securely.

8. Secure the power cable to the Thor VM2 using the Strain Relief Cable Clamps.

9. Place Thor VM2 in the Dock

10. If using the Screen Blanking feature, install the screen blanking box or switch.

11. Press the Power Switch on the back of the Thor VM2 dock.

12. Press the Power Button on the front of the Thor VM2 to turn on the Thor VM2.

Once installation is complete, remember to start the Thor VM2 and select the desired Power Scheme to enable Auto-On, Ignition Control or Manual Control of the Thor VM2 boot up process.

See the **Power Schemes** tab of the Power Options control panel.

Ignition Control Wiring Diagram

Ignition wire must be connected and either of the Ignition Control power modes must be selected from the **Power Schemes** tab of the Power Options control panel. When switched vehicle power is available the Thor VM2 ignition signal wire can be connected (less than 1mA over input voltage range) to the switched circuit to allow the Thor VM2 to power on when the vehicle is switched on. When the vehicle is switched off, more aggressive power management settings are enabled to preserve the vehicle battery charge.

Existing Circuitry On Vehicle

Battery

Main Switch

+Vo   -Vo   Ignition

Fuse - See *Warning* statement below

See *Caution* statement below

Quick Mount Smart Dock

Cable for optional screen blanking connection

COM1 or COM2 Connector

Red/White (if present)

Red

Black/White (if present)

Black

Green

Blue

Circular Power Connector

Caution: For battery powered vehicles:

- Red wire is connected to battery positive. If there is a red wire and a red/white wire, twist them together and connect to battery positive.

- Black wire must be connected to battery negative. If there is a black wire and a black/white wire, twist them together and connect to battery negative.

- Green wire must be connected to the vehicle chassis ground.

Caution: For internal combustion engine powered vehicles:

- Red wire is connected to battery positive. If there is a red wire and a red/white wire, twist them together and connect to battery positive.

- Black wire must be connected to battery negative. If there is a black wire and a black/white wire, twist them together and connect to battery negative.

- Green wire is connected to the vehicle chassis ground, which can also be battery negative.

Fuse Requirements

Warning: For proper and safe installation, the input power cable must be connected to a fused circuit on the vehicle. If the supply connection is made directly to the battery, the fuse should be installed in the positive lead within 5 inches of the battery's positive (+) terminal. Use VM3055FUSE (or equivalent) to install the fuse as shown below:

- For **12VDC** input, use the 10A fuse from the kit or a slow blow fuse that has a DC voltage rating greater than 12VDC.

- For **24VDC** input, use the 6A fuse from the kit or a slow blow fuse that has a DC voltage rating greater than 24VDC.

- For **36VDC** input, use the 4A fuse from the kit or a slow blow fuse that has a DC voltage rating greater than 36VDC.

- For **48VDC** input, use the 3A fuse from the kit or a slow blow fuse that has a DC voltage rating greater than 48VDC.

Note: *For North America, a UL Listed fuse is to be used.*

Auto-On power mode must be selected on the **Power Schemes** tab of the Power Options control panel. The vehicle supply connections should be made to vehicle switched power to allow the terminal to automatically power-up when vehicle power is switched on or when the power switch on the back of the dock is placed in the On position. The Ignition wire is not used and should be left disconnected.

Caution: For battery powered vehicles:

- Red wire is connected to battery positive. If there is a red wire and a red/white wire, twist them together and connect to battery positive.

- Black wire must be connected to battery negative. If there is a black wire and a black/white wire, twist them together and connect to battery negative.

- Green wire must be connected to the vehicle chassis ground.

Caution: For internal combustion engine powered vehicles:

- Red wire is connected to battery positive. If there is a red wire and a red/white wire, twist them together and connect to battery positive.

- Black wire must be connected to battery negative. If there is a black wire and a black/white wire, twist them together and connect to battery negative.

- Green wire is connected to the vehicle chassis ground, which can also be battery negative.

Warning: For proper and safe installation, the input power cable must be connected to a fused circuit on the vehicle. If the supply connection is made directly to the battery, the fuse should be installed in the positive lead within 5 inches of the battery's positive (+) terminal. Use VM3055FUSE (or equivalent) to install the fuse as shown below:

- For **12VDC** input, use the 10A fuse from the kit or a slow blow fuse that has a DC voltage rating greater than 12VDC.

- For **24VDC** input, use the 6A fuse from the kit or a slow blow fuse that has a DC voltage rating greater than 24VDC.
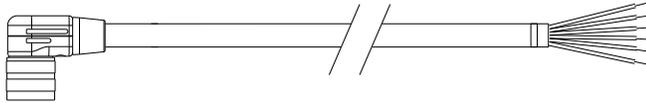
- For **36VDC** input, use the 4A fuse from the kit or a slow blow fuse that has a DC voltage rating greater than 36VDC.

- For **48VDC** input, use the 3A fuse from the kit or a slow blow fuse that has a DC voltage rating greater than 48VDC.

Note: *For North America, a UL Listed fuse is to be used.*

Ignition wire must be left unconnected and AC/DC power mode must be from the **Power Schemes** tab of the Power Options control panel.

! Caution: For battery powered vehicles:

• Red wire is connected to battery positive. If there is a red wire and a red/white wire, twist them together and connect to battery positive.

• Black wire must be connected to battery negative. If there is a black wire and a black/white wire, twist them together and connect to battery negative.

• Green wire must be connected to the vehicle chassis ground.

! Caution: For internal combustion engine powered vehicles:

• Red wire is connected to battery positive. If there is a red wire and a red/white wire, twist them together and connect to battery positive.

• Black wire must be connected to battery negative. If there is a black wire and a black/white wire, twist them together and connect to battery negative.

• Green wire is connected to the vehicle chassis ground, which can also be battery negative.

> ⚠ **Warning: For proper and safe installation, the input power cable must be connected to a fused circuit on the vehicle. If the supply connection is made directly to the battery, the fuse should be installed in the positive lead within 5 inches of the battery's positive (+) terminal. Use VM3055FUSE (or equivalent) to install the fuse as shown below:**

- For **12VDC** input, use the 10A fuse from the kit or a slow blow fuse that has a DC voltage rating greater than 12VDC.

- For **24VDC** input, use the 6A fuse from the kit or a slow blow fuse that has a DC voltage rating greater than 24VDC.

- For **36VDC** input, use the 4A fuse from the kit or a slow blow fuse that has a DC voltage rating greater than 36VDC.

- For **48VDC** input, use the 3A fuse from the kit or a slow blow fuse that has a DC voltage rating greater than 48VDC.

Note: *For North America, a UL Listed fuse is to be used.*

60-144 VDC Vehicles (50-150 VDC Power Supply, Screws on Side of Lid)

⚠ These instructions are for use with VM1D Standard Dock and VM3D Enhanced Dock only.

This option requires DC/DC external power supply Honeywell Part no. 9000313PWR-SPLY.
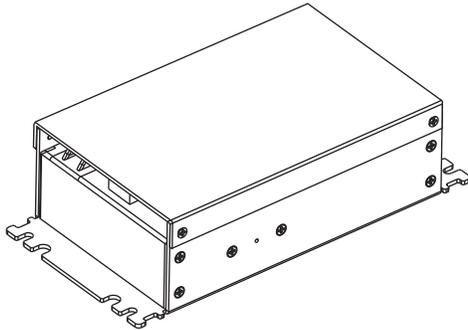
Shown With Lid Attached

• Lid is secured with screws on the side of lid.
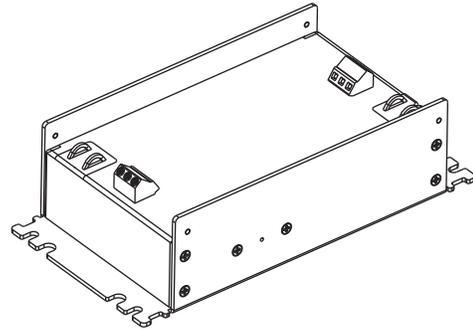
Shown With Lid Removed

• Input and output connector blocks under lid.

• One positive (Vin+), negative (Vin–) and ground (⏚) connection in input block.

• One positive (Vo+) and negative (Vo–) connection in output block.

If the DC/DC power supply does not have screws in the side of the lid, see 60-144 VDC Vehicles (50-150 VDC Power Supply, Screws on Top of Lid).

⚠ **Caution: For installation by trained service personnel only.**

⚠ **Caution: Usage in areas where moisture can affect the power supply connections should be avoided. The power supply should be mounted in a dry location within the vehicle or placed in a suitable protective enclosure.**

⚠ **Caution: Use caution when routing the power cable. See** Power Cable Cautions**.**

> **Warning: For proper and safe installation, the input power cable must be connected to a fused circuit on the vehicle. If the supply connection is made directly to the battery, the fuse should be installed in the positive lead within 5 inches of the battery's positive (+) terminal. Use VM3055FUSE (or equivalent) to install the fuse as shown below:**

- For **all voltages**, use the 3A fuse from the kit or a slow blow fuse that has a DC voltage rating greater than the vehicle input voltage.

Note: *For North America, a UL Listed fuse is to be used.*

Power Cable Identification

The DC power cable is included with the dock and is one of the two styles below:

Power cable with right angle connector and 6 wires:

Wire Color	Connection
Red	DC + (10-60 VDC)
Red/White	DC + (10-60 VDC)
Black	DC -
Black/White	DC -
Green	Ground
Blue	Ignition Input (optional)

> *Twist the red and red/white wires together and twist the black and black/white wires together before connecting to vehicle power.*

Power cable with straight connector and 4 wires:

Wire Color	Connection
Red	DC + (10-60 VDC)
Black	DC -
Green	Ground
Blue	Ignition Input (optional)

Note: *Correct electrical polarity is required for safe and proper installation. See Wiring Diagram for additional wire color-coding specifics.*

The Thor VM2 DC input wires (Red, Red/White DC+ and Black, Black/White DC–) and the Blue ignition input wire are galvanically isolated. The Green ground input is used for electrostatic discharge (ESD) protection.

Vehicle 50-150VDC Power Connection

1. Please review the Wiring Diagram, before beginning power cable install.

2. The Thor VM2 must not be mounted in the dock. The power switch on the dock must be turned *Off*. The power cable must be UNPLUGGED from the dock.

3. Route the cable from the Thor VM2 to the DC/DC power supply. Route the power cable the shortest way possible. The cable is rated for a maximum temperature of 105°C (221°F). When routing this cable, it should be protected from physical damage and from surfaces that might exceed this temperature. Do not expose the cable to chemicals or oil that may cause the wiring insulation to deteriorate. Always route the cable so that it does not interfere with safe operation and maintenance of the vehicle.

4. Cut the cable to length and strip the wire ends.

5. Remove the lid from the DC/DC power supply.

6. Connect the stripped end of the positive wires (red and red/white twisted together or a single red wire) to the output block. See Power Cable Identification.

7. Connect the stripped end of the negative wires (black and black/white twisted together or a single black wire) to the output. See Power Cable Identification.

> *Note:* The input block has V_{IN}+, V_{IN}- and GND terminals. The output block has V_O+ and V_O- terminals.
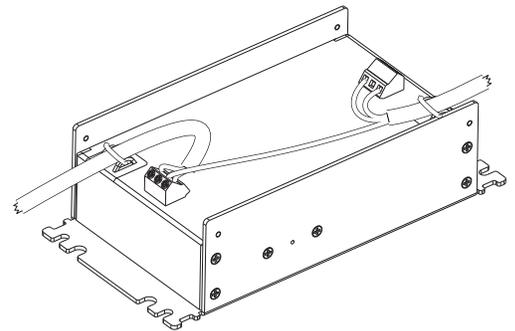
8. Connect the ground (green) wire from the Thor VM2 to the GND terminal on the input side of the DC/DC power supply.

9. Route the wiring from the DC/DC power supply to the vehicle's electrical system. **Do not connect to vehicle power at this time.**

10. Strip the wire ends and connect to the input side of the DC/DC power supply.

11. Use looms and wire ties to secure all wiring as shown.

12. Reattach the cover with the screws.

13. Connect the DC/DC power supply to the vehicle's electrical system as directed below:

> ⚠️ **Caution: For battery powered vehicles:**

- V_{IN}+ is connected to battery positive.
- V_{IN}- must be connected to battery negative.
- GND must be connected to the vehicle chassis ground.

> ⚠️ **Caution: For internal combustion engine powered vehicles:**

- $V_{IN}+$ is connected to battery positive.

- $V_{IN}-$ is connected to battery negative.

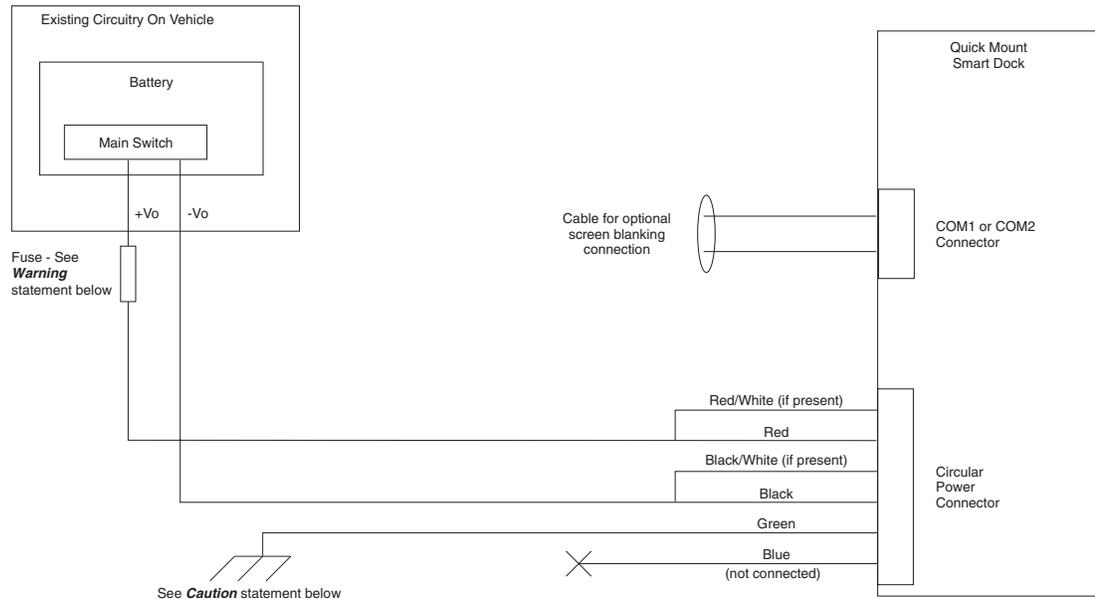- GND is connected to the vehicle chassis ground, which can also be battery negative.

14. While observing the Fuse Requirements connect the power cable as close as possible to the actual battery terminals of the vehicle. When available, always connect to unswitched terminals in the vehicle fuse panel, after providing proper fusing.

    ATTENTION: For uninterrupted power, electrical supply connections should not be made at any point after the ignition switch of the vehicle.

15. Use proper electrical and mechanical fastening means for terminating the cable. Properly sized "crimp" type electrical terminals are an accepted method of termination. Select electrical connectors sized for use with 18AWG (1mm^2) conductors.

16. Provide mechanical support for the cable by securing it to the vehicle structure at approximately one foot intervals, taking care not to over tighten and pinch conductors or penetrate the outer cable jacket.

17. Connect the watertight connector end of the power cable to the Thor VM2 dock power connector by aligning the connector pins to the power connector; push down on the watertight connector and twist it to fasten securely. Flip the power switch on the back of the dock to On.

18. Secure the power cable to the Thor VM2 using the Strain Relief Cable Clamps.

19. Place Thor VM2 in the Dock.

20. If using the Screen Blanking feature, install the screen blanking box or switch.

21. Press the Power Switch on the back of the Thor VM2 dock.

22. Press the Power Button on the front of the Thor VM2 to turn on the Thor VM2.

Once installation is complete, remember to start the Thor VM2 and select the desired Power Scheme to enable Auto-On or Manual Control of the Thor VM2 boot up process.

See the **Power Schemes** tab of the Power Options control panel.

Note: *Ignition control is not available for trucks over 60VDC.*

Wiring Diagram


```
┌─────────────────────────────────┐                                    ┌──────────────────────┐
│  Existing Circuitry on Vehicle  │                                    │   Quick Mount        │
│  ┌───────────────────────────┐  │                                    │   Smart Dock         │
│  │     Forklift Battery      │  │                                    │                      │
│  │  ┌─────────────────────┐  │  │          User supplied serial      │   COM1 or COM2       │
│  │  │    Main Switch      │  │  │          cable for optional        │   Connector          │
│  │  └─────────────────────┘  │  │          screen blanking           │   on Dock            │
│  └───────────────────────────┘  │          connection,               │                      │
│            +Vo    -Vo           │          see below                 │                      │
└─────────────────────────────────┘                                    │                      │
                                                                        │   Circular           │
Fuse - See                                        Red/White (if present)│   Power              │
Warning                                                    Red          │   Connector          │
statement below                                  Black/White (if present)│   on Dock           │
                                                          Black          │                      │
See Caution    GND  VIN+  VIN-                            Green          │                      │
statement                            Vo+                  Blue           │                      │
below                                Vo-              (not connected)    └──────────────────────┘
               DC/DC
               Power
               Supply
```

⚠ **Caution: For battery powered vehicles:**

•   GND must be connected to the vehicle chassis ground.

⚠ **Caution: For internal combustion engine powered vehicles:**

•   GND is connected to the vehicle chassis ground, which can also be battery negative.

Fuse Requirements

⚠ **Warning: For proper and safe installation, the input power cable must be connected to a fused circuit on the vehicle. If the supply connection is made directly to the battery, the fuse should be installed in the positive lead within 5 inches of the battery's positive (+) terminal. Use VM3055FUSE (or equivalent) to install the fuse as shown below:**

•   For **all voltages**, use the 3A fuse from the kit or a slow blow fuse that has a DC voltage rating greater than the vehicle input voltage.

Note: *For North America, a UL Listed fuse is to be used.*

60-144 VDC Vehicles (50-150 VDC Power Supply, Screws on Top of Lid)

> ⚠ These instructions are for use with VM1D Standard Dock and VM3D Enhanced Dock only.

This option requires DC/DC power supply Honeywell Part no. VX89303PWRSPLY shown below.
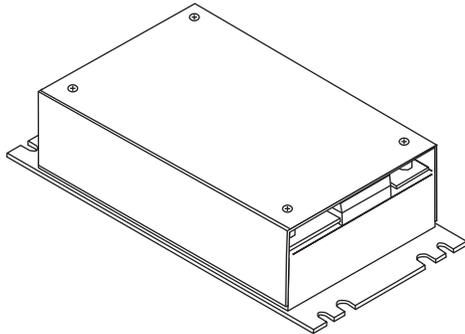
Shown With Lid Attached

- Lid is secured with screws on the top of lid.
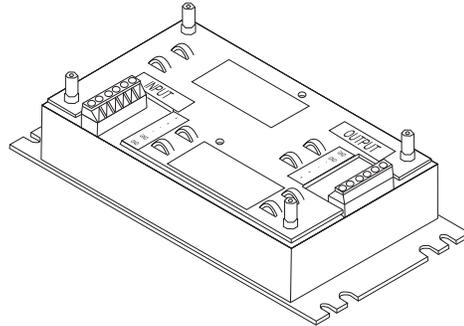
Shown With Lid Removed

- Input and output connector blocks under lid.

- Two positive (+), negative (–) and ground (⊕) connections per terminal block

If the DC/DC power supply does not have screws in the top of the lid, see 60-144 VDC Vehicles (50-150 VDC Power Supply, Screws on Side of Lid).

⚠ **Caution: For installation by trained service personnel only.**

⚠ **Caution: The VX89303PWRSPLY power supply is sealed per IPXX. Usage in areas where moisture can affect the power supply connections should be avoided. The power supply should be mounted in a dry location within the vehicle or placed in a suitable protective enclosure.**

⚠ **Caution: Use caution when routing the power cable. See** Power Cable Cautions**.**

> **Warning:** **For proper and safe installation, the input power cable must be connected to a fused circuit on the vehicle. If the supply connection is made directly to the battery, the fuse should be installed in the positive lead within 5 inches of the battery's positive (+) terminal. Use VM3055FUSE (or equivalent) to install the fuse as shown below:**
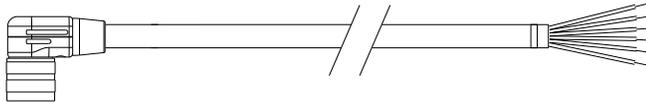
- For **all voltages**, use the 3A fuse from the kit or a slow blow fuse that has a DC voltage rating greater than the vehicle input voltage.

Note: *For North America, a UL Listed fuse is to be used.*

Power Cable Identification

The DC power cable is included with the dock and is one of the two styles below:

Power cable with right angle connector and 6 wires:

Wire Color	Connection
Red	DC + (10-60 VDC)
Red/White	DC + (10-60 VDC)
Black	DC –
Black/White	DC –
Green	Ground
Blue	Ignition Input (optional)

> *Twist the red and red/white wires together and twist the black and black/white wires together before connecting to vehicle power.*

Power cable with straight connector and 4 wires:

| Wire Color	Connection
Red	DC + (10-60 VDC)
Black	DC –
Green	Ground
Blue	Ignition Input (optional)

Note: *Correct electrical polarity is required for safe and proper installation. See Wiring Diagram for additional wire color-coding specifics.*

The Thor VM2 DC input wires (Red, Red/White DC+ and Black, Black/White DC–) and the Blue ignition input wire are galvanically isolated. The Green ground input is used for electrostatic discharge (ESD) protection.

Vehicle 50-150VDC Power Connection

1. Please review the Wiring Diagram, before beginning power cable install.

2. The Thor VM2 must not be mounted in the dock. The power switch on the dock must be turned *Off*. The power cable must be UNPLUGGED from the dock.

3. Route the cable from the Thor VM2 to the DC/DC power supply. Route the power cable the shortest way possible. The cable is rated for a maximum temperature of 105ºC (221ºF). When routing this cable, it should be protected from physical damage and from surfaces that might exceed this temperature. Do not expose the cable to chemicals or oil that may cause the wiring insulation to deteriorate. Always route the cable so that it does not interfere with safe operation and maintenance of the vehicle.

4. Cut the cable to length and strip the wire ends.

5. Remove the lid from the DC/DC power supply.

6. Connect the stripped end of the positive wires (red and red/white twisted together or a single red wire) to the output block. See Power Cable Identification.

7. Connect the stripped end of the negative wires (black and black/white twisted together or a single black wire) to the output. See Power Cable Identification.

Note: *The input and output blocks each have two + (plus), two – (minus) and two ⊕ (ground) connectors. Either connector in the block can be used to connect the matching polarity wire.*
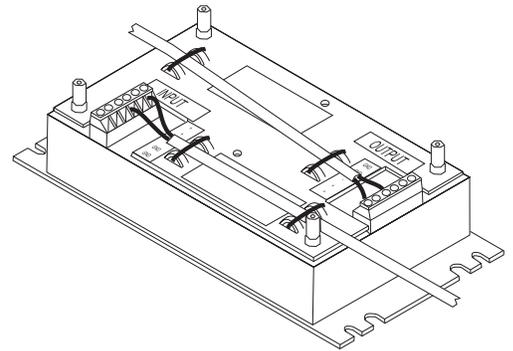
8. Route the wiring from the DC/DC power supply to the vehicle's electrical system. Do not connect to vehicle power at this time.

9. Strip the wire ends and connect to the input side of the DC/DC power supply.

10. Use looms and wire ties to secure all wiring as shown.

11. Reattach the cover with the screws.

12. Connect the DC/DC power supply to the vehicle's electrical system as directed below:

   ⚠ **Caution: For battery powered vehicles:**

   • + is connected to battery positive.

   • – must be connected to battery negative.

   • ⊕ must be connected to the vehicle chassis ground.

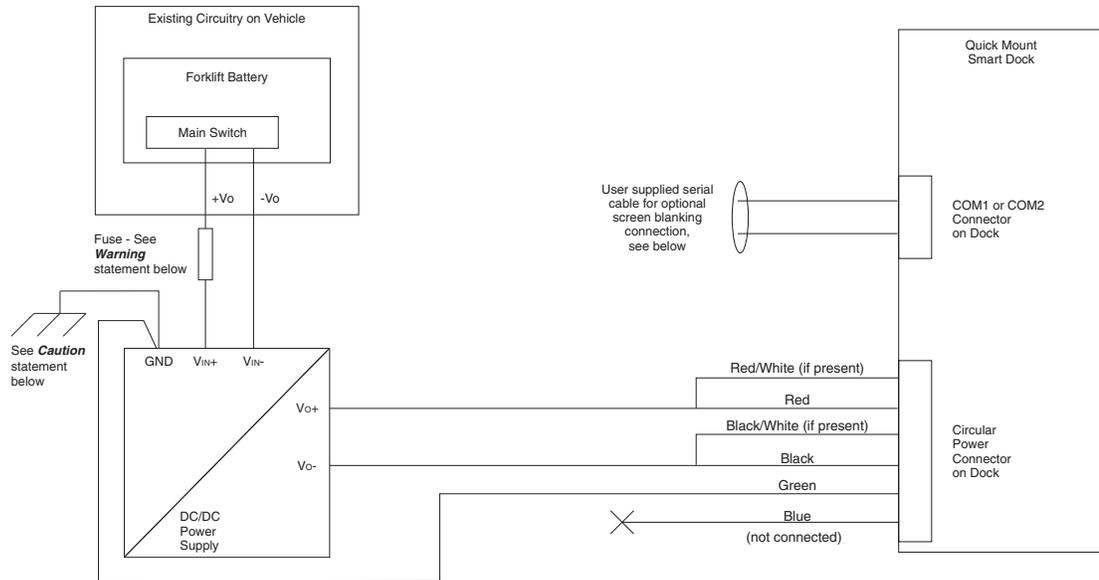   ⚠ **Caution: For internal combustion engine powered vehicles:**

   • + is connected to battery positive.

   • – must be connected to battery negative.

   • ⊕ must be connected to the vehicle chassis ground.

13. While observing the Fuse Requirements, connect the power cable as close as possible to the actual battery terminals of the vehicle. When available, always connect to unswitched terminals in the vehicle fuse panel, after providing proper fusing.

    ATTENTION: For uninterrupted power, electrical supply connections should not be made at any point after the ignition switch of the vehicle.

14. Use proper electrical and mechanical fastening means for terminating the cable. Properly sized "crimp" type electrical terminals are an accepted method of termination. Select electrical connectors sized for use with 18AWG ($1mm^2$) conductors.

15. Provide mechanical support for the cable by securing it to the vehicle structure at approximately one foot intervals, taking care not to over tighten and pinch conductors or penetrate the outer cable jacket.

16. Connect the watertight connector end of the power cable to the Thor VM2 dock power connector by aligning the connector pins to the power connector; push down on the watertight connector and twist it to fasten securely. Flip the power switch on the back of the dock to On.

17. Secure the power cable to the Thor VM2 using the Strain Relief Cable Clamps.

18. Place Thor VM2 in the Dock.

19. If using the Screen Blanking feature, install the screen blanking box or switch.

20. Press the Power Switch on the back of the Thor VM2 dock.

21. Press the Power Button on the front of the Thor VM2 to turn on the Thor VM2.

Once installation is complete, remember to start the Thor VM2 and select the desired Power Scheme to enable Auto-On or Manual Control of the Thor VM2 boot up process.

See the **Power Schemes** tab of the Power Options control panel.

Note: *Ignition control is not available for trucks over 60VDC.*

Wiring Diagram
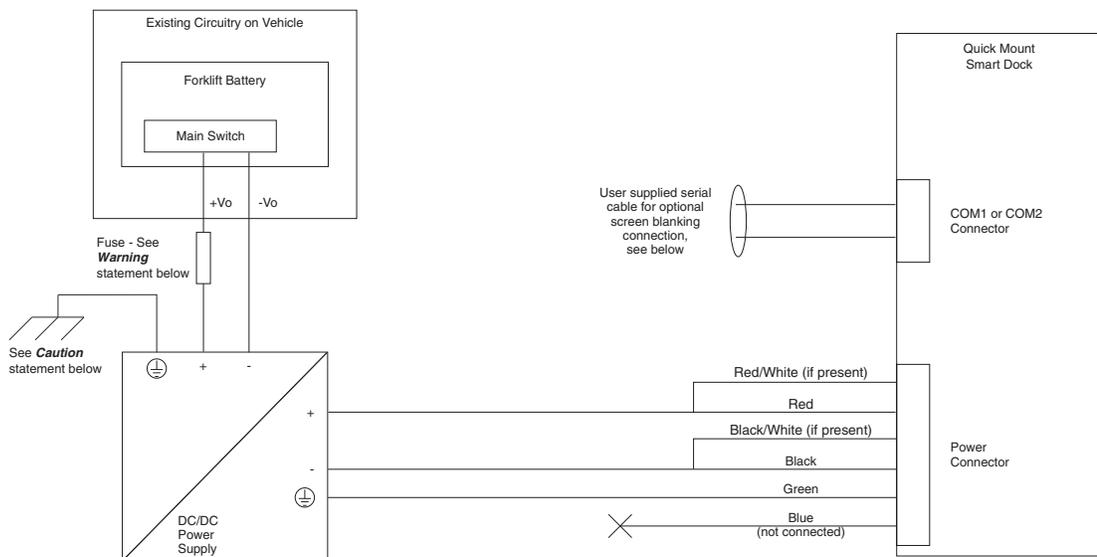
!   **Caution: For battery powered vehicles:**

⏚ must be connected to the vehicle chassis ground.

⚠ **Caution: For internal combustion engine powered vehicles:**

⏚ is connected to the vehicle chassis ground, which can also be battery negative.

Fuse Requirements

⚠ **Warning: For proper and safe installation, the input power cable must be connected to a fused circuit on the vehicle. If the supply connection is made directly to the battery, the fuse should be installed in the positive lead within 5 inches of the battery's positive (+) terminal. Use VM3055FUSE (or equivalent) to install the fuse as shown below:**

- For **all voltages**, use the 3A fuse from the kit or a slow blow fuse that has a DC voltage rating greater than the vehicle input voltage.

Note: *For North America, a UL Listed fuse is to be used.*

VX6 / VX7 Adapter Cable

⚠ These instructions are for use with VM1D Standard Dock and VM3D
Enhanced Dock only.

An adapter cable is available to attach the Thor VM2 to a vehicle previously equipped
with a VX6/VX7 DC power cable. The adapter cable has a 5-pin connector to match with
the VX6/VX7 power supply cable on one end and a 6-pin connector to match to the Thor
VM2 on the other end. This section assumes the VX6/VX7 power cable is properly con-
nected to vehicle power. Refer to the VX6 or VX7 Vehicle Mounting Reference Guide for
details.

⚠ **Warning: Because the VX6/VX7 supports 10-60 VDC power input, verify
input voltages before using this adapter cable with an existing
VX6 or VX7 power connection installation.**

To Power Connector on Dock

To VX6/VX7 Power Supply Cable

When this adapter cable is used, there is no provision for an ignition switch input.
Therefore the vehicle ignition monitoring function is not available when using this
cable.

Connect to VX6 / VX7 Power Cable

1. Connect the adapter cable to the Thor VM2 power cable by aligning the connector
   pins to the power connector; push down on the watertight connector and twist it to
   fasten securely.

2. The cable is rated for a maximum temperature of 105°C (221°F). Therefore, routing
   this cable it should be protected from physical damage and from surfaces that
   might exceed this temperature. Cable should be protected from physical damage
   from moving parts. Do not expose the cable to chemicals or oil that may cause the
   wiring insulation to deteriorate. Always route the cable so that it does not interfere
   with safe operation and maintenance of the vehicle.

3. Provide mechanical support for the cable by securing it to the vehicle structure at
   approximately one foot intervals, taking care not to over tighten and pinch
   conductors or penetrate outer cable jacket.

4. Connect the watertight connector end of the power cable to the Thor VM2 dock
   power connector by aligning the connector pins to the power connector; push down
   on the watertight connector and twist it to fasten securely.

5. Secure the power cable to the Thor VM2 using the Strain Relief Cable Clamps.

6. Place Thor VM2 in the Dock

7. If using the Screen Blanking feature, install the screen blanking box or switch.

8. Press the Power Switch on the back of the Thor VM2 dock.

9. Press the Power Button on the front of the Thor VM2 to turn on the Thor VM2.

Thor VX8 / Thor VX9 Adapter Cable

> ⚠ These instructions for use with VM1D Standard Dock and VM3D Enhanced Dock only. This cable is not used for the VMXD Enhanced Dock

An adapter cable is available to attach the Thor VM2 to a vehicle previously equipped with a VX8/VX9 DC power cable. The adapter cable has a 6-pin connector to match the VX8/XVX9 power supply cable on one end and a 6-pin connector to match the Thor VM2 on the other end. The cable also has bare wires for ground and ignition sense connection plus a D9 cable to connect to a COM port on the Thor VM2 dock to provide a screen blanking signal. This section assumes the VX8/VX9 power cable is properly connected to vehicle power. Refer to the VX8 or VX9 Vehicle Mounting Reference Guide for details.
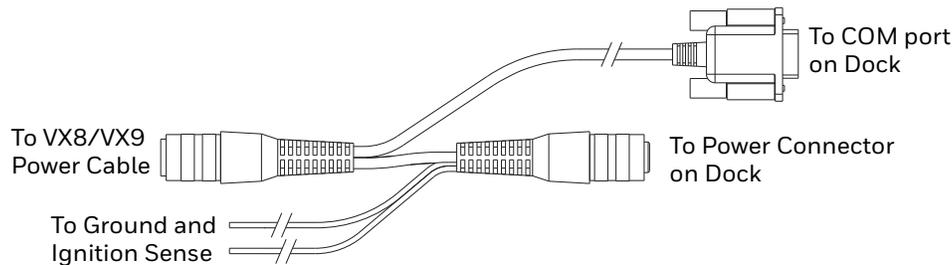
Connect to Thor VX8 / VX9 Power Cable

1. Connect the adapter cable to the Thor VX8/VX9 power cable by aligning the connector pins to the power connector; push down on the watertight connector and twist it to fasten securely.

2. Connect the green wire to vehicle ground

   > ⚠ **Caution: For battery powered vehicles:**

   • The green wire must be connected to the vehicle chassis ground.

   > ⚠ **Caution: For internal combustion engine powered vehicles:**

   • The green wire is connected to the vehicle chassis ground, which can also be battery negative.

3. If ignition control will be used, connect the blue wire to an ignition switched circuit (less than 1mA over input voltage range). If ignition control is not used, the blue wire can be left disconnected,

4. If the VX8/VX9 cable is connected to a screen blanking box or switch, connect the D9 connector to a COM port on the dock.

5. The cable is rated for a maximum temperature of 105°C (221°F). Therefore, when routing this cable it should be protected from physical damage and from surfaces that might exceed this temperature. Cable should be protected from physical damage from moving parts. Do not expose the cable to chemicals or oil that may cause the wiring insulation to deteriorate. Always route the cable so that it does not interfere with safe operation and maintenance of the vehicle.

6. Provide mechanical support for the cable by securing it to the vehicle structure at approximately one foot intervals, taking care not to over tighten and pinch conductors or penetrate outer cable jacket.

7. Connect the watertight connector end of the power cable to the Thor VM2 dock power connector by aligning the connector pins to the power connector; push down on the watertight connector and twist it to fasten securely.

8. Secure the power cable to the Thor VM2 using the Strain Relief Cable Clamps.

9. Place Thor VM2 in the Dock.

10. If using the Screen Blanking feature, install the screen blanking box or switch if not previously installed.

11. Press the Power Switch on the back of the Thor VM2 dock.

12. Press the Power Button on the front of the Thor VM2 to turn on the Thor VM2.

CV61 Adapter Cable

⚠ These instructions for use with VM1D Standard Dock and VM3D Enhanced Dock only.

An adapter cable is available to attach the Thor VM2 to a vehicle previously equipped with a CV61 DC power cable. The adapter cable has a 5-pin connector to match with the VV61 power supply cable on one end and a 6-pin connector to match to the Thor VM2 on the other end. This section assumes the CV61 power cable is properly connected to vehicle power. Refer to the CV61 documentation for details.

To Power Connector on Dock

To CV41 Power Supply Cable

When this adapter cable is used, there is no provision for an ignition switch input. Therefore the vehicle ignition monitoring function is not available when using this cable.

Connect to CV61 Power Cable

1. Connect the adapter cable to the CV61 power cable by aligning the connector pins to the power connector; push down on the watertight connector and twist it to fasten securely.

2. The cable is rated for a maximum temperature of 105°C (221°F). Therefore, routing this cable it should be protected from physical damage and from surfaces that might exceed this temperature. Cable should be protected from physical damage from moving parts. Do not expose the cable to chemicals or oil that may cause the wiring insulation to deteriorate. Always route the cable so that it does not interfere with safe operation and maintenance of the vehicle.

3. Provide mechanical support for the cable by securing it to the vehicle structure at approximately one foot intervals, taking care not to over tighten and pinch conductors or penetrate outer cable jacket.

4. Connect the watertight connector end of the power cable to the Thor VM2 dock power connector by aligning the connector pins to the power connector; push down on the watertight connector and twist it to fasten securely.

5. Secure the power cable to the Thor VM2 using the Strain Relief Cable Clamps.

6. Place Thor VM2 in the Dock

7. If using the Screen Blanking feature, install the screen blanking box or switch.

8. Press the Power Switch on the back of the Thor VM2 dock.

9. Press the Power Button on the front of the Thor VM2 to turn on the Thor VM2.

Screen Blanking

Prerequisite: The steps outlined in either 12-48 VDC Vehicles (10-60 VDC Direct Connection), 60-144 VDC Vehicles (50-150 VDC Power Supply, Screws on Side of Lid) or 60-144 VDC Vehicles (50-150 VDC Power Supply, Screws on Top of Lid) have been completed.

Screen blanking is accomplished by either a Screen Blanking Box or a user supplied switch.

⚠ **Caution: For installation by trained service personnel only.**

Fuse Requirements

⚠ **Warning: For proper and safe installation, the input power lead to the Screen Blanking Box requires a 3 Amp maximum time delay (slow blow) high interrupting rating fuse.**

Note: *For North America, a UL Listed fuse is to be used.*

Screen Blanking Cable

Refer to Screen Control to configure the Thor VM2 for screen blanking.

When routing any additional cables for screen blanking:

- Route the cable the shortest way possible removing any left-over cable
- Fuses and cabling are user supplied. Therefore, route these cables so they are protected from physical damage and from surfaces that might exceed the cable's rated temperature threshold.
- Cable should be protected from physical damage from moving parts
- Do not expose the cable to chemicals or oil that may cause the wiring insulation to deteriorate
- Always route the cable so that it does not interfere with safe operation and maintenance of the vehicle.
- Provide mechanical support for the cable by securing it to the vehicle structure at approximately one foot intervals, taking care not to over tighten and pinch conductors or penetrate outer cable jacket.

Honeywell Screen Blanking Box Cable

An optional Honeywell Screen Blanking Box Cable is available.
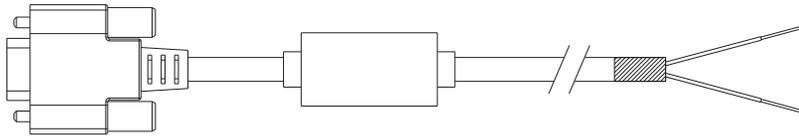
DB9 Female	Function with Screen Blanking Box	Wire color
1 –6, 9	Not Used	
7 (RTS)	Connected to Screen Blanking Box, unswitched side	Black (see note)
8 (CTS)	Connected to Screen Blanking Box, switched side	Gray (see note)

Note: *Wire colors only apply to optional Honeywell Screen Blanking Box Cable, VM1080CABLE. Wire colors may vary in a user-supplied cable.*

The optional Honeywell Screen Blanking Box Cable, VM1080CABLE, is installed as follows:

1. Connect the gray wire of the cable to the switched side of the Screen Blanking Box.

2. Connect the black wire of the cable to the unswitched side of the Screen Blanking Box.

3. Connect the D9 serial connector to either COM1 or COM2 serial port on the Thor VM2 dock.

User-Supplied Cable

A user-supplied cable can be used as well. Pins 7 and 8 must be connected as detailed below. No other pins are to be connected.
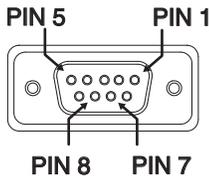
DB9 Female	Function with Screen Blanking Box	Function with Switch
1 –6, 9	Not Used	Not Used
7 (RTS)	Connected to Screen Blanking Box, unswitched side	Connected to Switch
8 (CTS)	Connected to Screen Blanking Box, switched side	Connected to Switch

The user-supplied cable is installed as follows:

1. Connect the wire from Pin 8 of the cable to the switched side of the Screen Blanking Box or to a user-supplied switch.

2. Connect the wire from Pin 7 of the cable to the unswitched side of the Screen Blanking Box or to a user-supplied switch.

3. Connect the D9 serial connector to either COM1 or COM2 serial port on the Thor VM2 dock.

Screen Blanking Box

Screen Blanking Box Terminal	Connection
12-xxV	Input from vehicle motion sensing circuitry. Please refer to label on Screen Blanking Box for allowable voltage input range.
GND	DC –
Unswitched Switched	These two terminals are for connecting a serial cable: • If using an optional Honeywell screen blanking cable, VM1080CABLE, connect the *gray* wire to the *switched* side of the connection and connect the *black* wire to the *unswitched* side. • If using a user-supplied cable, the cable must be constructed so that Pin 7 (RTS) connects to *switched* side of the connection and Pin 8 (CTS) connects to the *unswitched* side.

It is assumed that the motion sensing circuitry in the illustrations below is powered by internal vehicle circuitry.

Please refer to the appropriate illustration below for Screen Blanking Box wiring diagrams.

Warning: **Do not exceed the maximum input voltage, either 60 or 72VDC, specified on the Screen Blanking Box label when using this configuration.**
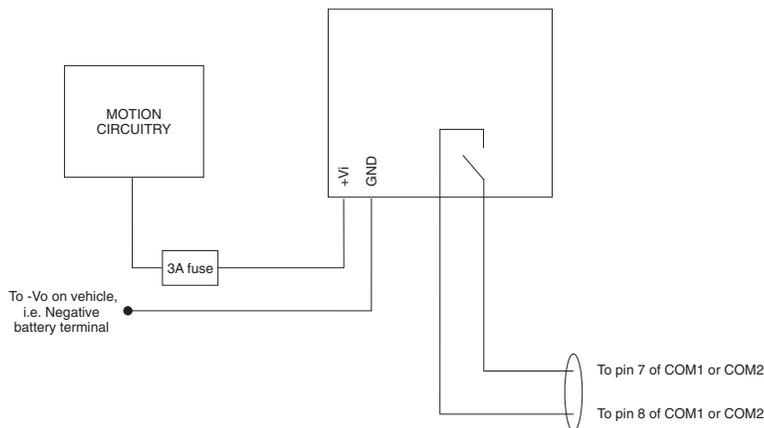
Note: *The black and gray wire colors in the illustration only apply to the optional Honeywell Screen Blanking Box Cable, VM1080CABLE. The wire colors may be different in a user-supplied cable.*

Screen Blanking with Switch

In applications where it is impractical to use the screen blanking box due to vehicle volt-age or lack of a motion sensing signal, screen blanking can be controlled via a user sup-plied switch or relay that provides an electrical conductive connection on vehicle motion.

To pins 7 and 8
of COM1 or COM2
port on dock
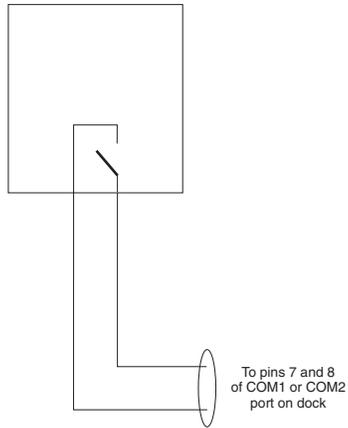
Pins 7 and 8 must be connected as shown in the illustration above. No other pins are to be connected.

VMXD Enhanced Dock with Thor VX8/Thor VX9 Power Cable

Caution: This dock is recommended for use when replacing an existing Thor VX8 or Thor VX9 where screen blanking is used. This dock eliminates the need for wiring changes by enabling the existing VX8/VX9 power cable and screen blanking box to be used when the VX8/VX9 is replaced by a Thor VM2 computer. These instructions are for this dock model only! The Ignition Control feature is not available when this dock is used.

Warning: The external DC/DC converter previously used with the Thor VX8 or Thor VX9 must be left in place to provide ground isolation. Connecting the dock power input directly to vehicle power could result in a safety hazard or equipment damage.

Warning: The cable shielding must be connected to chassis ground. Consult the instructions later in this section for the respective power supply type.

Caution: COM1 is used for screen blanking (via the power cable connector) and is unavailable when the screen blanking box is attached. When a screen blanking box is attached, any external serial device such as a scanner, must be connected to the COM2 port on the dock. If a screen blanking box is not connected via the power cable, the COM1 port on the dock is available for a serial device connection.

These instructions for use with VMXD Enhanced Dock only.

Determine the type of power supply used with the previous Thor VX8 or Thor VX9 installation:

- DC/DC Power Supply with Screws on Top of Lid
- DC/DC Power Supply with Screws on Side of Lid

⚠

Caution: **Inspect the cable shield to verify it is connected to chassis ground. If there is no connection from the cable shield to chassis ground, one must be added at this time. Use a jumper wire to connect the cable shield to chassis ground as shown below for the appropriate type of power supply installed on the vehicle. A jumper wire, as shown in the illustrations below, may be present to attach the chassis ground to the white wire of the power cable. This wire is not necessary but can be left in place if present. For proper screen blanking, verify the yellow and green wires are attached to the screen blanking box as shown in the illustrations below.**

For this model, follow the diagram below to attach the power cable shield to chassis ground:

⚠ **Caution:** **For battery powered vehicles:**

- + is connected to battery positive.
- – must be connected to battery negative.
- ⏚ must be connected to the vehicle chassis ground

Caution: **For internal combustion engine powered vehicles:**

- + is connected to battery positive.
- – is connected to battery negative.
- ⏚ is connected to the vehicle chassis ground, which can also be battery negative.

Caution: Inspect the cable shield to verify it is connected to chassis ground. If there is no connection from the cable shield to chassis ground, one must be added at this time. Use a jumper wire to connect the cable shield to chassis ground as shown below for the appropriate type of power supply installed on the vehicle. A jumper wire, as shown in the illustrations below, may be present to attach the chassis ground to the white wire of the power cable. This wire is not necessary but can be left in place if present. For proper screen blanking, verify the yellow and green wires are attached to the screen blanking box as shown in the illustrations below.

For this model, follow the diagram below to attach the power cable shield to chassis ground:

Existing Circuitry on Vehicle
Forklift Battery
Main Switch
MOTION CIRCUITRY
+Vi
GND
+Vo   -Vo
10A slow fuse Close to power source
3A fuse
VMX004VMCRADLE Vehicle Mount Smart Dock
GND   +Vi   -Vi
+Vo
-Vo
DC/DC Power Supply
Green   5
Yellow   6
Brown   1
White   3
Cable Shield
Circular Power Connector

Caution: For battery powered vehicles:

- VIN+ is connected to battery positive.
- VIN- must be connected to battery negative.
- GND must be connected to the vehicle chassis ground.

⚠ Caution: For internal combustion engine powered vehicles:

- $V_{IN}+$ is connected to battery positive.
- $V_{IN}-$ is connected to battery negative.
- GND is connected to the vehicle chassis ground, which can also be battery negative.

External AC/DC Power Supply

⚠ These instructions for use with VMXD Enhanced Dock for Off-Vehicle Use only.

The optional external AC/DC power supply is for use in environments, such as an office, where DC power is not available.

Note: *The Honeywell-approved AC/DC Power Supply and Adapter Cable are only intended for use in a 40ºC (104ºF) maximum ambient temperature environment.*

In North America, this unit is intended for use with a UL Listed ITE power supply with output rated 15 VDC, 4 Amp (maximum), 60 W (maximum). Outside North America, this unit is intended for use with an IEC certified ITE power supply with output rated 15 VDC, 4 Amp (maximum), 60 W (maximum).

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 to a properly grounded source of supply provided with maximum 15 Amp overcurrent protection (10 Amp for 230V circuits).

AC Input Cable (US only)

DC Output Cable

To DC Output Cable

To Dock
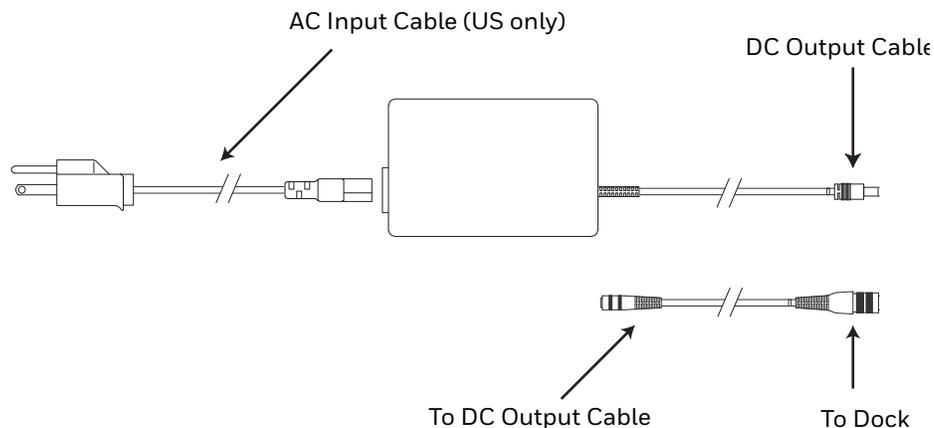
Connect External Power Supply

1. Connect the provided detachable cordset (US only, all others must order cable separately) to the external power supply (IEC 320 connector).

2. Plug cordset into appropriate, grounded, electrical supply receptacle (AC mains).

3. Connect the DC output cable end to the corresponding connector on the adapter cable.

4. Connect the watertight connector end of the Adapter Cable to the VMXD Off-Vehicle Dock power connector by aligning the connector pins to the power connector; push down on the watertight connector and twist it to fasten securely.

5. Press the Power Switch on the back of the Thor VM2 dock.

6. Press the Power Button on the front of the Thor VM2 to turn on the Thor VM2.

Table Stand

When the Thor VM2 is used in an office environment, it can be mounted in a table stand. To use the table stand:

1. Attach the RAM ball to the RAM Metal Table Stand with the supplied screws and nuts.

2. If not present, attach a RAM ball to the VMXD off-vehicle dock. If using an external keyboard mount, attach it now. See Step 2 – Attach RAM Mount Ball to the Thor VM2 Dock for more details.

3. Slide the size D RAM arm over the ball on the table mount.

4. Insert the ball on the dock into the RAM arm and tighten the knob on the RAM arm using the supplied RAM wrench.
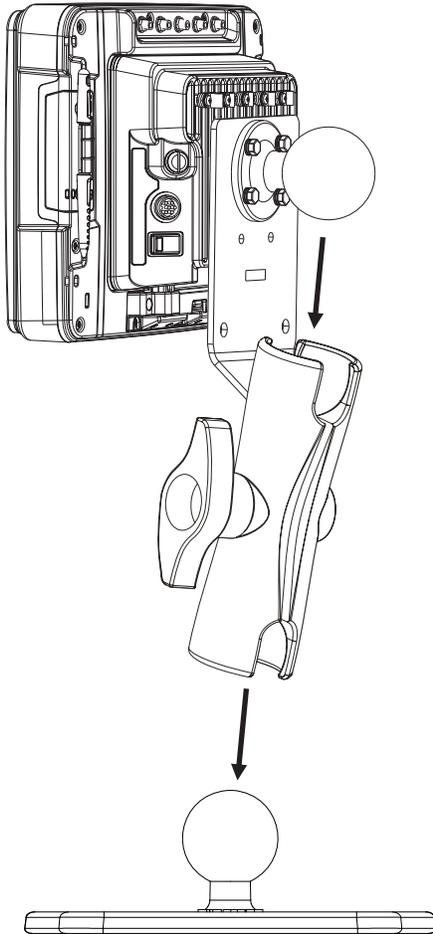
5. If the Thor VM2is not already mounted to the dock, Place Thor VM2 in the Dock.

6. If mounting the keyboard to the Thor VM2, see Step 5 – Attach Alphanumeric Keyboard to Mounting Plate (Optional) and Step 6 – Attach Keyboard Assembly to Thor VM2 Assembly (Optional).

Connect USB Keyboard

There are two external USB keyboard options

- 95-key keyboard (part number **164288-0001**)

- 21-key numeric keyboard.

These USB keyboards have a D9 connector which attaches to the USB port on the Standard Dock or the USB1 connector on the Enhanced Dock.
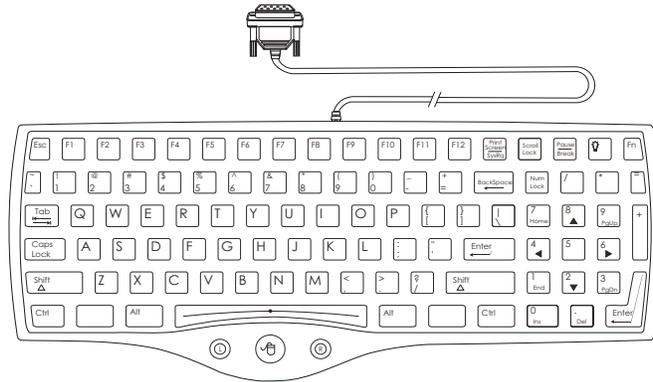
95-Key USB Keyboard
Part number **164288-0001**
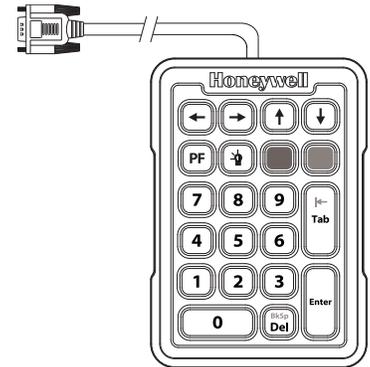
21-Key Numeric USB Keyboard

1. Seat the keyboard cable connector over the USB or USB1 connector on the dock.

2. Tighten the thumbscrews in a clockwise direction. Do not over tighten.

3. Secure the cable to the Thor VM2 with Strain Relief Cable Clamps.

Connect PS/2 Keyboard
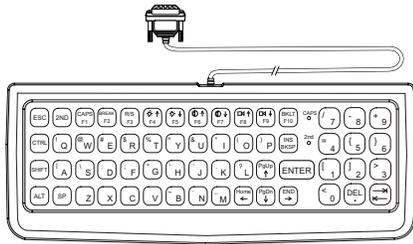
60-Key PS/2 Keyboard

Part number **160068-0001**

Requires PS/2 to USB adapter cable

Note: The keyboard backlight must be turned on manually. It does not come on automatically at boot up.
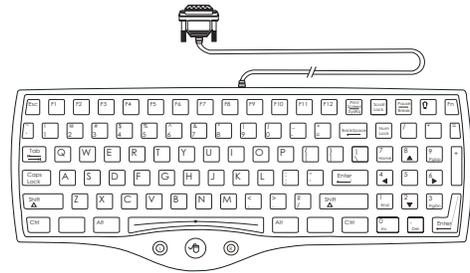
95-Key PS/2 Keyboard

Part number **160491-0001**

Requires PS/2 to USB adapter cable

Note: The mouse function is not supported with this keyboard.

Note: *While the 95-key USB keyboard and the 95-key PS/2 keyboard look similar the installation procedure is different.*

A legacy PS/2 keyboard (used with VX6, VX7, Thor VX8 or Thor VX9), available in either 60-key or 95-key versions can be used with the Thor VM2 via a PS/2 to USB adapter cable.
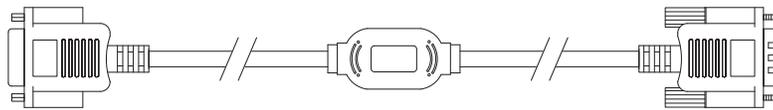
1. Seat the male connector of the cable over the USB connector on the Thor VM2 dock.

2. Tighten the thumbscrews in a clockwise direction. Do not over tighten.

3. Seat the keyboard connector over the female connector of the cable.

4. Tighten the thumbscrews in a clockwise direction. Do not overtighten.

5. Secure the cable to the Thor VM2 with Strain Relief Cable Clamps. The strain relief must capture the keyboard cable.
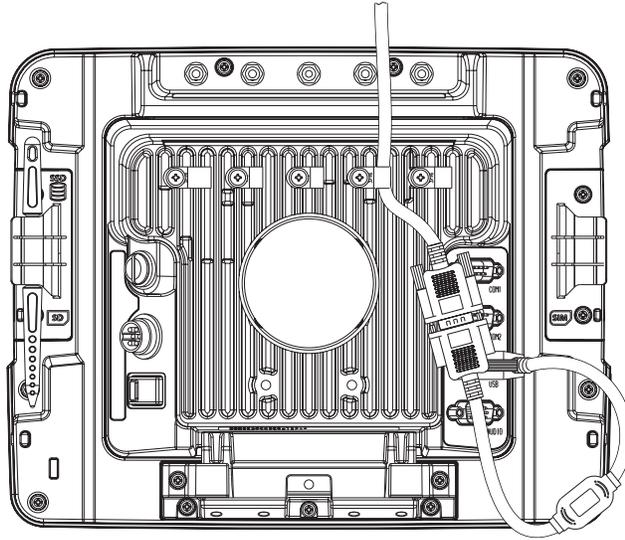
Connect USB Host

Host / Client Y Cable
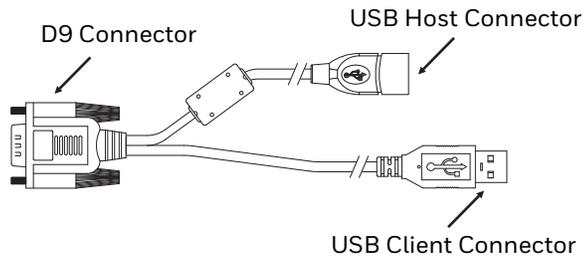
See USB and USB1 Connector for connector pinouts.

1. Seat the D9 connector firmly over the USB (Standard Dock) or USB1 (Enhanced Dock) connector on the dock.
2. Tighten the thumbscrews in a clockwise direction. Do not over tighten.
3. The USB-host connector provides a connector for a USB device such as a USB thumb drive.
4. Secure the cables to the Thor VM2 with Strain Relief Cable Clamps.

Dual Host Y Cable
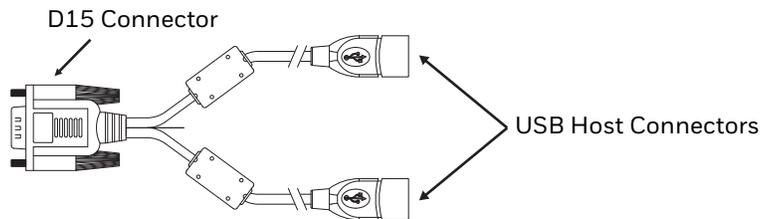
See USB2 Connector for connector pinouts.

1. Seat the D15 connector firmly over the USB2 (Enhanced Dock only) connector on the dock.
2. Tighten the thumbscrews in a clockwise direction. Do not over tighten.
3. The USB-host connectors provide a connector for a USB device such as a USB thumb drive.
4. Secure the cables to the Thor VM2 with Strain Relief Cable Clamps.

USB Scanner

There are several ways to attach a USB scanner:

• A USB scanner can be attached to the USB host port on the Enhanced Dock.
• A USB scanner can be attached to the host port on either USB adapter Y-cable.

- Certain USB scanners can be attached directly to the USB or USB-1 connector using cable CBL–500–300–S00, as shown below.

To use the CBL–500–300–S00 cable:

RJ50 (10-pin) Connector   D9 Connector
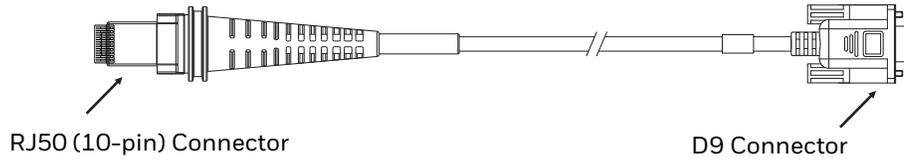
1. Seat the D9 connector of the cable over the USB or USB11 connector on the Thor VM2 dock.

2. Tighten the thumbscrews in a clockwise direction. Do not over tighten.

3. Follow the instructions provided with the scanner to attach the RJ50 end of the cable to the scanner.

See USB Host to Scanner Cable for pinout details.

Connect USB Client

Note: The USB client connection is not used on the Thor VM2 with a Windows 7, Windows Embedded Standard or Windows Embedded 7 operating system.

Connect Serial Device

Note: *Pin 9 of the desired COM port must be configured to provide +5V or RI as needed for the connected device. See the Options control panel for details.*

See COM1 and COM2 Connector for connector pinouts.

1. Seat the cable end connector firmly over the serial COM port on the dock.
2. Turn the thumbscrews in a clockwise direction. Do not over tighten.
3. Secure the cables to the Thor VM2 with Strain Relief Cable Clamps.
4. Connect the other cable end to the desired serial device.

Connect a Tethered Scanner

1. The scanner cable is attached to either the COM1 or COM2 port on the dock.
2. Connect the serial cable for the scanner as directed above.
3. When the Thor VM2 is powered on, it provides power to the serial scanner.
4. Configure the Data Collection (DC) Wedge to manipulate scanned data as desired.

Connect Headset Cable

The CANbus/Audio connector supports a headset adapter cable or a CANbus cable. The Thor VM2 does not support connecting audio and CANbus simultaneously.
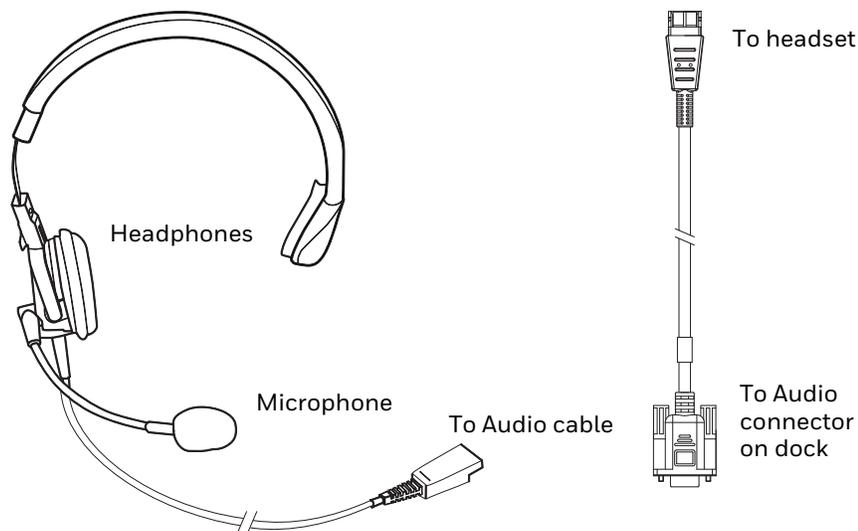
See CANbus / Audio Connector for connector pinouts.

1. Seat the D15 cable end connector firmly over the CANbus/Audio Connector on the dock.
2. Tighten the thumbscrews in a clockwise direction. Do not over tighten.
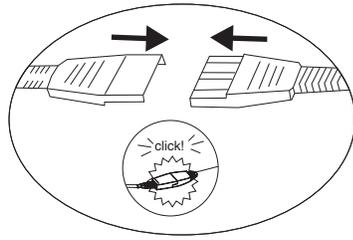
3. Slide the cable ends together until they click shut. Do not twist or bend the connectors. The Thor VM2 internal microphone and speakers are automatically disabled when the headset is connected.

Adjust Headset / Microphone and Secure Cable
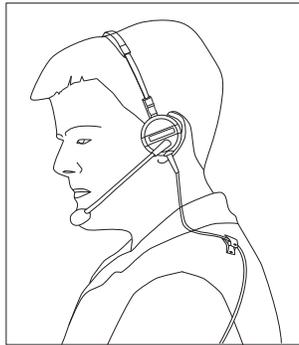
The headset consists of an earpiece, a microphone, a clothing clip and a cable.

1. Do not twist the microphone boom when adjusting the microphone. The micro-phone should be adjusted to be about two finger widths from your mouth.

2. Make sure the microphone is pointed at your mouth. Note the small "Talk" label near the mouthpiece. Make sure the Talk label is in front of your mouth. The microphone cable can be routed over or under clothing.

3. Follow the safety guidelines below when wearing the headset.

Under Clothing

• Leave the cable exposed only at the top of the collar.

• Be sure to leave a small loop of cable to allow movement of your head.

Over Clothing

• Use clothing clips to hold the cable close to your body.

• Tuck the cable under the belt, but leave a small loop where it goes under the belt.

• Do not wear the cable on the front of your body. It may get in your way or get caught on protruding objects.

Connect CANbus Cable

The CANbus/Audio connector supports a headset adapter cable or a CANbus Y cable. The Thor VM2 does not support connecting audio and CANbus simultaneously.
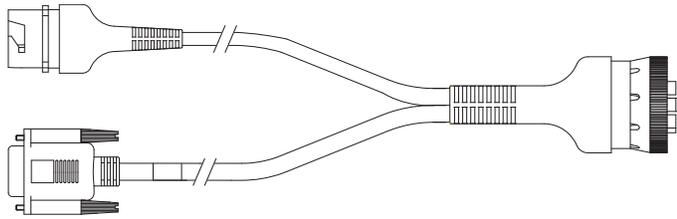
See CANbus / Audio Connector for connector pinouts.

1. Seat the D15 cable end connector firmly over the CANbus/Audio Connector on the dock.
2. Tighten the thumbscrews in a clockwise direction. Do not over tighten.
3. The CANbus Y cable has a 9 pin F SAE J1939 (Deutsch) and 9 pin M SAE J1939 (Deutsch) connector. Connect the appropriate cable connector as needed.

Install External Antenna

The external antenna cannot be used by devices with an internal antenna.

> ⚠ **Caution:** If the Thor VM2 has connectors for external antennas, do not power up the Thor VM2 without the external antennas connected. Damage to the WLAN radio may result.

1. Remove the rubber cap, if present, from the antenna connector before connecting an external antenna.
2. Place the antenna over the antenna connector. If only one antenna is used, be sure to connect it to the Wi-Fi Main connector.
3. Push down and twist the antenna base clockwise until secure.
4. Repeat for second antenna, if used.

Install Remote Antenna

Remote antennas are available for the 802.11 WLAN radio, the WWAN radio and the GPS.

⚠ Caution: **If the Thor VM2 has connectors for external antennas, do not power up the Thor VM2 without the external antennas connected. Damage to the WLAN radio may result.**

802.11 Remote Mount Antenna
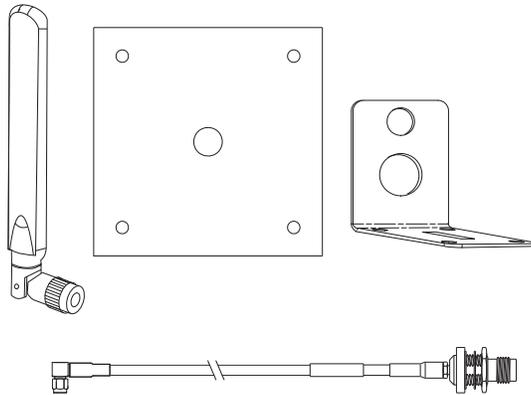
The Remote Antenna Installation Kit consists of two brackets (base plate and right angle), cable, and antenna. Tools are not included.
The desired remote antenna bracket is mounted on the top of a forklift, truck or other vehicle and cabled to the Thor VM2 inside the vehicle.
The Vehicle Remote Mount Antenna cannot be used by devices with an internal antenna.

Components and Mounting Diagram
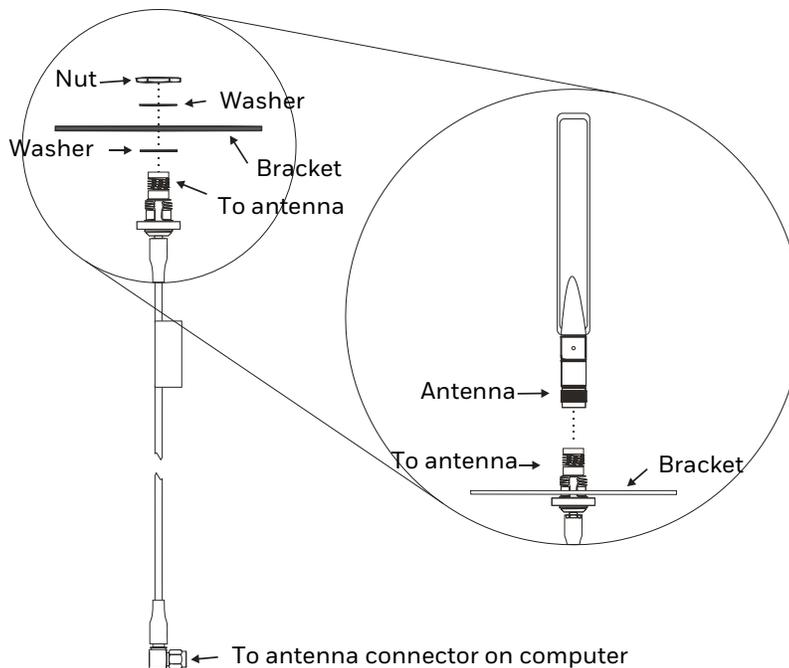
Typical Installation
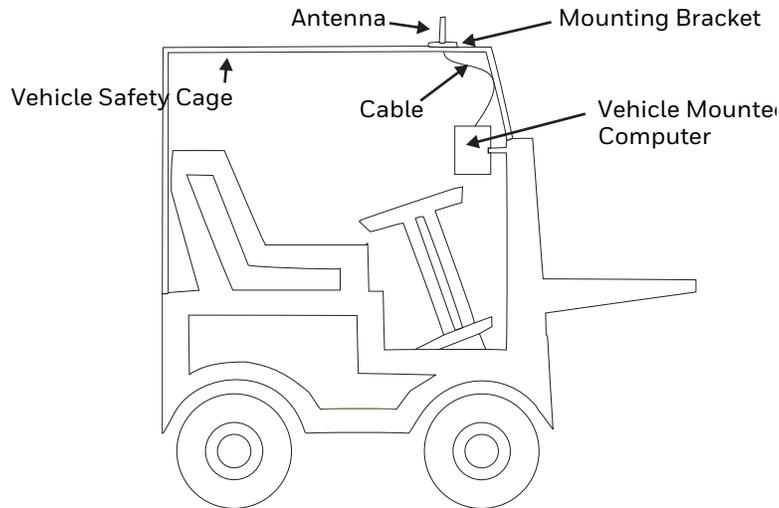
Mounting Instructions

1. Attach and secure the desired mounting bracket to the highest point on the safety cage, following these precautions:

   • The plate must be mounted so the antenna is not damaged while the vehicle or any of its parts are moving.

   • The antenna mounting portion of the bracket must be parallel to the floor.

   • If using two antennas, they must be mounted at least 12 inches (304.8mm) apart.

2. Attach the female connector of the coaxial cable to the antenna connector on the vehicle mounted Thor VM2.

3. Secure the whip antenna to the mounting bracket.

4. Connect the antenna cable to the whip antenna.

5. Use cable ties to secure the coaxial cable to the vehicle as necessary. Make sure the cable is routed so it is not damaged by any moving parts of the vehicle.

6. Connect the cable to the antenna connector (Wi-Fi Main or Wi-Fi Aux) on the Thor VM2. If only one antenna is used, be sure to connect it to the Wi-Fi Main connector.

7. Repeat the steps above for the second 802.11 antenna.

WAN Remote Mount Antenna

The WAN remote mount antenna can be either a magnetic mount or an adhesive mount antenna.

Magnetic Mount WAN Antenna

To extension cable

To antenna

To antenna connector on computer
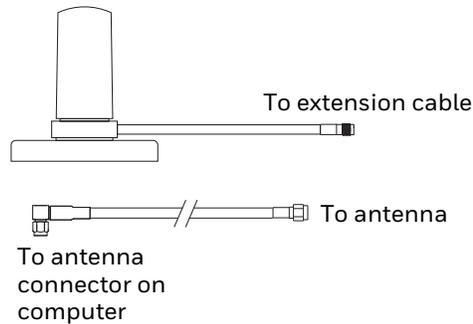
Adhesive Mount WAN Antenna

To extension cable

To antenna

To antenna connector on computer
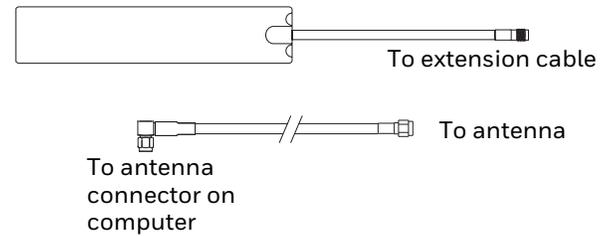
The Remote Antenna Installation Kit consists of the WAN antenna and an extension cable. The remote antenna is mounted on the top of a forklift, truck or other vehicle and cabled to the Thor VM2 inside the vehicle.

1. Locate a mounting position on highest point on the vehicle, following these precautions:

   • The antenna must be mounted so the antenna is not damaged while the vehicle or any of its parts are moving.

2. Clean the area where the antenna is to be mounted.

3. If using an adhesive mount antenna, remove the protective backing paper from the adhesive on the antenna.

4. Position the antenna on the vehicle.

5. Attach the one end of the coaxial cable to the antenna and the other end to the Mobile Net WWAN connector on the vehicle mounted Thor VM2.

6. Use cable ties to secure the coaxial cable to the vehicle as necessary. Make sure the cable is routed so it is not damaged by any moving parts of the vehicle.

GPS Remote Mount Antenna

The external GPS antenna is an adhesive mount antenna.
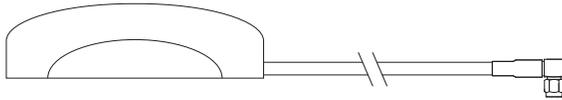
The Remote Antenna Installation Kit consists of the antenna and an inte-grated cable. The remote antenna is mounted on the top of a forklift, truck or other vehicle and cabled to the Thor VM2 inside the vehicle.

1. Locate a mounting position on highest point on the vehicle, following these precau-tions:

    •   The antenna must be mounted so the antenna is not damaged while the vehicle or any of its parts are moving.

2. Clean the area where the antenna is to be mounted.

3. Remove the protective backing paper from the adhesive on the antenna and position the antenna on the vehicle.

4. Attach the connector on the coaxial cable to the GPS antenna connector on the vehicle mounted Thor VM2.

5. Use cable ties to secure the coaxial cable to the vehicle as necessary. Make sure the cable is routed so it is not damaged by any moving parts of the vehicle.

Apply Touch Screen Protective Film

The optional Thor VM2 touch screen protective film is shipped in packs of 10. The protective film is flexible and treated with an anti-glare coating on the outer surface.

Pull Tab
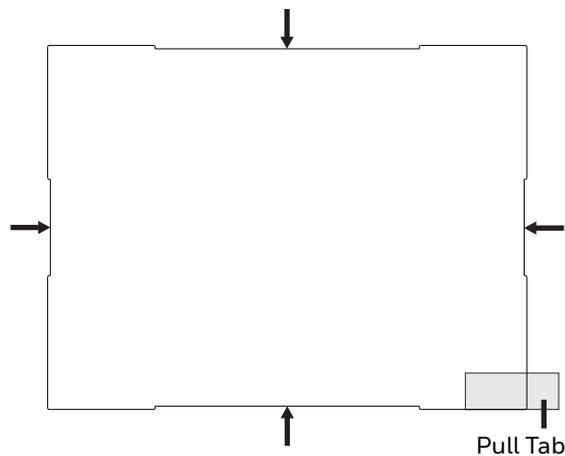
The protective film is slightly larger than the Thor VM2 touch screen, however the notches on the edge of the protective film (indicated by the arrows) correspond to the display size of the Thor VM2. The protective film is not adhesive. The corner edges are designed to fit between the Thor VM2 display and the display housing to hold the protective film in place.

A protective backing is applied to the rear surface of the protective film. A pull tab is attached to the protective backing for easy removal of the protective backing from the film.

Installation

1. Make sure the touch screen is clean and dry before installation. See Cleaning for instructions on suitable cleaning agents.

2. Pull the release tab to separate the protective backing from the rear of the protective film. Avoid touching the rear side of the protective film while removing the liner.

3. Place the rear side of the protective film against the Thor VM2 display, roughly centering the protective film over the display.

4. Slide the protective film until one corner can be slid back between the touch screen and the display housing as the protective film is re-centered on the display. It may be necessary to press the edges of the protective film against the display to ensure the entire edge slides under the display housing. It is easiest to start with one of the bottom corners.

5. Slide the protective film away from the other bottom corner. The film may bulge slightly away from the Thor VM2 as it is being slid. Only slide the protective film enough so that the protective film can slide under the display housing on that corner when the protective film is returned to center.

6. Repeat with each of the top corners, sliding the protective film away from the corner just enough that the protective film can slide under the display housing when the protective film is returned to center.

7. It may be necessary to flex the protective film during the install, however use care not to flex the protective film so much that the protective film kinks.

8. Once all corners are secure under the display housing, adjust the protective film, if necessary, so it is centered on the touch screen.

Removal

1. To remove the protective film, slide the protective film in one direction until the edge clears.

2. Lift up on the edge of the protective film so it does not slide between the touch screen and display housing when the protective film is slid back to the center.

3. Repeat until all edges are free and remove the protective film.

Disconnect UPS Battery

⚠️ **Caution:** **The UPS battery must be disconnected before you ship the Thor VM2 or** Replace Front Panel**.**

Equipment Required

The following equipment is user-supplied:

- Torquing tool capable of measuring inch pounds
- #2 Phillips screwdriver bit

Disconnect Procedure

1. For convenience, the Thor VM2 can be removed from the dock, though it is not necessary.

2. If the Thor VM2 remains in the dock, disconnect the power cable from the dock.

3. Shutdown the Thor VM2.

4. Place the Thor VM2 face down on a stable surface.

5. Using a #2 Phillips bit loosen the M3 screws and then remove the tethered access panel with the SIM label. This panel is on the right hand side when the Thor VM2 is face down with the top away from the user.

6. Locate the small push button located just below the SIM card installation slot.

7. Press the push button to disconnect the UPS. The UPS battery maintains its charge but is disconnected from the power circuitry of the Thor VM2.

8. Reattach the access panel, torquing the M3 screws to 4-5 inch pounds using a #2 Phillips bit.

9. When the Thor VM2 is attached to external power, the UPS battery is automatically reconnected.

10. Restart the Thor VM2.
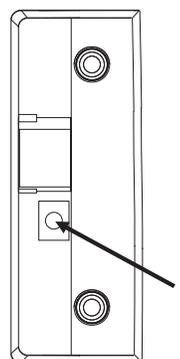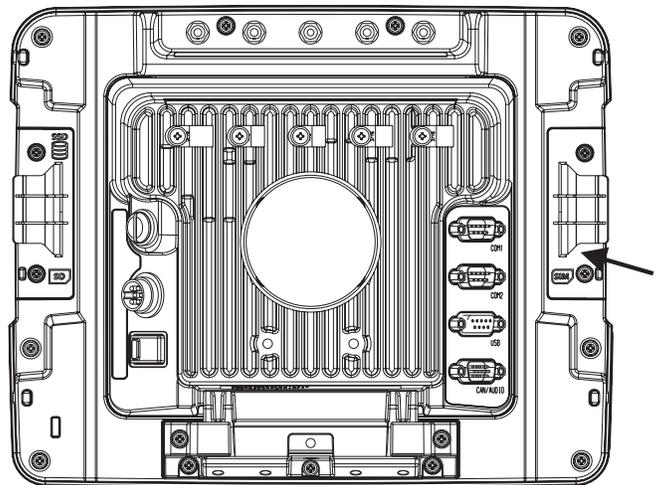
Install SD Card

An SD card slot is provided for storage expansion.

Equipment Required

The following equipment is user-supplied:

- Torquing tool capable of measuring inch pounds
- SD card – The following commercially available SD cards are recommended:
  - ATP 2GB Industrial Grade SDHC card – AF2GSDI-5ADXX
  - ATP 4GB Industrial Grade SDHC card – AF4GSDI-5ACXX
  - SanDisk® 2GB SDHC card – SDSDB-2048
  - SanDisk® 4GB SDHC card – SDSDB-004G
- #2 Phillips screwdriver bit

Installation Procedure

1. For convenience, the Thor VM2 can be removed from the dock, though it is not necessary.

2. If the Thor VM2 remains in the dock, disconnect the power cable from the dock.

3. Shutdown the Thor VM2.

4. Place the Thor VM2 face down on a stable surface.

5. Using a #2 Phillips bit loosen the M3 screws and then remove the tethered access panel with the SIM label. This panel is on the left hand side when the Thor VM2 is face down with the top away from the user.

6. Locate the SD card installation slot.

7. Slide the SD card into the slot. The label side (front) of the SD card faces toward the back of the Thor VM2.

8. Reattach the access panel, torquing the screws to 4–5 inch pounds.

9. If removed, reinstall the Thor VM2 in the dock.

10. Restart the Thor VM2.

11. When using Windows explorer to view My Computer, the SD card is identified as **Removable Disk** or as a **Device with Removable Storage**, usually Drive D: or E:.
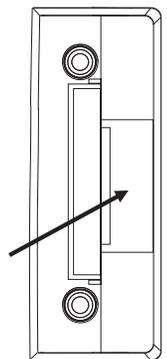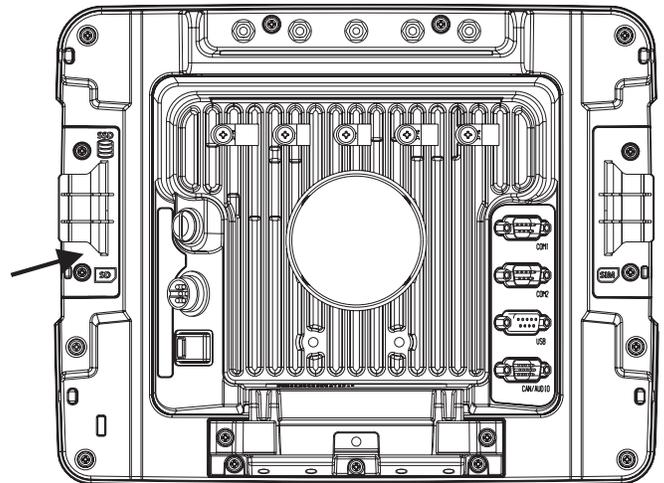
Install SIM Card

A SIM card may be required for WWAN.

Note: *The SIM card is not hot-swappable. After installing or removing a SIM card, the Thor VM2 must be rebooted for the change to take effect.*

Equipment Required

The following equipment is user-supplied:

- SIM card for desired carrier
- Torquing tool capable of measuring inch pounds
- #2 Phillips screwdriver bit

Installation Procedure

1. For convenience, the Thor VM2 can be removed from the dock, though it is not necessary.
2. If the Thor VM2 remains in the dock, disconnect the power cable from the dock.
3. Shutdown the Thor VM2.
4. Place the Thor VM2 face down on a stable surface.
5. Using a #2 Phillips bit loosen the M3 screws and then remove the tethered access panel with the SIM label. This panel is on the right hand side when the Thor VM2 is face down with the top away from the user.
6. Locate the SIM card installation slot, as highlighted to the right.
7. Slide the SIM card into the slot.
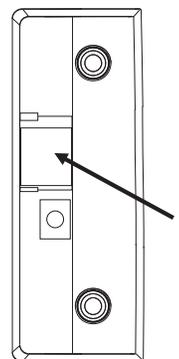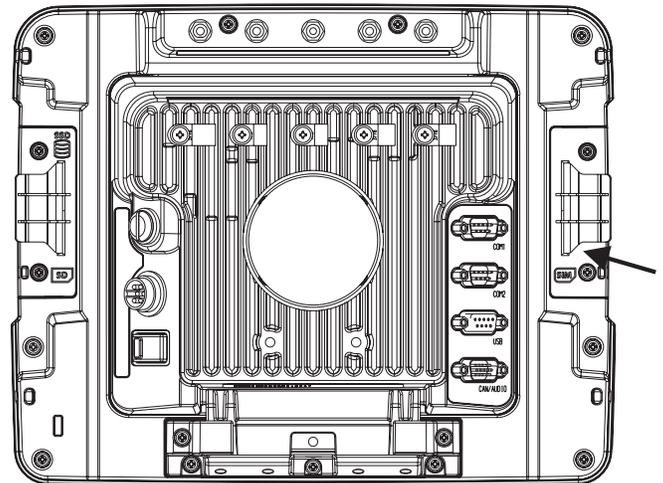
Note: *The entire SIM slot is not visible due to the design of the Thor VM2 case. However, the entire slot is shown below to help with installation.*
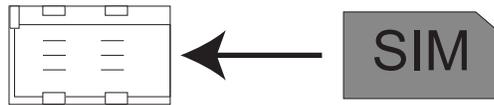
8. Do not force the SIM into the slot. The SIM slot is not a "spring lock" holder. When the SIM card is fully inserted, it will trip the SIM detect switch as indicated by the arrow below. The access panel has a tab that holds the SIM card in place.
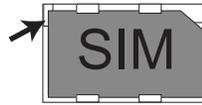
9. Reattach the access panel, torquing the screws to 4-5 inch pounds.

10. If the SIM card is not detected, contact Technical Assistance for troubleshooting.

11. If removed, reinstall the Thor VM2 in the dock.

12. Restart the Thor VM2.

Replace Front Panel

The front panel of the Thor VM2 is field replaceable. The front panel assembly contains the integrated keypad and touch screen. Should either of these components fail, the front panel assembly can easily be replaced to reduce downtime.

Equipment Required

The following equipment is user-supplied:

- Torquing tool capable of measuring inch pounds
- #2 Phillips screwdriver bit

Replacement Procedure

⚠ **Caution: Before replacing the Thor VM2 front panel,** Disconnect UPS Battery**.**

1. Place the Thor VM2 on a clean, well-lit sur-face before performing the front panel replacement.
2. Shutdown the Thor VM2.
3. Remove the Thor VM2 from the dock.
4. Disconnect UPS Battery.
5. Loosen the twelve (12) captive M3 screws holding the front panel. Use a #2 Phillips bit.
6. Carefully lift the front panel away from the device.
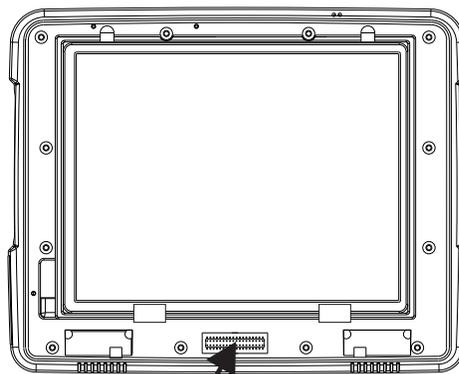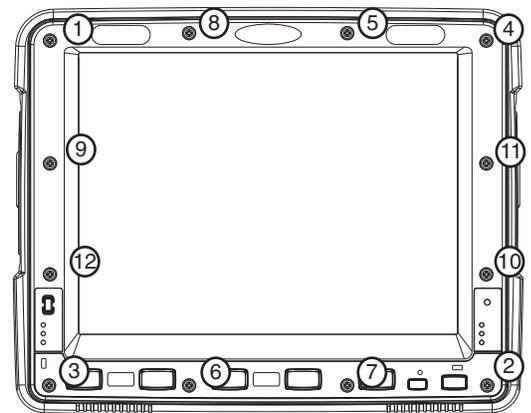
Wiring Connector
on Thor VM2
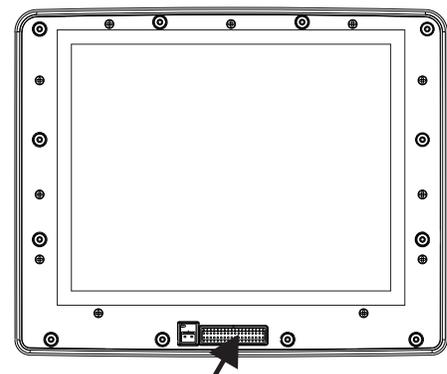
Wiring Connector
on Front Panel

7. Position the replacement front panel so wiring connector on the back of the front panel lines up with the connector on the Thor VM2.
8. Gently press the front panel into place.

9. Tighten the twelve (12) captive M3 screws. In the order shown in the top figure above, use a #2 Phillips bit and torque the screws to 6–7 inch pounds.

10. Reinstall the Thor VM2 in the dock.

11. When the Thor VM2 is placed in the powered dock, the UPS battery automatically reconnects.

12. Restart the Thor VM2.

13. The Thor VM2 is ready for use.

CHAPTER

5 SOFTWARE

Microsoft Windows Setup and Configuration

After the system files are processed, Microsoft Windows begins to load. Windows maintains a System Registry and INI files. Standard Windows configuration options apply to the Thor VM2. Configuration options are located in the System Tray or the Control Panel:

- The System Tray contains icons for adjusting the time, date or volume level.
- The Control Panel contains icons for many other configuration options, such as Power Management, Regional and Language Options, etc.
- The Control Panel icons are also used to add, delete or modify software installed on the Thor VM2.

For Microsoft Windows 7 and Windows Embedded 7:

⚠ It is necessary to run to run RFTerm and Bluetooth EZ Pairing as an administrator when modifying settings because these programs must be able to access and make changes to the Windows registry.

Drive C Folder Structure

Microsoft Windows is installed in the \Windows folder. In addition, Microsoft Windows creates other folders and several subfolders. For more information on the folder structure, please refer to commercially available Microsoft Windows OS reference guides.

Software Loaded on Drive C

Note: *This section assumes the* Thor VM2 is *ordered with an operating system. The Thor VM2 is also available without an operating system installed. See* Thor VM2 with no Operating System*.*

The software loaded on the Thor VM2 computer includes:

- BIOS
- Microsoft operating system (Windows Embedded Standard 2009, Windows Embedded Standard 7 or Windows 7 Professional)

- device drivers
- radio software, see Summit Client Utility or Laird Configuration Manager.
- touch screen software
- keyboard wedge software, see Freefloat Link*One Wedge
- soft keyboard software, see Freefloat Key*One
- Automatic Firmware Update Utility
- Configuration Cloning Utility (CCU)

The software installed on the Thor VM2 is summarized below.

Note: *Due to the complex folder structure and System Registry under Microsoft Windows, software should not be removed manually. Instead use the applicable Windows Control Panel.*

- Add or Remove Programs (Windows Embedded Standard 2009)
- Programs and Features (Windows Embedded Standard 7 or Windows 7 Professional).

Microsoft Windows

Microsoft Windows is installed in the \Windows subfolder, which is the Windows default. In addition, Windows places files in other folders and subfolders during installation. For more information, please refer to commercially available Microsoft Windows OS user guides.

Device Drivers

Device drivers are installed for all installed hardware options, such as the display, touch screen, radios, etc. For more information on Microsoft Windows device drivers, please refer to commercially available Windows OS reference guides.

Radio Software

The Thor VM2 is delivered with the radio software installed. Because the Thor VM2 uses a Microsoft Windows operating system, the radio installation includes Windows device drivers.

Touch Screen Software

PenMount Universal software is installed for calibrating the touch screen. See Touch Screen Calibration for more information.

Software is installed for calibrating the standard resistive touch screen. See Touch Screen Calibration for more information.

Touch screen calibration is not necessary with the optional Projective Capacitance (PCAP) touch screen.

RFTerm

Optional terminal emulation software. The application can also be accessed by double-clicking the RFTerm desktop icon.

> ⚠ For Microsoft Windows 7 and Windows Embedded Standard 7:
>
> - It is necessary to run to run RFTerm as an administrator when modifying settings because RFTerm must be able to access and make changes to the Windows registry.
> - *Rather than selecting to run as administrator each time, right-click on the RFTerm icon and select* Properties*. Tap the* **Compatibility** *tab and check* **Run this program as an administrator***. This modification affects the current user only unless* Change settings for all users is tapped *before changing the privilege level.*

Summit Client Utility

⊞ **(Start) > Control Panel > Wi-Fi,** or SCU icon on desktop

Manage the wireless 802.11 client installed in the Thor VM2. If the Summit Client Utility is not present, the Laird Configuration Manager may be installed.

Laird Configuration Manager

LCM icon on desktop

Manage the wireless 802.11 network device installed in the Thor VM2. If the Laird Configuration Manager is no present, the Summit Client Utility may be installed.

Freefloat Link*One Wedge

Link*One bar code decoder configuration software is installed on the Thor VM2. A pdf User's Manual for Link*One is included as part of the installation at C:\Program Files\Freefloat\Freefloat Link One. Refer to this manual or the Freefloat website for information on configuring and using Link*One.

Freefloat Access*One TE (Optional)

Access*One terminal emulation software is available on the Thor VM2. A pdf User's Manual for Access*One is included as part of the installation at C:\Program Files\Freefloat\Freefloat Access One. Refer to this manual or the Freefloat website for information on configuring and using Access*One.

Freefloat Key*One

Key*One input panel (soft keyboard) software is installed on the Thor VM2. A pdf User's Manual for Key*One is included as part of the installation at C:\Program Files\Freefloat\Freefloat Key One. Refer to this manual or the Freefloat website for information on configuring and using Key*One.

Selecting Keyboard Layout

Several keyboard layouts are included with the Key*One install. To select or change the keyboard layout, select ⊞ **(Start) > All Programs > Freefloat Key > Keyboard Layouts**. Several predefined keyboard layouts are listed for SVGA and VGA. Tap the desired key-board layout to select and launch that keyboard.

Launching Keyboard

To launch the keyboard with the preselected layout, select ⊞ **(Start) > Runtime Key-board** (from the shortcuts menu) or ⊞ **(Start) > All Programs > Freefloat Key> Runtime Keyboard**.

To close the keyboard, tap the **X** (close control) usually located in the upper right corner of the keyboard.

Launching Keyboard with Programmable Key

To assign a Programmable Key to launch Key*One, follow these instructions:

1. Review the Remap a Key to Run a Command for detailed instructions on how to assign a key to run a command, i.e. Run Cmd1.

2. On the **RunCmd** tab, enter the desired keyboard layout in the applicable text box. The keyboard layouts are located at C:\ProgramData\Freefloat Key\Layouts. Some example commands are provided below:

    -   To launch the Big Numeric keypad: C:\ProgramData\Freefloat Key\Layouts\Big Numeric.key

    -   To launch the US English keyboard: C:\ProgramData\Freefloat Key\Layouts\aga-en.key

3. No entries are needed for parm.

4. Tap **OK** to save.

5. Different keyboard layouts can be assigned to different programmable keys as desired.

Creating Customized Layout

Key*One includes a keyboard designer. To launch the designer select ⊞ **(Start) > All Programs > Freefloat Key> Designer**. For information on using the designer, refer to the Key*One manual or the website.

Drive D Folder Structure

Windows 7 Professional and Windows Embedded Standard 7 only)

The CompactFlash hard drive includes a D: partition. This partition is used by the Automatic Firmware Update Utility. No other files should be stored on the D: drive.

Control Panel

Most control panel applets on the Thor VM2 are standard Microsoft Windows items. The control panels and other functions listed below may differ from a standard Microsoft Windows equipped PC or laptop.

Note: *Unless otherwise noted, the control panel items in this section apply to all operating systems. The illustration may only show the Windows Embedded Standard 2009 control panel but the Windows 7 Professional and Windows Embedded Standard 7 panels are similar.*

About

⊞ **(Start) > Control Panel > About** (Large or Small Icon View)

Software
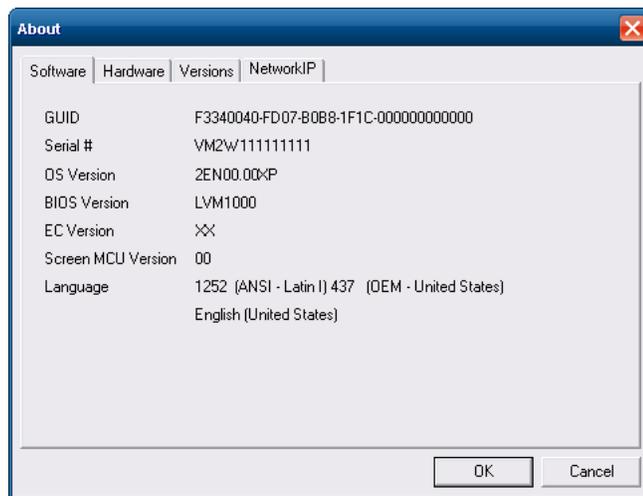
Firmware Versions

The **Software** tab lists the firmware versions installed. The BIOS, Embedded Controller (EC) and Screen MCU firmware versions are shown on this tab.

Language

The **Software** tab displays the localized language version of the OS image. The language is identified as English or + an additional language.

The Thor VM2 may be preloaded with an English only OS. Contact Technical Assistance for information on ordering a recovery DVD with an additional language.

Versions

The **Versions** tab displays the versions of many of the software programs installed. Not all installed software is included in this list and the list varies depending on the applications loaded on the Thor VM2. The Image line displays the revision of the system software installed. Refer to the last three digits to determine the revision level.

Versions Tab and the Registry

The **Versions** tab displays program version details from the registry. Customized information can be displayed by modifying the Registry using the Registry Editor. Use caution when editing the Registry and make a backup copy of the registry before changes are made.

The registry settings for the **Versions** tab are under `HKEY_LOCAL_MACHINE \ Software \ LXE \ Version` in the registry.

To add a user application to the Version panel, create a new string value under the `HKEY_LOCAL_MACHINE \ Software \ LXE \ Version` 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.

Version strings can be equal to or less than 254 characters. Because the strings are displayed in a text box, any number can be accommodated, up to the 64K byte text box limitation.

Network IP

MAC Address

The **Network IP** tab displays the MAC address of the network card(s) such as the Summit WLAN radio and the Bluetooth module.

Bluetooth

⚠ For a Thor VM2 with Windows Embedded Standard 7 or Windows 7 Professional:

In order to make changes to the settings on the Bluetooth (EZPair) panels, it is necessary to stop the Bluetooth process and restart it as an administrator. If not, changes made do not get written to the system registry. Follow this process to configure Bluetooth parameters:

1. Press **Ctrl + Alt + Del** on the external keyboard.

2. Select **Start Task Manager**.

3. Select the **Processes** tab.

4. Locate **BTC.exe** in the process listing and select it.

5. Tap the **End Process** button.

6. Close the Task Manager window.

7. Locate the Bluetooth icon on the desktop. Right click and select **Run as administrator**.

8. The Bluetooth process is now running as administrator. Double tap the Bluetooth icon again to open the Bluetooth EZ Pair panels. If prompted with a User Access Control warning, allow BTC.exe to make changes.

9. Configure Bluetooth parameters as desired.

10. Restart the Thor VM2. After the restart, Bluetooth is no longer running as administrator.

Note: *Do not right click on the Bluetooth icon and use the Properties settings to always run Bluetooth EZ Pair as an administrator as this will prevent the Bluetooth process from automatically launching when theThor VM2 is powered on.*

🏁 **(Start) > Control Panel > Bluetooth**

Discover and manage pairing with nearby Bluetooth devices.

⚠ To use the Honeywell/Intermec SR61 Bluetooth scanner with the Thor VM2:

• The EZPair software must be version 2ab or greater. See the Bluetooth About control panel for the version installed. Contact Technical Assistance for software upgrade information.

• The EZPair bar code on the Thor VM2 cannot be used to connect the SR61 scanner. Follow this procedure:

1. Make sure the scanner is on and within range of the Thor VM2.

2. Tap the **Discover** button on the Bluetooth Devices tab.

3. From the list of discovered devices, tap the SR61 scanner and select Pair as a Scanner

Factory Default Settings

Discovered Devices	None
Settings	
Turn off Bluetooth	Disabled
Computer is connectable	Enabled
Computer is discoverable	Disabled
Prompt if devices request to pair	Enabled
Continuous search	Disabled
Filtered Mode	Enabled
Printed Port - COM7:	Disabled (unchecked) by default in both Filtered and Non Filtered Modes. The option is dimmed in Non Filtered Mode.
Logging	Disabled
Computer friendly name	System Computer Description
Reconnect	
Report when connection lost	Enabled
Report when reconnected	Disabled
Report failure to connect	Enabled
Clear Pairing Table on Boot	Disabled
Auto Reconnect on Boot	Enabled
Auto Reconnect	Enabled

Bluetooth taskbar Icon state and Bluetooth device Icon states change as Bluetooth devices are discovered, paired, connected and disconnected. There may be audible or visual signals as paired devices re-connect with the Thor VM2.

- The default Bluetooth setting is On.
- The Thor VM2 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.
- When Filtered Mode is enabled, the Thor VM2 can pair with one Bluetooth scanner and one Bluetooth printer.
- When Filtered Mode is disabled, the Thor VM2 can pair with up to four Bluetooth devices.
- It is not necessary to disconnect a paired scanner and printer before a different scanner or printer is paired with the Thor VM2.
- The target Bluetooth device should be as close as possible (up to 32.8 ft (10 meters) Line of Sight) to the Thor VM2 during the pairing process.

Assumption: The System Administrator has Discovered and Paired targeted Bluetooth devices for the Thor VM2. The Thor VM2 operating system has been upgraded to the revision level required for Bluetooth client operation. An application (or API) is available that will accept data from serial Bluetooth devices.

Bluetooth Devices

The **Bluetooth Devices** tab displays any device previously discovered and paired with the Thor VM2.
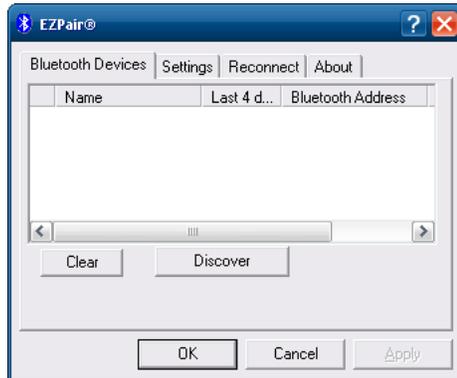
Discover

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

Stop Button

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

Note: *When an active paired device enters Suspend Mode, is turned Off or leaves the Thor VM2 Bluetooth scanning range, the Bluetooth connection between the paired device and the Thor VM2 is lost. There may be audible or visual signals as paired devices disconnect from the Thor VM2.*

Bluetooth Device List

The discovered paired devices may or may not be identified with an icon. Discovered devices without an icon can be paired. The Bluetooth panel assigns an icon to the device name.

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

An icon with a white background indicates the device is connected to the Thor VM2 and the device's Bluetooth connection is active.

Double-tap a device in the list to open the device properties menu. The target device does not need to be active.

Clear Button

Deletes all devices from the Device table that are not currently paired. A dialog box is presented, "Delete all disconnected devices?" Tap the **Yes** button to remove disconnected or deleted devices from the device table. The devices are removed from the Device table after closing and reopening the Bluetooth window. Tap the **No** button to make no changes.

Bluetooth Device Menu

Prerequisite: The **Discover** button has been clicked and there are Bluetooth devices listed.

Click on a device in the list to highlight it. Double-click the highlighted device to display the Bluetooth Device right-click menu as shown below. The Bluetooth device does not need to be active.
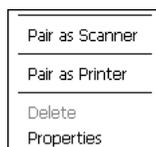
Right-Click Menu Options

Pair as Scanner	Receive data from the highlighted Bluetooth scanner or Bluetooth imager.
Pair as Printer	Send data to the highlighted Bluetooth printer.
Disconnect	Stop the connection between the Thor VM2 and the highlighted paired Bluetooth device.
Delete	Remove an unpaired device from the Bluetooth device list. The highlighted device name and identifier is removed from the Thor VM2 Bluetooth Devices panel after the user taps **OK**.
Properties	More information on the highlighted Bluetooth device.

Bluetooth Device Properties

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

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

Turn Off Bluetooth

Tap the button to toggle the Bluetooth client On or Off. The button title changes from *Turn Off Bluetooth* to *Turn On Bluetooth*.

Default

The default value is Bluetooth On.

Options

Option	Information
Computer is connectable	This option is Enabled by default. Disable this option to inhibit Thor VM2 connection initiated by a Bluetooth scanner.
Computer is discoverable	This option is Disabled by default. Enable this option to ensure other devices can discover the Thor VM2.
Prompt if devices request to pair	This option is Enabled by default. A dialog box appears on the Thor VM2 screen notifying the user a Bluetooth device requests to pair with the Thor VM2. The requesting Bluetooth device does not need to have been Discovered by the Thor VM2 before the pairing request is received. Tap the **Accept** button or the **Decline** button to remove the dialog box from the screen. In some cases, if a Bluetooth device is already paired this setting cannot be changed. If this is the case, an error message is displayed and the option is not changed. The Bluetooth device must be disconnected before changing this setting.
Continuous Search	This option is Disabled by default. When enabled, the Bluetooth connection never stops searching for a device it has paired with when the connection is broken (such as the paired device entering Suspend mode, going out of range or being turned off). When disabled, after being enabled, the Thor VM2 stops searching after 30 minutes.
Filtered Mode	This option is Enabled by default. Determines whether the Bluetooth client discovers and displays all serial Bluetooth devices in the vicinity (Filtered Mode is disabled/unchecked) or the discovery result displays Bluetooth scanners and printers only (Filtered Mode is enabled/checked). When Filtered Mode is disabled, the Thor VM2 can pair with up to four Bluetooth devices. A Restart is required every time Filtered Mode is toggled on and off. When in non-filtered mode, the Thor VM2 supports SPP only.
Printer Port – COM9	This option is Disabled by default. This option assigns Bluetooth printer connection to COM9 instead of COM19. To enable this option, Filtered Mode must be enabled.
Logging	This option is Disabled by default. When logging is enabled, the Thor VM2 creates **bt_log.txt** and stores it in the C:/ Program Files\LXE\Bluetooth folder. Bluetooth activity logging is added to the text file as activity progresses. A **bt_log_bak.txt** file contains the data stored by **bt_log.txt** prior to reboot. During a reboot process, the Thor VM2 renames **bt_log.txt** to **bt_log_bak.txt**. If a file already exists with that name, the existing file is deleted, the new **bt_log_bak.txt** file is added and a new **bt_log.txt** is created.

Option	Information
Computer Friendly Name	Default: Computer description (**Control Panel > System > Computer Name** tab). The name, or identifier, entered in this space by the System Administrator is used exclusively by Bluetooth devices and during Bluetooth communication. The Computer Description field is blank by default, so unless this field is modified before Bluetooth is installed, Computer Friendly Name is also blank, but can be edited by the user.

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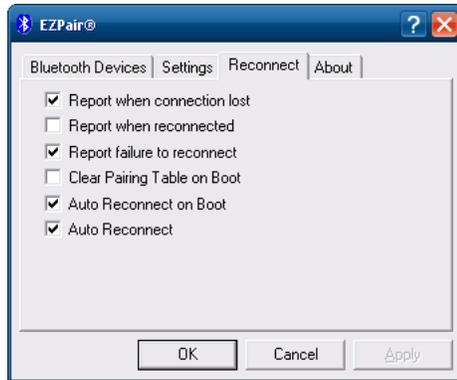
Note: *These options can still be checked or unchecked whether Bluetooth connection is enabled or disabled.*

Options

Option	Function
Report when connection lost	This option is Enabled (checked) by default. 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 notifying the user the connection between one (or all) of the paired Bluetooth devices has stopped. Tap the **OK** button to remove the dialog box from the screen.
Report when reconnected	This option is Disabled (unchecked) by default. There may be an audio or visual signal when a connection between a paired, active device is made. A visual signal may be a dialog box placed on the display notifying the user the connection between one (or all) of the paired Bluetooth devices has resumed. Tap the **OK** button to remove the dialog box from the screen.
Report failure to reconnect	This option is Enabled (checked) by default. The default 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 fails to re-connect. A visual signal may be a dialog box placed on the display notifying the user the connection between one (or all) of the previously paired Bluetooth devices has failed. 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.
Clear Pairing Table on Boot	This option is Disabled (unchecked) by default. When enabled (checked), all previous paired information is deleted upon any reboot sequence and no devices are reconnected. When enabled (checked) "Auto Reconnect on Boot" is automatically disabled (dimmed).
Auto Reconnect on Boot	This option is Enabled (checked) by default. All previously paired devices are reconnected upon any reboot sequence. When disabled (unchecked), no devices are reconnected upon any reboot sequence.

Option	Function
Auto Reconnect	This option is Enabled (checked) by default. This option controls the overall mobile Bluetooth device reconnect behavior. When Auto Reconnect is disabled (unchecked), **Auto Reconnect on Boot** is automatically disabled and dimmed. When Auto Reconnect is disabled (unchecked), no devices are reconnected in any situation. The status of **Auto Reconnect on Boot** is ignored and no devices are reconnected on boot. The status of **Clear Pairing Table on Boot** controls whether the pairing table is populated on boot. When Auto Reconnect is enabled (checked) and **Auto Reconnect on Boot** is disabled (unchecked), devices are not reconnected on boot, but are reconnected in other situations (example: return from out-of-range). When Auto Reconnect is enabled (checked) and **Clear Pairing Table on Boot** is enabled (checked), devices are not reconnected on boot, but are reconnected in other situations (example: return from out-of-range). The pairing table is cleared on boot. The status of **Auto Reconnect on Boot** is ignored and the option is automatically disabled (unchecked) and dimmed.

About

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.

Using Bluetooth

(Start) > Control Panel > Bluetooth or Bluetooth icon in taskbar or Bluetooth icon on desktop

![Bluetooth icon] or ![Bluetooth icon]	Tap the Bluetooth icon in the taskbar to open the Bluetooth EZPair application.
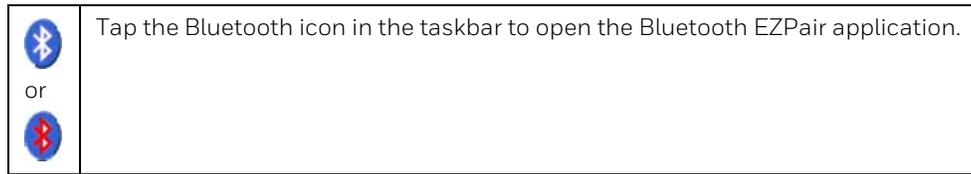
The Thor VM2 default Bluetooth setting is Enabled.

The Thor VM2 Bluetooth module is designed to Discover and pair with nearby Bluetooth devices.

Prerequisite: The remote Bluetooth devices have been setup to allow them to be "Discovered" and "Connected/Paired". The System Administrator is familiar with the pairing function of the remote Bluetooth devices.

Bluetooth Devices Display – Before Discovering Devices
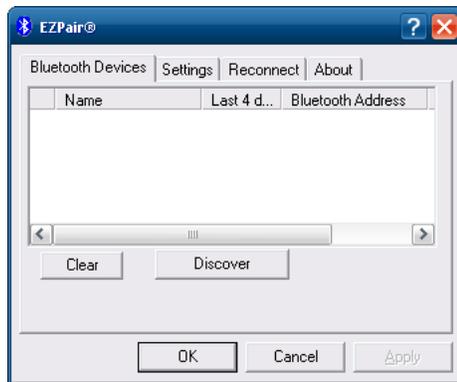
Note: *When Filtered Mode is enabled, only Bluetooth printers or Bluetooth scanners/imagers are recognized and displayed in the Bluetooth panel. All other Bluetooth devices are ignored.*

Initial Configuration

1. Select **(Start) >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 Thor VM2 default name is the Computer Description. Honeywell strongly urges assigning every Thor VM2 a unique name (up to 32 characters) before Bluetooth Discovery is initiated.
4. Check or uncheck the Thor VM2 Bluetooth options on the **Settings** tab.
5. Tap the **OK** button to save your changes or the **X** button to discard any changes.

Subsequent Use

> **Note:** *Taskbar and Bluetooth device Icon states change as Bluetooth devices are discovered, paired, connected and disconnected. 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 EZPair 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. Highlight a Bluetooth device in the Discovered window and double-tap to open the device properties menu.

6. Tap **Pair as Scanner** to set up the Thor VM2 to receive scanner data.

7. Tap **Pair as Printer** to set up the Thor VM2 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 Thor VM2 Bluetooth Devices list. The device is deleted from the list after the **OK** button is clicked.

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 Thor VM2 display.

10. Whenever the Thor VM2 is turned On, all previously paired, live, Bluetooth devices in the vicinity are paired, one at a time, with the Thor VM2. If the devices cannot connect to the Thor VM2 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.

Bluetooth Indicators

The Bluetooth taskbar Icon state changes as Bluetooth devices are discovered, paired, connected and disconnected.

There may be audible or visual signals as paired devices re-connect with the Thor VM2.

Taskbar Icon	Legend
	Thor VM2 is connected to one or more of the targeted Bluetooth device(s).
	Thor VM2 is not connected to any Bluetooth device. Thor VM2 is ready to connect with any Bluetooth device. Thor VM2 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 Thor VM2 Bluetooth scan range, the Bluetooth connection between the paired device and the Thor VM2 is lost. There may be audible or visual signals as paired devices disconnect from the Thor VM2.*

Bluetooth LED	Legend
Blue, blinking slowly	Bluetooth is active but not connected to a device.
Blue, blinking medium	Bluetooth is paired and connected to a device.
Blue, blinking fast	Bluetooth is discovering other Bluetooth devices.
Off	Bluetooth hardware has been turned off or does not exist in the Thor VM2.

Bluetooth Bar Code Reader Setup

Please refer to the Bluetooth scanner manufacturer's User Guide; it may be available on the manufacturer's web site.

Honeywell supports several different types of bar code readers. This section describes the interaction and setup for a mobile Bluetooth laser scanner or laser imager connected to the Thor VM2 using Bluetooth functions.

Prerequisites

- If the Thor VM2 has a Bluetooth address identifier bar code label affixed, then Bluetooth hardware and software is installed.

- The mobile Bluetooth laser scanner / laser imager battery is fully charged.

- The Thor VM2 is connected to AC or DC (vehicle) power.

- **Important**: The bar code numbering examples in this segment are not real and should not be created nor scanned with a Bluetooth scanner.

- To open the EZPair program, tap **(Start) > Control Panel > Bluetooth** or tap the Bluetooth icon on the desktop or tap the Bluetooth icon in the taskbar.

LnkB00440fd01020 - Sample

Locate the bar code label, similar to the one shown above, attached to the Thor VM2. The label is the Bluetooth address identifier for the Thor VM2.

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

Important: The Thor VM2 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 bar code readers.

Thor VM2 with Label

If the Thor VM2 has a Bluetooth address bar code label attached, follow these steps:

1. Scan the Bluetooth address bar code label, attached to the Thor VM2, with the Bluetooth mobile scanner.

2. If this is the first time the Bluetooth scanner has scanned the Thor VM2 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 EZPair panel ((Start) > **Control Panel > Bluetooth**).

4. Tap **Discover**. Locate the Bluetooth scanner in the Discovery panel.

5. Double-tap the stylus on the Bluetooth scanner. The right–mouse-click menu appears.

6. Select **Pair as Scanner** to pair the Thor VM2 with the Bluetooth mobile scanner.

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

Note: *After scanning the Thor VM2 Bluetooth label, if there is no beep and no LED flash from the Bluetooth device, the devices are currently paired.*

Thor VM2 without Label

If the Thor VM2 Bluetooth address bar code label does not exist, follow these steps to create a unique Bluetooth address bar code for the Thor VM2:
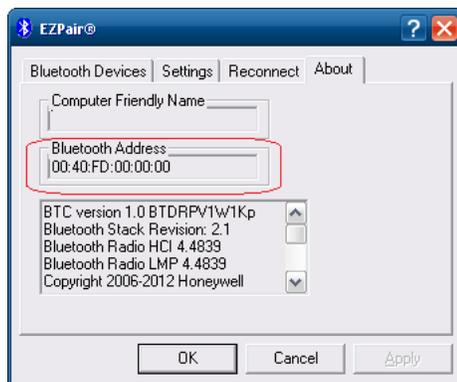
Next, create a Bluetooth address bar code label for the Thor VM2.

The format for the bar code label is as follows:

• Bar code 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 Thor VM2 Bluetooth address bar code label with the Bluetooth bar code reader.

The devices are paired. The Bluetooth bar code reader responds with a series of beeps and LED flashes.

Note: *After scanning the Thor VM2 Bluetooth label, if there is no beep and no LED flash from the Bluetooth bar code reader, the devices are currently paired.*

See Bluetooth Beep and LED Indications.

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 Bluetooth device sounds a long tone, this means the Bluetooth device has not passed its automatic Selftest and has entered isolation mode. If the Bluetooth device is reset, the sequence is repeated. Contact Technical Assistance for assistance.

Bluetooth Printer Setup

The Bluetooth managed device should be as close as possible, in direct line of sight, with the Thor VM2 during the pairing process.

1. Open the Bluetooth EZPair Panel.

2. Tap **Discover**. Locate the Bluetooth printer in the Discovery panel.

3. Tap and hold the stylus (or double-tap) on the Bluetooth printer ID until the right-mouse-click menu appears.

Select **Pair as Printer** to pair the Thor VM2 with the Bluetooth managed printer.

The devices are paired. The Bluetooth managed printer may respond with a series of beeps or LED flashes.

Please refer to the Bluetooth managed printer manufacturer's User Guide; it may be available on the manufacturer's web site. Contact Technical Assistance for Bluetooth product assistance.

Note: *If there is no beep or no LED flash from the Bluetooth managed printer, the Thor VM2 and the printer are currently paired.*

Easy Pairing and Auto-Reconnect

The Bluetooth module can establish relationships with new devices after the user taps the **Discover** button. It can auto-reconnect to devices previously known but which have gone out of range and then returned within range (up to 32.8 ft (10 meters) Line of Sight).

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.

Disk Lock

These features are supported on Windows Embedded Standard 7 only.

Configure support for Enhanced Write Filter (EWF) and Hibernate Once Resume Many (HORM).

EWF write-protects the system volume (C: drive). Though the user may appear to be able to write to the C: drive, the changes are actually stored in RAM.

HORM provides additional functionality over EWF. When HORM is enabled the Thor VM2 resumes from the hibernate image rather than restarting,
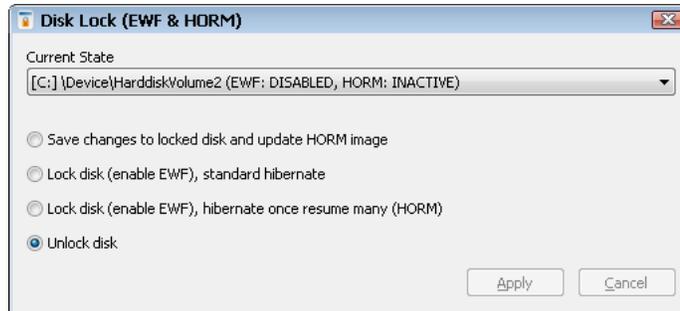
Current State

Lists the current state of the specified volume, i.e.: EWF Enabled/Disabled, HORM Active/Inactive.

Tap the **Apply** button to apply any changes made. A restart may be required for the changes to take effect. If so, a warning box is displayed with an option to restart now or restart later. If restart later is selected, the changes do not take effect until after the restart. At anytime before the restart, returning to this control panel and tapping Cancel discards those changes.

Tap Cancel to exit without making any changes.

The disk lock options are detailed below. If prompted with a User Access Control prompt when opening this control panel, tap Yes to allow the program to make changes.

Save changes to locked disk and update HORM image

Use this option to save changes to the previous HORM image. If this option is selected, the Thor VM2 must be restarted. After the restart, select Hibernate the Thor VM2 to update the HORM image.

Lock disk (enable EWF), standard hibernate

EWF is enabled but HORM is inactive.:

- The user can make changes to drive C:. These changes are stored in RAM rather than written to the C: drive,
- These changes persist across a Hibernate cycle.
- These changes are lost after a Restart or Shutdown cycle.

Lock disc (enable EWF), hibernate once resume many (HORM)

EWF is enabled and HORM is active.

- The user can make changes to drive C:. These changes are stored in RAM rather than written to the C: drive.

- These changes persist across a Hibernate cycle.

- When a user selects Restart the Thor VM2 does not perform a traditional restart. Instead the Thor VM2 shuts down and then resumes from the HORM image. Any user-made changes persist across the restart cycles.

- When a user selects Shutdown the Thor VM2 shuts down. When the Thor VM2 is restarted it resumes from the HORM image rather than performing a traditional restart. Any user-made changes persist across the restart cycles.

- By hibernating rather than restarting, the Thor VM2 boots up faster.

Unlock disk

EWF is disabled and HORM is inactive.

This is the default behavior. The C: drive is not write protected. Any changes made by the user are written to the C: drive and persist across Hibernate, Restart and Shutdown cycles.

Display

Windows Embedded Standard 2009

⊞ **(Start) > Control Panel > Display** (Classic View)

⊞ **(Start) >Control Panel > Appearance and Themes** (Category View)

Windows Embedded Standard 7, Windows 7 Professional

⊞ **(Start) > Control Panel > Appearance and Personalization > Adjust Screen Resolution** (Category View)

⊞ **(Start) > Control Panel > Display > Adjust resolution** (Large or Small Icon View)
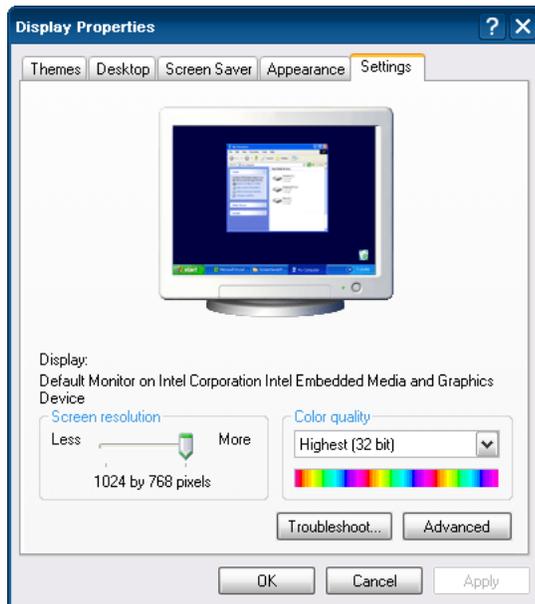
Windows Embedded Standard 2009
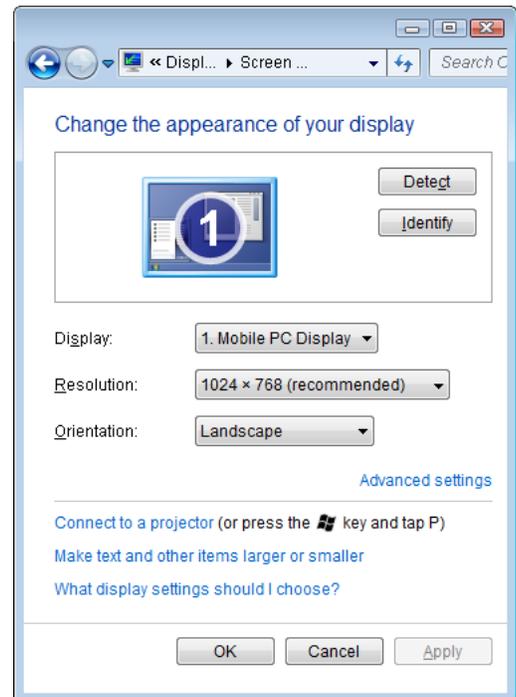
Windows Embedded Standard 7
Windows 7 Professional

The Thor VM2 supports a maximum 1024 x 768 pixel display resolution.

Screen Rotation and Screen Blanking are configured on a separate control panels.

Options

Windows Embedded Standard 2009

![Start] **(Start)** > **Control Panel** > **Options** (Classic view)

Windows Embedded Standard 7, Windows 7 Professional

![Start] **(Start)** > **Control Panel** > **Options** (Large or Small Icon View)
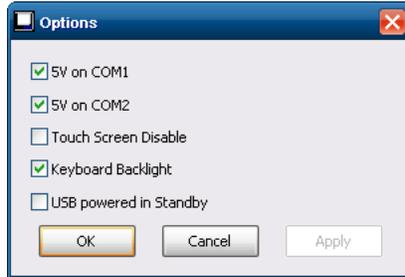
Windows Embedded Standard 2009
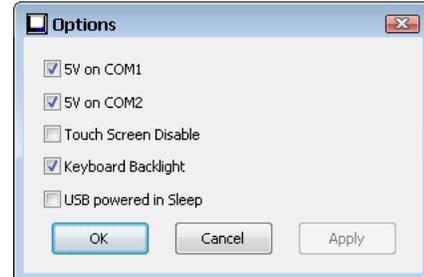
Windows Embedded Standard 7
Windows 7 Professional

5V on COM1

By default, Pin 9 of COM1 provides +5V, such as for an external scanner tethered to the COM1 port. Uncheck this box to configure Pin 9 of COM1 to provide RI.

5V on COM2

By default, Pin 9 of COM2 provides +5V, such as for an external scanner tethered to the COM2 port. Uncheck this box to configure Pin 9 of COM2 to provide RI.

Touch Screen Disable

By default, this option is unchecked and the touch screen is enabled. If this option is checked, it may be necessary to attach an external keyboard or USB mouse to access this screen to re-enable the touch screen unless a Programmable Key has been assigned to enable the touch screen.

Note: *Tapping **Apply** disables the touch screen but does not dismiss this panel. The panel must be dismissed via an external keyboard or mouse. This panel is dismissed when the **OK** button is tapped after selecting Touch Screen Disable.*

Keyboard Backlight

By default, the integrated keyboard backlight follows the display backlight. Uncheck this box to turn the keyboard backlight off regardless of the display backlight status.

USB Powered in Standby or Sleep

Standby mode is supported for a Thor VM2 with a Windows Embedded Standard 2009 OS. Sleep mode is supported for a Thor VM2 with either a Windows Embedded Standard 7 or a Windows 7 Professional OS.

By default, power is removed from attached USB devices when the Thor VM2 is in Standby or Sleep mode. Check this box to maintain power to attached USB devices in Standby or Sleep

Power Options

Select a Power Scheme or Power Plan

The Thor VM2 has four customized power management schemes/plans defined. The active Power Scheme/Plan depends on:

- The user selected Power Scheme/Plan

- And, for Ignition Control, the status of the ignition input signal.

Each power management scheme/plan includes two sets of time out values:

- Plugged in for when external power is present (such as vehicle power or from an AC power adapter)

- Running on batteries for when external power is not present and the Thor VM2 is operating on UPS power.

Power Schemes

Windows Embedded Standard 2009 only

⊞ **(Start) > Control Panel > Power Options > Power Schemes** tab (Classic View)

⊞ **(Start) >Control Panel > Performance and Maintenance> Power Options > Power Schemes** tab (Category View)
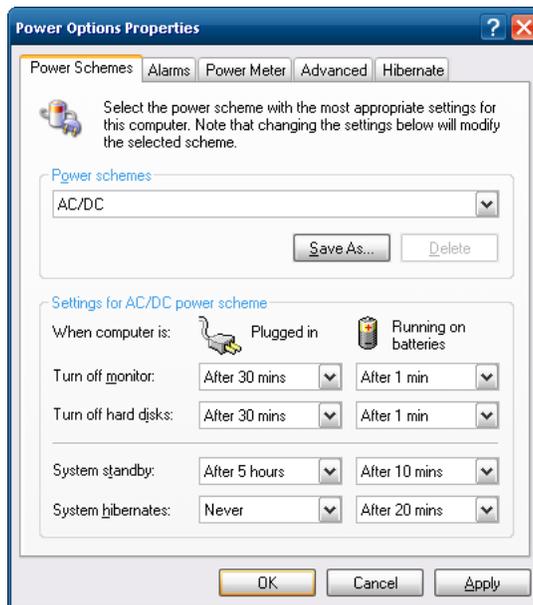
Select a Power Plan

Windows Embedded Standard 7 and Windows 7 Professional only

![Start icon] **(Start) > Control Panel > Power Options** (Large or Small Icon View)
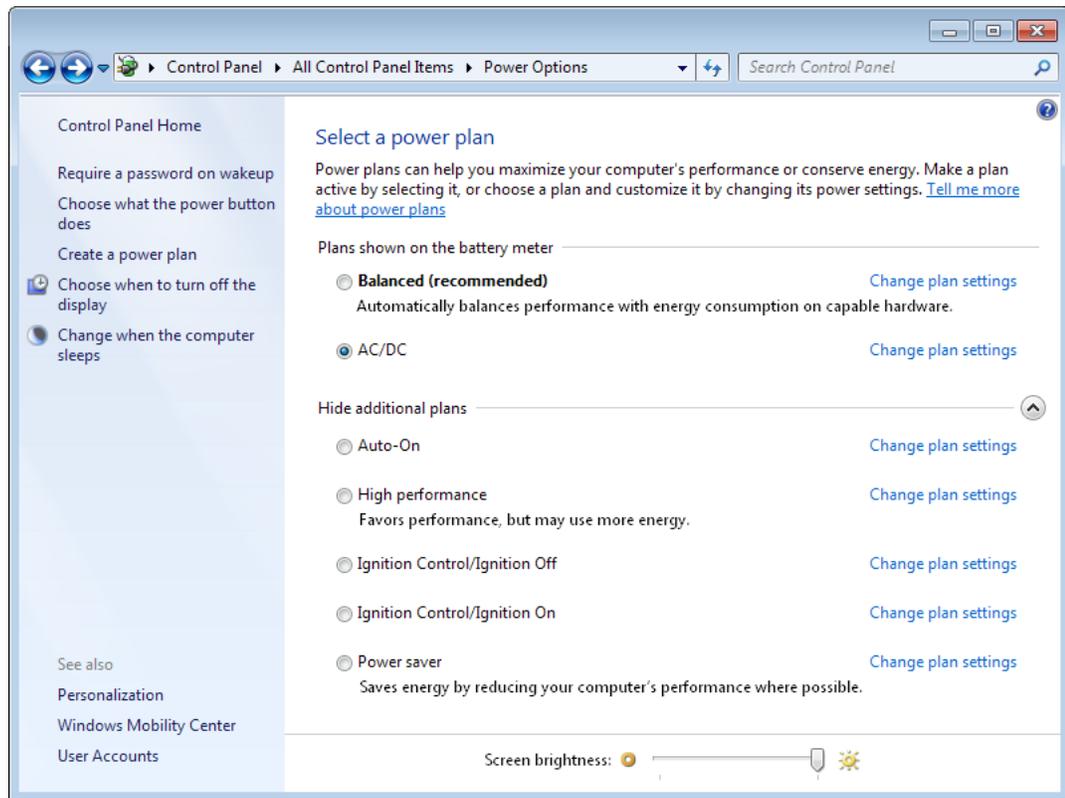
The Thor VM2 has four power management as described in the following sections.

AC/DC

Select the AC/DC power scheme/plan when it is desired that the Thor VM2 power on when external power is connected.

In AC/DC mode, the Thor VM2 is turned On by the presence of external power with no user interaction required. Ignition input is ignored when AC/DC mode is enabled.

Note: *When the UPS battery has been depleted or disconnected (the Thor VM2 is first powered out of the box, the front panel has been replaced, etc.) power the Thor VM2 manually by pressing the power button. After the initial power up, the Thor VM2 powers on automatically when power is attached and AC/DC mode is enabled.*

The following default timeouts are used in the AC/DC power scheme/plan.

Windows Embedded Standard 7, Windows 7 Professional		
Setting	**Plugged In (AC or DC Power)**	**Running on Batteries (UPS Power)**
Dim the display	Never	Never
Turn of the display	30 minutes	1 minute
Put the computer to sleep	Never (see note)	Never (see note)
Hibernate after	300 minutes	20 minutes

Windows Embedded Standard 2009		
Setting	**Plugged In (AC or DC Power)**	**On Battery (UPS Power)**
Turn off monitor	30 minutes	1 minute
Turn of hard disks	30 minutes	1 minute
System standby	5 hours	10 minutes
System hibernate	Never	20 minutes

Note: *By default Sleep is disabled and Hibernate is enabled. Because the Thor VM2 with Windows Embedded Standard 7 or Windows 7 Professional cannot transition from Sleep to Hibernate due to a limitation of the operating system, Sleep is disabled. Power savings are significantly greater using Hibernate.*

Note: *When the Thor VM2 has a Windows 7 operating system and a 32 GB SSD drive the files necessary for hibernate may result in low disk space if installed applications or data are using large amounts of hard drive space.*

AC/DC Behavior

When the AC/DC scheme/plan is selected and external power is present the Thor VM2 behaves as described below. If external power is not present, refer to the UPS section for Thor VM2 behavior.

Thor VM2 is Off

The Thor VM2 is Off and gets external power, such as

- Thor VM2 is installed on a powered dock with the dock power switch On
- Thor VM2 is already mounted to a dock and external power is applied to the dock
- Thor VM2 is already mounted to a dock and the dock power switch is turned On

The Thor VM2 boots. Once booted the Thor VM2 follows the AC/DC power scheme/plan with timers reset after the boot completes.

Thor VM2 is On

The Thor VM2 is On and gets external power, such as

- Thor VM2 is installed on a powered dock with the dock power switch On
- Thor VM2 is already mounted to a dock and external power is applied to the dock
- Thor VM2 is already mounted to a dock and the dock power switch is turned On

The Thor VM2 continues to run and follows AC/DC power scheme/plan with timers reset at the time power was connected.

Ignition Control/Ignition On

Select either the Ignition Control/Ignition On or the Ignition Control/Ignition Off power scheme/plan when ignition control of the Thor VM2 power on process is desired.

The Thor VM2 aromatically switches between the Ignition Control/Ignition On or the Ignition Control/Ignition Off power schemes/plans depending on the state of the vehicle ignition input.

The following default timeouts are used in the Ignition Control/Ignition On power scheme./plan

Setting	Plugged In (AC or DC Power)	Running on Batteries (UPS Power)
Dim the display	Never	Never
Turn of the display	30 minutes	1 minute
Put the computer to sleep	Never (see note)	Never (see note)
Hibernate after	300 minutes	20 minutes

Windows Embedded 2009		
Setting	Plugged In (AC or DC Power)	Running on Batteries (UPS Power)
Turn off monitor	30 minutes	1 minute
Turn of hard disks	30 minutes	1 minute
System standby/sleep	5 hours	10 minutes
System hibernate	Never	20 minutes

Note: *By default Sleep is disabled and Hibernate is enabled. Because the Thor VM2 with Windows Embedded Standard 7 or Windows 7 Professional cannot transition from Sleep to Hibernate due to a limitation of the operating system, Sleep is disabled. Power savings are significantly greater using Hibernate.*

Note: *When the Thor VM2 has a Windows 7 operating system and a 32 GB SSD drive the files necessary for hibernate may result in low disk space if installed applications or data are using large amounts of hard drive space.*

The ignition input wire must be connected. If the user selects this power scheme/plan but the ignition is Off, the Ignition Control/Ignition Off scheme/plan is used instead.

Ignition Control/Ignition On Behavior

When either Ignition Control power scheme/plan is selected and external power is present the Thor VM2 behaves as described below. If external power is not present, refer to the UPS section for Thor VM2 behavior.

Thor VM2 is Off and Vehicle Ignition is Switched to On

Conditions

The Thor VM2 is Off and vehicle ignition changes from Off to On.

Result

The Thor VM2 boots. Once booted the Thor VM2 follows the Ignition Control/Ignition On power scheme/plan with timers reset after the boot completes.

Thor VM2 is On and Vehicle Ignition is Switched to On

Conditions

The Thor VM2 is On and vehicle ignition changes from Off (or not present) to On.

Result

The Thor VM2 continues to run and follows the Ignition Control/Ignition On power scheme/plan with timers reset at the time Ignition switched to Active.

An example of this case would be a Thor VM2 that is running on UPS and is then mounted on a dock that has truck power and the ignition switch is already On.

Ignition Control/Ignition Off

Select either the Ignition Control/Ignition On or the Ignition Control/Ignition Off power scheme/plan when ignition control of the Thor VM2 power on process is desired.

The Thor VM2 automatically switches between the Ignition Control/Ignition On or the Ignition Control/Ignition Off power schemes/plans depending on the state of the vehicle ignition input. Default timeouts are shorter in this scheme to conserve the vehicle battery charge.

The following default timeouts are used in the Ignition Control/Ignition Off power scheme/plan.

Windows Embedded Standard 7, Windows 7 Professional		
Setting	Plugged In (AC or DC Power)	On Battery (UPS Power)
Dim the display	Never	Never
Turn of the display	1 minute	1 minute
Put the computer to sleep	Never (see note)	Never (see note)
Hibernate after	60 minutes	20 minutes

Windows Embedded Standard 2009		
Setting	Plugged In (AC or DC Power)	Running on Batteries (UPS Power)
Turn off monitor	1 minute	1 minute
Turn of hard disks	5 minutes	1 minute
System standby/sleep	1 hour	10 minutes
System hibernate	6 hours	20 minutes

Note: *By default Sleep is disabled and Hibernate is enabled. Because the Thor VM2 with Windows Embedded Standard 7 or Windows 7 Professional cannot transition from Sleep to Hibernate due to a limitation of the operating system, Sleep is disabled. Power savings are significantly greater using Hibernate.*

Note: *When the Thor VM2 has a Windows 7 operating system and a 32 GB SSD drive the files necessary for hibernate may result in low disk space if installed applications or data are using large amounts of hard drive space.*

The ignition input wire must be connected. If the user selects this power scheme/plan but the ignition is On, the Ignition Control/Ignition On scheme/plan is used instead.

Ignition Control/Ignition Off Behavior

When either Ignition Control power scheme/plan is selected and external power is present the Thor VM2 behaves as described below. If external power is not present, refer to the UPS section for Thor VM2 behavior.

Thor VM2 is Off and Vehicle Ignition is Off

Conditions

The Thor VM2 is Off and vehicle ignition is Off.

Result

The Thor VM2 remains Off regardless of external power. UPS charging is disabled.

Conditions

The Thor VM2 has external power but vehicle ignition is Off. The power button is pressed.

Result

The Thor VM2 boots. Once booted the Thor VM2 follows the Ignition Control/Ignition Off power scheme/plan with timers reset after the boot completes.

Thor VM2 is On and Vehicle Ignition is Switched to Off

Conditions

The Thor VM2 is On and vehicle ignition changes from On to Off.

Result

The Thor VM2 follows the Ignition Control/Ignition Off power scheme/plan with timers reset at the time Ignition switched to Inactive. UPS charging is disabled.

An example of this case would be a Thor VM2 that is running on UPS and is then mounted on a dock that has truck power and the ignition switch is already Off.

Auto-On

Select the Auto-On power scheme/plan when it is desired that the Thor VM2 power on when external power is connected.

In Auto-On mode, the Thor VM2 is turned On by the presence of external power with no user interaction required. Ignition input is ignored when Auto-On Mode is enabled.

Note: *When the UPS battery has been depleted or disconnected (the Thor VM2 is first powered out of the box, the front panel has been replaced, etc.) power the Thor VM2 manually by pressing the power button. After the initial power up, the Thor VM2 powers on automatically when power is attached and Auto-On mode is enabled.*

The following default timeouts are used in the Auto-On power scheme/plan.

Windows Embedded Standard 7, Windows 7 Professional		
Setting	Plugged In (AC or DC Power)	Running on Batteries (UPS Power)
Dim the display	Never	Never
Turn of the display	30 minutes	1 minute
Put the computer to sleep	Never (see note)	Never (see note)
Hibernate after	300 minutes	20 minutes

Windows Embedded Standard 2009		
Setting	Plugged In (AC or DC Power)	Running on Batteries (UPS Power)
Turn off monitor	30 minutes	1 minute
Turn of hard disks	30 minutes	1 minute
System standby/sleep	5 hours	10 minutes
System hibernate	Never	20 minutes

Note: *By default Sleep is disabled and Hibernate is enabled. Because the Thor VM2 with Windows Embedded Standard 7 or Windows 7 Professional cannot transition from Sleep to Hibernate due to a limitation of the operating system, Sleep is disabled. Power savings are significantly greater using Hibernate.*

Note: *When the Thor VM2 has a Windows 7 operating system and a 32 GB SSD drive the files necessary for hibernate may result in low disk space if installed applications or data are using large amounts of hard drive space.*

Auto-On Behavior

When the Auto-On power scheme/plan is selected and external power is present the Thor VM2 behaves as described below. If external power is not present, refer to the UPS section for Thor VM2 behavior.

Thor VM2 is Off

The Thor VM2 is Off and gets external power, such as

- Thor VM2 is installed on a powered dock with the dock power switch On
- Thor VM2 is already mounted to a dock and external power is applied to the dock
- Thor VM2 is already mounted to a dock and the dock power switch is turned On

Result

The Thor VM2 boots. Once booted the Thor VM2 follows the Auto-On power scheme/plan with timers reset after the boot completes.

Thor VM2 is On

Conditions

The Thor VM2 is On and gets external power, such as

- Thor VM2 is installed on a powered dock with the dock power switch On
- Thor VM2 is already mounted to a dock and external power is applied to the dock
- Thor VM2 is already mounted to a dock and the dock power switch is turned On

Result

The Thor VM2 continues to run and follows Auto-On power scheme/plan with timers reset at the time power was connected.

UPS

When the Thor VM2 is operating on the UPS the timeouts from the battery section for the selected power scheme/plan are used. By default, the timeouts for UPS are the same for each power scheme/plan.

UPS Behavior

The Thor VM2 behavior when operating from UPS power is described below.

Thor VM2 is Off

Conditions

The Thor VM2 is Off and the power button is pressed the Thor VM2 and both the following conditions are met:

- UPS power is over 10% capacity
- CPU temperature is over 20ºC

Result

The Thor VM2 boots and follows the selected power scheme's Running on Batteries (or power plan's On battery) timeouts with power management timers reset at boot up.

Conditions

The Thor VM2 is Off and the power button is pressed the Thor VM2 and at least one of the following conditions are met:

- UPS power is under 10% capacity
- CPU temperature is under 20ºC

Results

The Thor VM2 remains Off.

Thor VM2 is On

Conditions

The Thor VM2 is On and external power is removed, such as:

- Thor VM2 is removed from a powered dock (Dock power switch On)
- Thor VM2 is mounted to a dock and truck power is removed from the dock
- Thor VM2 is mounted to a dock and the dock power switch is turned Off

Result

The Thor VM2 boots and follows the selected power scheme's Running on Batteries (or power plan's On battery) timeouts with power management timers reset at the time of power removal. UPS charging is disabled.

View UPS Battery Status

Power Meter

Windows Embedded Standard 2009 only

⊞ **(Start) > Control Panel > Power Options > Power Schemes** tab (Classic View)

⊞ **(Start) > Control Panel > Performance and Maintenance> Power Options > Power Schemes** tab (Category View)
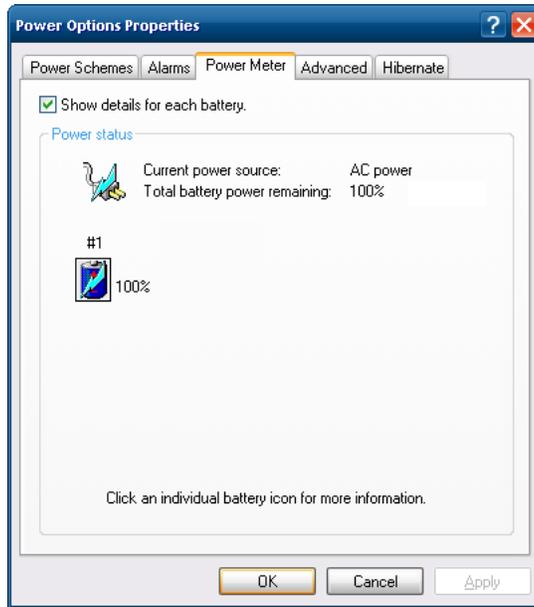
On the **Power Meter** tab, battery #1 refers to the UPS battery.

Shows power status: external power or UPS battery and the total battery power remaining before a recharge is necessary.

Power Notification Icon

Windows Embedded 7 and Windows 7 Professional only

The Power icon in the notification area provides an indication of the level of UPS battery charge. The icon also indicates if external power is connected. Some samples are shown below

	External power is connected and the UPS battery is approximately 50% charged.
	External power not connected and the UPS battery is approximately 100% charged.

Configure Power Button Behavior

Windows Embedded Standard 2009 only

⊞ **(Start) > Control Panel > Power Options > Power Schemes** tab (Classic View)

⊞ **(Start) >Control Panel > Performance and Maintenance> Power Options > Advanced** tab (Category View)

Advanced
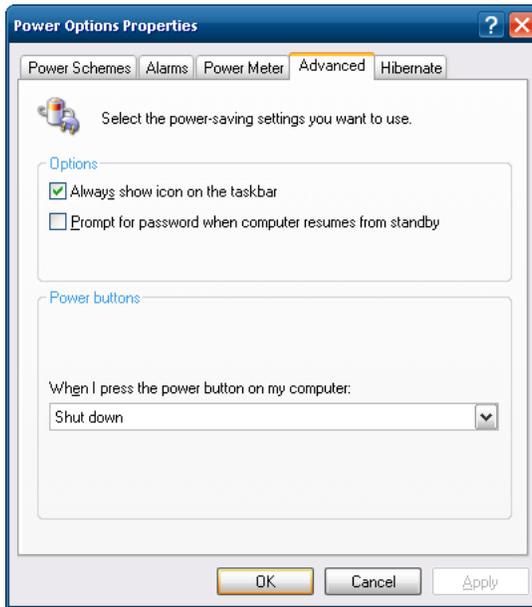
The **Advanced** panel allows setting the power button behavior when the unit is on and the power button is pressed. Options are:

- Do nothing
- Ask me what to do
- Stand by
- Shut down.

The default is to shut down. The Thor VM2 performs an orderly shut down when the power key is pressed when this option is enabled.

Choose What the Power Button Does

Windows Embedded 7 and Windows 7 Professional only

⊞ **(Start) > Control Panel > Power Options** (Large or Small Icon View)
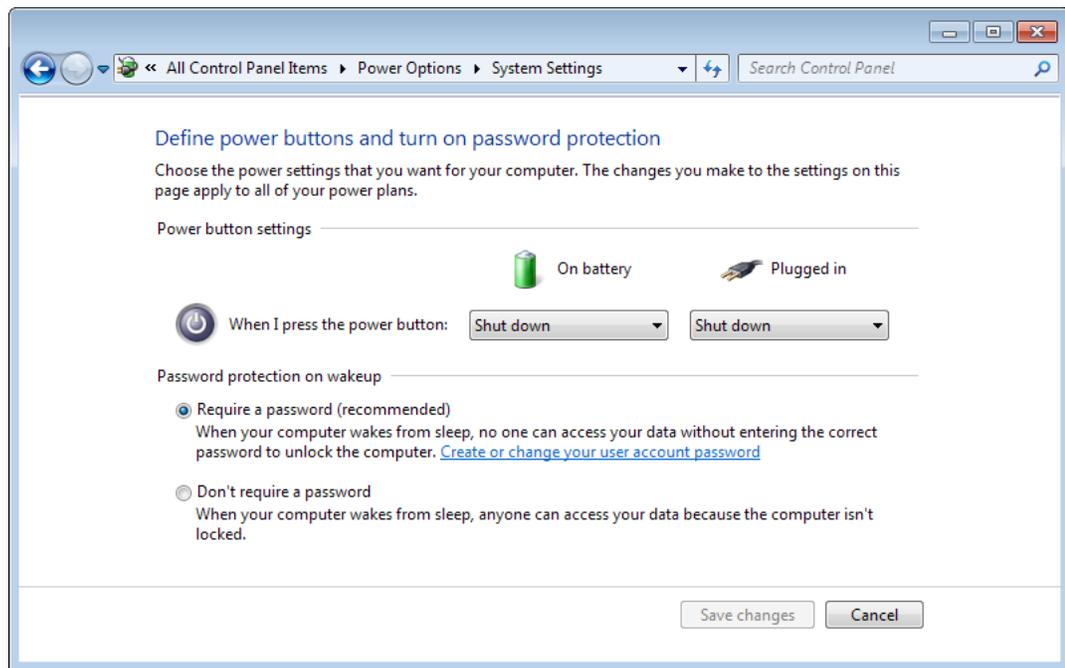
Tap **Choose what the power button does**. For both battery and external power, the power button press may be configured as follows:

- Do nothing
- Sleep
- Hibernate
- Shut down.

Note: *For Windows Embedded Standard 7, it may be necessary to tap* **Change settings that are currently unavailable** *before making changes to the power button behavior.*

Hibernate

Enable Hibernation

Windows Embedded Standard 2009 only

 (Start) > Control Panel > Power Options > Hibernate tab (Classic View)

 (Start) >Control Panel > Performance and Maintenance> Power Options > Hibernate tab (Category View)

By default, hibernate is enabled on the Thor VM2. The default can be changed on this page.

The disk space necessary for hibernation plus the free disk space on the hard drive are listed.

Configure Hibernation

Windows Embedded 7 and Windows 7 Professional only

⊞ **(Start) > Control Panel > Power Options** (Large or Small Icon View)

By default, hibernate is enabled on the Thor VM2.

To change the hibernate settings:

1. Open the Power Options control panel (⊞ **(Start) > Control Panel > Power Options**).
2. For the desired power plan, tap Change plan settings. It may be necessary to tap Show additional plans if the desired plan is not the currently active power plan.
3. Tap Change advanced power settings.
4. From the popup window, tap the + in front of Sleep.
5. Tap the + in front of Hibernate after.
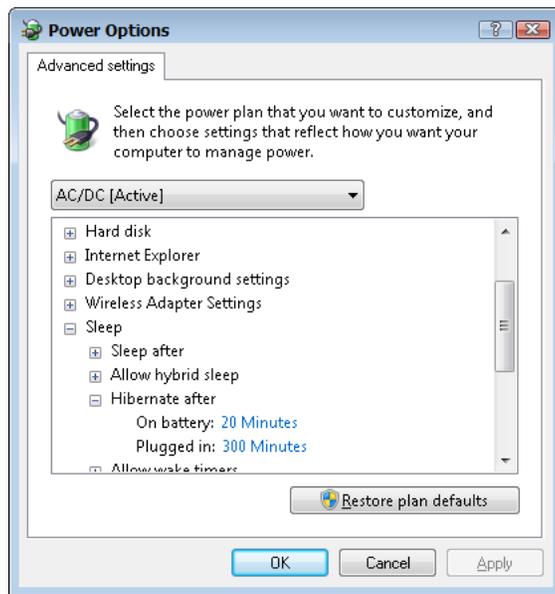
6. Enter the new timeout period in minutes. The hibernate timeout can be specified for on battery and plugged in. Enter 0 to disable hibernation for the specified plan and power source (battery or external).

7. Tap **OK** and close all open power control panels.

Programmable Key

(Start) > Control Panel > Programmable Key (Classic view)

his function remaps P1-P5 keys integrated into the front panel of the Thor VM2. The keys on the optional external (21-key numeric) USB keyboard are not remappable.

Programmable Key	Default Value	
	Windows Embedded Standard 2009	**Windows 7 Professional Windows Embedded Standard 7**
P1	F1	F1
P2	F2	F2
P3	F3	F3
P4	F4	Toggle SIP
P5	F5	Enter
P6 (Orange + P1)	<no key>	<no key>
P7 (Orange + P2)	<no key>	<no key>
P8 (Orange + P3)	<no key>	<no key>
P9 (Orange + P4)	<no key>	<no key>
P10 (Orange + P5)	<no key>	<no key>

The Programmable Key panels can be used to perform the following functions:

- Remap a Key to a Single Key
- Remap a Key to a Unicode Value
- Remap a Key to a Key Sequence
- Remap a Key to a Sequence of Unicode Values
- Remap a Key to a Special Function
- Remap a Key to Launch an Application
- Remap a Key to Run a Command

Keymap
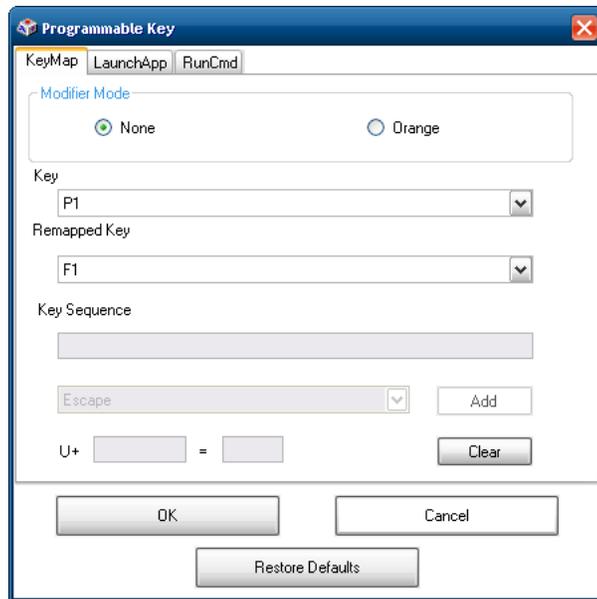
A key or combination of keys can be remapped to provide a single keypress or a string of keypresses.

Assign settings by clicking radio buttons and selecting keys from the drop down boxes.

Tap the **OK** button to save changes and exit the Programmable Keys control panel.

Tap the **Cancel** button to discard any changes and exit the Programmable Keys control panel.

Tap the **Restore Defaults** to return all Programmable Keys to their default values and exit the Programmable Keys control panel.

Remap a Key to a Single Key

1. Select the modifier key from the Modifier Mode options.
2. Select the key to be remapped from the Key pull-down list.
3. Select the value for the remapped key from the Remapped Key pull-down list.
4. Click **OK** to save the result and close the control panel.

Remap a Key to a Unicode Value

1. Select the modifier key from the Modifier Mode options.
2. Select the key to be remapped from the Key pull-down list.
3. Select **Unicode** from the Remapped Key pull-down list.
4. There are two Unicode text boxes located on the lower part of this tab. Enter the Unicode value in the text box to the right of ALT + and the Unicode character is displayed in the box to the right of =.
5. Click **OK** to save the result and close the control panel.

Remap a Key to a Key Sequence

Up to 16 keys may be specified for the key sequence. The sequence can consist of keys and Unicode values.

1. Select the modifier key from the Modifier Mode options.

2. Select the key to be remapped from the Key pull-down list.

3. Select **Key Sequence** from the Remapped Key pull-down list.

4. Select the first key for the multiple key sequence from the pull-down list.

5. Press the **Add** button to add the key to the multiple key sequence shown in the Key Sequence box.

6. Repeat this steps 4 and 5 until all desired keys have been added to the key sequence. If necessary, use the **Clear** button to erase all entries in the Key Sequence box.

7. Click **OK** to save the result and close the control panel.

Remap a Key to a Sequence of Unicode Values

Up to 16 Unicode values may be specified for the key sequence. The sequence can consist of keys and Unicode values.

1. Select the modifier key from the Modifier Mode options.

2. Select the key to be remapped from the Key pull-down list.

3. Select **Key Sequence** from the Remapped Key pull-down list.

4. Select **Unicode** from the Key Sequence pull-down list.

5. There are two Unicode text boxes located on the lower part of this tab. Enter the Unicode value in the text box to the right of ALT + and the Unicode character is displayed in the box to the right of =.

6. Press the **Add** button to add the key to the multiple key sequence shown in the Key Sequence box.

7. Repeat this steps 4 through 6 until all desired characters have been added to the key sequence. If necessary, use the **Clear** button to erase all entries in the Key Sequence box.

8. Click **OK** to save the result and close the control panel.

Remap a Key to a Special Function

1. Select the modifier key from the Modifier Mode options.

2. Select the key to be remapped from the Key pull-down list.

3. Select the special function from the remapped key from the Remapped Key pull-down list. Special functions that can be assigned are:

   • Toggle SIP (soft keyboard) state between displayed and hidden

   • Toggle touch screen state between enabled and disabled

   • Toggle integrated keyboard backlight state between on and off

- Launch the touch screen calibration utility

4. Click **OK** to save the result and close the control panel.

Remap a Key to Launch an Application

1. Select the modifier key from the Modifier Mode options.

2. Select the key to be remapped from the Key pull-down list.

3. Select **Launch App**1-4 from the remapped key from the Remapped Key pull-down list.

4. Click on the LaunchApp tab.

5. Make sure the **APP** radio button is selected.

6. In the text box (LaunchApp1-4) corresponding to the number selected for Launch App1-4, enter the application to launch.

7. If any parameters are needed for the application, click on the **OPT** radio button. This clears the text box (though the application name is saved). Enter the desired parameters in the appropriate text box.

8. Click **OK** to save the result and close the control panel.

9. If the **KeyMap** tab is accessed again, the application plus any specified parameters is displayed in the Key Sequence text box when the remapped key is again selected.

Remap a Key to Run a Command

1. Select the modifier key from the Modifier Mode options.

2. Select the key to be remapped from the Key pull-down list.

3. Select **RunCmd**1-4 from the remapped key from the Remapped Key pull-down list.

4. Click on the RunCmd tab.

5. Make sure the **CMD** radio button is selected.

6. In the text box (RunCmd1-4) corresponding to the number selected for RunCmd1-4, enter the desired command.

7. If any parameters are needed for the command, click on the **PARM** radio button. This clears the text box (though the command is saved). Enter the desired parameters in the appropriate text box.

8. Click **OK** to save the result and close the control panel.

9. If the **KeyMap** tab is accessed again, the command plus any specified parameters is displayed in the Key Sequence text box when the remapped key is again selected.

LaunchApp

The default for all text boxes is Null or " ". The text boxes accept string values only.

The executables and parameters are not checked for accuracy by the keyboard driver. If the launch fails, the Thor VM2 displays a popup error message. If the launch is successful, no notification is displayed.
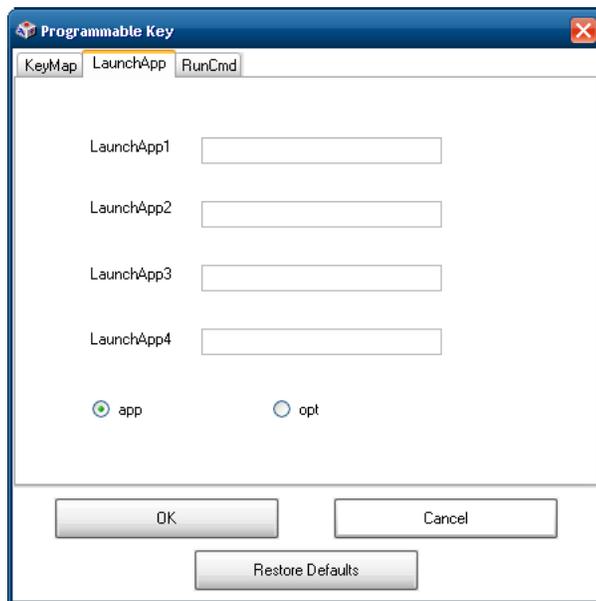
The Launch App command is defined for use by system administrators. These instructions are parsed and executed directly by the keyboard driver.

1. Place the cursor in the text box next to the App you wish to run, e.g., App1, App2.

2. Enable the **app** radio button if the application is an EXE file.

3. Enter the path and name of the executable file including the file extension, e.g.: C:\Windows\System32\notepad.exe.

4. Enable the **opt** radio button to add options or parameters for the executable file in the same text box. Switching from app to opt clears the text box (but the information previously entered is stored), allowing parameter entry.

5. Tap the **OK** button to save changes and exit the Programmable Keys control panel.

Tap the **Cancel** button to discard any changes and exit the Programmable Keys control panel.

Tap the **Restore Defaults** to return all Programmable Keys to their default values and exit the Programmable Keys control panel.

The result of the application (app) and options (opt) entries are displayed on the **Key-Map** tab in the Key Sequence box when the key mapped to the LauchApp is selected.

RunCmd

The default for all text boxes is Empty, Null or " ". The text boxes accept string values only.

The executables and parameters are not checked for accuracy by the keyboard driver. If the launch fails, the Thor VM2 displays a popup error message. If the launch is successful, no notification is displayed.
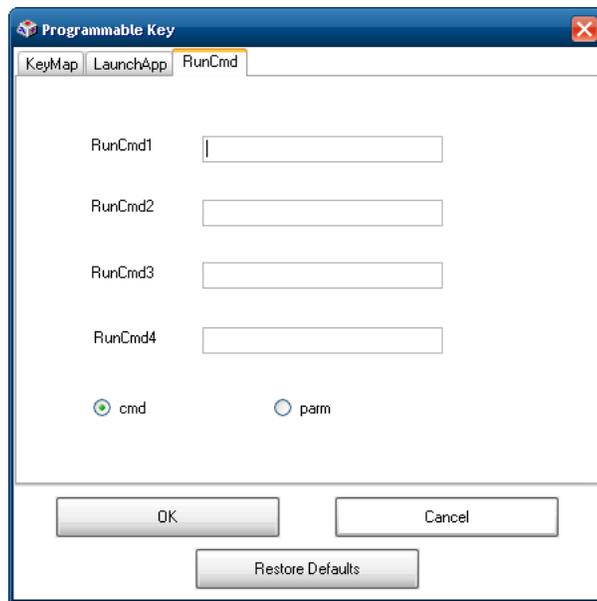
The Run Cmd command is defined for use by system administrators. These instructions call the ShellExecuteEx API, which opens documents directly.

1. Place the cursor in the text box next to the Cmd you wish to run, e.g., Cmd1, Cmd2.

2. Enable the file radio button and enter the name of the file.

3. Enable the **PARM** radio button to add parameters for file/exe execution in the same text box.

4. Tap the **OK** button to save changes and exit the Programmable Keys control panel.

Tap the **Cancel** button to discard any changes and exit the Programmable Keys control panel.

Tap the **Restore Defaults** to return all Programmable Keys to their default values and exit the Programmable Keys control panel.

Windows 7 Professional:

! Some executables may require elevated privileges to run. For example, an executable such as regedit.exe may not run for a standard user but does run for an admin user.

Region and Language

The instructions for installing, changing and uninstalling languages in this section are applicable to Thor VM2 *with Windows Embedded Standard 7 OS only*. While similar control panels are present on other operating systems, the instructions below are not valid for those systems. See Languages for information on installing languages for a Thor VM2 with a Windows 7 Professional or Windows Embedded Standard 2009 OS.

 (Start) > Control Panel > Region and Language > Keyboards and Languages tab (Large or Small Icon View)
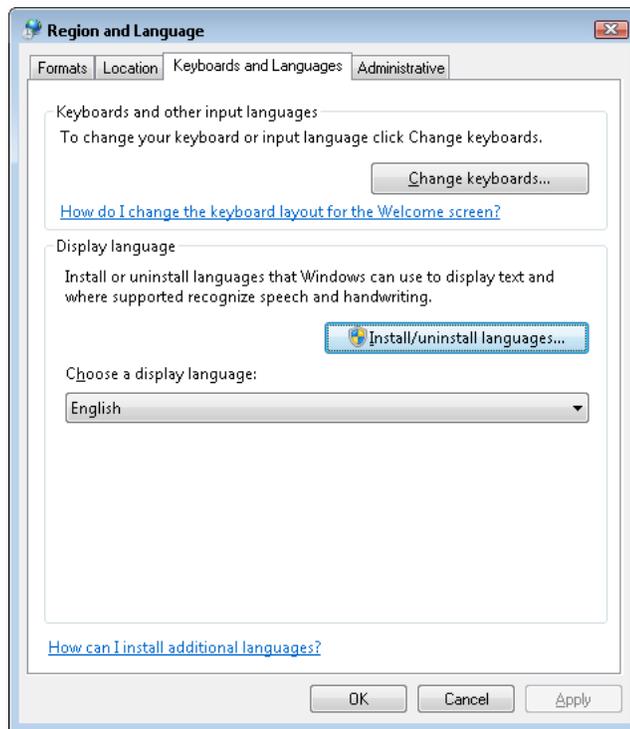
The Thor VM2 may be shipped with an English only Windows Embedded Standard operating system. When only one language (English) is installed, the Choose a display language option is not displayed on the **Keyboard and Languages** tab.

Install a Language

1. Tap I**nstall/uninstall languages...** on the **Keyboards and Languages** tab.

2. If prompted with a User Access Control prompt, tap **Yes** to allow the program to make changes.

3. When prompted, tap **Install display languages**.

4. Tap **Browse** computer or network.

5. Tap the **Browse** button and browse to C:\LangPack and locate the folder for the desired language. The end of the folder name identifies the language:

   • de-de German

   • es-es Spanish

- fr-fr French

- it-it Italian

- ja-jp Japanese

- ko-kr Korean

- pt-pt Portuguese

- ru-ru Russian

- th-th Thai

- zh-cn Simplified Chinese

- zh-tw Traditional Chinese

6. Select the folder for the desired language and tap **OK**.

7. The language is now ready to install. Check the checkbox in front of the language name and tap **Next**.

8. Review the Microsoft Software License Terms and indicate if you accept. If so, tap **Next**.

9. The installation process continues. This process may require several minutes. Tap **Next** when the installation completes.

10. Select the display language from the list of installed languages. When switching display languages, select if the language should also be applied to the welcome screen and all system accounts.

11. When switching display languages, it may be necessary to log or restart off before the changes can take effect. If so, a popup message is displayed. Close any open work and select **Log off now** or **Restart now** for the changes to take effect.

Change Display Language

When more than one language is installed, the display language can be switched between those installed languages.

1. Select the desired language from the **Choose a display language** pull-down list on the **Keyboard and Languages** tab.

2. Select the desired language from the list and tap **OK**.

3. When switching display languages, it may be necessary to log off before the changes can take effect. If so, a popup message is displayed. Close any open work and select **Log off now** for the changes to take effect.

Uninstall Language

1. Tap **Install/uninstall languages...** on the **Keyboards and Languages** tab.

2. If prompted with a User Access Control prompt, tap **Yes** to allow the program to make changes.

3. When prompted, tap **Uninstall display languages**.

4. Check the checkbox in front of the language name to uninstall and tap **Next**. English is the system language and cannot be removed.

5. The uninstallation process continues. This process may require several minutes. Tap **Next** when the installation completes.

6. If prompted to restart, close any work and select **Restart now** for the changes to take effect.

Screen Control

 (Start) > Control Panel > Screen (Classic View)

Set screen properties for the Thor VM2.

Factory Default Settings

Screen Blanking (Blackout)	
Enable screen blanking	Enabled
Screen on delay (ms)	1000
COM Port	COM1
Current Level	
LCD Brightness (%)	100
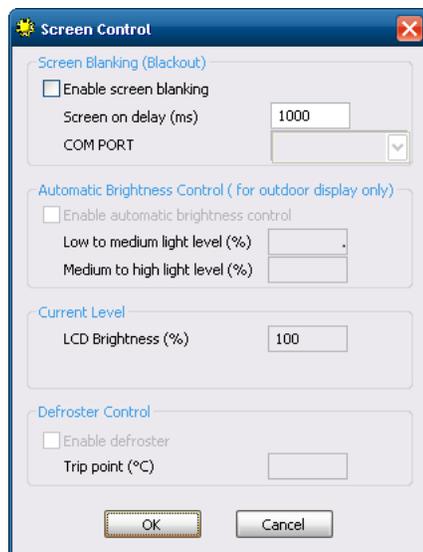
Screen Blanking

Screen blanking allows the Thor VM2 display to automatically be turned off whenever the vehicle is in motion.

Use the Screen on delay to specify the period of time in ms (milliseconds) between when the vehicle stops and the Thor VM2 screen turns on. For example, use the 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. The default value is 1000 ms.

Specify the COM Port to which the screen blanking cable is attached. If a COM port is in use by another application, that COM port is grayed out and cannot be selected for screen blanking.

⚠️ Do not enable Screen Blanking until the cable is properly connected to the specified COM port.

To disable screen blanking, uncheck the **Enable screen blanking** checkbox.

See Screen Blanking for hardware requirements.

Refer to the wiring instructions, including appropriate cautions and warnings, in the Connect Power section.

Screen Rotation

 (Start) >**Control Panel** > **Screen Rotation** (Classic view)

The Screen Rotation panel provides options for rotating the display:

0 Degree – Returns screen to the default orientation.

90 Degree – Rotates the screen counter clockwise 90 degrees as compared to the default orientation.

180 Degree – Rotates the screen 180 degrees as compared to the default orientation.

270 Degree – Rotates the screen counter clockwise 270 degrees as compared to the default orientation.

Select the desired rotation and tap **OK**. The screen may briefly go blank during the rotation process.

Tap Close to dismiss the panel and keep the current screen rotation.

Sounds

![Start icon] **(Start) > Control Panel > Sounds and Audio Devices** (Classic View)

![Start icon] **(Start) >Control Panel > Sounds, Speech and Audio Devices** (Category View)
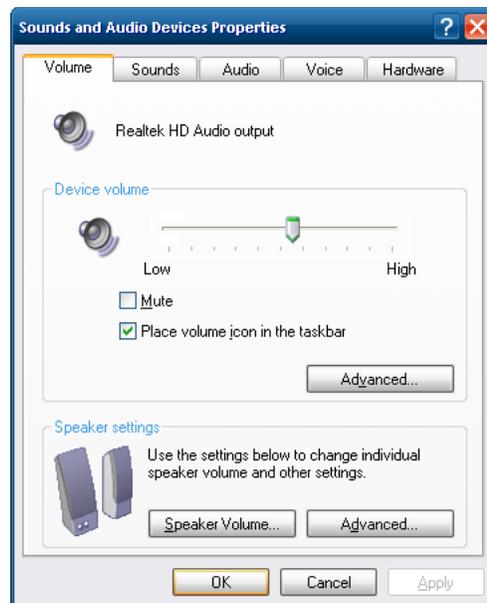
Use the slider bar to adjust the volume level as desired.

Alternatively:

- Tap the Volume icon, if present, in the taskbar and move the slider until the volume level is as desired.

- Use the integrated keypad – press the **Blue** key then **P1** to adjust volume up or **Blue** then **P2** to adjust volume down.

System Rating (Windows Experience Index)

![Start icon] **(Start) > Control Panel > System** (Icon View)

Windows Embedded 7 only

The system rating may not be available. Tapping the **Rate this computer** button has no effect as this feature is disabled.

Windows Embedded 7 and Windows 7 Professional only

The system rating is displayed. However the button to update the rating has no effect as this feature is disabled.

Tablet PC Settings (Touch Screen Calibration)

Windows Embedded 7 and Windows 7 Professional only

(Start) > Control Panel > Tablet PC Settings (Icon View)

The Thor VM2 uses the PenMount touch screen driver. The **Calibrate...** button on this control panel is not used. Instead use the PenMount Control Panel, see Touch Screen Calibration for information on calibrating the touch screen.

User Accounts

⚠️ If creating additional user accounts do not use # character (known as the number sign, pound sign, hash symbol, etc.) in the user account name.

Note: *The following applies to a Thor VM2 that is not part of a domain. When the Thor VM2 is part of a domain, the user is prompted for credentials at Windows startup or log on.*

The Thor VM2 is preconfigured with an administrator account named Administrator. By default, the Thor VM2 automatically logs onto the Administrator account at Windows startup.

If the user assigns a password to the Administrator account:

- The password is stored and used when the Thor VM2 logs onto the Administrator account at Windows startup. The user is not prompted to enter a password.

- If the user logs off, the password must be manually entered to log back onto the Thor VM2.

- At the logon prompt, the user could specify a different user account (and password, if necessary) to log on, assuming the account has been added to the Thor VM2.

- When the Thor VM2 is restarted, the Administrator account automatically becomes the active user account, regardless of the active account before the restart.

If using certificates for authentication, the user must assign a password to the active (Administrator) account.

Wi-Fi

🏁 **(Start) > Control Panel > Wi-Fi** (Classic view)

Provides a shortcut to access the 802.11a/b/g/n radio configuration utility.

Tap the Wi-Fi icon to access the Summit Client Utility.

Bar Code Readers

The Thor VM2 can use the following external bar code readers:

- Tethered hand-held scanners are tethered to a serial port or a USB host port (via a dongle cable) on the Thor VM2 dock and are configured by scanning the engine-specific bar codes in the scanner manufacturer's programming guide. The manufacturer's guides are usually shipped with the bar code reader.

- Wireless hand-held Bluetooth scanners are configured by scanning the engine-specific bar codes in the scanner manufacturer's programming guide. The manufacturer's guides are usually shipped with the bar code reader.

- The body worn Bluetooth Ring Scanner module may be using a Symbol 4400 Ring Imager or a Symbol 955 Ring Scanner. The BTRS module is configured by scanning the bar codes in the Bluetooth Ring Scanner Guide.

Scanner Wedge

Honeywell provides Freefloat Link*One for bar code decoding needs on the Thor VM2. Refer to the Freefloat website for documentation on Freefloat Link*One.

Touch Screen Calibration

 (Start) > **Programs > PenMount Windows Universal Driver**
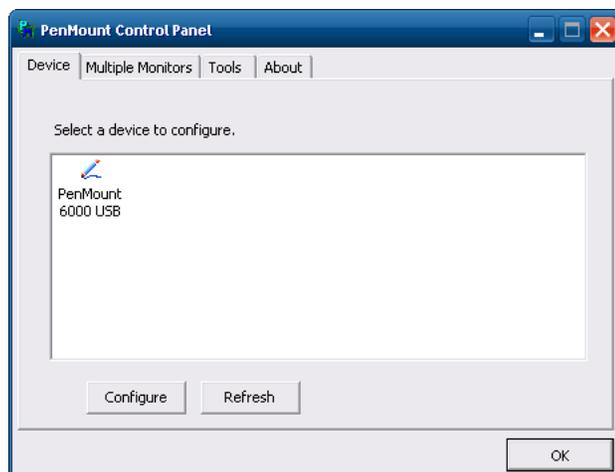
To calibrate the touch screen, tap **(Start) >Programs > PenMount Universal Driver > Utility > PenMount Control Panel**. Select **PenMount 6000 USB** and then tap Configure. Select Standard Calibration or Advance Calibration.

Advanced Calibration allows the user to select the number of calibration points. With either option, follow the on screen instructions to touch the red square, hold the touch and then lift the stylus to complete the calibration process.

BIOS

The Microsoft Windows operating system is installed before shipping. The default BIOS parameters are configured at that time. In most cases, it is unnecessary to modify the BIOS parameters.

Generally, it is only necessary to enter the BIOS setup to change the boot order of the drives.

This section is not intended to detail all features of the BIOS, instead it is intended to cover the most commonly used setup options.

Caution: **Be very careful when using this utility to modify BIOS Setup parameters. The Thor VM2 may generate unexpected results when incorrect or conflicting parameter values are entered. Selecting incorrect or invalid options may require the Thor VM2 to be returned for repairs.**
The parameters should only be modified by Information Services personnel or the system administrator

The Thor VM2 front panel key can be used to maneuver the BIOS screens in the event an external keyboard is not used. See Integrated Keypad and BIOS for front panel key assignments.

Accessing the BIOS Setup

When the Embedded BIOS screen (Phoenix Technologies) is displayed press the Del key on an external keyboard to enter BIOS setup.

Use the arrow keys to move around the screen.

Boot Order

To view or edit the boot order, select the **Boot** tab.

By default, the first device in the boot order is USB Hard Drive.

The second device is the Windows CE Image.

If a USB drive, such as a thumb drive is attached to the Thor VM2, the device attempts to boot from the USB drive:

• If the USB drive contains a bootable sector, the Thor VM2 boots from the USB drive.

• If the USB drive does not contain a bootable sector, the Thor VM2 does not boot. Remove the USB drive and boot the Thor VM2 again.

Exiting BIOS Setup

To exit the BIOS setup, select the **Exit** tab and select from these options:

• Save Setting and Restart

- Exit Setup without Saving Changes
- Reload Factory-Defaults and Restart
- Discard Changes
- Save Changes

Thor VM2 Recovery DVD

A recovery DVD is available to restore the operating system on your Thor VM2 to the same state it had when it was shipped from the factory. The recovery DVD may not reload all factory installed software, but the Thor VM2 Drivers DVD can be used to install software applications. Depending on the operating system, a separate recovery DVD may be provided for English, Traditional Chinese, Simplified Chinese, Japanese, Korean, French, Spanish, Germain and Thai languages or some or all of these languages may be distributed on one DVD. Contact Technical Assistance for information on the recovery DVD and for assistance installing other factory loaded software.

To use the recovery DVD:

1. Attach a USB DVD drive and an external keyboard to the Thor VM2.

2. Insert the recovery DVD into the DVD drive.

3. Reboot the Thor VM2.

4. Repeatedly press the **P5** key on the Thor VM2 front panel or the **F5** key on the external keyboard.

5. When the Boot Menu is displayed, use the arrow keys on the external keyboard to select the USB DVD drive.

6. Follow the on-screen instructions to complete the recovery process.

7. When the process is complete, disconnect the USB DVD drive and start the Thor VM2.

Thor VM2 Drivers DVD

The drivers DVD contains drivers and software for the Thor VM2.

There is a driver installation document. Install the drivers in the order listed in this document, rebooting when specified.

Thor VM2 with no Operating System

The Thor VM2 can be ordered with no operating system. In this case, the user must have:

• Windows 7 installation media

• A valid product licensing key

• Thor VM2 drivers DVD

When prompted for driver locations during installation and setup, direct the device wizard to the drivers DVD. If desired the drivers can be copied to a different media, such as a USB drive.

Upgrading the Thor VM2

There may be firmware and BIOS upgrades available for the Thor VM2. Contact Technical Assistance for upgrade information and instructions. In some cases, it may be necessary to upgrade firmware before upgrading the operating system.

Contact Technical Assistance for upgraded firmware or operating system files. Follow the upgrade instructions provided by Technical Assistance.

⚠️ The Thor VM2 must be connected to external power before upgrading the BIOS, firmware or operating systems.
If the Thor VM2 is operating on UPS battery power, the upgrade process does not initiate and the Thor VM2 is not upgraded.

Automatic Firmware Update Utility

This utility is included with Windows Embedded Standard 7 and Windows 7 Professional.

An update may be required with Windows Embedded Standard 2009 to support the automatic firmware update utility:

- If the CompactFlash drive has both a C: and D: partition the operating system may already be updated.
- If the hard drive contains just a C: partition, contact Technical Assistance for update files and installation instructions. After the update is installed, the hard drive is divided into C: and D: partitions.

The automatic firmware update utility provides an automated process to update the firmware on the Thor VM2. Firmware that can be updated includes BIOS, EC (Embedded Controller) and Screen MCU (Micro Controller Unit). Firmware updates are distributed as cabinet (.cab) files. The .cab file contains the necessary firmware files (BIOS, EC and Screen MCU) and a utility to install firmware files. The firmware update utility is installed as part of the factory software load. This utility can be used to install newer firmware or to revert to older firmware.

Use the **Software** tab of the About control panel to determine the currently installed firmware versions.

It may be necessary to update firmware before installing an updated operating system.

Requirements

The automatic firmware update utility requires the hard drive (CompactFlash card) to have both C: and D: partitions. When the Thor VM2 is shipped with either a Windows 7 Professional or Windows Embedded Standard 7 operating system, these partitions are created during the manufacturing process.

The automatic firmware update utility is not supported for a Thor VM2 with a Windows Embedded Standard 2009 operating system.

Firmware Distribution Files

The following software files must be copied to drive D: in the order listed. The files can be copied to the D: drive manually or remotely. Contact Technical Assistance for upgrade files.

FWxxyyzz.cab – This file contains the firmware update files and a utility to verify version compatibility and install the firmware files. The file name is structured such that xx identifies the last digits of the BIOS firmware version, yy identifies the Embedded Controller firmware version and zz identifies the screen MCU version.

UpdateFW.tag – The file that triggers the update utility to begin. Be sure to copy this file only after all the .cab file has been copied. As soon as the Thor VM2 detects the presence of this file, the unit reboots in five seconds.

Update Process

1. Copy the files listed above to the D: drive. Copy the.cab file first then the .tag file.

   ⚠ Be sure to copy the updatefw.tag file to the D: drive last. The Thor VM2 begins the reboot process after detecting this file.

2. The Thor VM2 automatically reboots and starts the update process after detecting the updatefw.tag file. No user intervention is required to reboot the Thor VM2 or run the update utility after the reboot. The update utility operates in a DOS screen.

3. If the update is not successful, the update is tried three more times.

4. If the update fails, drive D: is cleaned up leaving flashapp.exe, a flashlog.txt and a retry.tag file.

5. Review the flashlog.txt file. The log file lists what firmware (if any) has been installed. If an error has occurred during the update process, it is detailed in the flashlog.txt file.

6. Review the **Software** tab of the About to verify the installed firmware versions. Compare the digits from the name of the cab file (see above) with those shown in the About control panel.

Configuration Cloning Utility (CCU)

This utility is included with Windows Embedded Standard 7 and Windows 7 Professional.

An update may be required with Windows Embedded Standard 2009 to support the CCU:

- If the Thor VM2 has a CCU.exe shortcut on the desktop the operating system is already updated.

- If the CCU.exe shortcut is not present on the desktop contact Technical Assistance for update files and installation instructions.

This utility provides an automated process to read the configuration settings from one Thor VM2 and then apply those settings to one or more other Thor VM2s with the same operating system. The Configuration Cloning Utility (CCU) is installed as part of the factory software load. Configuration settings for the following items may be included:

- RFTerm
- EZ-Pair (Bluetooth)
- Honeywell Control Panels:
  - Screen blanking
  - USB powered in Sleep
  - Enable/disable touch screen
  - COM port pin 9 +5V or RI
  - EWF and HORM (Windows Embedded Standard 7 only).

The CCU allows a configuration file (ccf file) to be created by:

- Reading the current program settings from the source Thor VM2
- Reading the default program settings from a ddf file.

If desired, settings can be modified (advanced user only) before saving the ccf file. If any changes have been made, the CCU can also apply them to the source Thor VM2.

The configuration file can then be copied and deployed to the destination Thor VM2(s). Options include:

- Import changes only - Only those configuration settings which have been modified from their default value are applied to the destination Thor VM2. All other settings on the destination Thor VM2 are left unchanged.
- Import changes and defaults - All configuration settings are applied to the destination Thor VM2. If a setting was modified on the source Thor VM2 the modified value is applied to the destination Thor VM2. Otherwise the default value is applied for that setting on the destination Thor VM2.

The Configuration Cloning Utility can be run as a GUI or command line interface.

Windows Embedded Standard 7 and Windows 7 Professional:

- Before attempting to import settings from RFTerm, or Bluetooth EZPair, open the program as an administrator and make any desired changes before importing. These programs do not write to the system registry until they have been opened as an administrator.

Windows Embedded Standard 2009:

- Before attempting to import settings from RFTerm, or Bluetooth EZPair, open the program and make any desired changes before importing. These programs do not write to the system registry until they have been opened.

Launching Configuration Cloning Utility GUI

To launch the Client Configuration Utility follow the instructions below for the operating system installed on the Thor VM2.

Windows Embedded Standard 2009

1. Locate the CCU icon either on the desktop or by selecting ⊞ **(Start)** > **All Programs** > **Honeywell** > **Configuration Cloning**.

2. Double-tap the icon to launch the CCU.

Windows Embedded Standard 7 and Windows 7 Professional:

1. Locate the CCU icon either on the desktop or by selecting ⊞ **(Start)** > **All Programs** > **Honeywell** > **Configuration Cloning**.

2. Right click on the icon.

3. Select Run as administrator to launch the CCU.

> It is necessary to run the CCU as an administrator because the CCU must be able to access and make changes to the Windows registry.

> ⚠ *Rather than selecting to run as administrator each time, right click on the CCU icon and select* Properties. *Tap the* **Compatibility** *tab and check* **Run this program as an administrator**. *This modification affects the current user only unless* Change settings for all users is tapped *before changing the privilege level.*

If a User Account Control message is displayed, you must allow the CCU to make changes to the computer.

Windows Embedded Standard 2009

1. Locate the CCU icon either on the desktop or by selecting ⊞ **(Start)** > **All Programs** > **Honeywell** > **Configuration Cloning**.

2. Double-tap the icon to launch the CCU.

Windows Embedded Standard 7 and Windows 7 Professional:

1. Locate the CCU icon either on the desktop or by selecting ⊞ **(Start)** > **All Programs** > **Honeywell** > **Configuration Cloning**.

2. Right click on the icon.

3. Select Run as administrator to launch the CCU.

   It is necessary to run the CCU as an administrator because the CCU must be able to access and make changes to the Windows registry.

   ⚠️ *Rather than selecting to run as administrator each time, right click on the CCU icon and select* Properties. *Tap the* **Compatibility** *tab and check* **Run this program as an administrator**. *This modification affects the current user only unless* Change settings for all users is tapped *before changing the privilege level.*

4. If a User Account Control message is displayed, you must allow the CCU to make changes to the computer.

Using Configuration Cloning Utility GUI
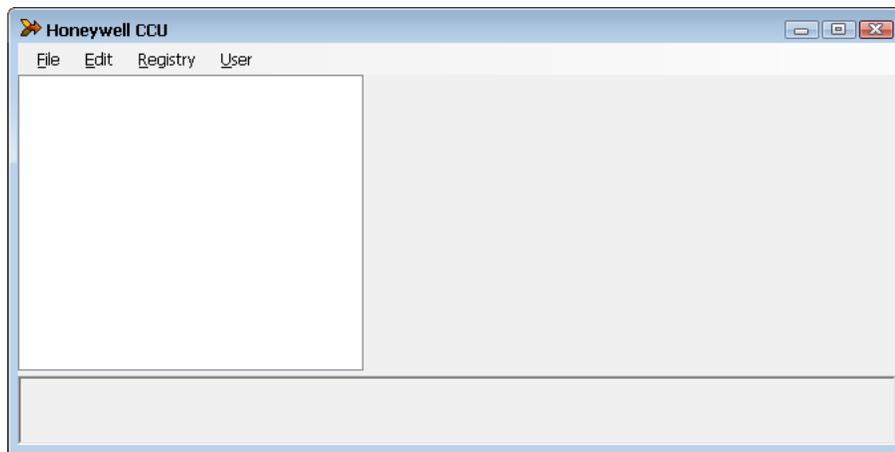
Menu Options

File

The File menu contains information for working with the configuration files.

About

Displays version and copyright information for the Configuration Cloning Utility.

Open

Opens a configuration file. The CCU looks for configuration files in the C:\Windows\DDF folder. CCU can open the following files types:

- ddf files – These files contain the factory default values for the software. These files are placed on the Thor VM2 when the applicable software was installed or upgraded. Use this option if you wish to start a configuration settings file based on the factory defaults.

- ccf files – These files contain the modified values for the software settings. These files are created with the CCU . ccf files are encrypted for security. Once a ccf file is created on one Thor VM2 it can be copied to other Thor VM2s to duplicate the configuration.

An existing ccf file can be opened, modified, applied to the Thor VM2, saved, saved with a different name, etc.

Close

Closes the open data file.

Save

Saves the open data file as a ccf file.

- If a ccf file was opened, it is saved with the same name and in the same location.
- If a ddf file was opened, a prompt is displayed for the name to assign to the new ccf file. By default a new file is saved at C:\Windows\DDF though a different location can be specified.

Save As

Saves the open data file as a ccf. If a ccf file was opened, this option allows a new name or location for the data file to be specified during the save process.

Exit

Exits the CCU. A prompt may be displayed if there are unsaved ccf changes.

Edit

Provides access to the standard Windows Cut, Copy and Paste functions. These functions can be used to manipulate the settings within the configuration file.

Registry

Reads values from and writes values to the system registry.

Import Settings

Imports the current settings from the Windows registry for the selected application(s). When selected, the available programs from which settings can be read are displayed in a tree format.

Apply Settings

Applies the current settings to the Windows registry for the selected applications. During the process, a Default all Non-Configured Parameters prompt is displayed:

- Tap Yes to set all parameters not configured in the ccf file to defaults on the destination device.
- Tap No to apply the values from the ccf file and leave all other parameters as-is on the destination device.
- Tap Cancel to exit with no changes to the destination device.

Upon completion, exit the CCU and reboot the Thor VM2 so changes can take effect.

User

Selects the desired user access level:

- Basic – Basic users can open files and import setting from the system registry. Basic users cannot modify settings from an opened file or setting imported from the registry. Basic users can apply setting to the system registry.
- Advanced – Advanced users can open files and import settings registry. Advanced users can modify the values from either an opened file or imported from the system registry. Advanced users can apply settings to the system registry.

Shortcuts

The table below lists the valid shortcut key combinations within the CCU.

Shortcut key	Action
CTRL + A	Opens About screen
CTRL + O	Opens folder with CCF files (C:\Windows\DDF)
CTRL + C	Closes the open file (only valid when a ccf or ddf file
CTRL + S	Application is saved
CTRL + E	Application is closed
CTRL + X	Cuts the data
CTRL + C	Copies the selected data to the clipboard
CTRL + V	Pastes the data from the clipboard at the current location
CTRL + I	Displays import setting list
CTRL + L	Modified settings are applied
CTRL + B	Basic settings are displayed
CTRL + D	Advanced settings are displayed

Modifying Settings

Advanced user only. Basic user cannot view the expanded tree or modify settings.

When settings have been loaded (either from **Registry** > **Import Settings** or **File** > **Open**) the following screen is displayed.
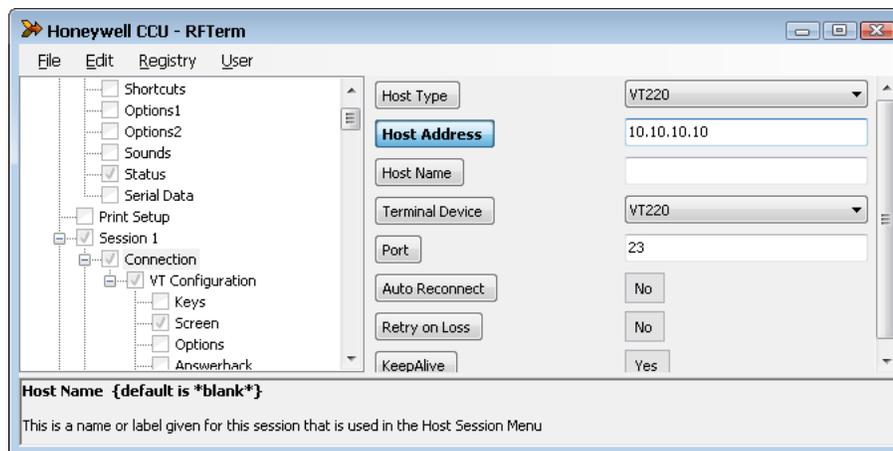
The left side of the upper pane displays the current program settings that have been imported or are part of the open ccf file. Click the + icon to expand the tree or the – icon to condense the tree. When the tree is expanded sufficiently to view the settings, the settings are displayed in the right portion of the upper pane. When a parameter is selected, the name of the parameter is highlighted in blue. The parameter name remains highlighted in blue (regardless of if the value was changed or not) until the parameter name button is tapped a second time. Enter a new value for the parameter as desired. Depending on the parameter selected, the following entry types are available:

- Text box – This is an open entry field and a new value can be typed into the text box. Depending on the parameter, there may be validity checking to ensure the entry in the text box is within the valid range.

- Pull–down list – A down arrow indicates the setting must be selected from a pull–down list of available values. Expand the list and select the desired setting from the list of options.

- Button – Items with two choices (such as Off or On) are displayed as a button. Tapping the button switches the value for the parameter.

When all desired parameter settings have been made, tap **File > Save** to save as a ccf file which can be used to deploy these settings on another Thor VM2.

If the parameter setting changes should also be applied to this Thor VM2, select **Registry > Import Settings**. After importing the settings, a reboot is necessary for the changes to take effect on the Thor VM2.

Do not attempt to modify programmable key settings within the CCU GUI. Instead, make all programmable key changes using the Programmable Key control panel before importing the OS Control Panel into the CCU.

Using the CCU

Refer to the following examples for instructions on using the CCU.

Example 1: Import the current settings and save to a file

To import the current settings from the Thor VM2 running the CCU:

1. If you want to view the settings, tap User and select Advanced.
2. Tap **Registry > Import Settings**.
3. Select the desired program(s) from which to import the settings.
4. Select **File > Save** then specify a file name and tap Save to save the settings to a ccf file.
5. The ccf file can be used to configure another Thor VM2. See Example 4.

Example 2: Modify settings on the current device and save to a file

To modify the settings on the Thor VM2 running the CCU:

1. Tap User and select Advanced.
2. Tap **Registry > Import Settings**.

3. Select the desired program(s) from which to import the settings.

4. Make any desired changes to the settings.

5. Tap **Registry > Apply Settings**

6. Select **File > Save** then specify a file name and tap Save to save the settings to a ccf file.

7. Reboot the Thor VM2 for the new settings to take effect.

8. The ccf file can be used to configure another Thor VM2. See Example 4.

Example 3: Reset a device to system defaults

To import and apply the default values to the Thor VM2 running the CCU:

1. If you want to view the default settings before applying, User and select Advanced.

2. Tap **File > Open** and change the file type to ddf files (*.ddf).

3. Select the desired ddf file(s) for the software program(s) to return to default values.

4. Tap **File > Save** and specify a file name for the ccf file.

5. Tap **Registry > Apply Settings**.

6. Reboot the Thor VM2 for the new settings to take effect.

7. The ccf file can be used to configure another Thor VM2. See Example 4.

Example 4: Clone settings to another device

1. Create a ccf file using any of the above examples.

2. Copy the ccf file to C:\Windows\DDF on the destination Thor VM2.

Note: *Rather than using the CCU GUI, the command line can be used to apply the settings to the destination device.*

3. Open the CCU on the destination device.

4. Tap **File > Open** and select the ccf file that was copied to the device.

5. Tap **Registry > Import**.

6. When prompted to Default all Non-Configured Parameters:

   • Tap Yes to set all parameters not configured in the ccf file to defaults on the destination device.

   • Tap No to apply the values from the ccf file and leave all other parameters as–is on the destination device.

   • Tap Cancel to exit with no changes to the destination device.

7. Reboot the Thor VM2 for the new settings to take effect.

Configuration Cloning Utility Command Line Interface

Note: *The CCU GUI must be closed before launching the command line interface.*

To launch the Client Configuration Utility from the command line, select ⊞ (**Start) > All Programs > Accessories** and right click on the Command Prompt icon. Select Run as administrator.

⚠ It is necessary to open the command window as an administrator because the CCU must be able to access and make changes to the Windows registry.

The command utility can be run from the installed location (C:\Program Files\Honey-well\Configuration Cloning Utility) or in portable mode (such as from a USB drive). When running in portable mode copy the following files to the USB drive:

- Configuration Cloning Utility.exe (from installation directory)
- PrivateKeyLoaded.dll (from installation directory)
- ccf file(s) (from C:\Windows\DDF or other user-specified folder)

A batch file (.bat) can be created to run the CCU commands.

Refer to the examples below to use the command line.

Example 1: Launch GUI

```
CCU.exe
```

If ran with no parameters, the GUI CCU interface is opened.

Example 2: Import settings

```
CCU.exe -import -[programs] -C:\myfile.ccf
```

Us this command line example to import the current settings from the Thor VM2 running the CCU.

Where:

import directs the CCU to read the settings from the system registry.

[programs] is replaced by one or more of the following programs from which to import settings, separated by an asterisk (*):

- RFTerm - RFTerm terminal emulation settings
- BTDRWIN7 - Bluetooth EZ Pair settings
- ThorWin7 - certain Honeywell specific control panels settings
- *.* can be used to import settings from all available programs.

C:\myfile.ccf is the path and filename assigned to the file to settings read from the device. The file must have a .ccf extension. If a file name is specified without a path, the ccf file is saved to C:\Windows\DDF.

```
CCU.exe -import -*.* -C:\myfile.ccf
```

The example above imports settings from all available programs into a file named myfile.ccf.

```
CCU.exe -import -RFTerm -C:\myfile.ccf
```

The example above imports RFTerm settings into a file named myfile.ccf.

```
CCU.exe -import -RFTerm-ThorVM3_Win7 -C:\myfile.ccf
```

The example above imports RFTerm and Honeywell control panel settings into a file named myfile.ccf.

Example 3: Apply settings

```
CCU.exe -apply -reset -e:\myfile.ccf
```

Use this command line example to read the settings from the specified ccf file and apply them to the Thor VM2 running the CCC.

Where:

apply directs the CCU to read the settings from the ccf file and apply them to the system registry.

reset is optional. When -reset is specified, all setting are reset to their default values before the customized settings in the ccf file are applied. Any prior changes made to these settings on the Thor VM2 are lost. If -reset is not specified, only the changed values in the ccf file are applied. Any other setting previously made on the Thor VM2 are retained.

E:\myfile.ccf is the path and filename of the ccf file containing the changes to be applied. If the path is not specified, the ccf file must be located at C:\Windows\DDF.

Note: *After using the -apply parameter, the Thor VM2 must be rebooted for the changes to take effect.*

```
CCU.exe -apply -e:\myfile.ccf
```

The example above applies the settings from the ccf file to the device leaving all other settings untouched.

```
CCU.exe -apply -reset -e:\myfile.ccf
```

The example above resets all values to defaults then applies the settings to the device.

WIRELESS NETWORK CONNECTIONS

Identify Wireless Configuration Utility

Depending on the operating system and regulatory domain, the 802.11 radio may be configured by one of two different utilities:

- Laird Wireless Network Configuration
- Summit Wireless Network Configuration

Network Connections Control Panel

For best results, do not use the Network Connections panel **(Start > Control Panel > Network Connections**) to disable the Summit wireless adapter. Due to a limitation of the system architecture, if the Summit wireless adapter is disabled in the Network Connections panel, it cannot be re-enabled from this control panel. Instead, the Thor VM2 must be rebooted to enable the Summit wireless adapter.

The Device Manager (**Control Panel > System > Hardware > Device Manager**) can be used to disable and enable the Summit wireless adapter without rebooting the Thor VM2.

Laird Wireless Network Configuration

The Laird client device is a Laird 802.11a/b/g/n radio, capable of 802.11a, 802.11b, 802.11g and 802.11n data rates. The radio can be configured for no encryption, WEP encryption or WPA security.

Important Notes

It is important that all dates are correct on the Thor VM2 and host computers when using any type of certificate. Certificates are date sensitive and if the date is not correct authentication will fail.
For Microsoft Windows 7 and Windows Embedded Standard 7:

It is necessary to run Laird Connection Manager (LCM) as an administrator because LCM must be able to access and make changes to the Windows registry.

Rather than selecting to run as an administrator each time, right click on the Laird Connection Manager icon and select **Properties**. Tap the **Compatibility** tab and check **Run this program as an administrator**. This modification only affects the current user unless **Change settings for all users** is tapped before changing the privilege level.
Caution: When using the 802.11a radio, the U–NII 1 band is the preferred band for indoor operation. For regulatory domains in which the U–NII 3 band is allowed, the following channels are supported: 149, 153, 157 and 161. The AP must be configured accordingly.

After making any changes to the wireless configuration, restart the Thor VM2.

Laird Connection Manager

Note: *When making changes to profile or global parameters, the device should be restarted afterwards.*

Start > **All Programs** > **Laird** > **Laird Connection Manager** *or*

Laird Connection Manager Icon on Desktop

The Status tab contains information on the current connection.

The Configuration tab is used to configure radio parameters.

The Diagnostics tab provides utilities to troubleshoot the radio.

Tray Icon

The Windows Wireless icon (located in the taskbar) displays the status of the wireless connection. The LCM tray icon is not displayed on these operating systems.

Wireless Zero Config Utility

- The WZC utility has an icon in the toolbar indicating the Wireless Zero Config application is enabled but the connection is inactive at this time (the device is not connected to a network). The WZC icon may not be visible until control is passed to the WZC utility as described below.

- You can use either the Wireless Zero Configuration Utility or the Laird Configuration Manager to connect to your network. The Laird Configuration Manager is recommended because the Wireless Zero Configuration Utility cannot control the complete set of security features of the radio.

To Switch Control to the Wireless Zero Config Utility

1. Select **Configuration > Manage Profiles > Globals**.
2. Change the value for the Supplicant property value to **Third Party**.
3. Tap **Commit**.
4. Restart the Thor VM2.

The Laird Connection Manager passes control to Wireless Zero Config and the WZC Wireless Information control panel. Using the options in the Wireless Zero Config panels, set up radio and security settings. There may be a slight delay before the Wireless Zero Config icon indicates the status of the connection.

To Switch Control to LCM

1. To switch back to LCM control, select **Configuration > Manage Profiles > Globals**.
2. Change the value for the Supplicant property value to **Laird**.
3. A message appears that a Power Cycle is required to make settings activate properly.
4. Tap **Commit**.
5. Restart the Thor VM2.

Radio control is passed to the LCM.

Start > All Programs > Laird > Laird Connection Manager > Status tab
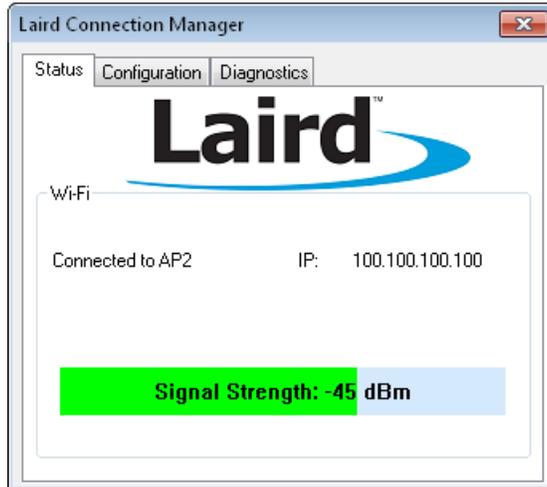
This screen provides information on the radio:

- The status of the radio card:
  - **Down** – The radio is not recognized by the LCM.
  - **Disabled** – The radio is disabled.
  - **Not Associated** – The radio has not established a connection with an access point.
  - **Associated** – The radio has made a connection to an access point but has not EAP authenticated. If the encryption type is set to WEP or None, the radio can communicate in the associated state. Otherwise the radio cannot communicate unless it is associated and EAP authenticated.
  - **Connected to (SSID)** – The radio is connected to the specified SSID.
- IP address.
- Signal strength (RSSI) displayed in dBm 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 connected.*

Configuration

Start > All Programs > Laird > Laird Connection Manager > Configuration tab

Wi-Fi Checkbox

When checked, the Wi-Fi radio is enabled. Wi-Fi is enabled by default.

Manage Profiles

Tap this button to edit an existing profile, create a new profile, delete a profile, edit global parameters or login as an admin.

Profile
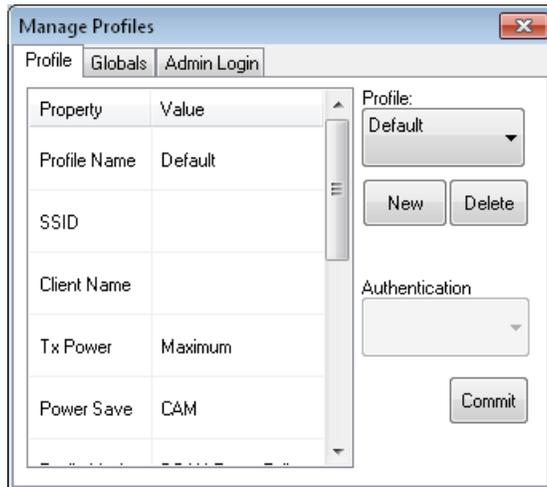
Profile:

Use the pull down list to select a previously created profile to edit or delete. The Default profile is created automatically.

New

Tap the **New** button to create a new profile. Each profile must have a unique name. Enter the name and tap **OK** to create a new profile or tap Cancel to exit without creating a profile.

Delete

Tap Delete to delete the currently highlighted profile in the Profile: drop down box. Tap Yes to delete the profile or No to exit without deleting.

Note: *You cannot delete the currently active profile.*

Parameters

The items on the **Parameters** tab only affect the selected profile.

When a property is selected from the list either a text box or a pull down list is displayed to the right for the entry of a value for that property. After changing the desired properties, tap the **Commit** button.

Property	Default Value	Explanation
Profile Name	Blank	The name entered when the profile was created. The profile can be renamed with this option.
SSID	Blank	A string of up to 32 alphanumeric characters. Establishes the Service Set Identifier (SSID) of the WLAN to which the client connects.
Client Name	Blank	A string of up to 16 characters. The client name is assigned to the network card and the device using the network card. The client name may be passed to networking wireless devices, e.g. Access Points.
Tx Power	Maximum	Maximum setting regulates Tx power to the Max power setting for the current regulatory domain. Options are: Maximum, 10%, 25%, 50%, 75%.
Power Save	Fast	Power save mode. Options are: Constantly Awake Mode (CAM), Maximum (power saving mode) and Fast (power saving mode). When using power management, use FAST for best throughput results.
Radio Mode	BGA Rates Full	Specify 802.11a, 802.11b and/or 802.11g rates when communicating with the AP. The options displayed for this parameter depend on the type of radio installed in the mobile device. Options: B rates only (1, 2, 5.5 and 11 Mbps) BG Rates Full (All B and G rates) G rates only (6, 9, 12, 18, 24, 36, 48 and 54 Mbps) Ad Hoc (when connecting to another client device instead of an AP) Default: BG Rates Full
Auth Type	Open	802.11 authentication type used when associating with the Access Point. Options are: Open or Shared.
WPA	None	None, WPA/WPSA2, WPA2
Encryption	None	Type of encryption to be used to protect transmitted data. Options are: None, WPA TKIP, AES-CCMP, or WEP.

Property	Default Value	Explanation
Authentic ation	None	Extensible Authentication Protocol (EAP) type used for 802.1x authentication to the Access Point. Options are: None, LEAP, EAP-FAST, PEAP-MSCHAP, PEAP-GTC, EAP-TLS, EAP-TTLS, PEAP-TLS, or PSK.
Fast Reauth	None	None, PMK, CCKM
Additional profile entires may be present depending on the encryption and authentication options selected.		

Globals
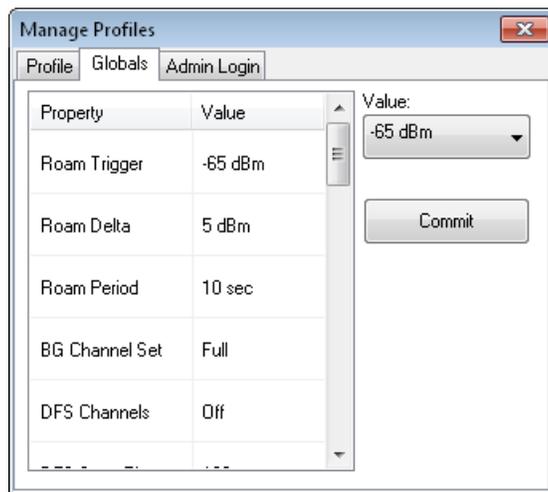
Items on the **Globals** tab affect all profiles.

When a property is selected from the list either a text box or a pull down list is displayed to the right for the entry of a value for that property. After changing the desired proper-ties, tap the **Commit** button.

Property	Default Value	Explanation
Roam Trigger	–65 dBm	If signal strength is less than this trigger value, the client looks for a different Access Point with a stronger signal. Options are: -50 dBm, -55, -60, -65, -70, -75, -80, -85, -90 dBm or Custom.
Roam Delta	5 dBm	The amount by which a different Access Point signal strength must exceed the current Access Point signal strength before roaming to the different Access Point is attempted. Options are: 5 dBm, 10, 15, 20, 25, 30, 35 dBm or Custom.
Roam Period	10 sec.	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 are: 5, 10, 15, 20, 25, 30, 35, 40, 45, 50, 55, 60 seconds or Custom.

Property	Default Value	Explanation
BG Channel Set	Full	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 are: Full (all channels) 1,6,11 (the most commonly used channels) 1,7,13 (for ETSI and TELEC radios only) or Custom.
DFS Channels	Off	Support for 5GHZ 802.11a channels where support for DFS is required. Options are: On, Off, Optimized. Not supported (always off) in some releases.
DFS Scan Time	120 ms.	The amount of time the radio will passively scan each DFS channel to see if it will receive a beacon. Recommended value is 1.5 times that of the AP's beacon period.
Ad Hoc Channel	1	Use this parameter when the Radio Mode profile parameter is set to Ad Hoc. Specifies the channel to be used for an Ad Hoc connection to another client device. If a channel is selected that is not supported by the by the radio, the default value is used. Options are: 1 through 14 (the 2.4GHz channels) 36, 40, 44, 48 (the UNII-1 channels)
Aggressive Scan	On	When set to On and the current connection to an AP weakens, the radio aggressively scans for available APs. Aggressive scanning works with standard scanning (set through Roam Trigger, Roam Delta and Roam Period). Aggressive scanning should be set to On unless there is significant co-channel interference due to overlapping APs on the same channel. Options are: On, Off
CCX Features	Optimized	Use of Cisco Compatible Extensions (CCX) radio management and AP specified maximum transmit power features. Options are: Full - Use Cisco IE and CCX version number, support all CCX features. The option known as "On" in previous versions. Optimized –Use Cisco IE and CCX version number, support all CCX features except AP assisted roaming, AP specified maximum transmit power and radio management. Off - Do not use Cisco IE and CCX version number. Cisco IE = Cisco Information Element.
WMM	Off	Use of Wi-Fi Multimedia extensions.
Auth Server	Type 1	Specifies the type of authentication server. Options are: Type 1 (ACS server) and Type 2 (non-ACS server)
TTLS Inner Method	Auto-EAP	Authentication method used within the secure tunnel created by EAP-TTLS. Options are: AUTO-EAP (Any available EAP method), MSCHAPV2, MSCHAP, PAP CHAP, EAP-MSCHAPV2

Property	Default Value	Explanation
PMK Caching	Standard	Type of Pairwise Master Key (PMK) caching to use when WPA2 is in use. PMK caching is designed to speed up roaming between APs by allowing the client and the AP to cache the results of 802.1X authentications, eliminating the need to communicate with the ACS server. Standard PMK is used when there are no controllers. The reauthentication information is cached on the original AP. The client and the AP use the cached information to perform the four-way handshake to exchange keys. Opportunistic PMK (OPMK) is used when there are controllers. The reauthentication information cached on the controllers. The client and the controller behind the AP use the cached information to perform the four-way handshake to exchange keys. If the selected PMK caching method is not supported by the network infrastructure, every roam requires full 802.11X authentication, including interaction with the ACS server. If the active profile is using WPA2 CCKM, the global PMK Caching setting is ignored and the client attempts to use CCKM. Options are: Standard, OPMK
TX Diversity	On	How to handle antenna diversity when transmitting packets to the Access Point. Options are: Main only, Aux only, and On.
RX Diversity	On-start on Main	How to handle antenna diversity when receiving packets from the Access Point. Options are: Main only, Aux only, On-start on main, and On-start on Aux.
Frag Thresh	2346	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 wireless interference. Options are: Any number between 256 bytes and 2346 bytes.
RTS Thresh	2347	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. This parameter cannot be changed.
LED	Off	The LED on the wireless card is not visible to the user when the wireless card is installed in a sealed mobile device. Options are: On, Off.
Tray Icon	N/A	The tray icon is not displayed when the Thor VM2 is running a Windows Embedded Standard 2009, Windows Embedded Standard 7 or Windows 7 Professional operating system.
Admin Password	SUMMIT (or Blank)	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 dialog box. The password is case sensitive. This value is masked when the Admin is logged out. Options are: none.
Auth Timeout	8 seconds	Specifies the number of seconds the Laird 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 are: An integer from 3 to 60.

Property	Default Value	Explanation
Certs Path	C:\Program Files\Laird\ Certs	A valid directory path, of up to 64 characters, where WPA Certificate Authority and User Certificates are stored on the mobile device when not using the Windows certificates store. Ensure the Windows folder path exists before assigning the path in this parameter. See Certificates for instructions on obtaining CA and User Certificates. This value is masked when the Admin is logged out. Options are: none. The complete path is C:\Program Files\Laird\certs
Supplicant	Laird	Selected the supplicant to be used, Laird or Third Party. When Laird is selected the LCM is used to configure the radio, When Third Party is selected the LCM is not used to configure the radio.
Auto Profile	Off	Determines if this profile

Admin Login

To login to Administrator mode, enter the admin password and tap the **Login** button.

Once logged in, the button label changes to **Logout**. The admin is automatically logged out when the LCM is exited.
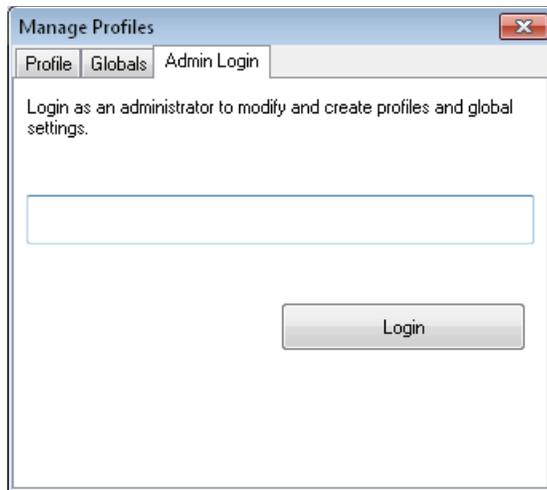
Enter the Admin password (the default password is SUMMIT and is case sensitive) and tap **OK**. If the password is incorrect, an error message is displayed.

The Administrator default password can be changed on the **Globals** tab.

The end-user can:

- Turn the radio on or off on the **Configuration** tab.
- Select an active Profile on the **Configuration** tab.
- View the current parameter settings for the profiles on the **Profile** tab.
- View the global parameter settings on the **Globals** tab.
- View the current connection details on the **Status** tab.
- View radio status, software versions and regulatory domain on the **Diagnostics** tab.

- Access additional troubleshooting features on the **Diagnostics** tab.

After Admin Login, the end-user can also:

- Create, edit, rename and delete profiles on the **Profile** tab.
- Edit global parameters on the **Globals** tab.

Diagnostics

Start > All Programs > Laird > Laird Configuration Manager > Diagnostics tab

The Diagnostics screen can be used for troubleshooting network traffic and radio connectivity issues.

This screen displays the status of the Wi-Fi radio.

- About – Use this button to view the version of the LCM and other software information.
- Advanced – Use this to access details status information, ping tools and other utilities.

Status

The Status screen shows the active profile and connection details.
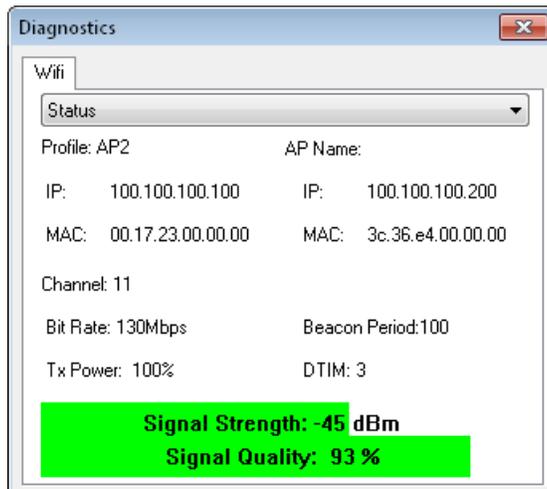
Ping

The Ping screen is used to ping another device.
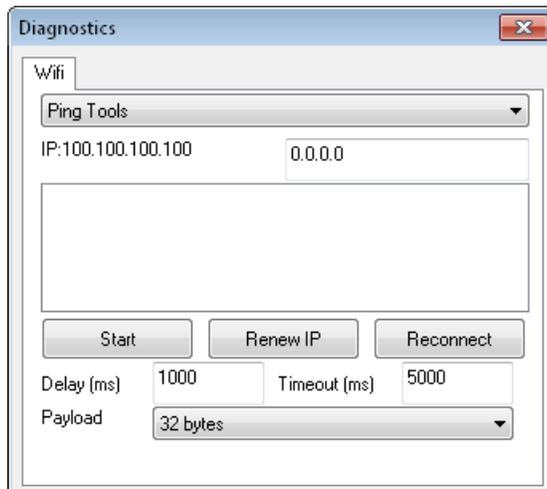
IP – Displays the IP address of the Thor VM2

Use the text box at the upper right to enter the IP address to ping. Information on the selected function is displayed in the output box in the center of the screen.

Start (Stop) - Start a continuous ping to the IP address specified in the text box in the upper right of this screen. Once the button is clicked, the ping begins and the button label changes to **Stop**. Clicking the button ends the ping. The ping also ends when any other button on this screen is clicked. The results of the ping are displayed in the output box. The parameters below are used to configure the ping process:

Parameter	Default	Description
Delay (ms)	1000	The amount of time, in milliseconds, between each ping after a **Start Ping** button tap. Options are: Any number between 0 and 30000 ms.
Timeout (ms)	5000	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 are: Any number between 0 and 30000 ms.
Payload	32 bytes	Maximum amount of data to be transmitted on a ping. Options are: 32 bytes, 64, 128, 256, 512, or 1024 bytes.

Renew IP – Obtain a new IP address through release and renew. All activity is logged in the 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.

Reconnect – 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 output box.

Utilities

This screen displays the regulatory domain and logging options.
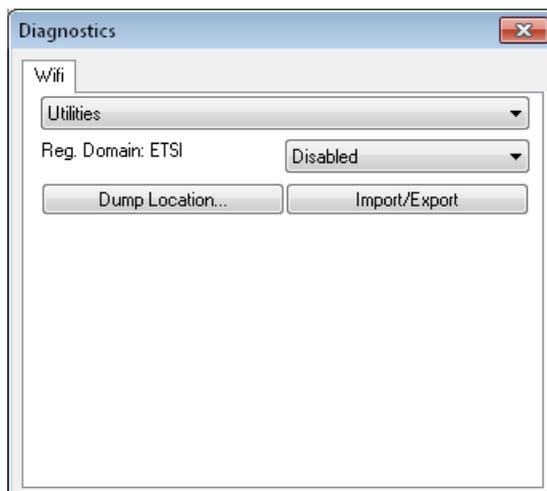
Reg. Domain - The regulatory domain for which the network card is configured.

Use the pull down list to select the desired level of logging:

Disabled (no logging, default)

1- Text (Low)

2 - Text

3 – Text (High)

4 – Serial (Low)

5 – Serial

6 – Serial (High)

Dump Location – Tap this button and browse to save the log files. Using a standard Windows explorer interface a file name and location can be specified. The default is to save the log file as sdc_diags.txt in the Windows Documents Library.

Import/Export – Use this option to import radio configuration from or export radio configuration to a file. Use the browse feature to specify location and file name.

Sign-On vs. Stored Credentials

When using wireless security that requires a user name and password to be entered, the Laird Configuration Manager offers these 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.

- When using LCM with the Thor VM2, there is an option on the **Global** tab to use the Windows user name and password to log on instead of any username and password stored in the profile.

⚠ Windows 7 Professional and Windows Embedded Standard 7 only:

The credentials login and password entry window may not always display in the foreground. When the Thor VM2 attempts to connect to the network, click the flashing icon in the Notification bar to display the login screen. Enter the user name and password and click **OK** to close the window. This procedure may need to be followed after the following events:

- The Thor VM2 returns from sleep, hibernate or sleep

- The Thor VM2 is restarted

- A different active profile is selected from the **Configuration** tab

- Invalid credentials have been entered

To Use Stored Credentials

1. After completing the other entries in the profile, scroll down for the credentials entry.
2. Enter the Username and Password.
3. Click the **Commit** button.
4. For LEAP and WPA/LEAP, configuration is complete.
5. Importing the CA certificate into the Windows certificate store is optional.
6. For EAP-TLS, import the User Certificate into the Windows certificate store.
7. Return to the **Profile** tab.
8. Select the CA certificate. The certificate can be specified by file name (from the Certs path), a certificate selected from the Windows certificate store or the full certificate store.
9. For EAP-TLS, select the User Cert (User Certificate filename).
10. If using EAP FAST and manual PAC provisioning, input the PAC filename and password.
11. Click the **Commit** button.

12. If changes are made to the stored credentials, click **Commit** to save those changes before making any additional changes to the profile or global parameters.

13. 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.

Note: *See Configuring the Profile for more details.*

Note: *If invalid credentials are entered into the stored credentials, the authentication will fail. No error message is displayed. The user may or may not be prompted to enter valid credentials.*

To Use Sign On Screen

1. After completing the other entries in the profile, leave the user name and password blank.

2. Importing the CA certificate into the Windows certificate store is optional.

3. For EAP-TLS, import the User Certificate into the Windows certificate store.

4. Select the CA certificate. The certificate can be specified by file name (from the Certs path), a certificate selected from the Windows certificate store or the full certificate store.

5. For EAP-TLS, select the User Cert (User Certificate filename).

6. If using EAP FAST and manual PAC provisioning, input the PAC filename and password.

7. Click 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.

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.

Note: *See Configuring the Profile for more details.*

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 tab **Diags** tab is clicked or
- the profile is modified and the **Commit** button is clicked.

Windows Certificate Store vs. Certs Path

Note: *It is important that all dates are correct on the Thor VM2 and host computers when using any type of certificate. Certificates are date sensitive and if the date is not correct authentication will fail.*

⚠ If using the Windows Certificate Store, the Windows Account must have a password. The password cannot be left blank. The Laird Configuration Manager uses the Windows user account credentials to access the Certificate Store. The Windows user account credentials need not be the same as the credentials entered in the Laird Configuration Manager.

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, see Generate a User Certificate.
- To import the user certificate into the Windows certificate store, see Install a User Certificate.
- A Root CA certificate is also needed. Refer to the section below.

Root CA Certificates

Root CA certificates are required for EAP/TLS, PEAP/GTC and PEAP/MSCHAP. Two options are offered for storing these certificates. They may be imported into the Windows certificate store or copied into the Certs Path directory.

Certs Path

1. See Generate a Root CA Certificate and follow the instructions to download the Root Certificate to a PC.
2. Copy the certificate to specified directory on the mobile device. The default location for Certs Path is C:\Program Files\Laird\certs. A different location may be specified by using the Certs Path global variable.
3. On the **Profile** tab, select **File Name** for the CA Cert property
4. Enter the certificate name in the pop-up window and tap **OK**.
5. Tap **Commit** to save the profile changes.

Windows Certificate Store

1. See Generate a Root CA Certificate and follow the instructions to download the Root Certificate to a PC.
2. To import the certificate into the Windows store, See Install a Root CA Certificate.
3. Either a specific certificate or the whole certificate store can be used.
   - On the **Profile** tab, choose **Use Full MS Store** to use all certificates in the store.

- On the **Profile** tab, choose **Select Cert for the CA Cert** property. From the pop-up window, select the desired certificate and tap **OK**.

4. Tap **Commit** to save the profile changes.

Configuring the Profile

Use the instructions in this section to complete the entries on the **Profile** tab according to the type of wireless security used by your 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:

- From the **Configuration** tab tap **Manage Profiles > Admin Login**. Enter the password and tap Login.

- If using a single profile, edit the default profile with the parameters for your network. Select the Default profile from the pull-down menu.

- 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.

IMPORTANT – Remember to click the **Commit** button after making changes to ensure the changes are saved. The LCM may display a reminder if the **Commit** button is not clicked before an attempt is made to close or browse away from the tab in focus if there are unsaved changes.

If changes are made to the *stored credentials*, click **Commit** to save those changes first before making any additional changes.

No Security

To connect to a wireless network with no security, make sure the following profile options are used.

1. Enter the SSID of the Access Point assigned to this profile

2. Set Auth Type to Open

3. Set WPA to None

4. Set Encryption to None

5. Set Authentication to None
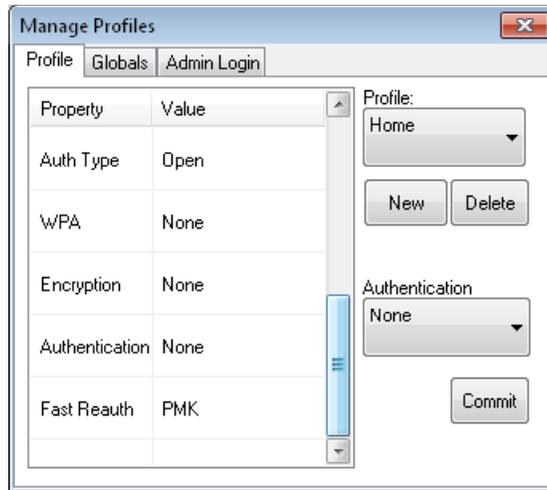
Once configured, click the **Commit** button.

Ensure the correct Active Profile is selected on the **Configuration** tab and restart. The **Status** tab shows the device is connected.

To connect using WEP, make sure the following profile options are used.

1. Enter the SSID of the Access Point assigned to this profile
2. Set Auth Type to Open
3. Set WPA to None
4. Set Encryption to WEP
5. Set Authentication to None

Scroll down to enter the WEP key(s).

Valid keys are 10 hexadecimal or 5 ASCII characters (for 40-bit encryption) or 26 hexa-decimal or 13 ASCII characters (for 128-bit encryption). Enter the key(s) and click **Commit**.

Ensure the correct Active Profile is selected on the **Configuration** tab and restart. The **Status** tab shows the device is connected.

To use LEAP (without WPA, also called WEP-LEAP), make sure the following profile options are used.

1. Enter the SSID of the Access Point assigned to this profile

2. Set Auth Type as follows:

- If the Cisco/CCX certified AP is configured for open authentication, set Auth Type to Open.

- If the AP is configured to use shared key or passphrase, set Auth Type to Shared.

3. Set WPA to None

4. Set Encryption to WEP
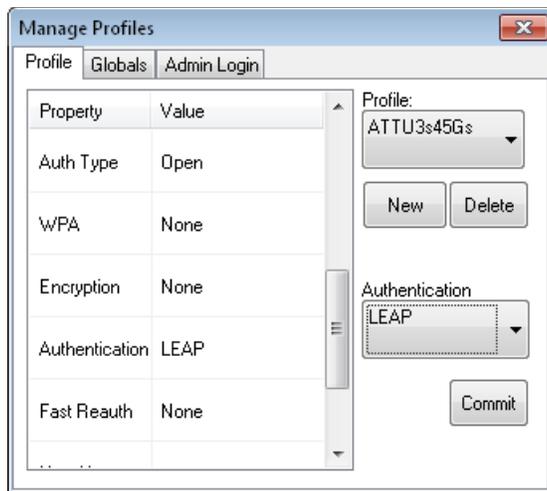
5. Set Authentication to LEAP

See Sign-On vs. Stored Credentials for information on entering credentials.

To use Stored Credentials, scroll down to enter the User Name and Password. No entries are necessary for Sign-On Credentials as the user will be prompted for the Username and Password when connecting to the network.
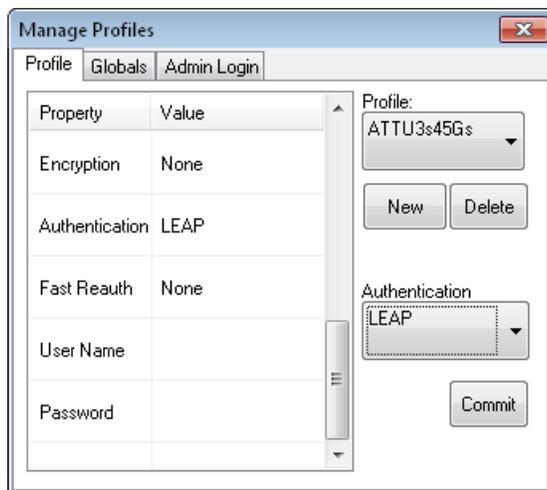
Enter the Domain\Username (if the Domain is required), otherwise enter the Username then click **Commit**.

Ensure the correct Active Profile is selected on the **Configuration** tab and restart. The **Status** tab shows the device is connected.

PEAP/MSCHAP

To use PEAP/MSCHAP, make sure the following profile options are used.

1. Enter the SSID of the Access Point assigned to this profile
2. Set Auth Type to Open
3. Set WPA as follows:
- Select WPA/WPA2 to use either TKIP/AES or AES-CCMP
- Select WPA2 to use AEX-CCMP
4. Set Encryption to either TKIP/AES or AES-CCMP depending on WPA type selected
5. Set Authentication to PEAP-MSCHAP

See Sign-On vs. Stored Credentials for information on entering credentials.

Scroll down to enter credentials:.

- 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.

Enter the Domain\Username (if the Domain 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 **Configuration** tab.

See Windows Certificate Store vs. Certs Path for more information on certificate storage.

Once successfully authenticated, import the CA certificate into the Windows certificate store. Return to the Credentials screen and check the Validate server checkbox.

If using the Windows certificate store:

1. Check the Use MS store checkbox. The default is to use the Full Trusted Store.
2. To select an individual certificate, click on the **Browse** button.
3. Uncheck the **Use full trusted store** checkbox.
4. Select the desired certificate and click Select. You are returned to the Credentials screen.
5. Click **OK** then click **Commit**.

If using the Certs Path option:

1. Leave the Use MS store box unchecked.
2. Enter the certificate filename in the CA Cert text box.
3. Click **OK** then click **Commit**.

The device should be authenticating the server certificate and using PEAP/MSCHAP for the user authentication.

Ensure the correct Active Profile is selected on the **Configuration** tab and restart. The **Status** tab shows the device is connected.

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.

1. Enter the SSID of the Access Point assigned to this profile
2. Set Auth Type to Open
3. Set WPA as follows:
* Select WPA/WPA2 to use either TKIP/AES or AES-CCMP
* Select WPA2 to use AEX-CCMP
4. Set Encryption to either TKIP/AES or AES-CCMP depending on WPA type selected
5. Set Authentication to PEAP/GTC

See Sign-On vs. Stored Credentials for information on entering credentials.

Scroll down to enter credentials.

* 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.

Enter these items as directed below.

Enter the Domain\Username (if the Domain 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 **Config-uration** tab.

See Windows Certificate Store vs. Certs Path for more information on certificate storage.

Once successfully authenticated, import the CA certificate into the Windows certificate store. Return to the Credentials screen and check the Validate server checkbox.

Note: *Some servers may be configured to allow only a single use of the password for PEAP/GTC. In this case, wait for the token to update with a new password before attempting to validate the server. Then enter the new password, check the Validate Server checkbox and proceed with the certificate process below.*

If using the Windows certificate store:

1. Check the Use MS store checkbox. The default is to use the Full Trusted Store.
2. To select an individual certificate, click on the **Browse** button.
3. Uncheck the **Use full trusted store** checkbox.
4. Select the desired certificate and click Select. You are returned to the Credentials screen.
5. Click **OK** then click **Commit**.

If using the Certs Path option:

1. Leave the Use MS store box unchecked.
2. Enter the certificate filename in the CA Cert text box.
3. Click **OK** then click **Commit**.

The device should be authenticating the server certificate and using PEAP/GTC for the user authentication.

Ensure the correct Active Profile is selected on the **Configuration** tab and restart. The **Status** tab shows the device is connected.

Note: *The date must be properly set on the device to authenticate a certificate.*

To use WPA/LEAP, make sure the following profile options are used.

1. Enter the SSID of the Access Point assigned to this profile

2. Set Auth Type as follows:

- If the Cisco/CCX certified AP is configured for open authentication, set Auth Type to Open.

- If the AP is configured to use shared key or passphrase, set Auth Type to Shared.

3. Set WPA as follows:

- Select WPA/WPA2 to use either TKIP/AES or AES-CCMP

- Select WPA2 to use AEX-CCMP

4. Set Encryption to either TKIP/AES or AES-CCMP depending on WPA type selected

5. Set Authentication to LEAP

See Sign-On vs. Stored Credentials for information on entering credentials.

Scroll down to enter credentials. No entries are necessary for Sign-On Credentials as the user will be prompted for the Username and Password when connecting to the network.
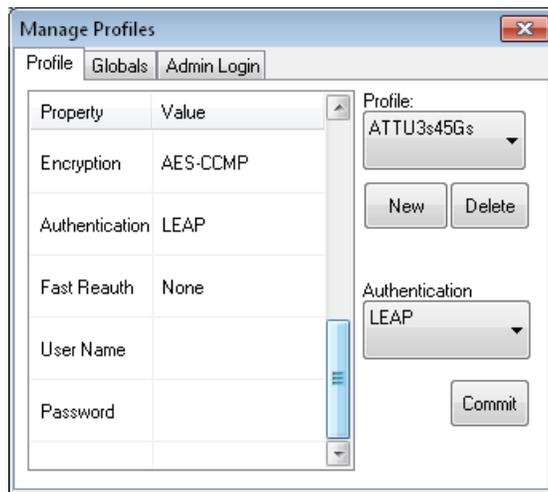
Enter the Domain\Username (if the Domain is required), otherwise enter the Username.

Enter the password.
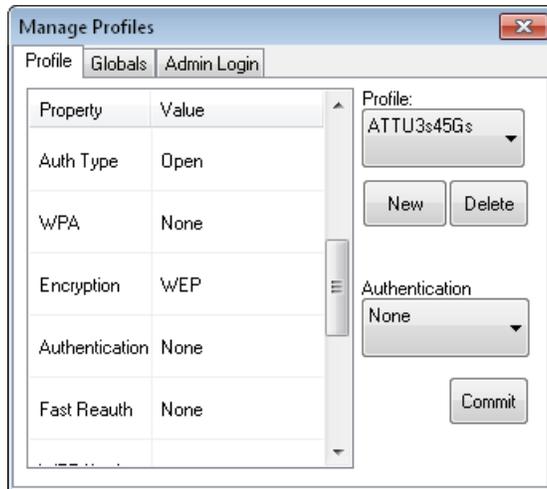
Click the **Commit** button.

Ensure the correct Active Profile is selected on the **Configuration** tab and restart. The **Status** tab shows the device is connected.
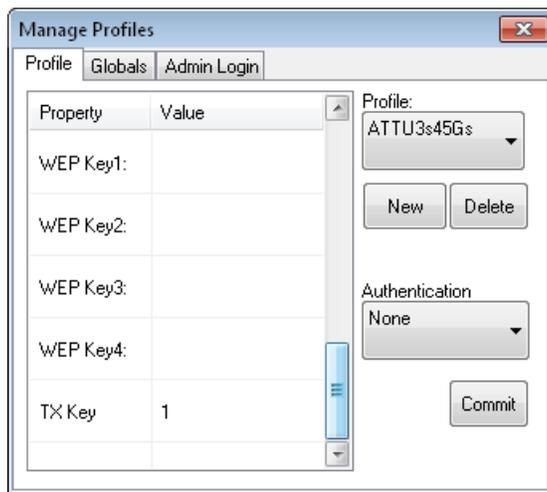
EAP-FAST

To use EAP-FAST, make sure the following profile options are used.

1. Enter the SSID of the Access Point assigned to this profile
2. Set Auth Type to Open
3. Set WPA as follows:
- Select WPA/WPA2 to use either TKIP/AES or AES-CCMP
- Select WPA2 to use AEX-CCMP
4. Set Encryption to either TKIP/AES or AES-CCMP depending on WPA type selected
5. Set Authentication to EAP-FAST

The LCM 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 Thor VM2.

For automatic PAC provisioning, once a username/password is authenticated, the PAC information is stored on the Thor VM2. The same username/password must be used to authenticate each time. See the note below for more details.

For manual PAC provisioning, the PAC filename and Password must be entered.

See Sign-On vs. Stored Credentials for information on entering credentials.

Scroll down to enter credentials. The entries necessary are determined by the type of credentials (stored or sign on) and the type of PAC provisioning (automatic or manual).

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.

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 Domain 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.

Ensure the correct Active Profile is selected on the **Configuration** tab and restart. The **Status** tab shows the device is connected.

Note: *When using Automatic PAC Provisioning, once authenticated, there is a file stored in the C:\Program Files\Laird\certs directory with the PAC credentials. If the username is changed, that file must be deleted. The filename is* `autoP.00.pac`*.*

To use EAP-TLS, make sure the following profile options are used.

1. Enter the SSID of the Access Point assigned to this profile
2. Set Auth Type to Open
3. Set WPA as follows:
- Select WPA/WPA2 to use either TKIP/AES or AES-CCMP
- Select WPA2 to use AEX-CCMP
4. Set Encryption to either TKIP/AES or AES-CCMP depending on WPA type selected
5. Set Authentication to EAP-TLS

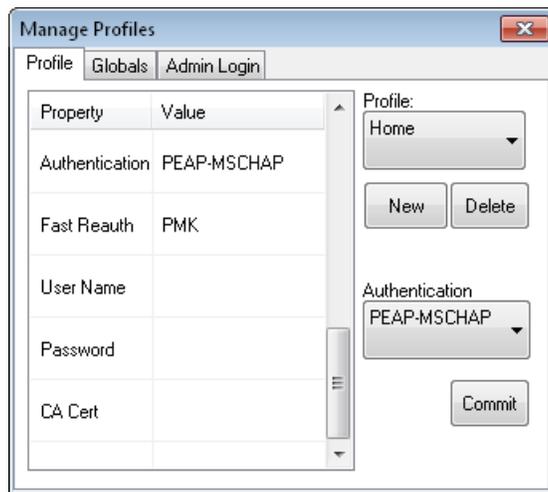See Sign-On vs. Stored Credentials for information on entering credentials.

Scroll down to enter credentials.

- 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 when connecting to the network.
- For Stored Credentials, User Certificate Filename and the CA Certificate Filename must be entered.

Enter these items as directed below.

Enter the Domain\Username (if the Domain is required), otherwise enter the Username.

Select a user certificate from the Windows certificate store. 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.

Some versions of the LCM require a User Cert password. If this entry field is present, enter the password for the user certificate in the User Cert pwd box.

If there are no user certificates in the Windows certificate store, follow these instructions for Generate a User Certificate and Install a User Certificate.

See Windows Certificate Store vs. Certs Path for more information on CA certificate storage.

Check the Validate server checkbox.

If using the Windows certificate store:

1. Check the Use MS store checkbox. The default is to use the Full Trusted Store.
2. To select an individual certificate, click on the **Browse** button.
3. Uncheck the **Use full trusted store** checkbox.
4. Select the desired certificate and click Select. You are returned to the Credentials screen.
5. Click **Commit**.

If using the Certs Path option:

1. Leave the Use MS store box unchecked.
2. Enter the certificate filename in the CA Cert text box.
3. Click **Commit**.

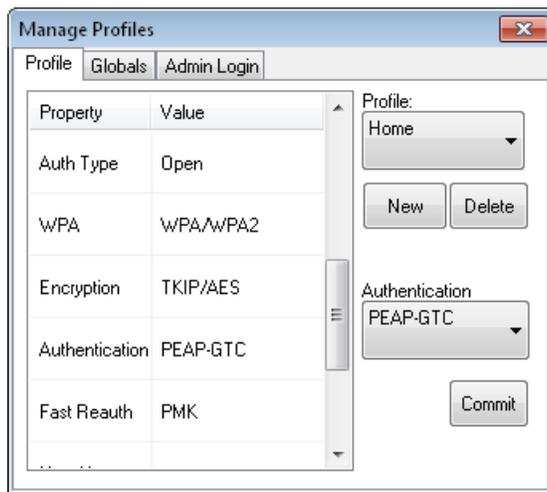The Thor VM2 should be authenticating the server certificate and using EAP-TLS for the user authentication.

Ensure the correct Active Profile is selected on the **Configuration** tab and restart. The **Status** tab shows the device is connected.

See Certificates for information on generating a Root CA certificate or a User certificate.

Note: *The date must be properly set on the device to authenticate a certificate.*

To use EAP-TTLS, make sure the following profile options are used.

1. Enter the SSID of the Access Point assigned to this profile
2. Set Auth Type to Open
3. Set WPA as follows:
*   Select WPA/WPA2 to use either TKIP/AES or AES-CCMP
*   Select WPA2 to use AEX-CCMP
4. Set Encryption to either TKIP/AES or AES-CCMP depending on WPA type selected
5. Set Authentication to EAP-TTLS
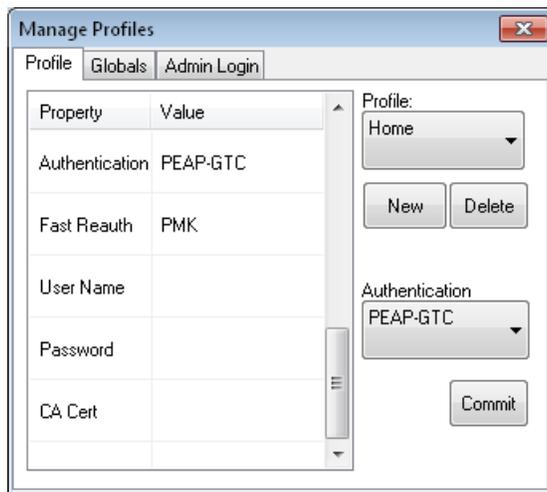

See Sign-On vs. Stored Credentials for information on entering credentials.

Scroll down to enter credentials:.

*   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.

Enter the Domain\Username (if the Domain 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 **Configuration** tab.

See Windows Certificate Store vs. Certs Path for more information on certificate storage.

Once successfully authenticated, import the CA certificate into the Windows certificate store. Return to the Credentials screen and check the Validate server checkbox.

If using the Windows certificate store:

1. Check the Use MS store checkbox. The default is to use the Full Trusted Store.

2. To select an individual certificate, click on the **Browse** button.

3. Uncheck the **Use full trusted store** checkbox.

4. Select the desired certificate and click Select. You are returned to the Credentials screen.

5. Click **OK** then click **Commit**.

If using the Certs Path option:

1. Leave the Use MS store box unchecked.

2. Enter the certificate filename in the CA Cert text box.

3. Click **OK** then click **Commit**.

The device should be authenticating the server certificate and using PEAP/MSCHAP for the user authentication.
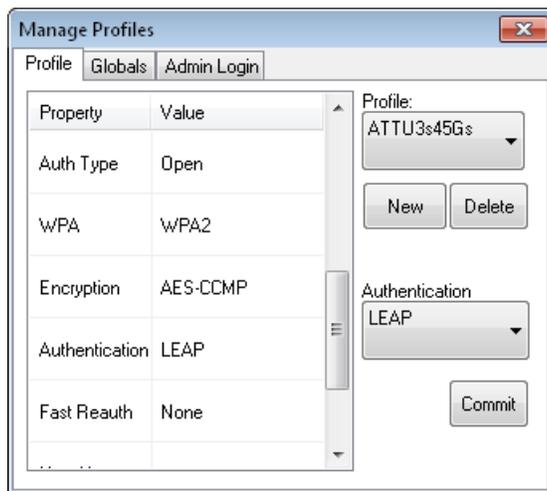
Ensure the correct Active Profile is selected on the **Configuration** tab and restart. The **Status** tab shows the device is connected.

**Note:** *The date must be properly set on the device to authenticate a certificate.*

PEAP-TLS

To use PEAP-TLS, make sure the following profile options are used.

1. Enter the SSID of the Access Point assigned to this profile
2. Set Auth Type to Open
3. Set WPA as follows:
- Select WPA/WPA2 to use either TKIP/AES or AES-CCMP
- Select WPA2 to use AEX-CCMP
4. Set Encryption to either TKIP/AES or AES-CCMP depending on WPA type selected
5. Set Authentication to PEAP-TLS

See Sign-On vs. Stored Credentials for information on entering credentials.

Scroll down to enter credentials.

- 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 when connecting to the network.
- For Stored Credentials, User Certificate Filename and the CA Certificate Filename must be entered.

Thor VM2 with with Microsoft Windows 7 or Windows Embedded Standard User Guide 247

Enter these items as directed below.

Enter the Domain\Username (if the Domain is required), otherwise enter the Username.

Select a user certificate from the Windows certificate store. 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.

Some versions of the LCM require a User Cert password. If this entry field is present, enter the password for the user certificate in the User Cert pwd box.

If there are no user certificates in the Windows certificate store, follow these instructions for Generate a User Certificate and Install a User Certificate.

See Windows Certificate Store vs. Certs Path for more information on CA certificate storage.

Check the Validate server checkbox.

If using the Windows certificate store:

1. Check the Use MS store checkbox. The default is to use the Full Trusted Store.

2. To select an individual certificate, click on the **Browse** button.

3. Uncheck the **Use full trusted store** checkbox.

4. Select the desired certificate and click Select. You are returned to the Credentials screen.

5. Click **Commit**.

If using the Certs Path option:

1. Leave the Use MS store box unchecked.

2. Enter the certificate filename in the CA Cert text box.

3. Click **Commit**.

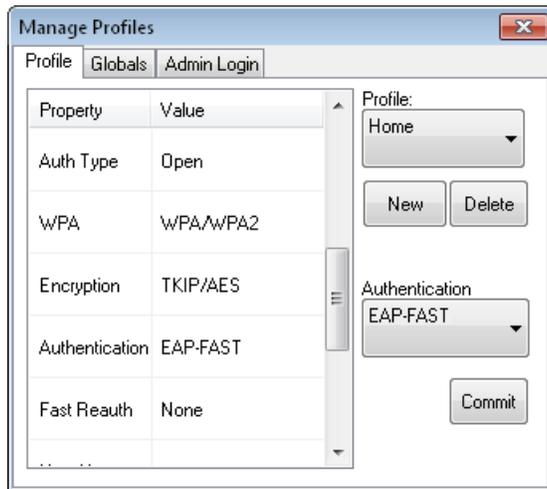The Thor VM2 should be authenticating the server certificate and using EAP-TLS for the user authentication.

Ensure the correct Active Profile is selected on the **Configuration** tab and restart. The **Status** tab shows the device is connected.

See Certificates for information on generating a Root CA certificate or a User certificate.

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:

1. Enter the SSID of the Access Point assigned to this profile
2. Set Auth Type to Open
3. Set WPA as follows:
- Select WPA/WPA2 to use either TKIP/AES or AES-CCMP
- Select WPA2 to use AEX-CCMP
4. Set Encryption to either TKIP/AES or AES-CCMP depending on WPA type selected
5. Set Authentication to PSK
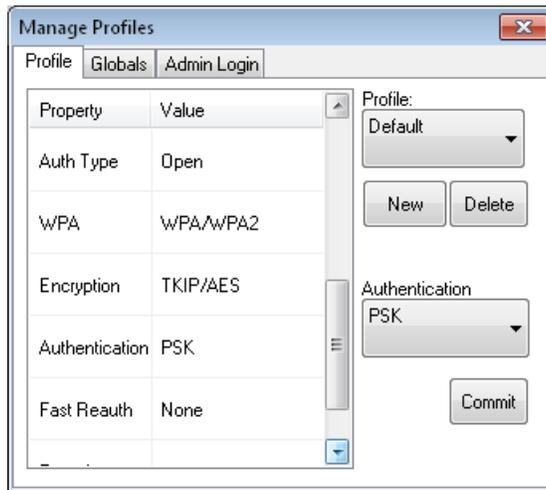
Click the **WEP keys/PSKs** button.
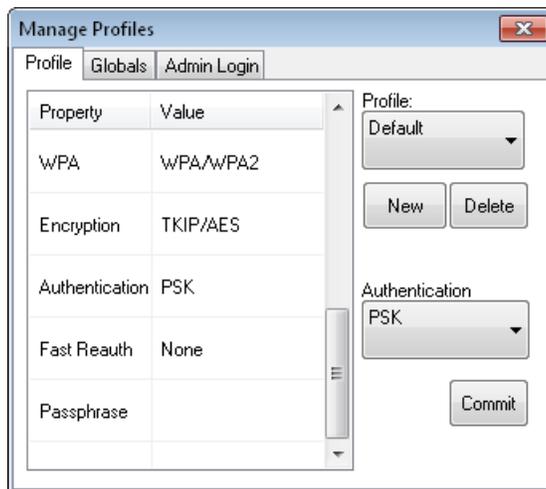
This value can be 64 hex characters or an 8 to 63 byte ASCII value. Enter the key and click **OK**.
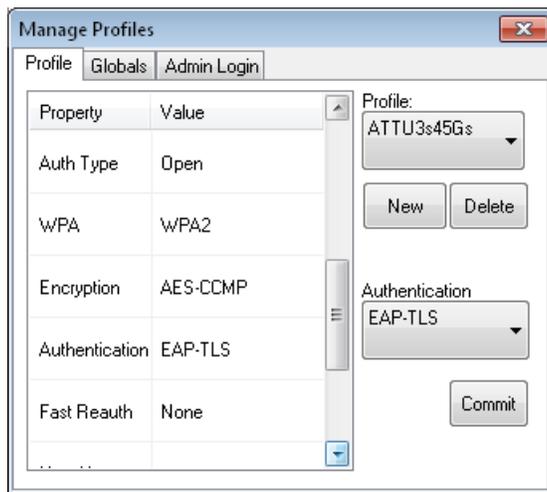
Once configured, click the **Commit** button.

Ensure the correct Active Profile is selected on the **Configuration** tab and restart. The **Status** tab shows the device is connected.

Summit Wireless Network Configuration

The Summit client device is a Summit 802.11a/b/g/n radio, capable of 802.11a, 802.11b, 802.11g and 802.11n data rates. The radio can be configured for no encryption, WEP encryption or WPA security.

Important Notes

It is important that all dates are correct on the Thor VM2 and host computers when using any type of certificate. Certificates are date sensitive and if the date is not correct authentication will fail.
For Microsoft Windows 7 and Windows Embedded Standard 7:

It is necessary to run Laird Connection Manager (LCM) as an administrator because LCM must be able to access and make changes to the Windows registry.

Rather than selecting to run as an administrator each time, right click on the Laird Connection Manager icon and select **Properties**. Tap the **Compatibility** tab and check **Run this program as an administrator**. This modification only affects the current user unless **Change settings for all users** is tapped before changing the privilege level.
It may be necessary to upgrade radio software in order to use certain Summit Client Utility (SCU) features. Contact Technical Assistance for details.

Caution: **When using the 802.11a radio, the U–NII 1 band is the preferred band for indoor operation. For regulatory domains in which the U–NII 3 band is allowed, the following channels are supported: 149, 153, 157 and 161. The AP must be configured accordingly.**

After making any changes to the wireless configuration, restart the Thor VM2.

Summit Client Utility

Note: *When making changes to profile or global parameters, the device should be restarted afterwards.*

Start > **All Programs** > **Summit** > **Summit Client Utility** *or*

SCU Icon on Desktop *or*

Summit Tray Icon (if present) *or*

Wi-FI Icon in the Windows Control Panel (if present)

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.

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.

Summit Tray Icon

The Summit tray icon is not shown when the Thor VM2 is running Windows Embedded Standard 2009, Windows Embedded 7 or Windows 7 Professional.

The Windows Wireless icon (located in the taskbar) may not display a successful wireless connection. The SCU **Main** tab should be used to verify the success of the connection instead.

Wireless Zero Config Utility

- The WZC utility has an icon in the toolbar indicating the Wireless Zero Config application is enabled but the connection is inactive at this time (the device is not connected to a network). The WZC icon may not be visible until control is passed to the WZC utility as described below.

- You can use either the Wireless Zero Configuration Utility or the Summit Client Utility to connect to your network. The Summit Client Utility is recommended because the Wireless Zero Configuration Utility cannot control the complete set of security features of the radio.

To Switch Control to the Wireless Zero Config Utility

1. Select ThirdPartyConfig in the Active Profile drop down box on the **Main** tab.
2. A message appears that a Power Cycle is required to make settings activate properly.
3. Tap **OK**.
4. Restart the Thor VM2.

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, set up radio and security settings. There may be a slight delay before the Wireless Zero Config icon indicates the status of the connection.

To Switch Control to SCU

1. To switch back to SCU control, select any other profile except ThirdPartyConfig in the SCU Active Config drop down list on the **Main** tab.
2. A message appears that a Power Cycle is required to make settings activate properly.
3. Tap **OK**.
4. Restart the Thor VM2.

Radio control is passed to the SCU.

Main

Start > All Programs > Summit > Summit Client Utility > Main tab

Factory Default Settings

Admin Login	SUMMIT
Radio	Enabled
Active Config/Profile	Default
Regulatory Domain	FCC, ETSI or Worldwide

The **Main** tab displays information about the wireless client device including:

- SCU (Summit Client Utility) version

- Driver version

- Radio Type (ABGN is an 802.11 a/b/g/n radio).

- Regulatory Domain

- Copyright Information can be accessed by tapping the **About SCU** button

- Active Config profile / Active Profile name

- Status of the client (Down, Associated, Authenticated, etc.).

The Active Profile can be switched without logging in to Admin mode. Selecting a different profile from the drop down list does not require logging in to Administrator mode. The profile must already exist. Profiles can be created or edited after the Admin login password has been entered and accepted.

When the profile named "ThirdPartyConfig" is chosen as the active profile, the Summit Client Utility passes control to Wireless Manager for configuration of all client and security settings for the network module.

The **Disable Radio** button can be used to disable the network card. Once disabled, the button label changes to **Enable Radio**. By default the radio is enabled.

The **Admin Login** button provides access to editing wireless parameters. Profile and Global may only be edited after entering the Admin Login password.

The password is case-sensitive.

Once logged in, the button label changes to **Admin Logout**. To logout, either tap the **Admin Logout** button or exit the SCU without tapping the **Admin Logout** button.

Admin Login

To login to Administrator mode, tap the **Admin Login** button.

Once logged in, the button label changes to **Admin Logout**. The admin is automatically logged out when the SCU is exited. The Admin can either tap the **Admin Logout** button, or the **OK** button to logout.

Enter the Admin password (the default password is SUMMIT and is case sensitive) and tap **OK**. If the password is incorrect, an error message is displayed.

The Administrator default password can be changed on the **Global** tab.

The end-user can:

- Turn the radio on or off on the **Main** tab.

- Select an 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 radio status, software versions and regulatory domain on the **Main** tab.

- Access additional troubleshooting features on the **Diags** tab.

After Admin Login, the end-user can also:

- Create, edit, rename and delete profiles on the **Profile** tab.

- Edit global parameters on the **Global** tab.

- Enable/disable the Summit tray icon in the taskbar.

Profile

Start > All Programs > Summit > Summit Client Utility > Profile tab

Note: *Tap the **Commit** button to save changes before leaving this panel or the SCU. If the panel is exited before tapping the **Commit** button, changes are not saved!*

Factory Default Settings

Profile	Default
SSID	Blank
Client Name	Blank
Power Save	CAM

Tx Power	Maximum
Bit Rate	Auto
Radio Mode	BGA rates full
Auth Type	Open
EAP Type	None
Encryption	None

When logged in as an Admin use the **Profile** tab to manage profiles. When not logged in as an Admin, the parameters can be viewed, and cannot be changed. The buttons on this tab are dimmed if the user is not logged in as Admin. The **Profile** tab was previously labeled Config.

Buttons

Button	Function
Commit	Saves the profile settings made on this screen. Settings are saved in the profile.
Credentials	Allows entry of a username and password, certificate names, and other information required to authenticate with the access point. The information required depends on the EAP type.
Delete	Deletes the profile. The current active profile cannot be deleted and an error message is displayed if a delete is attempted.
New	Creates a new profile with the default settings (see Profile Parameters) and prompts for a unique name. If the name is not unique, an error message is displayed and the new profile is not created.
Rename	Assigns a new, unique name. If the new name is not unique, an error message is displayed and the profile is not renamed.
Scan	Opens a window that lists access points that are broadcasting their SSIDs. Tap the **Refresh** button to view an updated list of APs. Each AP's SSID, its received signal strength indication (RSSI) and whether or not data encryption is in use (true or false). Sort the list by tapping on the column headers. If the scan finds more than one AP with the same SSID, the list displays the AP with the strongest RSSI and the least security. If you are logged in as an Admin, tap an SSID in the list and tap the **Configure** button, you return to the Profile window to recreate a profile for that SSID, with the profile name being the same as the SSID (or the SSID with a suffix such as "_1" if a profile with the SSID as its name exists already).
WEP Keys / PSK Keys	Allows entry of WEP keys or pass phrase as required by the type of encryption.

Note: *Unsaved Changes – The SCU will display a reminder if the **Commit** button is not clicked before an attempt is made to close or browse away from this tab.*

Important – The settings for Auth Type, EAP Type and Encryption depend on the security type chosen.

Profile Parameters

Parameter	Default	Explanation
Edit Profile	Default	A string of 1 to 32 alphanumeric characters, establishes the name of the Profile. Options are Default or ThirdPartyConfig.
SSID	Blank	A string of up to 32 alphanumeric characters. Establishes the Service Set Identifier (SSID) of the WLAN to which the client connects.
Client Name	Blank	A string of up to 16 characters. The client name is assigned to the network card and the device using the network card. The client name may be passed to networking wireless devices, e.g. Access Points.
Power Save	CAM	Power save mode. Options are: Constantly Awake Mode (CAM) power save off, Maximum (power saving mode) and Fast (power saving mode). When using power management, use FAST for best throughput results.
Tx Power	Maximum	Maximum setting regulates Tx power to the Max power setting for the current regulatory domain. Options are: Maximum, 50mW, 30mW, 20mW, 10mW, 5mW, or 1mW.
Bit Rate	Auto	Setting the rate to Auto will allow the Access Point to automatically negotiate the bit rate with the client device. Options are: Auto, 1 Mbit, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48 or 54 Mbit.
Auth Type	Open	802.11 authentication type used when associating with the Access Point. Options are: Open, LEAP, or Shared key.
EAP Type	None	Extensible Authentication Protocol (EAP) type used for 802.1x authentication to the Access Point. Options are: None, LEAP, EAP-FAST, PEAP-MSCHAP, PEAP-GTC, PEAP-TLS, EAP-TTLS, or EAP-TLS. EAP Type chosen determines whether the **Credentials** button is active and also determines the available entries in the Credentials pop-up window.
Encryption	None	Type of encryption to be used to protect transmitted data. Available options may vary by SCU version. Options are: None, WEP (or Manual WEP), WEP EAP (or Auto WEP), WPA PSK, WPA TKIP, WPA CCKM, WPA2 PSK, WPA2 AES, or WPA2 CCKM. CKIP is not supported in the Thor VM2. *Note:* *The Encryption type chosen determines if the **WEP Keys / PSK Keys** button is active and also determines the available entries in the WEP or PSK pop-up window.*
Radio Mode	BGA Rates Full	Specify 802.11a, 802.11b and/or 802.11g rates when communicating with the AP. The options displayed for this parameter depend on the type of radio installed in the mobile device. Options: B rates only (1, 2, 5.5 and 11 Mbps) BG Rates Full (All B and G rates) G rates only (6, 9, 12, 18, 24, 36, 48 and 54 Mbps) BG optimized or BG subset (1, 2, 5.5, 6, 11, 24, 36 and 54 Mbps) A rates only (6, 9, 12, 18, 24, 36, 48 and 54 Mbps) ABG Rates Full (All A rates and all B and G rates with A rates preferred) BGA Rates Full (All B and G rates and all A rates with B and G rates preferred) Ad Hoc (when connecting to another client device instead of an AP) Default: BGA Rates Full

It is important the Radio Mode parameter correspond to the AP to which the device is to connect. For example, if this parameter is set to G rates only, the Thor VM2 may only connect to APs set for G rates and not those set for B and G rates.

Status

Start > All Programs > Summit > Summit Client Utility > Status tab
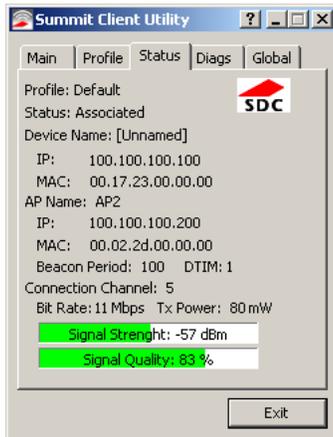
This screen provides information on the radio:

- 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 kilomicroseconds. (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

Start > All Programs > Summit > Summit Client Utility > Diags tab
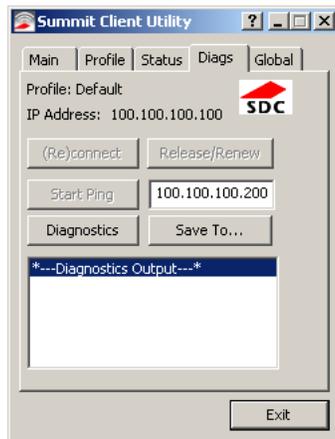
The Diags screen can be used for troubleshooting network traffic and radio connectivity issues.

- **(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 to 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

Start > All Programs > Summit > Summit Client Utility > Global tab

The parameters on this panel can only be changed when a user is loggin on with an admin password. The current values for the parameters can be viewed by the general user without requiring a password.

Note: Tap the **Commit** button to save changes. If the panel is exited before tapping the **Commit** button, changes are not saved!

Factory Default Settings

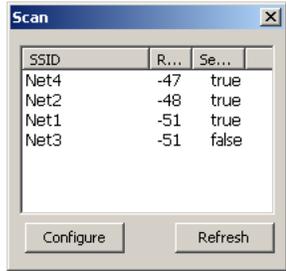|	
Roam Trigger	-65 dBm
Roam Delta	5 dBm
Roam Period	10 sec.
BG Channel Set	Full
DFS Channels	Off
DFS Scan Time	120 ms.
Ad Hoc Channel	1
Aggressive Scan	On
CCX Features	Optimized
WMM	On
Auth Server	Type 1
TTLS Inner Method	Auto-EAP
PMK Caching	Standard
WAPI	Off (dimmed)
TX Diversity	On
RX Diversity	On Start on Main
Frag Threshold	2346
RTS Threshold	2347
LED	Off
Tray Icon	On
Hide Passwords	On
Admin Password	SUMMIT (or blank)
Auth Timeout	8 seconds
Certs Path	C:\Program Files\Summit\certs
Ping Payload	32 bytes
Ping Timeout	5000 ms
Ping Delay ms	1000 ms
Logon Options	Use SCU credentials
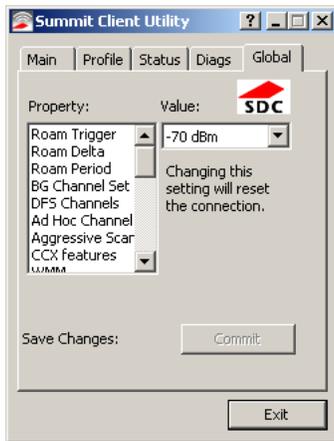
Custom Parameter Option

The parameter value is displayed as "Custom" when the operating system registry has been edited to set the Summit parameter to a value that is not available from the parameter's drop down list. Selecting Custom from the drop down list has no effect. Selecting any other value from the drop down list will overwrite the "custom" value in the registry.

Global Parameters

Parameter	Default	Function
Roam Trigger	–65 dBm	If signal strength is less than this trigger value, the client looks for a different Access Point with a stronger signal. Options are: -50 dBm, -55, -60, -65, -70, -75, -80, -85, -90 dBm or .
Roam Delta	5 dBm	The amount by which a different Access Point signal strength must exceed the current Access Point signal strength before roaming to the different Access Point is attempted. Options are: 5 dBm, 10, 15, 20, 25, 30, 35 dBm or Custom.
Roam Period	10 sec.	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 are: 5 sec, 10, 15, 20, 25, 30, 35, 40, 45, 50, 55, 60 seconds or Custom.
BG Channel Set	Full	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 are: Full (all channels) 1,6,11 (the most commonly used channels) 1,7,13 (for ETSI and TELEC radios only) or Custom.
DFS Channels	Off	Support for 5GHZ 802.11a channels where support for DFS is required. Options are: On, Off, Optimized. Not supported (always off) in some releases.
DFS Scan Time	120 ms.	ABG radio only. The amount of time the radio will passively scan each DFS channel to see if it will receive a beacon. Recommended value is 1.5 times that of the AP's beacon period.
Ad Hoc Channel	1	Use this parameter when the Radio Mode profile parameter is set to Ad Hoc. Specifies the channel to be used for an Ad Hoc connection to another client device. If a channel is selected that is not supported by the by the radio, the default value is used. Options are: 1 through 14 (the 2.4GHz channels) 36, 40, 44, 48 (the UNII-1 channels)
Aggressive Scan	On	When set to On and the current connection to an AP weakens, the radio aggressively scans for available APs. Aggressive scanning works with standard scanning (set through Roam Trigger, Roam Delta and Roam Period). Aggressive scanning should be set to On unless there is significant co-channel interference due to overlapping APs on the same channel. Options are: On, Off
CCX or CCX Features	Optimized	Use of Cisco Compatible Extensions (CCX) radio management and AP specified maximum transmit power features. Options are: Full - Use Cisco IE and CCX version number, support all CCX features. The option known as "On" in previous versions. Optimized –Use Cisco IE and CCX version number, support all CCX features except AP assisted roaming, AP specified maximum transmit power and radio management. Off - Do not use Cisco IE and CCX version number. Cisco IE = Cisco Information Element.

Parameter	Default	Function
WMM	On	Use of Wi-Fi Multimedia extensions. Devices running Windows XP can change the default value. Devices running all other OS cannot change the default value.
Auth Server	Type 1	Specifies the type of authentication server. Options are: Type 1 (ACS server) and Type 2 (non-ACS server)
TTLS Inner Method	Auto-EAP	Authentication method used within the secure tunnel created by EAP-TTLS. Options are: AUTO-EAP (Any available EAP method), MSCHAPV2, MSCHAP, PAP CHAP, EAP-MSCHAPV2
PMK Caching	Standard	Type of Pairwise Master Key (PMK) caching to use when WPA2 is in use. PMK caching is designed to speed up roaming between APs by allowing the client and the AP to cache the results of 802.1X authentications, eliminating the need to communicate with the ACS server. Standard PMK is used when there are no controllers. The reauthentication information is cached on the original AP. The client and the AP use the cached information to perform the four-way handshake to exchange keys. Opportunistic PMK (OPMK) is used when there are controllers. The reauthentication information cached on the controllers. The client and the controller behind the AP use the cached information to perform the four-way handshake to exchange keys. If the selected PMK caching method is not supported by the network infrastructure, every roam requires full 802.11X authentication, including interaction with the ACS server. If the active profile is using WPA2 CCKM, the global PMK Caching setting is ignored and the client attempts to use CCKM. Options are: Standard, OPMK
WAPI	Off	Default is Off and dimmed (cannot be changed).
TX Diversity	On	How to handle antenna diversity when transmitting packets to the Access Point. Options are: Main only, and On.
RX Diversity	On Start on Main	How to handle antenna diversity when receiving packets from the Access Point. Option is: On-start on Main This parameter cannot be changed for some Summit radios.
Frag Thresh	2346	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 wireless interference. Options are: Any number between 256 bytes and 2346 bytes.
RTS Thresh	2347	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. This parameter cannot be changed.
LED	Off	The LED on the wireless card is not visible to the user when the wireless card is installed in a sealed mobile device. Options are: On, Off.

Parameter	Default	Function
Tray Icon	On	Determines if the Summit icon is displayed in the System tray. Options are: On, Off The tray icon is not displayed when the Thor VM2 is running a Windows Embedded Standard 2009, Windows Embedded Standard 7 or Windows 7 Professional operating system.
Hide Password	On	When On, the Summit Config Utility masks passwords (characters on the screen are displayed as an *) as they are typed and when they are viewed. When Off, password characters are not masked. Options are: On, Off.
Admin Password	SUMMIT (or Blank)	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 dialog box. The password is case sensitive. This value is masked when the Admin is logged out. Options are: none.
Auth Timeout	8 seconds	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 are: An integer from 3 to 60.
Certs Path	certificates	A valid directory path, of up to 64 characters, where WPA Certificate Authority and User Certificates are stored on the mobile device when not using the Windows certificates store. Ensure the Windows folder path exists before assigning the path in this parameter. See Certificates for instructions on obtaining CA and User Certificates. This value is masked when the Admin is logged out. Options are: none. The complete path is C:\Program Files\Summit\certs
Ping Payload	32 bytes	Maximum amount of data to be transmitted on a ping. Options are: 32 bytes, 64, 128, 256, 512, or 1024 bytes.
Ping Timeout ms	5000	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 are: Any number between 0 and 30000 ms.
Ping Delay ms	1000	The amount of time, in milliseconds, between each ping after a **Start Ping** button tap. Options are: Any number between 0 and 30000 ms.
Logon Options	SCU	Use SCU or Windows login credentials.

Note: *Tap the **Commit** button to save changes. If this panel is closed before tapping the **Commit** button, changes are not saved!*

Logon Options

There are two options available, a Single Signon option which uses the Windows user-name and password as the credentials for 802.1x authentication and a Pre-Logon Connection option which uses saved credentials for 802.1x authentication before Windows logon.

If either option is enabled, the credentials entered here take precedence over any cre-dentials entered on the **Profile** tab.

To use either option, select Logon Options from the Property list which activates the **Logon Options** button.

Click the **Logon Options** button.

Single Signon

To use the **Single Signon** option, select the checkbox for **Use the Windows username and password when available**. When the active profile is using LEAP, PEAP-MSCHAP, PEAP-GTC or EAP-FAST, the SCU ignores the username and password, if any, saved in the profile. Instead, the username and password used for Windows logon is used. Any certificates needed for authentication must still be specified in the profile.

Click **OK** then click **Commit**.

Pre-Logon Connection

To use the Pre_logon connection, select the checkbox for Enable pre-logon connection. This option is designed to be used when:

- EAP authentication is required for a WLAN connection
- Single Signon is configured, so the Windows username and password are used as credentials for EAP authentication
- The WLAN connection needs to be established before the Windows login.

Once this option is enabled, the Authentication delay and Association timeout values can be adjusted as necessary. Both values are specified in milliseconds (ms).

The default authentication delay is 5000 ms and the valid range is 0 – 600,000 ms.

The default association timeout is 10,000 ms and the valid range is 10,000 to 600,000 ms.

Click on the **Credentials** button to enter the logon credentials.

If using the Windows certificate store:

1. Check the **Use MS store** checkbox. The default is to use the Full Trusted Store.
2. To select an individual certificate, click on the Browse button.
3. Uncheck the **Use full trusted store** checkbox.
4. Select the desired certificate and click Select. You are returned to the Credentials screen.
5. Click **OK** then click **Commit**.

If using the Certs Path option:

1. Leave the **Use MS store** box unchecked.
2. Enter the certificate filename in the CA Cert text box.
3. Click **OK** then click **Commit**.

Sign-On vs. Stored Credentials

When using wireless security that requires a user name and password to be entered, the Summit Client Utility offers these 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.

- When using Summit with the Thor VM2, there is an option on the **Global** tab to use the Windows user name and password to log on instead of any username and password stored in the profile.

⚠️ Windows 7 Professional and Windows Embedded Standard 7 only:

The credentials login and password entry window may not always display in the foreground. When the Thor VM2 attempts to connect to the network, click the flashing icon in the Notification bar to display the login screen. Enter the user name and password and click **OK** to close the window. This procedure may need to be followed after the following events:

- The Thor VM2 returns from sleep, hibernate or sleep

- The Thor VM2 is restarted

- A different active profile is selected from the **Configuration** tab

- Invalid credentials have been entered

To Use Stored Credentials

1. After completing the other entries in the profile, click on the **Credentials** button.

2. Enter the Username and Password on the Credentials screen and click the **OK** button.

3. Click the **Commit** button.

4. For LEAP and WPA/LEAP, configuration is complete.

5. For PEAP-MSCHAP and PEAP-GTC, importing the CA certificate into the Windows certificate store is optional.

6. For EAP-TLS, import the CA certificate into the Windows certificate store. Also import the User Certificate into the Windows certificate store.

7. Access the Credentials screen again. Make sure the Validate server and Use MS store checkboxes are checked.

8. 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.

9. For EAP-TLS, also enter the User Cert (User Certificate filename) on the credentials screen by using the **Browse** button.

10. If using EAP FAST and manual PAC provisioning, input the PAC filename and password.

11. Click the **OK** button then the **Commit** button.

12. If changes are made to the stored credentials, click **Commit** to save those changes before making any additional changes to the profile or global parameters.

13. 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.

Note: *See Configuring the Profile for more details.*

Note: *If invalid credentials are entered into the stored credentials, the authentication will fail. No error message is displayed. The user may or may not be prompted to enter valid credentials.*

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 LEAP/WPA.

2. For PEAP-MSCHAP and PEAP-GTC, importing the CA certificate into the Windows certificate store is optional.

3. For EAP-TLS, import the CA certificate into the Windows certificate store. 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.

10. Verify the device is authenticated by reviewing the **Status** tab. When the device is property configured, the indicates the device is Authenticated and the method used.

11. The sign-on screen is displayed after a reboot.

Note: *See Configuring the Profile for more details.*

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 **Diags** tab clicked or

- the profile is modified and the **Commit** button is clicked.

To Use Windows Username and Password

Please see Logon Options for information.

Windows Certificate Store vs. Certs Path

Note: *It is important that all dates are correct on the Thor VM2 and host computers when using any type of certificate. Certificates are date sensitive and if the date is not correct authentication will fail.*

⚠ If using the Windows Certificate Store, the Windows Account must have a password. The password cannot be left blank. The Summit Client Utility uses the Windows user account credentials to access the Certificate Store. The Windows user account credentials need not be the same as the credentials entered in the Summit Client Utility.

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, see Generate a User Certificate.
- To import the user certificate into the Windows certificate store, see Install a User Certificate.
- A Root CA certificate is also needed. Refer to the section below.

Root CA Certificates

Root CA certificates are required for EAP/TLS, PEAP/GTC and PEAP/MSCHAP. Two options are offered for storing these certificates. They may be imported into the Windows certificate store or copied into the Certs Path directory.

Certs Path

1. See Generate a Root CA Certificate and follow the instructions to download the Root Certificate to a PC.
2. Copy the certificate to specified directory on the mobile device. The default location for Certs Path is C:\Program Files\Summit\certs. A different location may be specified by using the Certs Path global variable.
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 text box.
5. Click **OK** to exit the Credentials screen and then **Commit** to save the profile changes.

Windows Certificate Store

1. See Generate a Root CA Certificate and follow the instructions to download the Root Certificate to a PC.
2. To import the certificate into the Windows store, See Install a Root CA Certificate.
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 the last step.

5. Otherwise, to select a specific certificate click on the **Browse (...)** button.

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 text box.

8. Click **OK** to exit the Credentials screen and then **Commit** to save the profile changes.

Configuring the Profile

Use the instructions in this section to complete the entries on the **Profile** tab according to the type of wireless security used by your 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.

- If using a single profile, edit the default profile with the parameters for your network. Select the Default profile from the pull–down menu.

- 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.

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 is made to close or browse away from the tab in focus if there are unsaved changes.

If changes are made to the *stored credentials*, click **Commit** to save those changes first before making any additional changes.

No Security

To connect to a wireless network with no security, make sure the following profile options are used.

1. Enter the SSID of the Access Point assigned to this profile

2. Set EAP Type to None

3. Set Encryption to None

4. Set Auth Type to Open

Once configured, click the **Commit** button.

Ensure the correct Active Profile is selected on the **Main** tab and restart. The SCU **Main** tab shows the device is associated after the radio connects to the network.

To connect using WEP, make sure the following profile options are used.

1. Enter the SSID of the Access Point assigned to this profile
2. Set EAP Type to **None**
3. Set Encryption to **WEP** or **Manual WEP** (depending on SCU version)
4. Set Auth Type to **Open**

Click the **WEP keys/PSKs** button.

Valid keys are 10 hexadecimal or 5 ASCII characters (for 40-bit encryption) or 26 hexadecimal or 13 ASCII characters (for 128-bit encryption). 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 restart. The SCU **Main** tab shows the device is associated after the radio connects to the network.

To use LEAP (without WPA, also called WEP-LEAP), make sure the following profile options are used.

1. Enter the SSID of the Access Point assigned to this profile
2. Set EAP Type to **LEAP**
3. Set Encryption to **WEP EAP** or **Auto WEP** (depending on SCU version)
4. 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 to use shared key or passphrase, set the Auth Type radio parameter to **Shared**.
    - If the AP is configured for network EAP only, set the Auth Type radio parameter to *LEAP*.

See Sign-On vs. Stored Credentials for information on entering credentials.

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.

Enter the Domain\Username (if the Domain 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 restart. The SCU **Main** tab shows the device is associated after the radio connects to the network.

To use PEAP/MSCHAP, make sure the following profile options are used.

1. Enter the SSID of the Access Point assigned to this profile
2. Set EAP Type to **PEAP-MSCHAP**
3. Set Encryption to **WPA TKIP**
4. Set Auth Type to **Open**

To use another encryption type, select WPA CCKM, WPA2 AES or WPA2 CCKM for encryption and complete other entries as detailed in this section.

See Sign-On vs. Stored Credentials for information on entering credentials.

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.

Enter the Domain\Username (if the Domain 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.

See Windows Certificate Store vs. Certs Path for more information on certificate storage.

Once successfully authenticated, import the CA certificate into the Windows certificate store. Return to the **Credentials** screen and check the Validate server checkbox.

If using the Windows certificate store:

1. Check the **Use MS store** checkbox. The default is to use the Full Trusted Store.
2. To select an individual certificate, click on the **Browse** button.
3. Uncheck the **Use full trusted store** checkbox.
4. Select the desired certificate and click Select. You are returned to the **Credentials** screen.
5. Click **OK** then click **Commit**.

If using the Certs Path option:

1. Leave the **Use MS store** box unchecked.
2. Enter the certificate filename in the CA Cert text box.
3. Click **OK** then click **Commit**.

The device should be authenticating the server certificate and using PEAP/MSCHAP for the user authentication.

Ensure the correct Active Profile is selected on the **Main** tab and restart. The SCU **Main** tab shows the device is associated after the radio connects to the network.

Note: *The date must be properly set on the device to authenticate a certificate.*

To use PEAP/GTC, make sure the following profile options are used.

1. Enter the SSID of the Access Point assigned to this profile
2. Set EAP Type to **PEAP-GTC**
3. Set Encryption to **WPA TKIP**
4. Set Auth Type to **Open**

To use another encryption type, select WPA CCKM, WPA2 AES or WPA2 CCKM for encryption and complete other entries as detailed in this section.

See Sign-On vs. Stored Credentials for information on entering credentials.

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.

Enter these items as directed below.

Enter the Domain\Username (if the Domain 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.

See Windows Certificate Store vs. Certs Path for more information on certificate storage.

Once successfully authenticated, import the CA certificate into the Windows certificate store. Return to the **Credentials** screen and check the **Validate server** checkbox.

Note: *Some servers may be configured to allow only a single use of the password for PEAP/GTC. In this case, wait for the token to update with a new password before attempting to validate the server. Then enter the new password, check the **Validate Server** checkbox and proceed with the certificate process below.*

If using the Windows certificate store:

1. Check the **Use MS store** checkbox. The default is to use the Full Trusted Store.
2. To select an individual certificate, click on the **Browse** button.
3. Uncheck the **Use full trusted store** checkbox.
4. Select the desired certificate and click **Select**. You are returned to the Credentials screen.
5. Click **OK** then click **Commit**.

If using the Certs Path option:

1. Leave the Use MS store box unchecked.
2. Enter the certificate filename in the **CA Cert** text box.
3. Click **OK** then click **Commit**.

The device should be authenticating the server certificate and using PEAP/GTC for the user authentication.

Ensure the correct Active Profile is selected on the **Main** tab and restart. The SCU **Main** tab shows the device is associated after the radio connects to the network.

Note: *The date must be properly set on the device to authenticate a certificate.*

To use WPA/LEAP, make sure the following profile options are used.

1. Enter the SSID of the Access Point assigned to this profile
2. Set EAP Type to **LEAP**
3. Set Encryption to **WPA TKIP**
4. 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 to use shared key or passphrase, set the Auth Type radio parameter to **Shared**.
   - If the AP is configured for network EAP only, set the Auth Type radio parameter to **LEAP**.

To use another encryption type, select WPA CCKM, WPA2 AES or WPA2 CCKM for encryption and complete other entries as detailed in this section.

See Sign-On vs. Stored Credentials for information on entering credentials.

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.

Enter the Domain\Username (if the Domain is required), otherwise enter the Username.

Enter the password.

Click **OK** then click the **Commit** button.

Ensure the correct Active Profile is selected on the **Main** tab and restart. 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.

1. Enter the SSID of the Access Point assigned to this profile
2. Set EAP Type to **EAP-FAST**
3. Set Encryption to **WPA TKIP**
4. Set Auth Type to **Open**

To use another encryption type, select WPA CCKM, WPA2 AES or WPA2 CCKM for encryption and complete other entries as detailed in this section.

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 Thor VM2.

For automatic PAC provisioning, once a username/password is authenticated, the PAC information is stored on the Thor VM2. The same username/password must be used to authenticate each time. See the note below for more details.

For manual PAC provisioning, the PAC filename and Password must be entered.

See Sign-On vs. Stored Credentials for information on entering credentials.

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.

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 Domain 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.

Ensure the correct Active Profile is selected on the **Main** tab and restart. 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 C:\Program Files\Summit\certs directory with the PAC credentials. If the username is changed, that file must be deleted. The filename is* `autoP.00.pac`*.*

To use EAP-TLS, make sure the following profile options are used.

1. Enter the SSID of the Access Point assigned to this profile
2. Set EAP Type to **EAP-TLS**
3. Set Encryption to **WPA TKIP**
4. Set Auth Type to **Open**

To use another encryption type, select WPA CCKM, WPA2 AES or WPA2 CCKM for encryption and complete other entries as detailed in this section.

See Sign-On vs. Stored Credentials for information on entering credentials.

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 when connecting to the network.

*   For Stored Credentials, User Certificate Filename and the CA Certificate Filename must be entered.

Enter these items as directed below.

Enter the Domain\Username (if the Domain is required), otherwise enter the Username.

Select a user certificate from the Windows certificate store. 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.

Some versions of the SCU require a User Cert password. If this entry field is present, enter the password for the user certificate in the User Cert pwd box.

If there are no user certificates in the Windows certificate store, follow these instructions for Generate a User Certificate and Install a User Certificate.

See Windows Certificate Store vs. Certs Path for more information on CA certificate storage.

Check the **Validate server** checkbox.

If using the Windows certificate store:

1. Check the **Use MS store** checkbox. The default is to use the Full Trusted Store.
2. To select an individual certificate, click on the **Browse** button.
3. Uncheck the **Use full trusted store** checkbox.
4. Select the desired certificate and click Select. You are returned to the Credentials screen.
5. Click **OK** then click **Commit**.

If using the Certs Path option:

1. Leave the **Use MS store** box unchecked.
2. Enter the certificate filename in the CA Cert text box.
3. Click **OK** then click **Commit**.

The Thor VM2 should be authenticating the server certificate and using EAP-TLS for the user authentication.

Ensure the correct Active Profile is selected on the **Main** tab and restart. The SCU **Main** tab shows the device is associated after the radio connects to the network.

See Certificates for information on generating a Root CA certificate or a User certificate.

Note: *The date must be properly set on the device to authenticate a certificate.*

To connect using WPA/PSK, make sure the following profile options are used:

1. Enter the SSID of the Access Point assigned to this profile
2. Set EAP Type to **None**
3. Set Encryption to **WPA PSK** or **WPA2 PSK**
4. Set Auth Type to **Open**

Click the **WEP keys/PSKs** button.

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 restart. The SCU **Main** tab shows the device is associated after the radio connects to the network.

Certificates

Note: *Please refer to the Security Primer to prepare the Authentication Server and Access Point for communication.*

Note: *It is important that all dates are correct on the Thor VM2 and host computers when using any type of certificate. Certificates are date sensitive and if the date is not correct authentication will fail.*

⚠️ If using the Windows Certificate Store, the Windows Account must have a password. The password cannot be left blank. The Summit Client Utility uses the Windows user account credentials to access the Certificate Store. The Windows user account credentials need not be the same as those entered in the Summit Client Utility.

Quick Start

Root Certificates are necessary for EAP-TLS, PEAP/GTC and PEAP/MSCHAP.

1. Generate a Root CA Certificate either from the Thor VM2 or using a PC.
2. If a PC was used to request the certificate, copy the certificate to the Thor VM2.
3. Install a Root CA Certificate.

User Certificates are necessary for EAP-TLS.

1. Generate a User Certificate either from the Thor VM2 or using a PC.
2. If a PC was used to request the certificate, copy the certificate to the Thor VM2.
3. Install a User Certificate.

Generate a Root CA Certificate

Note: *It is important that all dates are correct on the Thor VM2 and host computers when using any type of certificate. Certificates are date sensitive and if the date is not correct authentication will fail.*

The easiest way to get the root CA certificate is to use a browser on a PC or the Thor VM2 to navigate to the Certificate Authority. To request the root CA certificate, open a browser to

http://<CA IP address>/certsrv.

⚠️ Windows 7 Professional and Windows Embedded Standard 7 only:

It may be necessary to use a PC to request a certificate for these devices.

Sign into the CA with any valid username and password.
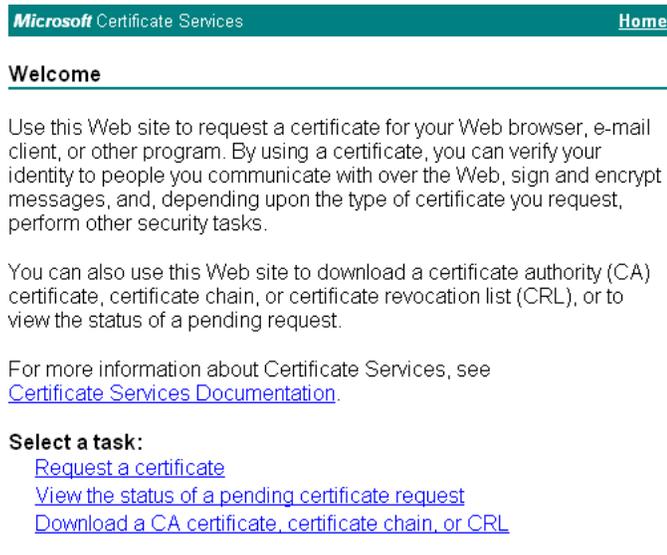
Click the Download a CA certificate, certificate chain or CRL link.

Make sure the correct root CA certificate is selected in the list box.

Microsoft Certificate Services   **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

Encoding method:

⊙ DER
○ Base 64

Download CA certificate
Download CA certificate chain
Download latest base CRL
Download latest delta CRL

Click the **DER** button.

To download the CA certificate, click on the Download CA certificate link.

Click the **Save** button and save the certificate. Make sure to keep track of the name and location of the certificate.

Next install the certificate on the Thor VM2.

Install a Root CA Certificate

Note: *This section is only if the Windows certificate store is used. If the certificate store is not used, copy the certificate to the C:\Program Files\Summit\certs folder or other path specified in the Summit Certs global parameter.*

Copy the certificate file to the Thor VM2. The certificate file has a .CER extension. Locate the file and double-tap on it. If presented with a security warning, confirm that you want to open the file.

If the Certificate Wizard does not start automatically when you double-tap the certificate .CER file:

1. Select **Start > Run** and type **certmgr.msc** in the text box and tap **OK** (*Windows Embedded Standard 2009 only*).

2. Select **Start** and type **certmgr.msc** in the search box and press Enter (*Windows Professional 7 and Windows Embedded Standard 7 only*).

3. In the left pane, right-click **Trusted Root Certificate Authorities** and select **All Tasks > Import**.

4. The Certificate Import Wizard starts.

5. Tap **Next** and use the **Browse..** button to locate the Root certificate copied to the Thor VM2 then tap **Open**.

6. The certificate filename and path are displayed. Tap **Next**.
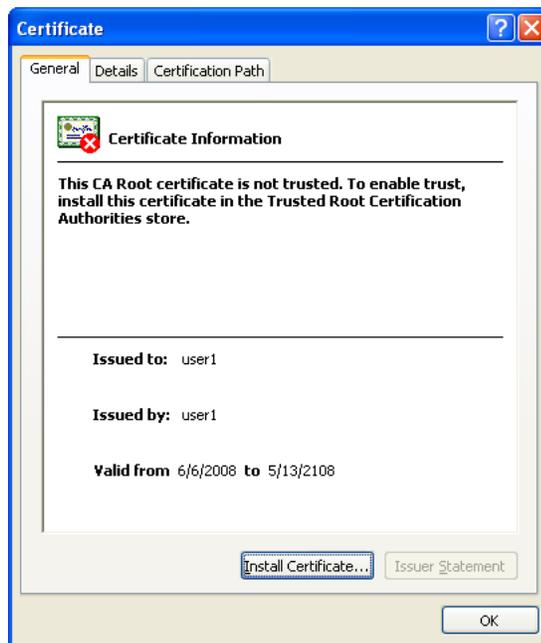
7. Tap the **Install Certificate** button.

8. The certificate import wizard starts. Tap **Next**.
   - Windows Embedded Standard 2009 only:

    a. Allow Windows to automatically select the certificate store.

    b. Tap **Next** and **Finish**.

    c. An import successful message is displayed.

    • Windows 7 Professional and Windows Embedded Standard 7 only:

    a. Select **Place all certificates in the following store**.

    b. Tap **Browse** and select **Trusted Root Certification Authorities**.

    c. Tap **OK** then tap **Next** and **Finish**.

    d. If presented with a security warning, confirm that you want to install this certificate.

    e. An import successful message is displayed.

9. Allow Windows to automatically select the certificate store.

10. Tap Next and Finish.

11. An import successful message is displayed.

Generate a User Certificate

The easiest way to get the user certificate is to use the browser on the Thor VM2 or a PC to navigate to the Certificate Authority. To request the user certificate, open a browser to

http://<CA IP address>/certsrv.

Windows 7 Professional and Windows Embedded Standard 7 only:

• It may be necessary to use a PC to request a certificate for these devices.

Sign into the CA with the username and password of the person who will be logging into the mobile device.

This process saves a user certificate file. There is no separate private key file as used on Windows CE devices.

Microsoft Certificate Services   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

Click the Request a certificate link.

Microsoft Certificate Services   Home

Request a Certificate

Select the certificate type:
    User Certificate

Or, submit an advanced certificate request.

Click on the User Certificate link.

User Certificate - Identifying Information

No further identifying information is required. To complete your certificate, press submit:

More Options >>

                    Submit >

Click on the **Submit** button. If there is a message box asking if you want to confirm the request, click Yes.

The User Certificate is issued.

Certificate Issued

The certificate you requested was issued to you.

    Install this certificate

Install the user certificate on the requesting computer by clicking the Install this certifi‐cate link.

If the requesting computer is the Thor VM2, then the process is finished. Otherwise, export the certificate as described below.

Exporting a User Certificate

Select **Tools > Internet Options > Content** and click the **Certificates** button.
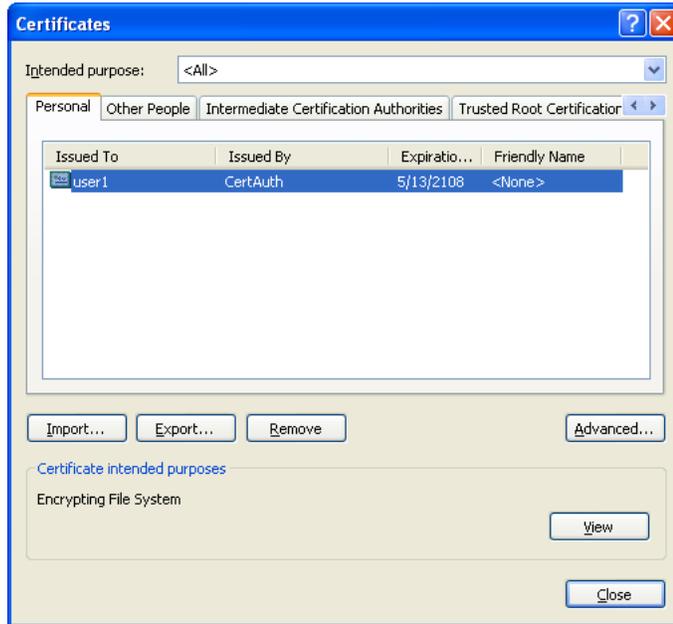
Make sure the **Personal** tab is selected. Highlight the certificate and click the **Export** button.

The Certificate Export Wizard is started

Select **Yes, export the private key** and click **Next**.

Uncheck **Enable strong protection** and click **Next**. The certificate type must be PKCS #12 (.PFX).

When the private key is exported, you must enter the password, confirm the password and click **Next**. Be sure to remember the password as it is needed when installing the certificate.

Supply the file name for the certificate. Use the **Browse** button to select the folder where you wish to store the certificate. The certificate is saved with a .PFX extension.

Click **Finish** and **OK** to close the Successful Export message.

Locate the User Certificate in the specified location. Copy to the Thor VM2. Install the User certificate.

Install a User Certificate

After generating and exporting the user certificate, install the user certificate.

1. Copy the certificate from the PC to the Thor VM2.

2. Locate the certificate file (it has a .PFX extension) and double-click on it. If clicking on the certificate file does not launch the certificate import wizard, follow the Manually Initiate Certificate Installation before continuing the instructions below.

3. The certificate import wizard starts. Tap Next.

4. Confirm the certificate file name and location.

5. Tap Next.

6. You are prompted for the password that was assigned when the certificate was exported.

7. It is not necessary to select either of the checkboxes displayed above.

8. Enter the password and tap Next.

9. On the next screen, allow Windows to automatically select the certificate store, then click Next and Finish. An import successful message is displayed.

Manually Initiate Certificate Installation

If the Certificate Wizard does not start automatically when you double-tap the certificate .PFX file:

1. Select **Start > Run** and type **certmgr.msc** in the text box and tap **OK** (*Windows Embedded Standard 2009 only*).

2. Select **Start** and type **certmgr.msc** in the search box and press **Enter** (*Windows Professional 7 and Windows Embedded Standard 7 only*).

3. In the left pane, right-click **Personal** and select **All Tasks > Import**.

4. The Certificate Import Wizard starts.

5. Tap **Next** and use the **Browse..** button to locate the User certificate copied to the Thor VM2. If necessary, change the file type drop down list at the bottom of the explorer window from *.cer* to *.pfx*. After selecting the .PFX file, tap **Open**.

6. The certificate filename and path are displayed. Tap **Next**.

7. Return to the installation instructions above.

OneClick Internet

This section contains the User Manual for the customized version of WebToGo's One-Click Internet for the Honeywell Thor VM2.

OneClick Internet is installed by Honeywell on all Thor VM2s equipped with a WWAN radio. Available carriers and OneClick features may vary by device.

OneClick Internet provides:

- Internet connection management
- Email download
- SMS Management
- Contact management for SIM and Microsoft Outlook
- GPS Management

Since WebToGo OneClick Internet is preinstalled, it is present on the Windows Start Menu. A desktop icon is also provided.

Honeywell does not recommend using standby/sleep on the Thor VM2 while the WWAN connection is active. When exiting standby/sleep, a delay of one minute or more may occur as the WWAN radio reads firmware files and initializes before reconnecting. If this delay is acceptable to the user, standby may be enabled.

When the One Click Internet utility is displayed on screen and the Thor VM2 enters standby/sleep, the touch screen may remain inactive for 10-15 seconds after the Thor VM2 resumes from standby/sleep.

Preparing for Initial Use on the Thor VM2

Install SIM Card

If using a CDMA carrier such as Verizon, skip this step because a SIM card is not used.

Install SIM Card in the Thor VM2.

Load Firmware

While the OneClick Internet utility is preinstalled, it is necessary to load the GOBI radio firmware for your selected carrier such as AT&T, T-Mobile or Verizon.

Note: *For carriers requiring a SIM card, the firmware may automatically be selected when a SIM card is installed in the Thor VM2.*

Double-tap the OneClick Internet icon on the Thor VM2 desktop.

OneClick
Internet

Tap the **Settings** button and select the **Firmware** tab. Select the firmware for your carrier from the list and tap Change.

For more details, see OneClick Internet Connection Manager and the Firmware tab.

Activation

This step is only necessary for Verizon.

You need the IMEI number for the Thor VM2 when you contact Verizon prior to activating service on the Thor VM2. The IMEI number can be found on the Info tab.

The activation screen is displayed automatically after the Verizon firmware is selected. If the activation screen is not automatically displayed, double-tap the OneClick Internet icon on the desktop. Select **Settings > General** tab and tap the **Activate** button.

Make sure **Automated Activation** is selected and tap **Next**.

Tap **Next** to complete the activation.

Once the activation is completed, OneClick Internet may be minimized to the tray.

To verify your settings, tap on the OneClick Internet icon in the system tray.

Tap **Settings**.

Tap the **Network** tab.

This screen contains the settings including the telephone number from the provider, in this case Verizon.

Using OneClick Internet

If OneClick Internet is not loaded, double-tap the desktop icon to load it. If OneClick Internet is loaded but minimized to the system tray, tap the OneClick Internet icon in the system tray to maximize it.

Connection Management

1. Launch the OneClick Internet Connection Manager and wait until the status icon is blue indicating ready.
2. If there is a problem, verify the SIM card is installed (AT&T, T-Mobile only), the proper firmware has been loaded, etc.
3. If PIN security is used, a popup window prompts for the SIM PIN.
4. Create a connection profile on the Settings menu.
5. Tap the **Connect** button.

The signal strength is indicated as well as the name of the mobile network you are using and the status of the WWAN device. Tap the **Disconnect** button to end the session.

Menu Buttons

Radio Button

The **Radio** button allows you to switch the WWAN radio on and off to save power or to disable the radio in instances where it is not desired (such as during airplane travel).

When the radio is switched off, the button is red. When on, it is green. If the radio is disabled by a hardware switch or if the device is not available, the button is disabled and is light gray/white.

Statistics Button

 The Statistics area provides advanced information about the connection. Values displayed are approximate.

Tap the **Statistics** button to enable the statistics viewing area, which is below the main area. When the statistics are displayed, tapping the **Statistics** button again hides the statistics viewing area.

Data In:	The amount of data received during the current connection.
Data Out:	The amount of data sent during the current connection.
Total:	The total amount of data transferred during the current connection.
Speed:	The current data transfer rate.
Max. Speed:	The maximum data transfer rate during this connection.
Time:	The duration of the current connection.

Update Button

 OneClick Internet provides a built-in online update functionality that allows for an automatic update of OneClick Internet application, device drivers, and APN database.

Honeywell DOES NOT recommend using this option. Contact *Technical Assistance* or information on upgrading to another version of OneClick Internet.

The update is triggered by pressing the **Update** button. The application will check the WebToGo server, if updates are available, and offer them for download if suitable.

In order to start the update, select a file from the list of available updates and tap **OK**.

Help Button

 OneClick Internet includes online help that can be accessed by tapping the **Help** button.

Settings Button

 Access the Settings menu by tapping the **Settings** button on the main window.

The following tabs are available:

- Profile

- Network

- History

- PIN

- Info

- Firmware

- General

Profile

Create a connection profile to store connection information. Once a profile has been created, its name appears in the drop down Profiles list, which replaces the Profile Name text box in the illustration above.

Buttons

Button	Description
	Create a new profile. When this option is selected, the Profile Name is a text box. Enter a name for the profile as well as other connection specific configuration. When finished, tap the **Save** button to save the new profile.
	Edit a current profile. Select a profile from the Profiles list and tap this button to edit the profile parameters. When finished, tap the **Save** button to save the profile changes.
	Delete a profile. Select a profile from the Profiles list and tap this button to delete the profile
	Save a profile. Save a new profile or save changes made when editing a profile.
Set Profile	**Set** Profile. Select a profile from the Profiles list and tap this button to make it the active profile used for connection.

Parameters

Label	Description
Profile Name	Profile name - Assign a unique name for each profile.
APN	Access Point Name of the network operator. Contact your network operator for more information When you are using a CDMA network, the APN field does not appear.
Username	Username. Contact your network operator for more information
Password	Password. Contact your network operator for more information
DNS	Domain Name Server. Contact your network operator for more information. When **Use Automatic DNS-settings** is selected, no additional DNS entries are required. Otherwise, enter the DNS addresses.
Proxy Settings	Proxy Settings for your network. Contact your network operator for more information. When **Use Proxy Server** is selected, no additional proxy entries are required. Otherwise, enter the Proxy and the Port.

Network

The appearance of the network tab depends on the type of firmware selected.

Network with SIM Card

Select Connection

Label	Description
Select automatically	Selects the best suited network automatically
Use GPRS/EDGE only	Use only GPRS/EDGE for a connection
Use UMTS/HSPA only	Use only UMTS/HSPA for a connection.

Select and tap Apply. A "Network changed successfully" message is displayed.

Close the tab and view the signal strength icon in the main window. Once the signal strength is displayed, you can establish a connection.

Select Network

Use this option to select from available networks.

Note: *When you are registered to a CDMA network, you cannot select the network. "All CDMA network" is shown instead.*

Note: *The network list only appears if the connection setting is **Only use GPRS** or **Only use UMTS/HSPA**.*

Select the network and tap on the **Register** button. If the change is successful you will see the message "Network changed successfully".

This item is useful when traveling . Automatic mode selects the preferred network of your network operator.

If enabled, Network Selection displays a list of network options.

1. Automatic Selection
2. Retrieving Networks..

The currently registered network is marked.

CDMA Network

Information on the CDMA network is displayed. There are no editable parameters on this screen.

History

The history shows the data volume transferred in a specified time frame. Select the From and To dates to see the data volume sent/received in the specified period. Tap Reset to reset the counter.

PIN

You can Activate/Deactivate the PIN or Change the PIN.

Activate/Deactivate PIN

This tab is only displayed when a firmware is loaded that requires a SIM card (such as AT&T or T-Mobile).

By default, you have to enter the PIN each time you start WebToGo OneClick Internet using a modem card. Deactivate the PIN to avoid entering the PIN each time.
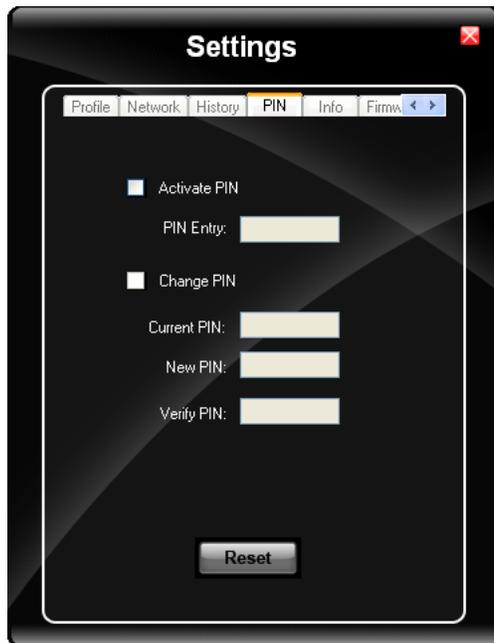
Change PIN

This dialog lets you change your PIN.

Label	Description
Current PIN	Enter the current PIN.
New PIN	Enter the new PIN.
Verify PIN	Verify the new PIN by entering it again.

Info
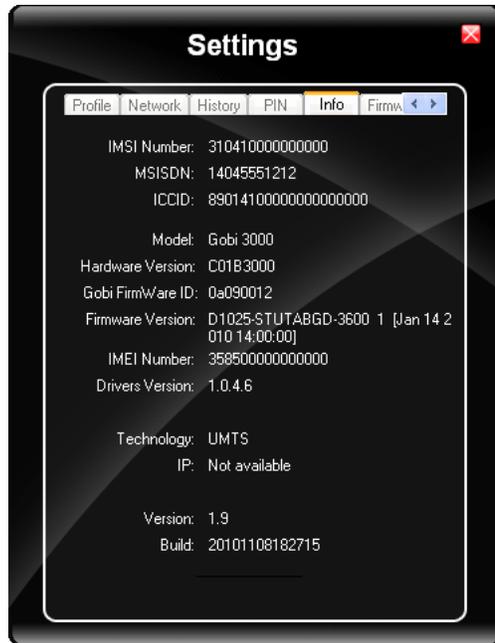
This tab displays SIM card, modem and system Information.

Firmware

OneClick Internet selects the correct Firmware matching your operator automatically, if a special firmware for your operator is available and a SIM card is inserted. If no specific firmware for your operator is available, generic firmware is selected. After a firmware has been selected, it appears as the Current Profile.

You can manually load your desired firmware. Select a new firmware manually by click-ing the Select New Profile dropdown menu, selecting a firmware from the menu and tapping the **Change** button to load. To return to automatic firmware selection, choose Automatic(UMTS) in the dropdown menu.

Note: *Switching between CDMA and UMTS firmware is not done automatically. You must select CDMA firmware manually to connect to CDMA networks. If you want to return to UMTS networks, you must manually select UMTS firmware.*

Activation on CDMA

When CDMA Firmware is selected, the activation of the modem on the CDMA network starts automatically. During the process of loading CDMA firmware, an activation win-dow pop up allowing a choice between Manual Activation and Automated Activation.

Label	Description
Manual Activation	Enter the requested items as direct by a representative from your carrier.
Automatic Activation	Use your modem to start an automated activation session

If you cancel the activation or if it fails, you can also start the activation manually by pressing the **Activate** button on the **General** tab.

General
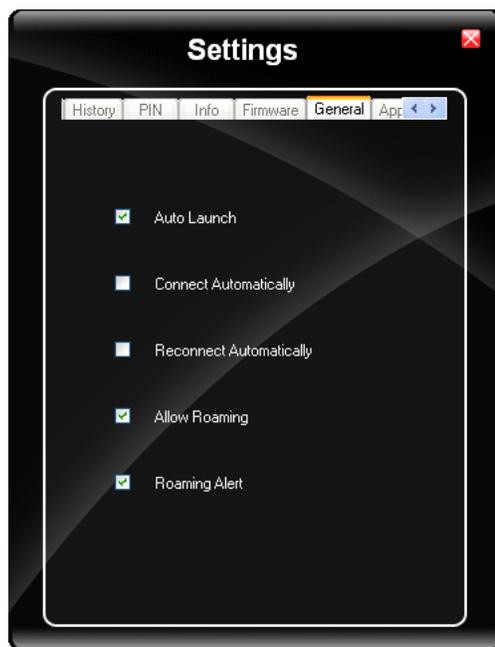
Label	Description
Auto Launch	When selected OneClick Internet launches automatically when the user starts the Thor VM2 and logs in.
Connect Automatically	When selected OneClick Internet automatically connects on start-up.
Reconnect Automatically	When selected OneClick Internet reconnects automatically when the Thor VM2 returns from standby/sleep or hibernate.

Label	Description
Allow roaming	When selected OneClick Internet allows connections in foreign networks. Use care when enabling roaming to avoid roaming charges.
Roaming Alert	When selected OneClick Internet displays an alert when roaming.
Gobi NDIS Auto Connect	When selected OneClick Internet connects automatically after powering up the operating system and before the user logs in.

Application
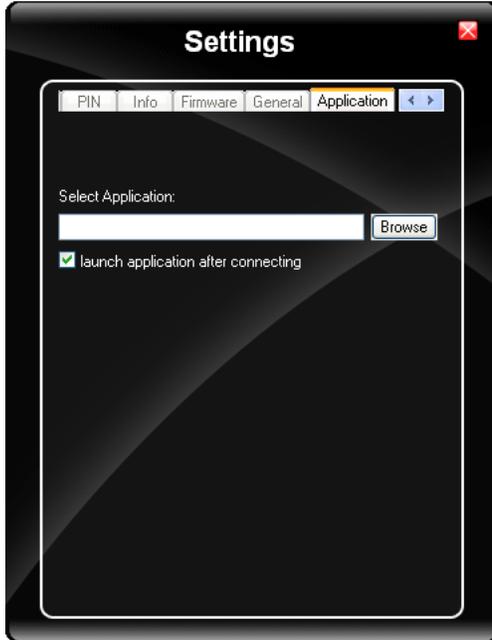
Use the **Application** tab to specify any application to launch automatically once the Internet connection is established. Use the **Browse** button to locate the desired application.

Application Buttons

SMS
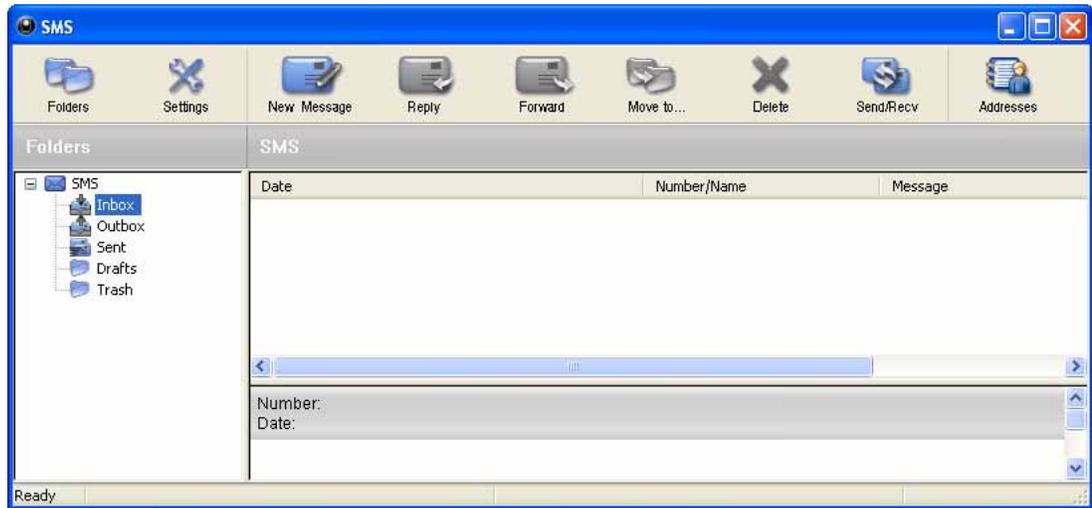
The SMS Center window is split into menu bar, folder view, folder content and preview window. To manage your short messages you may:

Button	Description
Folders	Manage SMS folders
Settings	Change SMS settings
New Message	Create new SMS/MMS messages
Reply	Reply to SMS
Forward	Forward SMS
Move to...	Move SMS to a folder
Delete	Delete SMS

Button	Description
Send/Recv	Send and receive SMS/MMS (if supported)
Addresses	Manage phone book contacts on SIM and in Email client.

Folder

By using this menu, you may change the folder structure of the SMS Center:

Button	Description
New Folder	Creates a new folder, name has to be unique
Rename	Renames an existing folder
Remove	Removes an existing folder (including the messages)

Note: *Predefined folders can't be deleted or modified.*

Settings

The settings window lets you change the deletion mode. You may choose whether to delete an SMS from the SMS Center, from the SIM or decide whether this should be asked at all. You may also activate an alarm signal when a new SMS arrives.

New SMS

The "New Message" window is used to enter the SMS text. You may also enter texts by copy & paste from other applications. The status bar at the lower right corner indicates the length of the SMS for your convenience: the first number tells you how many parts the SMS consists of (one part has max. 160 characters/unicode70), the second number counts down from 160/70 characters. The number in parenthesis () counts the total number of characters. The recipient for your SMS has to be entered in the "To" field. This can be either entered by typing digits or by clicking the **To** button to select a recipient from the address book. Recipient addresses may be taken from the SIM address book or from your Email client's contact folder. Just select an address and click **OK**. To send the message click "Send/Receive".

Reply

Highlight a message to which you want to reply, e.g. in the inbox folder, then click the **Reply** button. The **New Message** window opens and the recipient address is already filled in the **To** field. Continue as before when sending a new message.

Forward

Highlight a SMS, which you want to forward. Click the **Forward** button. The **New Message** window opens, however the message text is already copied. Continue as before when sending a new message.

Move SMS..

Highlight the SMS to be moved and click the **Move SMS** button. A small window opens that lets you select the destination folder. Select the folder to which the message should be moved, then click **Move**.

Delete

Highlight the SMS which you want to delete. Click **Delete**" to remove the message.

Send/Receive

Messages will be sent and/or received by clicking on this button.

Addresses

Clicking this button opens the address book. You may add new contacts to your personal address book or you may change existing addresses, delete addresses or exchange them with your SIM card and your Email client application, or export the data set.

Buttons	Description
New Contact	Create new contact.
Modify	Modify a contact.
Delete	Delete contacts, mark one or more and press the button.
Copy	Synchronization with MS Outlook.
Export	To export addresses you may select between two export formats: • CSV (comma separated text format, usually read by spread sheet applications) • VCard (business card format, used by MS Outlook and other applications)
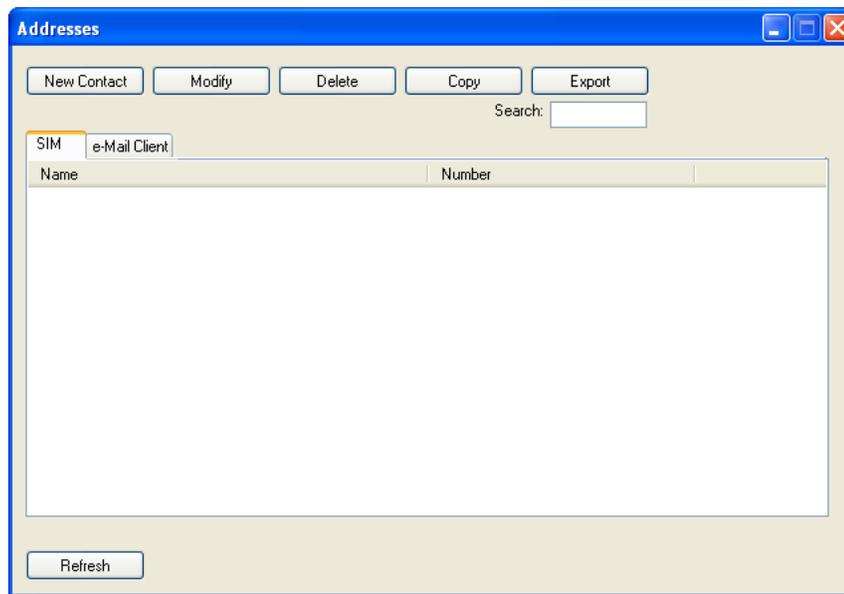
Web Browser

Clicking this button opens the Web Browser and allows the user to surf the Internet once the connection is established. The default browser is used, which is Internet Explorer by default on the Thor VM2.

Email

Clicking this button opens the Email application after the connection is established. The Email application is the default Email client set in the Control Panel (**Start > Control Panel > Internet Options > Programs** tab).

GPS

Tap the **GPS** button to open the GPS window. Press **Get GPS** to start the GPS. The rotating GPS button indicates the GPS is active.

After Latitude and Longitude Data are displayed, the user can tap **Track Me** to open Google Maps, showing their current location on a map.

Lat – Latitude – The location north or south of the equator in degrees.

Lon – Longitude: The angular distance from the Prime Meridian in degrees.

After Latitude and Longitude Data are displayed, the user can tap **Clipboard** and the latitude and longitude are copied to the clipboard cache. The data can be pasted into an email, document or other electronic media.

About

OneClick Internet allows the user to configure the WWAN connection by entering basic setup information. The network connection (service carrier) can be chosen based on the firmware loaded, GPS tracking can be enabled and SMS messaging can be configured.

Once configured, OneClick Internet allows the user to connect or disconnect from the mobile network.

System Requirements

OneClick Internet requires:

- Gobi 23000 3G Module (preinstalled by Honeywell)
- Gobi 23000 Driver package (loaded by Honeywell)

OneClick Internet for Gobi 23000is compatible with the following operating systems on the Thor VM2:

- Windows Embedded Standard 7
- Windows 7 Professional
- Windows Embedded Standard 2009

Supported Languages

OneClick Internet supports the following languages:

German, English, Spanish, French, Polish, Russian, Italian, Simplified Chinese and Traditional Chinese.

Note: *This does not mean that the Thor VM2 has been localized for these languages.*

Installing or Upgrading OneClick Internet

Note: *You must use the Honeywell supplied version of OneClick Internet. Do not change versions unless instructed by your Honeywell representative.*

One Click Internet is pre-installed before the Thor VM2 is shipped.

If you have an installed version of OneClick Internet and need to update to a newer version, you must uninstall the previous version first by selecting **Start > Control Panel > Add or Remove Programs**. Select **OneClick Internet** and tap **Remove**. Follow the on screen instructions.

Note: *OneClick Internet does not install the drivers for the Gobi 3000 devices. Device drivers are preloaded.*

When you double-click the Installer file for OneClick Internet, it extracts the files to install.
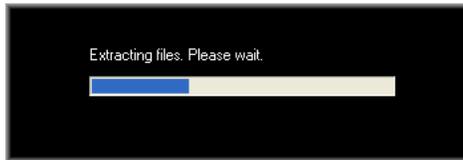
Next, select the application language. By default, the language of the OS is used (if available).
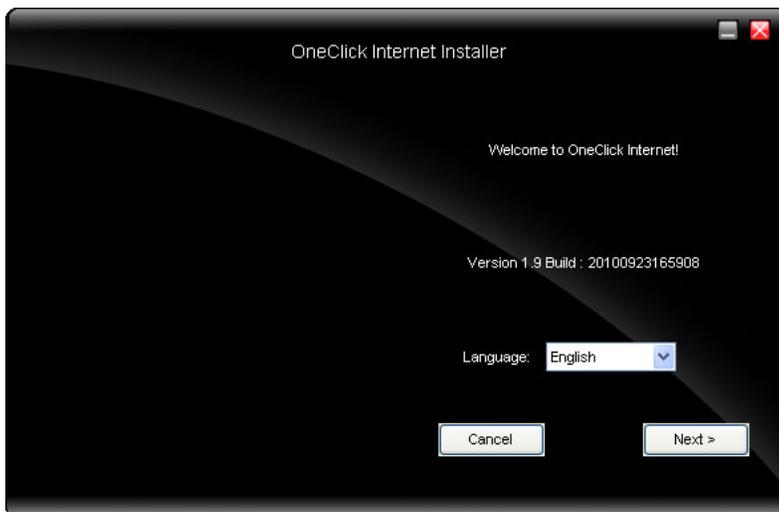
Review and accept the license agreement. Click Accept, if you agree. Otherwise please click Reject to cancel installation.
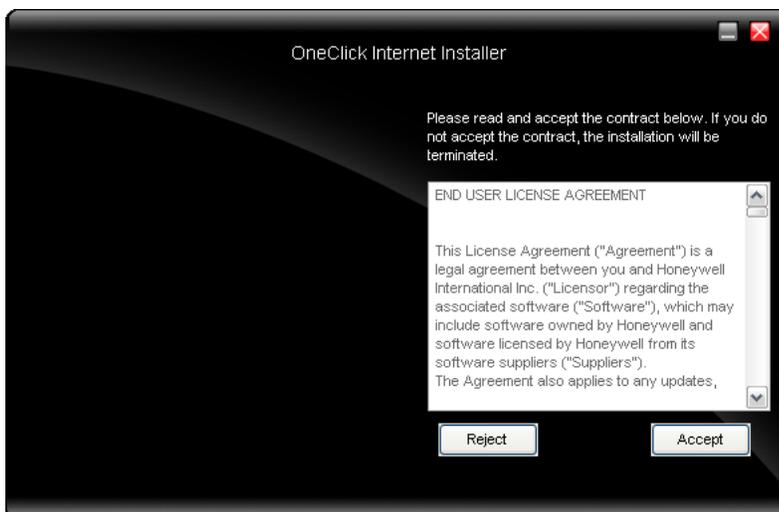
Next the installer asks for the installation directory. Use the **Browse** button to specify a location other than the default.
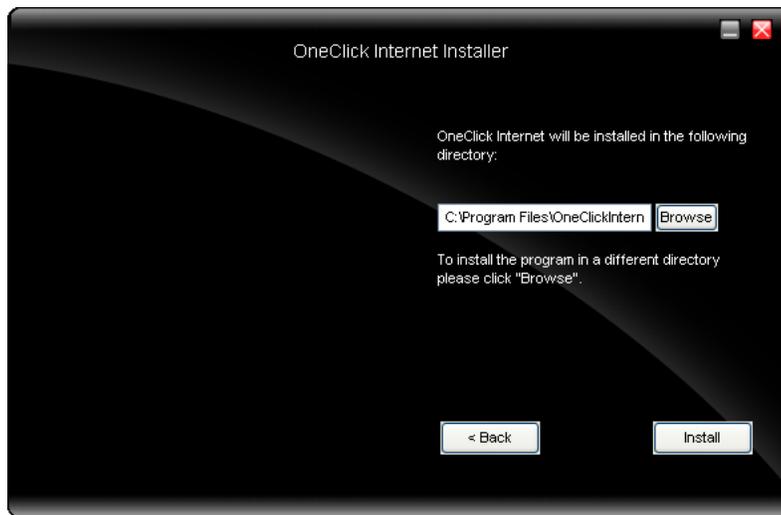
Installation process is indicated on screen. When completed. click the **Finish** button to exit the installer.
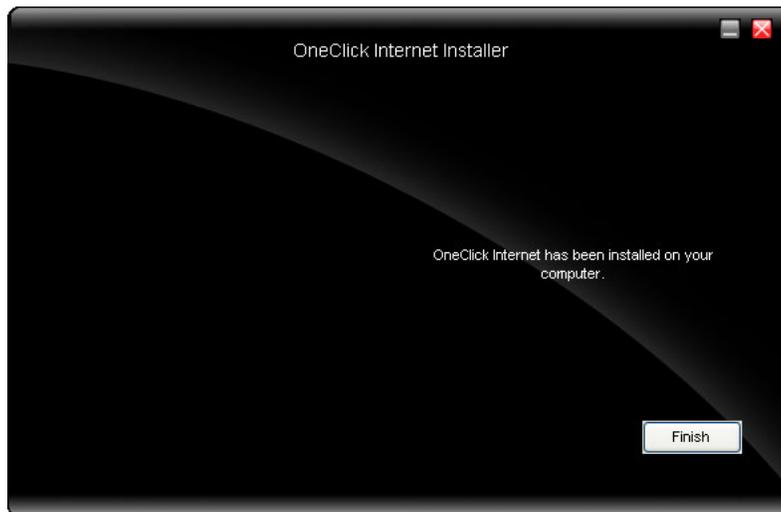
Start OneClick Internet from the Windows Program Menu or double-tap the desktop icon.

OneClick Internet Connection Manager

Launch OneClick Internet from the desktop icon or Windows Start Menu.

When OneClick Internet is active, a status icon appears in the system tray.

The main screen for OneClick Internet opens when the application is started. This screen displays basic information on the connection as well as access to more advanced features and details. From this screen you can connect to the Internet, send Emails, send short messages (SMS) and access the GPS.

General Windows controls for minimize and exit are located at the upper right of the screen.

Connection Management

Refer to the table below for descriptions of the items in the connection management area.

Icon	Description
	Network signal strength Additionally the network name is displayed to the right of the icon. The more green bars, the stronger the signal.
	Connect / Cancel / Disconnect Tap this button to connect or disconnect. The color of this button also indicates the status of the connection: The radio is disconnected. Tap the button to connect. The radio is currently connecting. The radio is connected. Tap the button to disconnect.

Icon	Description
	SMS The **SMS** button is enabled if no Internet connection is active. When this button is active, tapping it accesses the integrated SMS application.
	Web Tap this button to launch the default browser.
	Email Tap this button to launch the default Email application.
	GPS Tap this button access the integrated GPS tool.

Information Buttons

Icon	Description
	Radio On/Off Tap this button to switch the radio state. The color of this button also indicates the state of the radio: The radio is On. Tap the button to turn the radio Off. The radio is Off. Tap the button to turn the radio On. The radio is Connecting or the radio has been disabled. The button is inactive at this time.
	Statistics Show/Hide Tap the button to expand the screen to include connection statistics. See Statistics Button for details. Tap the button to hide the connection statistics.
	Settings Tap this button to access One Clink Internet settings. Select from several tabs to configure the connection settings. See Settings Button for details.
	Update Tap this button to access OneClick Internet **Update** tab. See Update Button.
	Help Click this button to view the online help.
Status	Ready. Tap the **Connect** button to establish a connection. Connecting. Tap the **Cancel** button to cancel the connection in process. Connected. Tap the **Disconnect** button to end the connection. Failure. Review the screen for messages such as "No Network", etc.

A KEY MAPS

Integrated Keypad

There are five integrated programmable keys located on the Thor VM2 below the display. Each programmable key can be modified by the Orange key for a total of 10 programmable keys.

See Programmable Key to remap these keys.

The default values for these keys are:

To get this Programmable Key	Press These Keys in this Order		Default Key Value
P1 (Programmable key 1)	P1		F1
P2 (Programmable key 2)	P2		F2
P3 (Programmable key 3)	P3		F3
P4 (Programmable key 4)	P4		F4
P5 (Programmable key 5)	P5		F5
P6 (Programmable key 6)	Orange	P1	<none>
P7 (Programmable key 7)	Orange	P2	<none>
P8 (Programmable key 8)	Orange	P3	<none>
P9 (Programmable key 9)	Orange	P4	<none>
P10 (Programmable key 10)	Orange	P5	<none>

The following key press sequences are not programmable:

To get this function	Press These Keys in this Order	
Increase speaker volume	Blue	P1
Decrease speaker volume	Blue	P2
Increase display brightness	Blue	P3

To get this function	Press These Keys in this Order	
Decrease display brightness	Blue	P4

The Blue plus P5 key press sequence causes no action.

Integrated Keypad and BIOS

The front panel keys have limited functionality before booting completes. However, the following key functions are available during BIOS setup.

- P1 – Move up to the previous item in a menu
- P2 – Move down to the next item in a menu
- P3 – Move to the previous menu
- P4 – Move to the next menu
- P5 – Cycle through values for the highlighted menu item
- Blue – Activate the highlighted menu choice (acts as 'Enter' key)
- If a Y/N question is presented, press P4 to confirm (Acts as 'Y') or P5 to deny (acts as 'N').

External 21-Key Keyboard

The table below shows the results of the keypresses. The Thor VM2 does not support remapped keys on this keyboard. The modifier keys (PF, green, yellow) only produce the results below. They do not modify keystrokes for the Thor VM2.

Key	Result
1	1
2	2
3	3
4	4
5	5
6	6
7	7
8	8
9	9
0	0
PF	p
Green	g
Yellow	y
Del	Delete
Tab	Tab
Left	Left
Right	Right
Up	Up
Down	Down

Note: *Back Tab (Yellow + Tab) and Backspace (Yellow + Delete) are not supported with the Thor VM2 on this keypad.*

External 95-Key Keyboard

These key functions apply to both the 95-Key USB Keyboard and the 95-key PS/2 Keyboard.

The key map table that follows lists the commands used for the Thor VM2. Note that since the Thor VM2 uses a Microsoft Windows operating system, no DOS Terminal Emulation keypress sequences are provided.

There are 10 hidden keys on the 95 key keyboard. Each of the hidden keys is accessed by pressing the <Fn> key (located in the top right hand corner) plus a key on the numeric keypad on the right. Additional function keys are supported as well.

To get this Key / Function	Press These Keys in this Order	
Insert	FN	0 (numeric keypad)
Home	FN	7 (numeric keypad)
Page Up	FN	9 (numeric keypad)
Delete	FN	. (numeric keypad)
End	FN	1 (numeric keypad)
Page Down	FN	3 (numeric keypad)
Up Arrow	FN	8 (numeric keypad)
Left Arrow	FN	4 (numeric keypad)
Down Arrow	FN	2 (numeric keypad)
Right Arrow	FN	6 (numeric keypad)

External 60-Key Keyboard
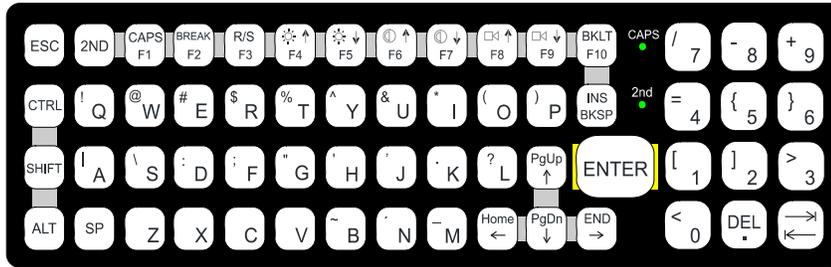
The key map table that follows lists the commands used when using the Thor VM2 with the 60-key PS/2 Keyboard.

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. The default for NumLock is On. Changes made to the NumLock status persist across a Windows restart.

When running RFTerm, please refer to the RFTerm Reference Guide for equivalent keys and keypress sequences.

60 Key KeyMap 101-Key Equivalencies

- The following keymap is used on a Thor VM2 that is NOT running RFTerm.
- When using a sequence of keys that includes the 2nd key, press the 2nd key first then the rest of the key sequence.
- When the Thor VM2 boots, the default condition of Caps (or CapsLock) is Off. The Caps (or CapsLock) condition can be toggled with a **2nd + F1** key sequence. The CAPS LED is illuminated when CapsLock is On. The keymaps below assume Caps is Off.
- The Thor VM2 keyboard has several control keys. The following control keys are not used:
  - The 2nd function of the **F3** key is not used as Windows Power Management controls all power management modes on the Thor VM2.
  - The 2nd functions of the **F4** and **F5** keys are not used as the display brightness is adjusted via the buttons on the front of the Thor VM2.
  - The 2nd functions of the **F6** and **F7** keys are not used as the Thor VM2 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 Thor VM2 is controlled with a Microsoft Windows Control Panel.
  - The 2nd function of the **F10** key is not used as the display backlight timer also controls the keyboard backlight.

To get this Key / Function	Press These Keys in this Order		
Power On/Off	Power		
2nd	2nd		

To get this Key / Function	Press These Keys in this Order		
Shift	Shift		
Alt	Alt		
Ctrl	Ctrl		
Esc	Esc		
Space	Sp		
Enter	Enter		
Enter (numeric)	2nd	Enter	
CapsLock (Toggle)	2nd	F1	
Back Space	BkSp		
Tab	Tab		
Back Tab	2nd	Tab	
Ctrl-Break	Ctrl	2nd	F2
Pause	2nd	F2	
Up Arrow	Up Arrow		
Down Arrow	Down Arrow		
Right Arrow	Right Arrow		
Left Arrow	Left Arrow		
Insert	2nd	Bksp	
Delete (numeric)	2nd	DOT	
Home	2nd	Left Arrow	
End	2nd	Right Arrow	
Page Up	2nd	Up Arrow	
Page Down	2nd	Down Arrow	
ScrollLock	2nd	Shift	F10
F1	F1		
F2	F2		
F3	F3		
F4	F4		
F5	F5		
F6	F6		
F7	F7		
F8	F8		
F9	F9		
F10	F10		
F11	2nd	Shift	F1
F12	2nd	Shift	F2
a	A		
b	B		
c	C		
d	D		

To get this Key / Function	Press These Keys in this Order		
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	Shift	A	
B	Shift	B	
C	Shift	C	
D	Shift	D	
E	Shift	E	
F	Shift	F	
G	Shift	G	
H	Shift	H	
I	Shift	I	
J	Shift	J	
K	Shift	K	
L	Shift	L	
M	Shift	M	
N	Shift	N	
O	Shift	O	
P	Shift	P	
Q	Shift	Q	
R	Shift	R	

To get this Key / Function	Press These Keys in this Order		
S	Shift	S	
T	Shift	T	
U	Shift	U	
V	Shift	V	
W	Shift	W	
X	Shift	X	
Y	Shift	Y	
Z	Shift	Z	
1	1		
2	2		
3	3		
4	4		
5	5		
6	6		
7	7		
8	8		
9	9		
0	0		
DOT	DOT		
<	2nd	0	
[	2nd	1	
]	2nd	2	
>	2nd	3	
=	2nd	4	
{	2nd	5	
}	2nd	6	
/ (numeric)	2nd	Ctrl	7
/ (alpha)	2nd	7	
– (numeric)	2nd	Ctrl	8
– (alpha)	2nd	8	
+ (numeric)	2nd	Ctrl	9
+ (alpha)	2nd	9	
* (numeric)	2nd	I (letter i)	
* (alpha)	2nd	Ctrl	I (letter i)
: (colon)	2nd	D	
; (semicolon)	2nd	F	
?	2nd	L	
`	2nd	N	
_ (underscore)	2nd	M	
, (comma)	2nd	J	

To get this Key / Function	Press These Keys in this Order		
' (apostrophe)	2nd	H	
~ (tilde)	2nd	B	
\	2nd	S	
|	2nd	A	
"	2nd	G	
!	2nd	Q	
@	2nd	W	
#	2nd	E	
$	2nd	R	
%	2nd	T	
^	2nd	Y	
&	2nd	U	
(	2nd	O	
)	2nd	P	

B SPECIFICATIONS AND REFERENCE MATERIAL

Technical Specifications

Thor VM2

Processor	Atom CPU operating at 1.6 GHz
Memory	2 GB SDRAM
Mass Storage	4 or 8 GB CompactFlash memory card (Window Embedded Standard 2009) 16 GB CompactFlash memory card (Window 7 Professional) 32 GB CompactFlash memory card (Window Embedded Standard 7)
Storage Expansion	Supports 1 to 4GB SD card: Factory installed 4GB SD card optional for Windows 7 Professional and Windows Embedded Standard 7, user installable on all others
Operating System	Microsoft Windows Embedded Standard 2009 Microsoft Windows Embedded Standard 7 Microsoft Windows 7 Professional No operating system
Radio Modules	802.11 a/b/g/n radio / Bluetooth, Optional GPS / WWAN
Scanner Options	No integrated scanner, Optional serial, USB or Bluetooth scanners
Display Technology	Intel GMA 500 graphics processor, SVGA compatible Active matrix TFT Resolution: 1024 x 768 pixels (maximum) 400 NIT brightness 9.7" (measured horizontally) display Transmissive with LED backlight Vehicle motion screen blanking available
Keyboard	Integrated 5-key keypad Optional 95-key USB keyboard
Touch Screen	Impact resistive, signature capture capability Field replaceable front panel including touch screen
External Connectors	Optional external 802.11 / GPS / WWAN antenna connectors Additional connectors on dock, see below
Beeper	Minimum loudness greater than 95dBm at 10 cm in front of unit
Power Supply	10 to 60 VDC isolated
Uninterruptible Power Supply	Internal UPS battery, 30-minute life at -20°C (-4°F)
Backup Battery (RCT)	Internal lithium battery maintains Real Time Clock

VM1D Standard Dock

⚠ **Caution: This dock is designed for DC power vehicle–mounted applications only.**

SKUs	VM1001VMCRADLE (with RAM ball) VM1002VMCRADLE VM1003VMCRADLE
Power Connector	6-pin connector: Direct10-60V DC input power Optional external converter for extended range DC (60-150 VDC)
COM1Connector	9-pin male, RS-232 serial port, COM1 with switchable power on pin 9
COM2 Connector	9-pin male, RS-232 serial port, COM2 with switchable power on pin 9
CANBUS/AUDIO Connector	15-pin male, CANbus/Audio connector supports either audio/microphone via adapter cable or J1939 Female and J1939 Male connectors via CANbus cable
USB Connector	9-pin female, USB connector supports USB host port via adapter cable
Power Switch	Sealed power switch
Input Power	DC Input Voltage: 10- 60 VDC, Input Current: 4.6 Amps (typical), Input Fuse: 8A Time Delay. Replace with same size, rating and type of fuse: • Littelfuse 0215008.MXP • Cooper Bussmann BK1/S506-8-R • Bel Fuse 5HT 8-R or equivalent.
External Power Supply	50-150 VDC DC power supply available for vehicles over 60 VDC *Note:* *Use dock VMX005VMCRADLE (VMXD Enhanced Dock of Off-Vehicle Use) in AC power applications.*

VM3D Enhanced Dock

⚠ **Caution: This dock is designed for DC power vehicle–mounted applications only.**

SKU	VM3001VMCRADLE
Power Connector	6-pin connector: Direct10-60V DC input power Optional external converter for extended range DC (60-150 VDC)
COM1Connector	9-pin male, RS-232 serial port, COM1 with switchable power on pin 9
COM2 Connector	9-pin male, RS-232 serial port, COM2 with switchable power on pin 9
CANBUS/AUDIO Connector	15-pin male, CANbus/Audio connector supports either audio/microphone via adapter cable or J1939 Female and J1939 Male connectors via CANbus cable
USB1 Connector	9-pin female, USB connector supports USB host port via adapter cable *Note:* *USB Client port may not be supported by the Thor VM2 operating system.*
USB2 Connector	15-pin female, USB connector supports two USB host ports via adapter cable
USB Host Connector	One USB Host connector behind waterproof cap
Ethernet	One RJ45 Ethernet connector behind waterproof cap *Note:* *For Windows 7 and Windows Embedded Standard 7: An upgrade is necessary to support the Ethernet port on this dock. See Thor VM2 and Enhanced Dock Support.* *Note:* *For Windows Embedded Standard 2009: The Ethernet port is not supported.*
Power Switch	Sealed power switch
Input Power	DC Input Voltage: 10– 60 VDC, Input Current: 4.6 Amps (typical), Input Fuse: 8A Time Delay. Replace with same size, rating and type of fuse: • Littelfuse 0215008.MXP • Cooper Bussmann BK1/S506-8-R • Bel Fuse 5HT 8-R or equivalent.
External Power Supply	50-150 VDC DC power supply available for vehicles over 60 VDC *Note:* *Use dock VMX005VMCRADLE (VMXD Enhanced Dock of Off-Vehicle Use) in AC power applications.*

VMXD Enhanced Dock

⚠️ **Caution: This dock is designed for DC power vehicle–mounted applications only.**

SKUs	VMX004VMCRADLE
Power Connector	6-pin connector: 13.2VDC input power; requires DC power supply Connector is also used for screen blanking via COM1 CTS and RTS signals
COM1Connector	9-pin male, RS-232 serial port, COM1 with switchable power on pin 9 Do not use COM1 when screen blanking box is attached to avoid port conflicts.
COM2 Connector	9-pin male, RS-232 serial port, COM2 with switchable power on pin 9
CANBUS/AUDIO Connector	15-pin male, CANbus/Audio connector supports either audio/microphone via adapter cable or J1939 Female and J1939 Male connectors via CANbus cable
USB1 Connector	9-pin female, USB connector supports USB host port via adapter cable *Note:* *USB Client port may not be supported by the Thor VM2 operating system.*
USB2 Connector	15-pin female, USB connector supports two USB host ports via adapter cable
USB Host Connector	One USB Host connector behind waterproof cap
Ethernet	One RJ45 Ethernet connector behind waterproof cap *Note:* *For Windows 7 and Windows Embedded Standard 7: An upgrade is necessary to support the Ethernet port on this dock. See Thor VM2 and Enhanced Dock Support.* *Note:* *For Windows Embedded Standard 2009: The Ethernet port is not supported.*
Power Switch	Sealed power switch
External Power Supply	AC Adapter, 120-240VAC to 12VDC
Input Power	DC Input Voltage: 13.2VDC, Input Current: 4.6 Amps (typical), Input Fuse: 8A Time Delay. Replace with same size, rating and type of fuse: • Littelfuse 0215008.MXP • Cooper Bussmann BK1/S506-8-R • Bel Fuse 5HT 8-R or equivalent.
External Power Supply	50-150 VDC DC power supply required for all installations *Note:* *Use dock VMX005VMCRADLE (VMXD Enhanced Dock of Off-Vehicle Use) in AC power applications.*

VMXD Enhanced Dock for Off-Vehicle Use (QM3AC)

⚠️ **Caution:** **This dock is designed for AC power (non vehicle-mounted)
applications only.**

SKU	VMX005VMCRADLE
Power Connector	6-pin connector: 15VDC input power via required AC/DC Adapter
COM1Connector	9-pin male, RS-232 serial port, COM1 with power on pin 9
COM2 Connector	9-pin male, RS-232 serial port, COM2 with power on pin 9
CANBUS/AUDIO Connector	15-pin male, CANbus/Audio connector supports either audio/microphone via adapter cable or J1939 Female and J1939 Male connectors via CANbus cable
USB1 Connector	9-pin female, USB connector supports USB host port via adapter cable ***Note:*** *USB Client port may not be supported by the Thor VM2 operating system.*
USB2 Connector	15-pin female, USB connector supports two USB host ports via adapter cable
USB Host Connector	One USB Host connector behind waterproof cap
Ethernet	One RJ45 Ethernet connector behind waterproof cap ***Note:*** *For Windows 7 and Windows Embedded Standard 7: An upgrade is necessary to support the Ethernet port on this dock. See Thor VM2 and Enhanced Dock Support.* ***Note:*** *For Windows Embedded Standard 2009: The Ethernet port is not supported.*
Power Switch	Sealed power switch
External Power Supply	AC Adapter, 120-240VAC to 15VDC
Input Power	DC Input Voltage: 15VDC, Input Current: 4 Amps (maximum), Input Fuse: 8A Time Delay. Replace with same size, rating and type of fuse: • Littelfuse 0215008.MXP • Cooper Bussmann BK1/S506-8-R • Bel Fuse 5HT 8-R or equivalent.
External Power Supply	AC Adapter, 120-240VAC to 15VDC required ***Note:*** *This dock for use in AC power applications. See other docks for DC power applications.*

Dimensions

Thor VM2

Width	10.6" (26.8 cm)
Height	8.4" (21.4 cm)
Depth	2.1" (5.3cm)
Weight	4.8 lb. (2.2 kg)

VM1D Standard Dock

Note: *The RAM ball is not included in the following measurements.*

Length	7.1" (18.0 cm)
Width	6.1" (15.5 cm)
Height	2.5" (6.4 cm), measurement includes strain relief cable clamps
Weight	3.2 lb. (1.5 kg)

VM3D and VMXD Enhanced Dock

Note: *The RAM ball is not included in the following measurements.*

Length	7.1" (18.0 cm)
Width	6.1" (15.5 cm)
Height	2.1" (5.4 cm), measurement includes strain relief cable clamps
Weight	2.4 lb. (1.1 kg)

Environmental Specifications

Thor VM2 and Dock

Operating Temperature	-4°F to 122°F (-20°C to 50°C) [non-condensing]
Storage Temperature	-22°F to 140°F (-30°C to 60°C) [non-condensing]
ESD	8 KV air, 4kV direct contact
Operating Humidity	Up to 90% non-condensing at 104°F (40°C)
Water and Dust	IEC 60529 compliant to IP66
Vibration	MIL-STD-810F, composite wheeled vehicles.
Crash	SAE-J 1455

Network Card Specifications

WLAN – Summit 802.11 a/b/g/n

Bus Interface	32-bit PCIe Mini Card
Wireless Frequencies (varies by regulatory domain)	2.4 to 2.4895 GHz IEEE 802.11b / 802.11g DSSS OFDM 5.15 to 5.82 GHz IEEE 802.11a DSSS OFDM
RF Data Rates	802.11a (OFDM) 6, 9, 12, 18, 24, 36, 48, 54 Mbps 802.11b (DSSS) 1, 2, 5.5, 11 Mbps 802.11g (OFDM) 6, 9, 12, 18, 24, 36, 48, 54 Mbps 802.11n (OFDM 20 MHz chs) 13, 26, 39, 52, 78, 104, 117, 130 Mbps 802.11n (OFDM 40 MHz chs) 27, 54, 81, 108, 162, 216, 243, 270 Mbps
RF Power Level	50 mW max.
Channels	FCC: 1-11, 36, 40 ,44, 48, 149, 153, 157, 161 ETSI: 1-13, 36, 40, 44 ,48
Connectivity	TCP/IP, Ethernet, ODI
Diversity	Yes

WPAN – Bluetooth

Bus Interface	USB
Enhanced Data Rate	Up to 3.0 Mbit/s over the air
Connection	No less than 32.80 feet (10 meters) line of sight
Bluetooth Version	2.0 + EDR
Operating Frequency	2.402 - 2.480 GHz
QDID	B013455

WWAN – Gobi 3000

Device	Gobi™ 2000 (data only), includes GPS
Device	Gobi™ 3000 (data only), includes GPS
Technology	Five-band UMTS/HSPA+ (800/850/900/1900/2100MHz), quadband GSM/GPRS/EDGE (850/900/1800/1900MHz) and dual-band EV-DO/CDMA (800/1900)

Port and Connector Pinouts

Power Supply Connector

VM1D Standard Dock and VM3D Enhanced Dock
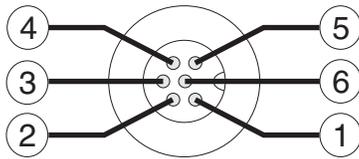
Pin	Signal	Description
1	V In+	10-60V DC input +
2	V In+	10-60V DC input +
3	V In-	input -
4	V In-	input -
5	GND	Chassis ground
6	Ignition	+0V to 60V to start terminal

VMXD Enhanced Dock
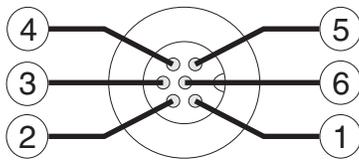
Pin	Signal	Description
1	V In+	13.2V DC Input + provided by DC/DC power supply
2	V In+	13.2V DC Input + provided by DC/DC power supply
3	V In-	Input -
4	V In-	Input -
5	COM1 RTS	Screen Blanking Box + The green wire in the power cable must be connected to the switched side of the screen blanking box. See the applicable wiring diagram below.
6	COM1 CTS	Screen Blanking Box - The white wire in the power cable must be connected to the unswitched side of the screen blanking box. See applicable wiring diagram below.
Cable shell provides chassis ground connection.		

VMXD Enhanced Dock for Off-Vehicle Use (QM3AC)

Pin	Signal	Description
1	V In+	15V DC Input + provided by AC/DC adapter
2	V In+	15V DC Input + provided by AC/DC adapter
3	V In-	Input -
4	V In-	Input -
5	GND	No connection.
6	Ignition	No connection
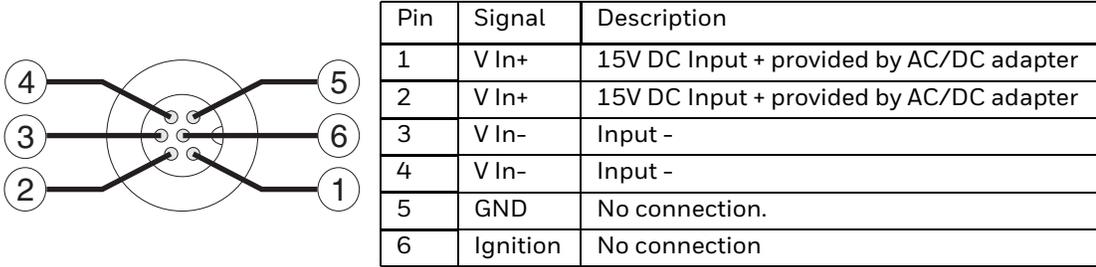
VMXD enhanced dock for off-vehicle use requires adapter cable VM1076CABLE to connect the dock to the AC/DC adapter. This cable is included in the AC kit for off-vehicle use.

COM1 and COM2 Connector

PIN 1   PIN 5

PIN 6   PIN 9
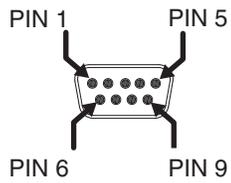
Pin	Signal	Description
1	DCD	Data Carrier Detect – Input
2	RXD	Receive Data – Input
3	TXD	Transmit Data – Output
4	DTR	Data Terminal Ready – Output
5	GND	Signal/Power Ground
6	DSR	Data Set Ready – Input
7	RTS	Request to Send – Output
8	CTS	Clear to Send – Input
9	+5VDC or RI	Bar Code Scanner Power - 500mA max or Ring Indicator - Input
Shell	CGND	Chassis Ground

VMXD Enhanced Dock only: Because the power supply connector port for the VMXD Enhanced Dock contains COM1 RTS and CTS signals, the COM1 port on the dock should not be used when the power cable is used for screen blanking to avoid port conflicts.

USB and USB1 Connector

The Standard Dock has a USB connector. The Enhanced Dock has a USB1 connector.
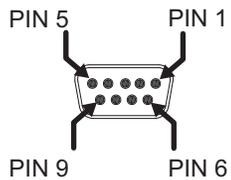
PIN 5   PIN 1

PIN 9   PIN 6

Pin	Signal	Description
1	GND	Common ground
2	USBC_D+	USB client data signal (not used)
3	USBC_D-	USB client data signal (not used)
4	USB_H1_PWR	USB host 1; 5V output power
5	GND	Common ground
6	GND	Common ground
7	USB_H1_D+	USB host 1 data signal
8	USB_H1_D-	USB host 1 data signal
9	USBC_VBUS	USB client 5V detect from attached host (not used)

USB Host/Client Y Cable

D9 Male Connector

PIN 1   PIN 5

PIN 6   PIN 9

Pin	Signal	Description
1	GND	Common ground
2	USBC_D+	USB client data signal (not used)
3	USBC_D-	USB client data signal (not used)
4	USB_H1_PWR	USB host 5V output power
5	GND	Common ground
6	GND	Common ground
7	USB_H1_D+	USB host 1 data signal
8	USB_H1_D-	USB host 1 data signal
9	USBC_VBUS	USB client 5V detect from attached host

USB Host Connector

PIN 4

PIN 1

Pin	Signal	Description
1	5V_USB	USB Power, Current Limited
2	USB_H1_D-	USB D-
3	USB_H1_D+	USB D+
4	GND	USB Power Return
Shell	CGND	Chassis Ground

USB Client Connector

The USB client connection is not supported on the Thor VM2 with the Windows Embedded Standard operating system.

USB Host to Scanner Cable

D9 Male Connector
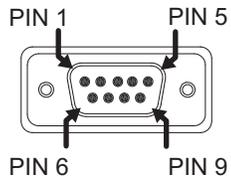
Pin	Signal	Description
1	Not used	
2	Not used	
3	Not used	
4	USB_H1_PWR	USB host 5V output power
5	GND	Common ground
6	Not used	
7	USB_H1_D+	USB host 1 data signal (twisted pair)
8	USB_H1_D-	USB host 1 data signal (twisted pair)
9	USBC_VBUS	USB client 5V detect from attached host

PIN 1   PIN 5

PIN 6   PIN 9

RJ50 Connector

PIN 10

PIN 1
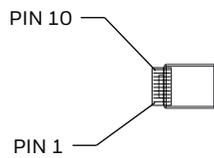
Pin	Signal	Description
1	Drain	To D9 connector shell
2	Not used	
3	GND	Common ground
4	Not used	
5	Not used	
6	Not used	
7	USB_H1_PWR	USB host 5V output power
8	Not used	
9	USB_H1_D+	USB host 1 data signal (twisted pair)
10	USB_H1_D-	USB host 1 data signal (twisted pair)

USB2 Connector

The USB2 connector is only present on the Enhanced Dock.
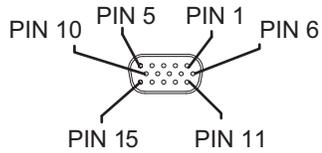
PIN 10 PIN 5   PIN 1 PIN 6

PIN 15   PIN 11

Pin	Signal	Description
1	Not Used	
2	Not Used	
3	Not Used	
4	Not Used	
5	Not Used	
6	USB_H2_PWR	USB host 2 5V output power
7	USB_H2_D+	USB host 2 data signal
8	USB_H2_D-	USB host 2 data signal
9	GND	Common ground
10	GND	Common ground
11	USB_H3_PWR	USB host 3 5V output power
12	USB_H3_D+	USB host 3 data signal
13	USB_H3_D-	USB host 3 data signal
14	GND	Common ground
15	GND	Common ground

USB Dual Host Y Cable

D15 Male Connector
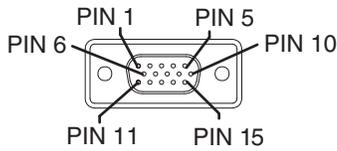
Pin	Signal	Description
1	Not Used	
2	Not Used	
3	Not Used	
4	Not Used	
5	Not Used	
6	USB_H2_PWR	USB host 2 5V output power
7	USB_H2_D+	USB host 2 data signal
8	USB_H2_D-	USB host 2 data signal
9	GND	Common ground
	GND	Common ground
	USB_H3_PWR	USB host 3 5V output power
	USB_H3_D+	USB host 3 data signal
	USB_H3_D-	USB host 3 data signal
	GND	Common ground
	GND	Common ground

USB Host Connectors

Pin	Signal	Description
1	5V_USB	USB Power, Current Limited
2	USB_H2_D-	USB D-
3	USB_H2_D+	USB D+
4	GND	USB Power Return
Shell	CGND	Chassis Ground

PS/2 to USB Keyboard Adapter Cable

D9 Male Connector - USB
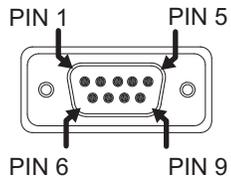
Pin	Signal	Description
1	Not Used	
2	Not Used	
3	Not Used	
4	USB_H1_PWR	USB host 5V output power
5	Not Used	
6	GND	Ground
7	USB_H1_D+	USB host 1 data signal
8	USB_H1_D-	USB host 1 data signal
9	USBC_VBUS	

PIN 1   PIN 5

PIN 6   PIN 9

D9 Female Connector – PS/2
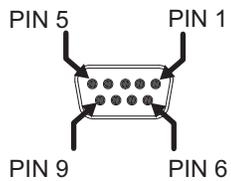
Pin	Signal	Description
1	KBDAT	Keyboard data
2	Not Used	
3	Not Used	
4	Not Used	
5	GND	Ground
6	Not Used	
7	KBCLK	Keyboard clock
8	GND	Ground
9	VCC	Keyboard power

PIN 5   PIN 1

PIN 9   PIN 6

CANbus / Audio Connector
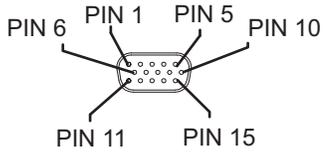
Pin	Signal	Description
1	–	CAN reserved
2	CAN_L	CAN_L bus line dominant low
3	CAN_GND	CAN Ground
4	–	CAN reserved
5	GND	Optional ground
6	Audio return	Headset return
7	Audio output	Headset output
8	Mic input	Microphone input
9	Mic return	Microphone return
10	Audio Return	
11	GND	Optional ground
12	CAN_SHLD	
13	CAN_H	CAN_H bus line dominant high
14	–	CAN reserved
15	CAN_V+	Option CAN external Power Supply

Headset Adapter Cable

D15 Female Connector
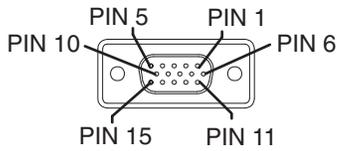
Pin	Signal	Description
1	Not used	
2	Not used	
3	Not used	
4	Not used	
5	Not used	
6	Audio return	Headset return
7	Audio output	Headset output
8	Mic input	Microphone input
9	Mic return	Microphone return
10	Not used	
11	Not used	
12	Not used	
13	Not used	
14	Not used	
15	Not used	

Quick Connect Headset Connector
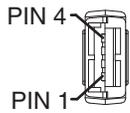
Pin	Signal	Description
1	Mic input	Microphone input
2	Mic return	Microphone return
3	Audio output	Headset output
4	Audio return	Headset return

CANbus Y Cable

D15 Female Connector

PIN 5   PIN 1
PIN 10   PIN 6
PIN 15   PIN 11
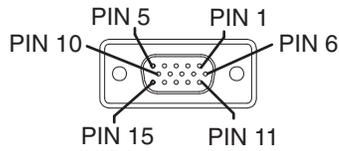
Pin	Signal	Description
1	Not Used	
2	CAN_L	CAN_L bus line dominant low
3	CAN_GND	CAN ground
4	Not Used	CAN reserved
5	GND	Ground
6	Not used	
7	Not used	
8	Not used	
9	Not used	
10	Not used	
11	GND	Optional ground
12	CAN_SHLD	
13	CAN_H	CAN_H bus line dominant high
14	Not Used	CAN reserved
15	CAN_V+	CAN external power supply

9-Pin J1939 (Deutsch) Connectors

Receptacle–
J1939 Female
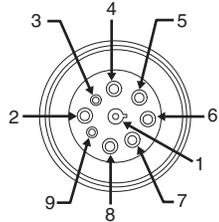
Socket
J1939 Male
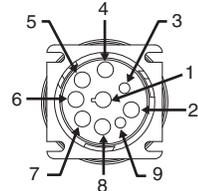
Pin	Signal	Description
1	CAN_GND	CAN Ground
2	CAN_V+	Option CAN external Power Supply
3	CAN_H	CAN_H bus line dominant high
4	CAN_L	CAN_L bus line dominant low
5	CAN_SHLD	
6	Not used	
7	Not used	
8	Not used	
9	Not used	

Hat Encoding

Desired ASCII	Hex Value	Hat Encoded	Desired ASCII	Hex Value	Hat Encoded
NUL	0X00	^@	HTJ	89	~^I
SOH	0X01	^A	VTS	8A	~^J
STX	0X02	^B	PLD	8B	~^K
ETX	0X03	^C	PLU	8C	~^L
EOT	0X04	^D	RI	8D	~^M
ENQ	0X05	^E	SS2	8E	~^N
ACK	0X06	^F	SS3	8F	~^O
BEL	0X07	^G	DCS	90	~^P
BS	0X08	^H	PU1	91	~^Q
HT	0X09	^I	PU2	92	~^R
LF	0X0A	^J	STS	93	~^S
VT	0A0B	^K	CCH	94	~^T
FF	0X0C	^L	MW	95	~^U
CR	0X0D	^M	SPA	96	~^V
SO	0X0D	^N	EPA	97	~^W
SI	0X0E	^O		98	~^X
DLE	0X0F	^P		99	~^Y
DC1 (XON)	0X10	^Q		9A	~^Z
DC2	0X11	^R	CSI	9B	~^[
DC3 (XOFF)	0X12	^S	ST	9C	~^\\
DC4	0X13	^T	OSC	9D	~^]
NAK	0X14	^U	PM	9E	~^^
SYN	0X15	^V	APC	9F	~^_ (underscore)
ETB	0X16	^W	(no-break space)	A0	~ (tilde and space)
CAN	0X17	^X	¡	A1	~!
EM	0X18	^Y	¢	A2	~"
SUB	0X19	^Z	£	A3	~#
ESC	0X1A	^[	¤	A4	~$
FS	0X1B	^\\	¥	A5	~%
GS	0X1C	^]	¦	A6	~&
RS	0X1D	^^	§	A7	~'
US	0X1E	^_ (underscore)	¨	A8	~(
	0X1F	^?	©	A9	~)
	80	~^@	ª	AA	~*
	81	~^A	«	AB	~+
	82	~^B	¬	AC	~,
	83	~^C	(soft hyphen)	AD	~- (dash)
IND	84	~^D	®	AE	~. (period)
NEL	85	~^E	¯	AF	~/
SSA	86	~^F	°	B0	~0 (zero)
ESA	87	~^G	±	B1	~1
HTS	88	~^H	²	B2	~2

Desired ASCII	Hex Value	Hat Encoded	Desired ASCII	Hex Value	Hat Encoded
³	B3	~3	Ú	DA	~Z
´	B4	~4	Û	DB	~[
µ	B5	~5	Ü	DC	~\\
¶	B6	~6	Ý	DD	~]
·	B7	~7	Þ	DE	~\^
¸	B8	~8	ß	DF	~_ (underscore)
¹	B9	~9	à	E0	~'
º	BA	~:	á	E1	~a
»	BB	~;	â	E2	~b
¼	BC	~<	ã	E3	~c
½	BD	~=	ä	E4	~d
¾	BE	~>	å	E5	~e
¿	BF	~?	æ	E6	~f
À	C0	~@	ç	E7	~g
Á	C1	~A	è	E8	~h
Â	C2	~B	é	E9	~i
Ã	C3	~C	ê	EA	~j
Ä	C4	~D	ë	EB	~k
Å	C5	~E	ì	EC	~l
Æ	C6	~F	í	ED	~m
Ç	C7	~G	î	EE	~n
È	C8	~H	ï	EF	~o
É	C9	~I	ð	F0	~p
Ê	CA	~J	ñ	F1	~q
Ë	CB	~K	ò	F2	~r
Ì	CC	~L	ó	F3	~s
Í	CD	~M	ô	F4	~t
Î	CE	~N	õ	F5	~u
Ï	CF	~O	ö	F6	~v
Ð	D0	~)	÷	F7	~w
Ñ	D1	~Q	ø	F8	~x
Ò	D2	~R	ù	F9	~y
Ó	D3	~S	ú	FA	~z
Ô	D4	~T	û	FB	~{
Õ	D5	~U	ü	FC	~|
Ö	D6	~V	ý	FD	~}
×	D7	~W	þ	FE	~~
Ø	D8	~X	ÿ	FF	~^?
Ù	D9	~Y			

GNU General Public License Version 2

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The 'Program', below, refers to any such program or work, and a 'work based on the Program' means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term 'modification'.) Each licensee is addressed as 'you'.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what theProgram does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and 'any later version', you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM 'AS IS' WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED

WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the 'copyright' line and a pointer to where the full notice is found.

```
one line to give the program's name and a brief idea of what it does. Copyright (C)
```

```
This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.
```

```
This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.
```

```
You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.
```

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

```
Gnomovision version 69, Copyright (C) year name of author Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type 'show w'. This is free software, and you are welcome to redistribute it under certain conditions; type 'show c' for details.
```

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than `show w' and `show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a 'copyright disclaimer' for the program, if necessary. Here is a sample; alter the names:

```
Yoyodyne, Inc., hereby disclaims all copyright interest in the program 'Gnomovision' (which makes passes at compilers) written by James Hacker.
```

```
signature of Ty Coon, 1 April 1989 Ty Coon, President of Vice
```

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Library General Public License instead of this License.

GNU General Public License Version 3

Version 3, 29 June 2007

Copyright (C) 2007 Free Software Foundation, Inc. http://fsf.org/

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The GNU General Public License is a free, copyleft license for software and other kinds of works.

The licenses for most software and other practical works are designed to take away your freedom to share and change the works. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change all versions of a program--to make sure it remains free software for all its users. We, the Free Software Foundation, use the GNU General Public License for most of our software; it applies also to any other work released this way by its authors. You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for them if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you these rights or asking you to surrender the rights. Therefore, you have certain responsibilities if you distribute copies of the software, or if you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must pass on to the recipients the same freedoms that you received. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

Developers that use the GNU GPL protect your rights with two steps: (1) assert copyright on the software, and (2) offer you this License giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains that there is no warranty for this free software. For both users' and authors' sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.

Some devices are designed to deny users access to install or run modified versions of the software inside them, although the manufacturer can do so. This is fundamentally incompatible with the aim of protecting users' freedom to change the software. The systematic pattern of such abuse occurs in the area of products for individuals to use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains, we stand ready to extend this provision to those domains in future versions of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents. States should not allow patents to restrict development and use of software on general-purpose computers, but in those that do, we wish to avoid the special danger that patents applied to a free program could make it effectively proprietary. To prevent this, the GPL assures that patents cannot be used to render the program non-free.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS

0. Definitions.

'This License' refers to version 3 of the GNU General Public License.

'Copyright' also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

'The Program' refers to any copyrightable work licensed under this License. Each licensee is addressed as 'you'. 'Licensees' and 'recipients' may be individuals or organizations.

To 'modify' a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a 'modified version' of the earlier work or a work 'based on' the earlier work.

A 'covered work' means either the unmodified Program or a work based on the Program.

To 'propagate' a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well.

To 'convey' a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays 'Appropriate Legal Notices' to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

1. Source Code.

The 'source code' for a work means the preferred form of the work for making modifications to it. 'Object code' means any non-source form of a work.

A 'Standard Interface' means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The 'System Libraries' of an executable work include anything, other than the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major

Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A 'Major Component', in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The 'Corresponding Source' for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work's System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

2. Basic Permissions.

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered by this License only if the output, given its content, constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed; section 10 makes it unnecessary.

3. Protecting Users' Legal Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of technological measures.

4. Conveying Verbatim Copies.

You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice; keep intact all notices stating that this License and any non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

5. Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

a) The work must carry prominent notices stating that you modified it, and giving a relevant date.

b) The work must carry prominent notices stating that it is released under this License and any conditions added under section 7. This requirement modifies the requirement in section 4 to 'keep intact all notices'.

c) You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it.

d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.

A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution medium, is called an 'aggregate' if the compilation and its resulting copyright are not used to limit the access or legal rights of the compilation's users beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate.

6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, in one of these ways:

a) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange.

b) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as long as you offer spare parts or customer support for that product model, to give anyone who

possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical medium customarily used for software interchange, for a price no more than your reasonable cost of physically performing this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge.

c) Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source. This alternative is allowed only occasionally and noncommercially, and only if you received the object code with such an offer, in accord with subsection 6b.

d) Convey the object code by offering access from a designated place (gratis or for a charge), and offer equivalent access to the Corresponding Source in the same way through the same place at no further charge. You need not require recipients to copy the Corresponding Source along with the object code. If the place to copy the object code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.

e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.

A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object code work.

A 'User Product' is either (1) a 'consumer product', which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, 'normally used' refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

'Installation Information' for a User Product means any methods, procedures, authorization keys, or other information required to install and execute modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in ROM).

The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

7. Additional Terms.

'Additional permissions' are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

a) Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or

b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or

c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or

d) Limiting the use for publicity purposes of names of licensors or authors of the material; or

e) Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or

f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on those licensors and authors.

All other non-permissive additional terms are considered 'further restrictions' within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions; the above requirements apply either way.

8. Termination.

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

10. Automatic Licensing of Downstream Recipients.

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An 'entity transaction' is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

11. Patents.

A 'contributor' is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's 'contributor version'.

A contributor's 'essential patent claims' are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For purposes of this definition, 'control' includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a 'patent license' is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To 'grant' such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. 'Knowingly relying' means you have actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient's use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is 'discriminatory' if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work

from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement, or that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.

12. No Surrender of Others' Freedom.

If conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot convey a covered work so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

13. Use with the GNU Affero General Public License.

Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed under version 3 of the GNU Affero General Public License into a single combined work, and to convey the resulting work. The terms of this License will continue to apply to the part which is the covered work, but the special requirements of the GNU Affero General Public License, section 13, concerning interaction through a network will apply to the combination as such.

14. Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of the GNU General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU General Public License 'or any later version' applies to it, you have the option of following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU General Public License, you may choose any version ever published by the Free Software Foundation.

If the Program specifies that a proxy can decide which future versions of the GNU General Public License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Program.

Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.

15. Disclaimer of Warranty.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM 'AS IS' WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

17. Interpretation of Sections 15 and 16.

If the disclaimer of warranty and limitation of liability provided above cannot be given local legal effect according to their terms, reviewing courts shall apply local law that most closely approximates an absolute waiver of all civil liability in connection with the Program, unless a warranty or assumption of liability accompanies a copy of the Program in return for a fee.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively state the exclusion of warranty; and each file should have at least the 'copyright' line and a pointer to where the full notice is found.

```
[one line to give the program's name and a brief idea of what it does.]

Copyright (C) [year] [name of author]

This program is free software: you can redistribute it and/or modify

it under the terms of the GNU General Public License as published by

the Free Software Foundation, either version 3 of the License, or

(at your option) any later version.

This program is distributed in the hope that it will be useful,

but WITHOUT ANY WARRANTY; without even the implied warranty of
```

```
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the

GNU General Public License for more details.

You should have received a copy of the GNU General Public License

along with this program. If not, see http://www.gnu.org/licenses/.
```

Also add information on how to contact you by electronic and paper mail.

If the program does terminal interaction, make it output a short notice like this when it starts in an interactive mode:

```
[program] Copyright (C) [year] [name of author]

This program comes with ABSOLUTELY NO WARRANTY; for details type 'show w'.

This is free software, and you are welcome to redistribute it

under certain conditions; type 'show c' for details.
```

The hypothetical commands 'show w' and 'show c' should show the appropriate parts of the General Public License. Of course, your program's commands might be different; for a GUI interface, you would use an 'about box'.

You should also get your employer (if you work as a programmer) or school, if any, to sign a 'copyright disclaimer' for the program, if necessary. For more information on this, and how to apply and follow the GNU GPL, see http://www.gnu.org/licenses/.

The GNU General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Lesser General Public License instead of this License. But first, please read http://www.gnu.org/philosophy/why-not-lgpl.html.

APPENDIX

C THOR VM2 AGENCY INFORMATION

Thor VM2 vehicle-mount computers meet or exceed the requirements of all applicable standards organizations for safe operation. The best way to ensure safe operation is to use the mobile computer according to the agency guidelines in this user guide and on the regulatory sheet shipped with the terminal. Read all guidelines before using your Dolphin terminal. To download product documentation for the Thor VM2 computer, go to www.honeywellaidc.com.

This documentation is relevant for the following Thor models: VM2C, VM2W.

The EU declaration of conformity, if applicable, and other publicly downloadable certificates are available at www.honeywellaidc.com/compliance.

Label Locations

Compliance labels are located in the dock well area on the back of the Thor VM2, as indicated by the shaded areas below. The Thor VM2 must be removed from the dock to view the labels.
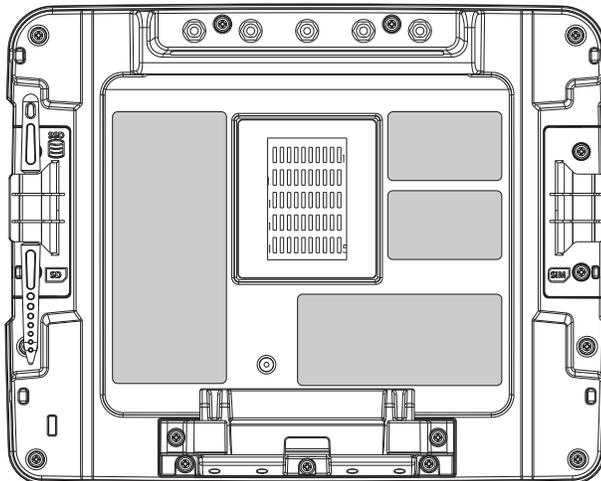
Model number, serial number and other identifiers are located on these labels.

Honeywell
9680 Old Bailes Road
Fort Mill, SC 29707

www.honeywellaidc.com