Honeywell

Thor™ VM2

Vehicle-Mounted Computer

Microsoft® Windows® Embedded Standard 2009 Operating System

Reference 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.

Web Address: www.honeywellaidc.com

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.

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

Summit Data Communications, the Laird Technologies Logo, the Summit logo, and "Connected. No Matter What" are trademarks of Laird Technologies, Inc.

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.

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

OneClick Internet is WebToGo's patented connection manager customized for Honeywell mobile devices. OneClick Internet documentation is copyright 2010 by WebToGo and modified by Honeywell with WebToGo's express permission.

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.

Acrobat® Reader © 2013 with express permission from Adobe Systems Incorporated.

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, please refer to www.honeywellaidc.com/patents.

Limited Warranty

Refer to www.honeywellaidc.com/warranty_information for your product's warranty information.

Table of Contents

Chapter 1 - Introduction

The Thor VM2 Vehicle Mount Computer (VMC) is a rugged, vehicle mounted computer running a Microsoft® Windows®Embedded Standard 2009 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 optional Bluetooth® module supports Bluetooth printers and scanners.

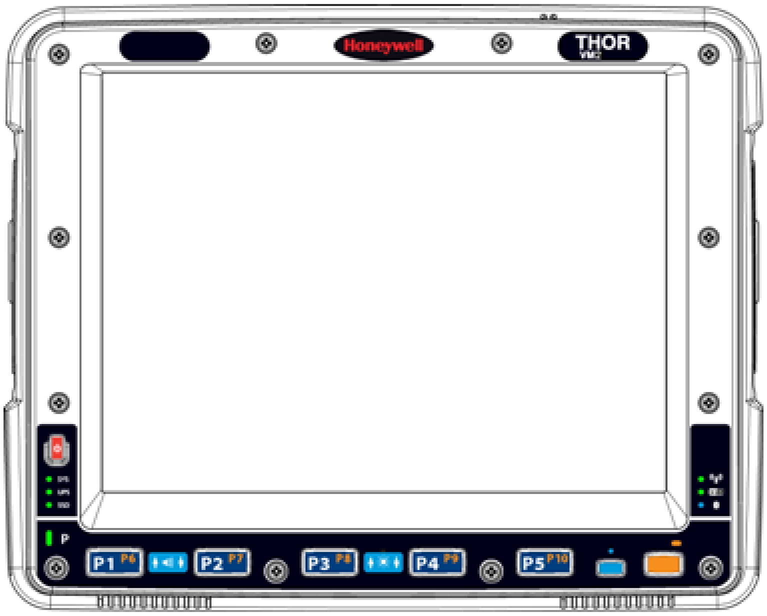
Caution ⚠	Before shipping the Thor VM2, the internal UPS battery must be disconnected.

The Thor VM2 is designed for use with a vehicle Quick Mount Smart 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 Quick Mount Smart Dock to another vehicle equipped with a Quick Mount Smart 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 Quick Mount Smart 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.



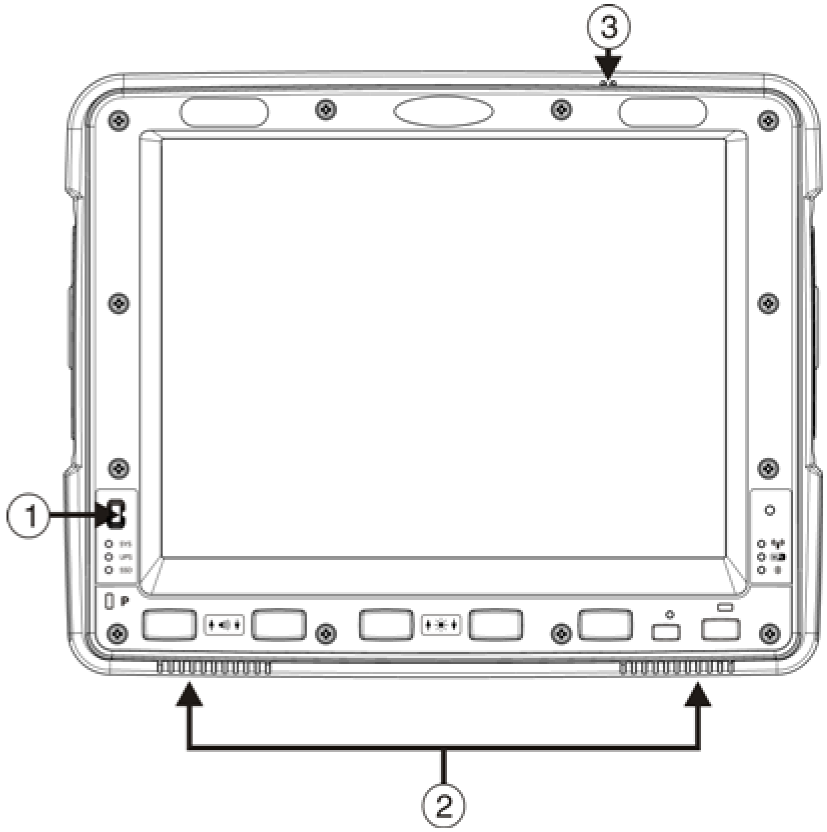
About this Guide

This Thor VM2 Reference Guide provides instruction for the system administrator to follow when configuring a Thor VM2.

This reference guide has been developed for a Thor VM2 with a Microsoft® Windows® Embedded Standard operating system.

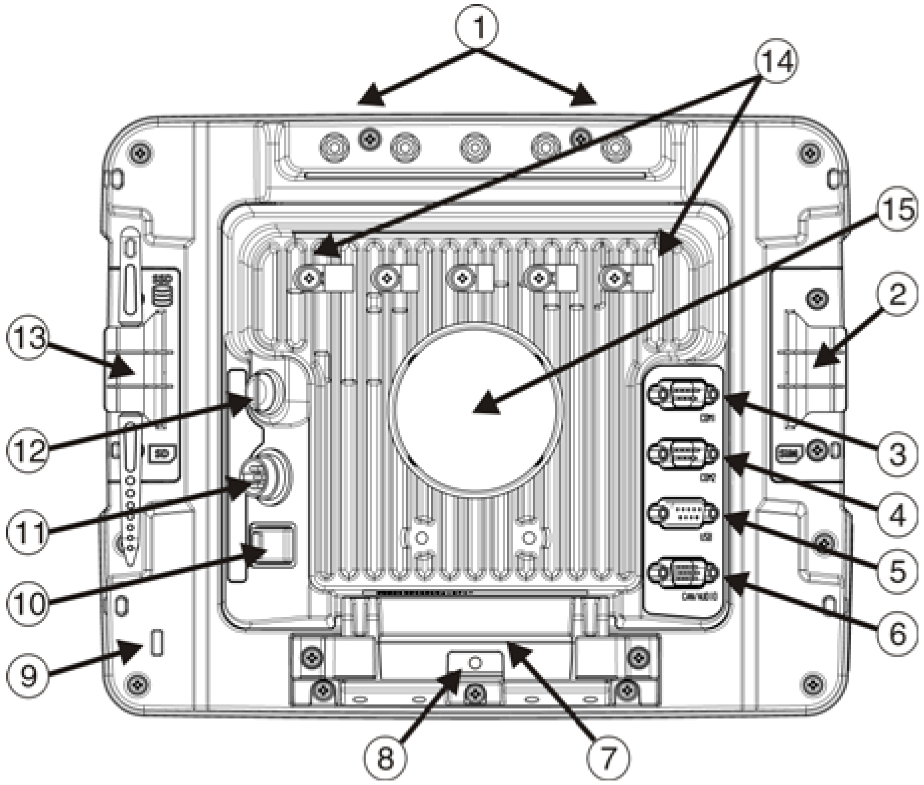
Components

Front View



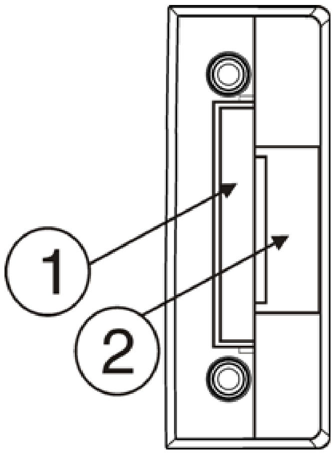
1. Power Button
2. Speakers
3. Microphone

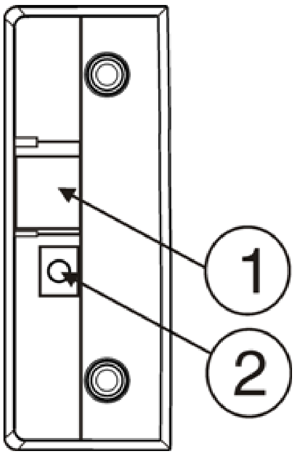
Back View with Quick Mount Smart Dock



1. Antenna Connectors (on Thor VM2)
2. SIM card Access Panel (on Thor VM2)
3. COM1 Connector (on Dock)
4. COM2 Connector (on Dock)
5. USB Connector (on Dock)
6. CAN/Audio Connector (on Dock)
7. Quick Release Handle (On Thor VM2)
8. Provision for Padlock (on Thor VM2)
9. Provision for Laptop Security Cable (on Thor VM2)
10. Power Switch (on Dock)
11. Power Connector (on Dock)
12. Fuse (on Dock)
13. SD Card Access Panel (On Thor VM2)
14. Strain Relief Clamps (on Dock)
15. RAM Ball (on Dock)

Access Panels





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

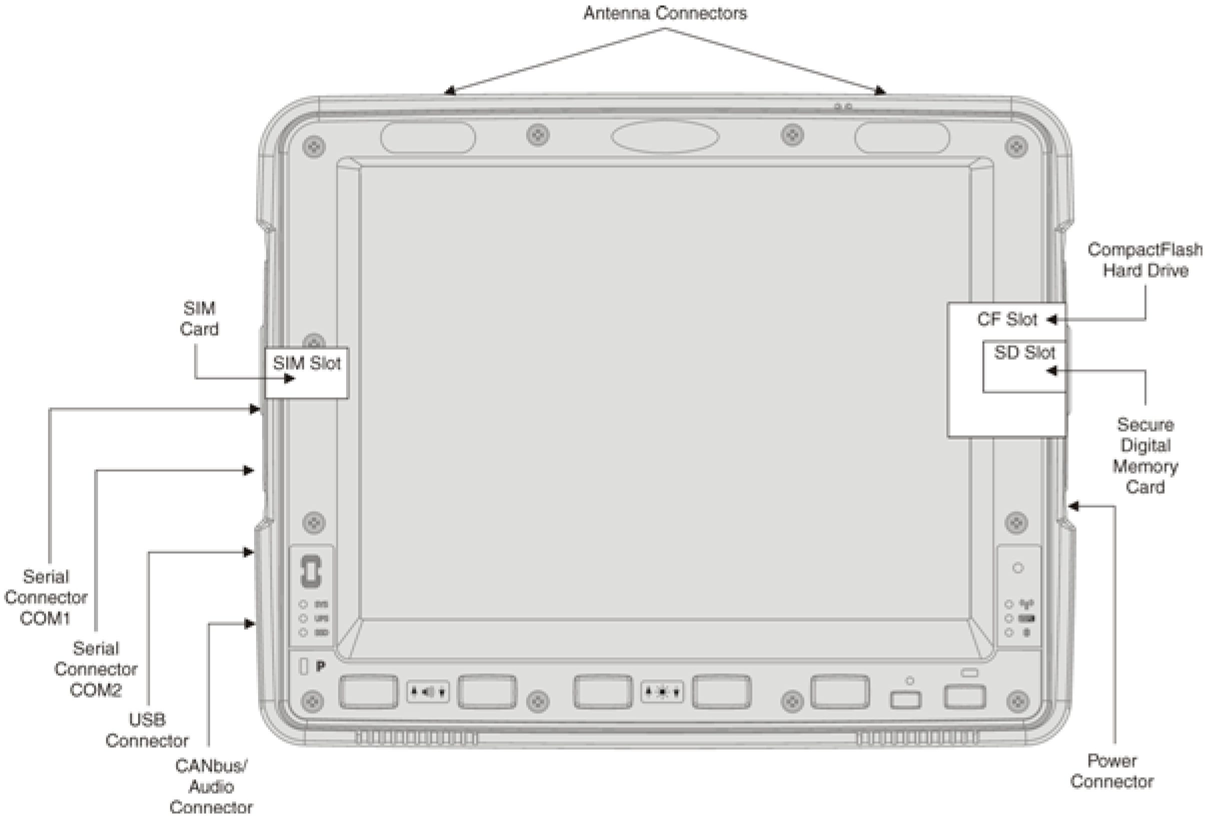
1. CompactFlash Hard Drive
2. SD (Secure Digital) Memory Card Slot

Access Panel Door is labeled with **SIM**.

1. SIM card slot for WWAN radio
2. UPS battery disconnect

Chapter 2 - Hardware

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.

Central Processing Unit

The CPU is a 1.6 GHz Intel Atom processor. The operating system is Microsoft Windows Embedded Standard 2009. The OS image is stored on an internal CompactFlash 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 configured as COM1 and COM2.
- One slot for SD memory card.
- CompactFlash (CF) drive.
- Integrated keyboard with programmable keys.
- Ports available via dongle cable:
  - USB Host port
  - USB Client port (Not available with Windows Embedded Standard OS)
  - CANbus
  - Audio

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 1024 x 768 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; beeps from the mobile Bluetooth scanner as the bar code data is accepted/rejected, and other beeps from the Thor VM2 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

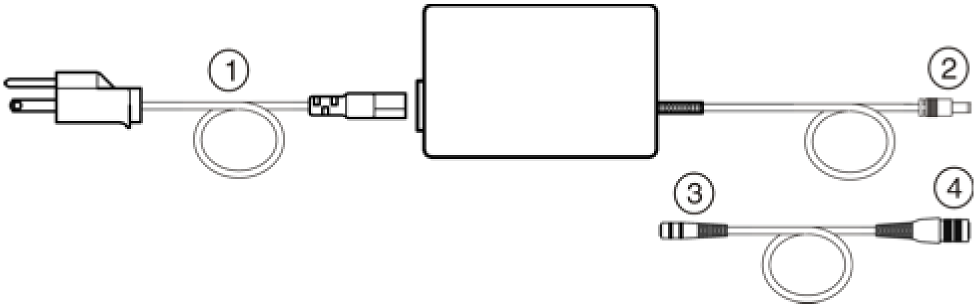
Vehicle power input for the Thor VM2 dock is 10V to 60V DC and is accepted without the need to perform any manual operation within the Thor VM2 dock. The dock provides a conditioned power output for the Thor VM2. By using a specified DC-to-DC adapter, input voltage of 72-144V DC nominal can be accepted.

If 10 to 60V DC power is not available – for example, in an office environment – an optional external Universal Input Power Supply can be used to convert AC wall power to an appropriate DC level.

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

External AC Power Supply

AC to DC power input for the Thor VM2 is delivered to the Quick Mount Smart Dock via an optional external power supply and adapter cable. One end of the adapter cable attaches to the dock and the other end is a barrel connector for the output cable from the adapter.



1. AC Input Cable (US only)
2. DC Output Cable
3. To DC Output Cable (see above)
4. To Thor VM2

In North America, this unit is intended for use with a UL Listed ITE power supply with output rated 12 – 48 VDC, minimum 15 W. Outside North America, this unit is intended for use with an IEC certified ITE power supply with output rated 12 – 48 VDC, minimum 15 W.

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

Please refer to the wiring instructions, including appropriate cautions and warnings, in the *Thor VM2 User Guide*.

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.

- A fully discharged UPS battery recharges in under 4 hours when the Thor VM2 is in a powered dock.
- Charging does not occur when either Ignition Mode power scheme is selected and the ignition is inactive.
- Charging of the UPS battery continues during power management of the Thor VM2.
- If the UPS battery is not charged before the timeout expires, the fault LED is lit.
- If the UPS battery cannot be charged due to a temperature extreme, the fault LED is lit. Move the Thor VM2 to a different location to charge the UPS battery.

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. 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.

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.

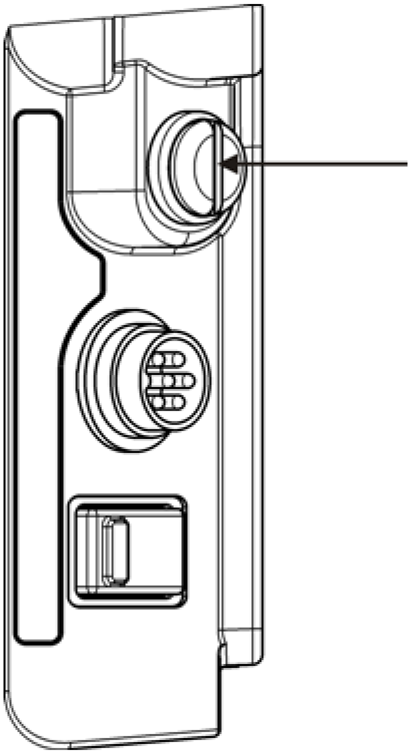
Note: The backup battery should only be changed by authorized service personnel.

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 Quick Mount Smart Dock. The fuse is accessed by unscrewing the cap as indicated below.

Should it need replacement, replace with same size, rating and type of fuse – Littelfuse 0215008.MXP 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: On, Standby, 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 Control Panel > Power Options > Advanced.

Standby Mode

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

When in Standby 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.

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

System Standby Wakeup Events

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

- Pressing and releasing the Power button.

Off Mode

By default, the Thor VM2 turns off if the user presses the power button when the Thor VM2 is On. This behavior can be configured on the Advanced tab of the Power control panel.

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 Configuration

Use the Power Schemes tab of the Power control panel to select the desired behavior.

AC/DC

The Thor VM2 is powered on manually. 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 "Plugged In" power management settings which correspond to the state of the vehicle ignition.

Auto-On

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.

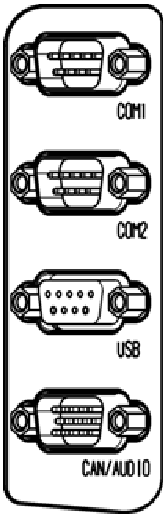
UPS

The Thor VM2 uses the UPS mode whenever external power is not available. When external power is not present the "Running on Batteries" power management timeouts from the selected Power Scheme are used.

External Connectors

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

Most external connectors for the Thor VM2 are located on the Quick Mount Smart Dock:



- COM1 connects to a serial bar code scanner, screen blanking cable, serial printer or PC.
- COM2 connects to a serial bar code scanner, screen blanking cable, serial printer or PC.
- USB accepts a dongle cable with a USB Host port and a USB Client port. USB Client is not used with the Windows Embedded Standard operating system.
- CANbus/Audio accepts a cable with connections for a mono headset/microphone or a cable with CANbus adapters.

The power connector is on the dock.

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

Serial Connector (COM1 and COM2)

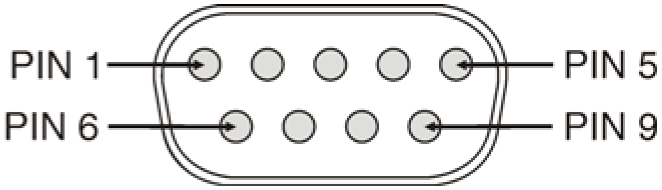
The COM1 and COM2 connectors are D-9 male connectors located on the back of the Quick Mount Smart Dock.

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.

Pin 9 is configured to provide +5V for an external bar code scanner.

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



Pinout

Pin	Signal	Description
1	DCD	Data Carrier Detect – Input
2	RXD	Receive Data – Input
3	TXD	Transmit Data – Output
4	DTR	Data Terminal Ready – Output
5	GND	Signal/Power Ground
6	DSR	Data Set Ready – Input
7	RTS	Request to Send – Output
8	CTS	Clear to Send – Input
9	+5VDC	Bar Code Scanner Power - 500mA max
Shell	CGND	Chassis Ground

Screen Blanking

The screen blanking signal can be provided either by a Honeywell Screen Blanking Box or a user supplied switch or relay.

- A screen blanking box can be used on a vehicle that provides voltage on vehicle motion. Voltage must be within the range specified on the screen blanking box label.
- A switch or relay can be used when an electrical signal is not available or is outside the acceptable range of the screen blanking box.

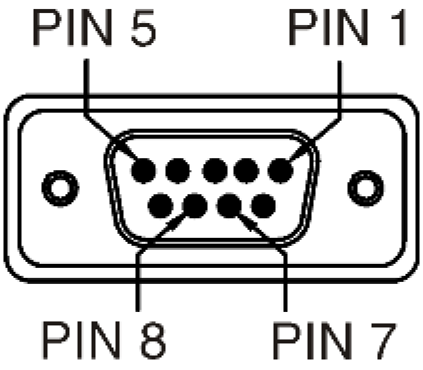
A serial cable must be used to connect the screen blanking device:

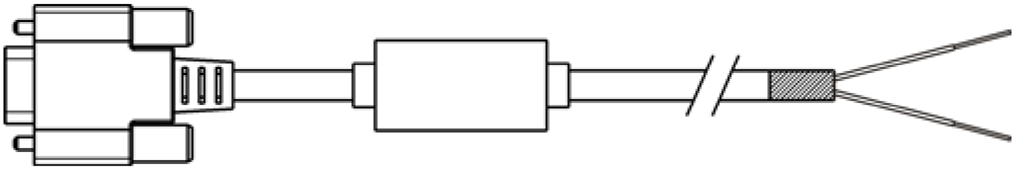
- An optional Screen Blanking Box Cable is available from Honeywell, or
- A user supplied serial cable can be used. The cable must provide wires from pins 7 and 8 of the connector. No other wires are used.

⚠	Do not enable Screen Blanking until the cable is properly connected to the specified COM port.

Serial Cable

Optional Honeywell Screen Blanking Box Cable (part number VM1080CABLE) or customer built cable with the following specifications.





DB9 Female	Function with Screen Blanking Box	Function with Switch	Wire color from Honeywell Cable
1	Not Used	Not Used	
2	Not Used	Not Used	
3	Not Used	Not Used	
4	Not Used	Not Used	
5	Not Used	Not Used	

DB9 Female	Function with Screen Blanking Box	Function with Switch	Wire color from Honeywell Cable
6	Not Used	Not Used	
7 (RTS)	Connected to Screen Blanking Box	Connected to Switch	Black (see note)
8 (CTS)	Connected to Screen Blanking Box	Connected to Switch	Gray (see note)
9	Not Used	Not Used	

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

Proper COM port settings to support screen blanking are located in Start > Control Panel > Screen.

Screen Blanking Box

Caution ⚠	Please refer to the label on the screen blanking box for allowable input voltage range.

The Screen Blanking Box is designed to monitor a connection to a vehicle motion sensing circuit. When motion is detected, the Screen Blanking Box opens the connection between the output feeds (which are connected to Pins 7 and 8 of the Thor VM2) and the display on the Thor VM2 is blanked. When motion is no longer detected the Screen Blanking Box provides a connection between the output feeds. After the configured Screen On delay, if any, the Thor VM2 screen is displayed.

Please refer to the wiring instructions, including appropriate cautions and warnings, in the *Thor VM2 Vehicle Mounting Reference Guide*.

Screen Blanking with Switch

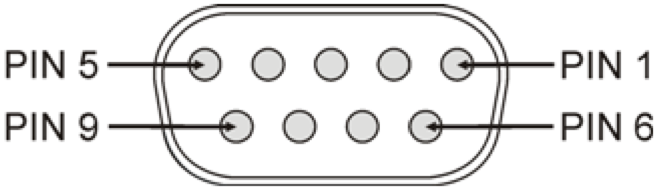
In applications where it is impractical to use the screen blanking box due to vehicle voltage or lack of a motion sensing signal, screen blanking can be controlled via a user supplied switch or relay that provides an electrical conductive connection between the wires connected to Pins 7 and 8 of the screen blanking cable on vehicle motion.

Please refer to the wiring instructions, including appropriate cautions and warnings, in the *Thor VM2 Vehicle Mounting Reference Guide*.

USB Connector

The USB connector is a D-9 female connector located on the back of the Quick Mount Smart Dock.

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

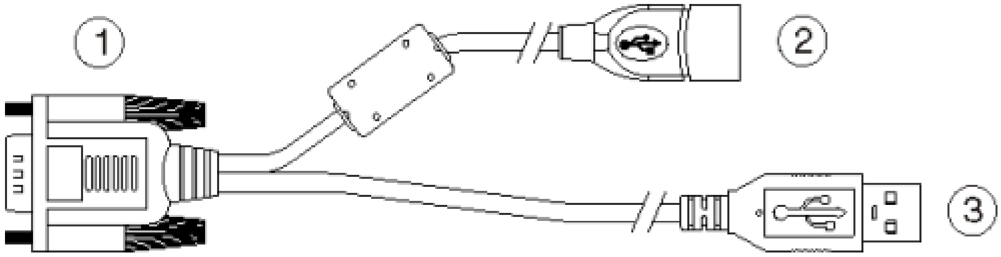


Pin	Signal	Description
1	GND	Common ground
2	USBC_D+	USB client data signal (not used)
3	USBC_D-	USB client data signal (not used)
4	USB_H1_PWR	USB host 1; 5V output power
5	GND	Common ground
6	GND	Common ground
7	USB_H1_D+	USB host 1 data signal
8	USB_H1_D-	USB host 1 data signal
9	USBC_VBUS	USB client 5V detect from attached host (not used)

USB Dongle Cable

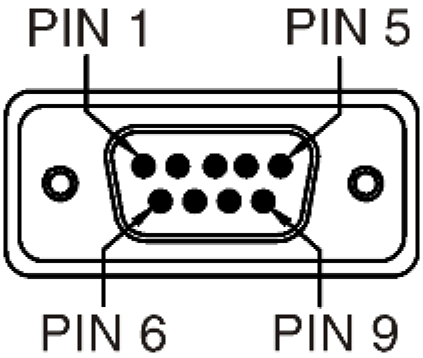
USB dongle cables have a Host port and a Client port.

The USB Client port is not used when the Thor VM2 has a Windows Embedded Standard operating system.



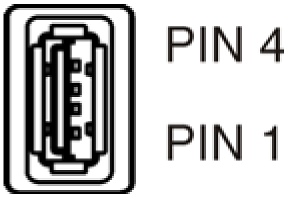
1. D9 Connector
2. USB Host Connector(s)
3. USB Client Connector (not used)

D9 Male Connector



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 (not used)

USB Host Connector

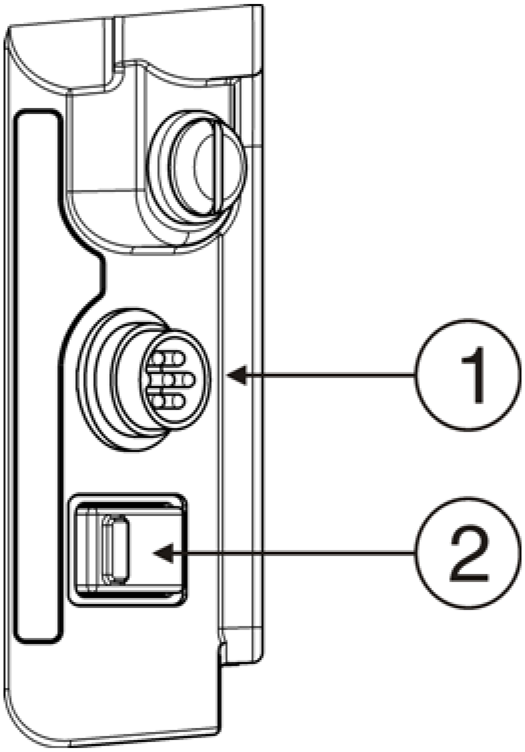


Pin	Signal	Description
1	5V_USB	USB Power, Current Limited
2	USB_H1_D-	USB D-
3	USB_H1_D+	USB D+
4	GND	USB Power Return
Shell	CGND	Chassis Ground

USB Client Connector

The USB Client connector is not supported on the Thor VM2 with the Windows Embedded Standard operating system.

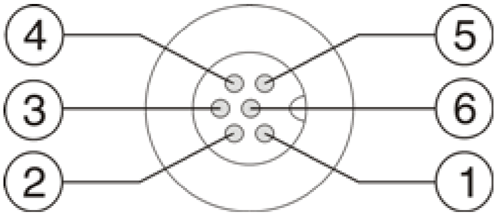
Power Supply Connector



1. Power Connector
2. Power Switch

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.

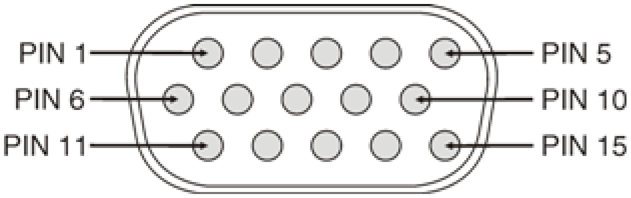


Pin	Signal	Description
1	V In+	10-60V DC input +
2	V In+	10-60V DC input +
3	V In-	input -
4	V In-	input -
5	GND	Chassis ground
6	Ignition	+0V to 60V to start terminal

CANbus / Audio Connector

The CANbus/Audio connector is a D-15 male connector located on the back of the Quick Mount Smart Dock.

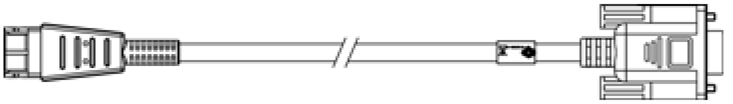
The connector supports a headset adapter cable or a CANbus cable. The Thor VM2 does not support connecting audio and CANbus simultaneously.



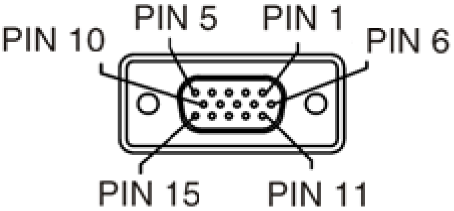
Pin	Signal Name	Description
1	-	CAN reserved
2	CAN_L	CAN_L bus line dominant low
3	CAN_GND	CAN Ground
4	-	CAN reserved
5	GND	Optional ground
6	Audio return	Headset return
7	Audio output	Headset output
8	Mic input	Microphone input
9	Mic return	Microphone return
10	Audio Return	
11	GND	Optional ground
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

The headset cable attaches to the CANbus / Audio connector and provides a quick connect connection for a headset.

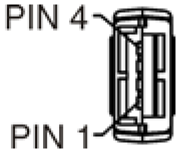


D15 Female Connector



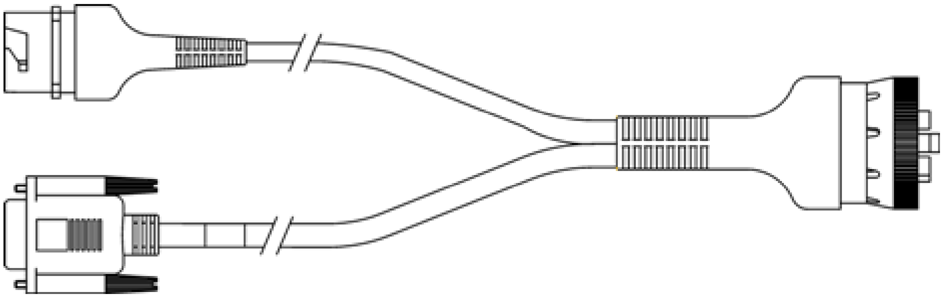
Pin	Signal	Description
1	-	Not used
2	-	Not used
3	-	Not used
4	-	Not used
5	-	Not used
6	Audio return	Headset return
7	Audio output	Headset output
8	Mic input	Microphone input
9	Mic return	Microphone return
10	-	Not used
11	-	Not used
12	-	Not used
13	-	Not used
14	-	Not used
15	-	Not used

Quick Connect Headset Connector



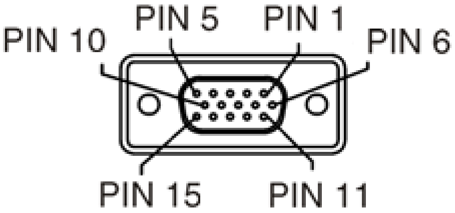
Pin	Signal	Description
1	Mic input	Microphone input
2	Mic return	Microphone return
3	Audio output	Headset output
4	Audio return	Headset return

CANbus Cable



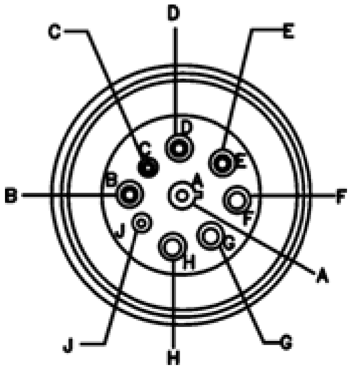
The CANbus interface is a virtual COM4 port. This port can be accessed using standard Windows API calls.

D15 Female Connector

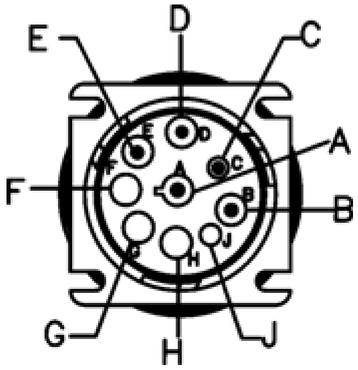


Pin	Signal	Description
1	-	Not used
2	CAN_L	CAN_L bus line dominant low
3	CAN_GND	CAN ground
4	-	CAN reserved
5	GND	Ground
6	-	Not used
7	-	Not used
8	-	Not used
9	-	Not used
10	-	Not used
11	GND	Optional ground
12	CAN_SHLD	
13	CAN_H	CAN_H bus line dominant high
14	-	CAN reserved
15	CAN_V+	CAN external power supply

9-Pin J1939 (Deutsch) Connectors



Receptacle
J1939 Female

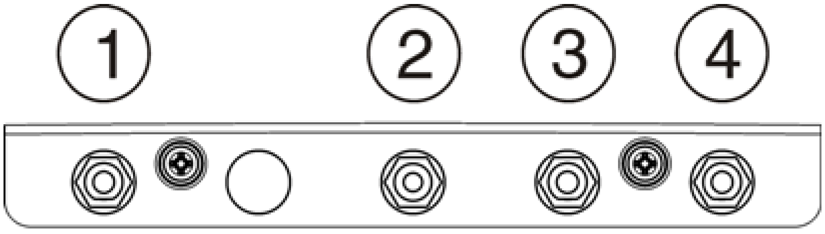


Socket
J1939 Male

Pin	Signal	Description
A	CAN_GND	CAN Ground
B	CAN_V+	Option CAN external Power Supply
C	CAN_H	CAN_H bus line dominant high
D	CAN_L	CAN_L bus line dominant low
E	CAN_SHLD	
F	-	Not used
G	-	Not used
H	-	Not used
J	-	Not used

Antenna Connections

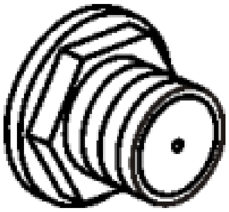
The Thor VM2 is equipped with an 802.11 radio and can be ordered with internal antennas, external antennas or external remote mount antennas. When the Thor VM2 is ordered with internal antennas, the external antenna connectors are not used. GPS and WWAN are optional on the Thor VM2 and require external 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

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 is connected to the 802.11 radio.



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

Internal WiFi Antenna

If the internal WiFi antenna option is ordered, an antenna is mounted inside the Thor VM2. The internal antenna is not user accessible.

External WiFi Antenna

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

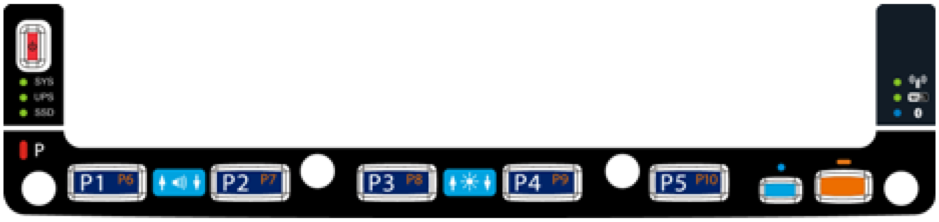
Vehicle Remote Antenna

The external antennas can be remotely mounted on the vehicle. See the *Thor VM2 Vehicle Mounting Reference Guide* for instruction. External antenna kits are available for the 802.11 WiFi radio, GPS and WWAN.

Keyboard Options

The Thor VM2 has an integrated keypad with five programmable keys and an available external keyboard.

Integrated Keypad



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 (Start > Control Panel > Programmable Key).
- Programmable keys persist across a reboot or power cycle.
- When used with the Blue modifier key, P1 through P4 keys are used to adjust speaker volume and display brightness.

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 Start > Control Panel > Power Options.
- The integrated keypad backlight can be disabled. See Start > Control Panel > Options.

Keypad LEDs

Blue LED

When the Blue LED is illuminated, the programmable keys are used to adjust speaker volume and display brightness.

- Blue + P1 = Increase speaker volume
- Blue + P2 = Decrease speaker volume
- Blue + P3 = Increase display brightness
- Blue + P4 = Decrease display brightness
- No function is assigned to Blue + P5

The Blue key has a five second timeout. If the Blue key is pressed and no additional key is pressed within the five second timeout period, the Blue modifier mode is exited and the Blue LED is turned off.

When the Blue modifier key is active, the LED located next to the key is illuminated. The Blue modifier key remains active until:

- The Blue key is pressed again, or
- The Orange key is pressed, or
- A five second timeout with no keypress occurs.

Orange LED

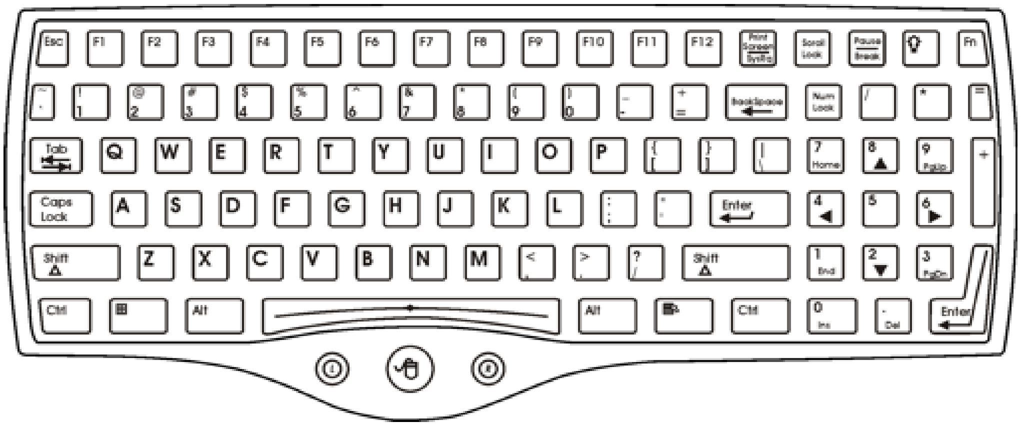
When the Orange LED is illuminated, the programmable keys provide the secondary function.

- Orange + P1 = P6
- Orange + P2 = P7, etc.

When the Orange modifier key is active, the LED located next to the key is illuminated. The Orange modifier key remains active until:

- The Orange key is pressed again, or
- The Blue key is pressed, or
- A non-modifier key is pressed.

95-Key Keyboard



The Thor VM2 uses an optional rugged QWERTY 95 key keyboard, designed for ease of use with the Windows CE operating system. The keyboard connects directly to the D9 USB connector on the Thor VM2 Quick Mount Smart 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. However USB power can be enabled during Standby which keeps the backlight on.

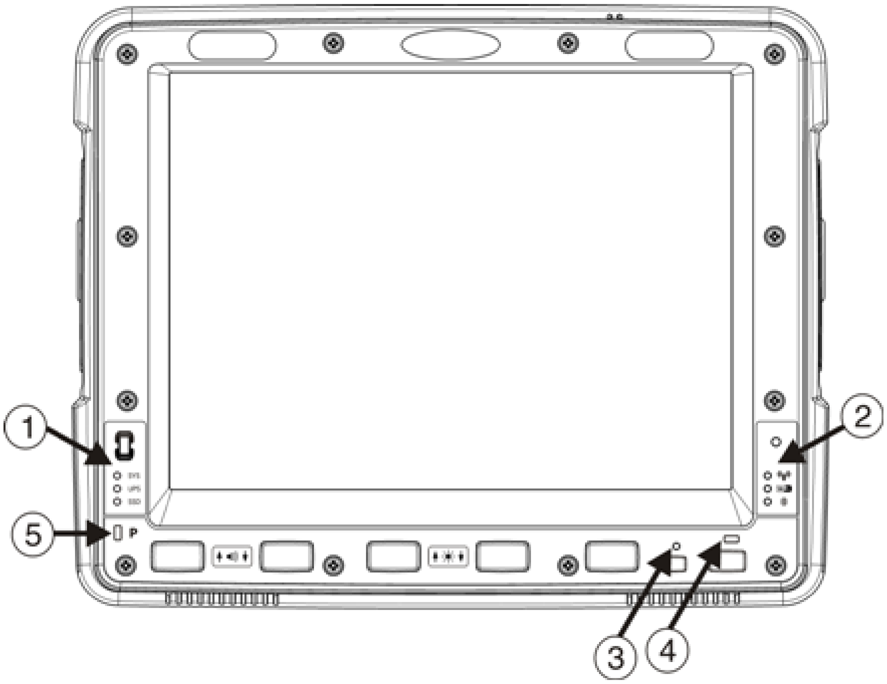
This behavior can be changed by enabling USB power in Standby. See Start > Control Panel > Options.

USB Keyboard / Mouse

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

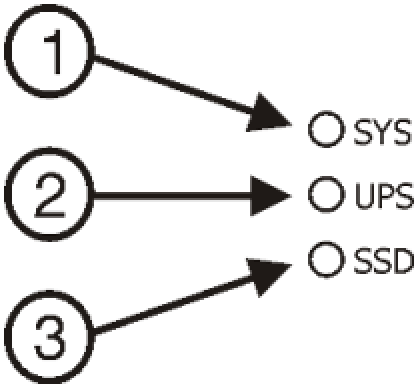
The dongle cable attaches to the Thor VM2 and provides a USB connector. Please refer to documentation provided with the USB keyboard or mouse for more information on their operation.

LED Functions



1. System LEDs
2. Connection LEDs
3. Blue LED
4. Orange LED
5. Programmable LED

System LEDs



1. SYS (System Status) LED
2. UPS (Uninterruptible Power Supply) LED
3. SSD (Solid State Drive) LED

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
Off External power present	• Off • Hibernate
Off External power not present	• Off, • Hibernate • Standby
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.
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 charging temperature range, • No UPS present, • Charge timeout.
Red	Low battery, less than 2 minutes runtime until shutdown

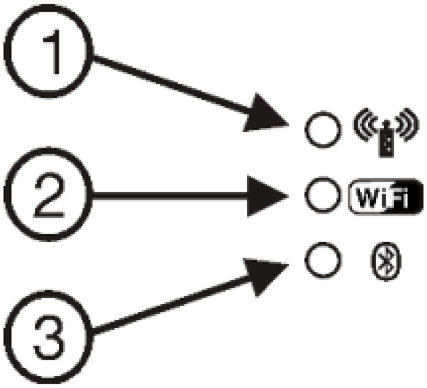
Charging State

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 Standby or 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



1. WWAN LED
2. WiFi LED
3. Bluetooth LED

WWAN LED

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

WiFi 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.

The LED behavior is controlled by the NLedDriverSetDevice API.

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 1024 x 768 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.

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.

Screen Blanking

Screen blanking (blackout) can be enabled when the vehicle is in motion. A serial cable must be attached to the Thor VM2 and the Thor VM2 must be configured to enable screen blanking (Start > Control Panel >Screen). Once screen blanking is enabled, the display is blanked out any time when the cable sends the signal 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:

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

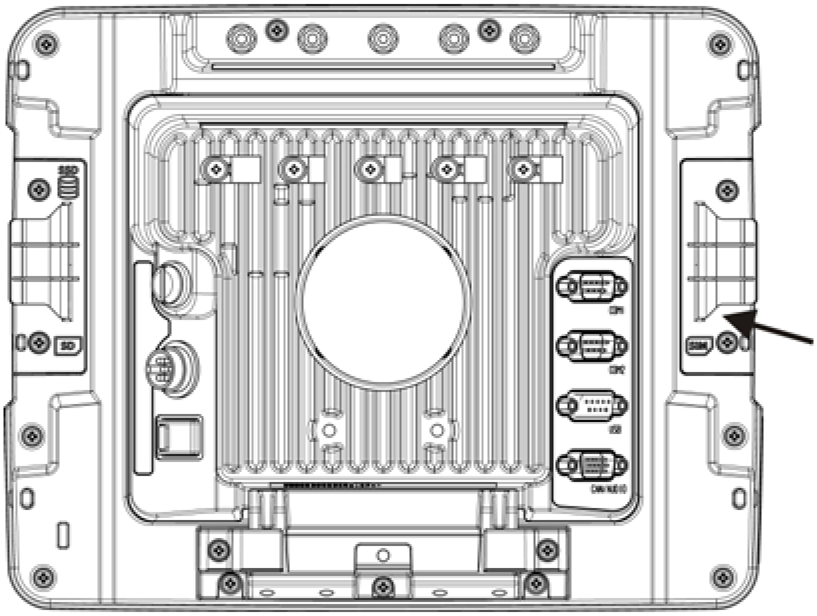
Disconnect UPS Battery

Equipment Required- User Supplied:

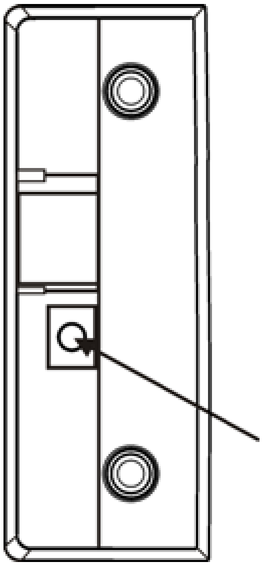
- Torquing tool capable of measuring inch pounds
- #2 Philips screwdriver bit

Caution ⚠	The UPS battery must be disconnected before shipping the Thor VM2 or replacing the front panel.

1. For convenience, the Thor VM2 can be removed from the Quick Mount Vehicle 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 Philips 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.



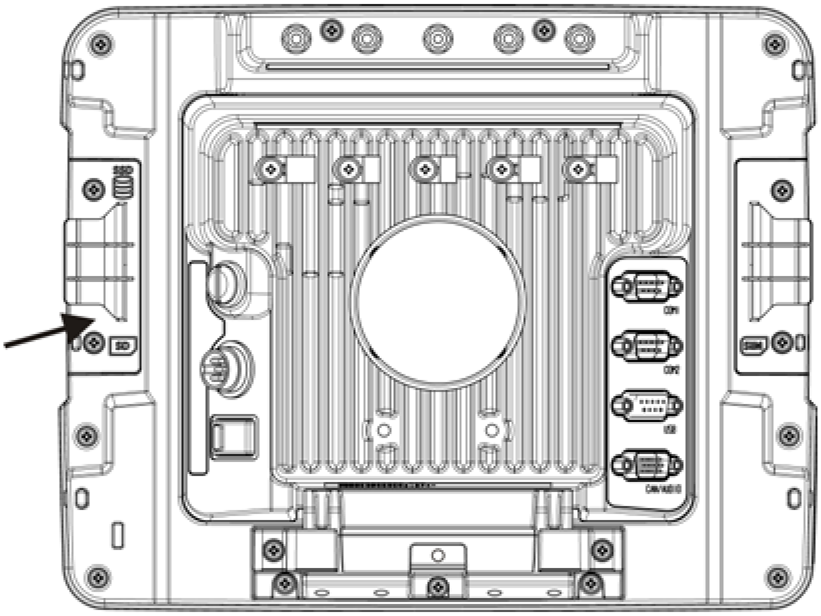
7. Press the push button to disconnect the UPS. The UPS battery maintains its charge but is disconnected from the power circuitry of the Thor VM2.
8. Reattach the access panel, torquing the M3 screws to 4-5 inch pounds using a #2 Philips bit.
9. When the Thor VM2 is attached to external power, the UPS battery is automatically reconnected.

Install SD Card

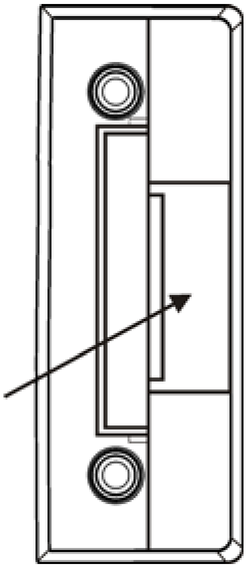
Equipment Required - User Supplied:

- Torquing tool capable of measuring inch pounds
- #2 Philips screwdriver bit
- SD card - The following commercially available SD cards are recommended:
  - Transcend® 2GB Industrial SD card (80X Speed) - **TS2GSD80I**
  - ATP 4GB Industrial Grade SDHC card - **AF4GSDI**

1. For convenience, the Thor VM2 can be removed from the Quick Mount Vehicle Dock, though it is not necessary.
2. Shutdown the Thor VM2 from the Windows menu.
3. Place the Thor VM2 face down on a stable surface.
4. Using a Phillips screwdriver (not supplied) loosen the screws and then remove the tethered access panel with the SSD and SD label. This panel is on the left hand side when the Thor VM2 is face down with the top away from the user.



5. Locate the SD card installation slot.



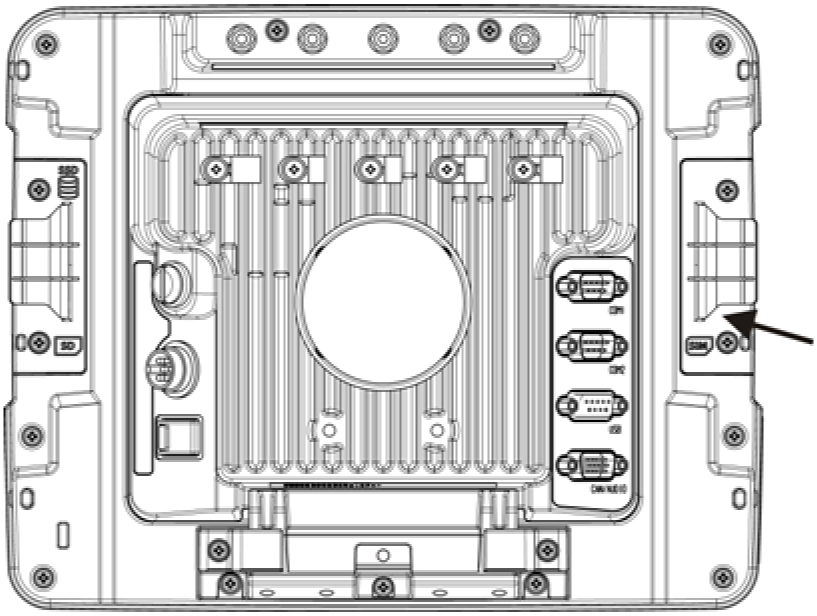
6. Slide the SD card into the slot. The label side (front) of the SD card faces toward the back of the Thor VM2.
7. Reattach the access panel, torquing the screws to 4-5 inch pounds.
8. If removed, reinstall the Thor VM2 in the Dock.
9. Restart the Thor VM2
10. When using Windows explorer to view **My Computer,** the SD card is identified as a **Removable Disk**, usually Drive D:

Install SIM Card

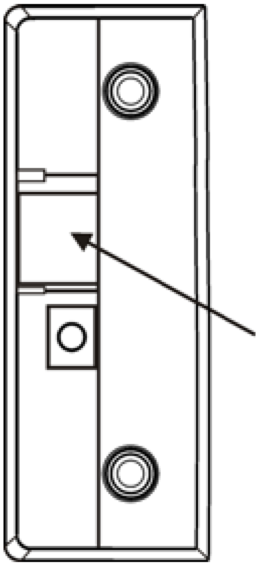
Equipment Required - User Supplied:

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

1. For convenience, the Thor VM2 can be removed from the Quick Mount Vehicle Dock, though it is not necessary.
2. Shutdown the Thor VM2 from the Windows menu.
3. Place the Thor VM2 face down on a stable surface.
4. Using a Phillips screwdriver (not supplied) loosen the 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.



5. Locate the SIM card installation slot.



6. Slide the SIM card into the slot.
7. Reattach the access panel, torquing the screws to 4-5 inch pounds.
8. If removed, reinstall the Thor VM2 in the Dock.
9. Restart the Thor VM2

Field Replaceable Front Panel

Equipment Required - User Supplied:

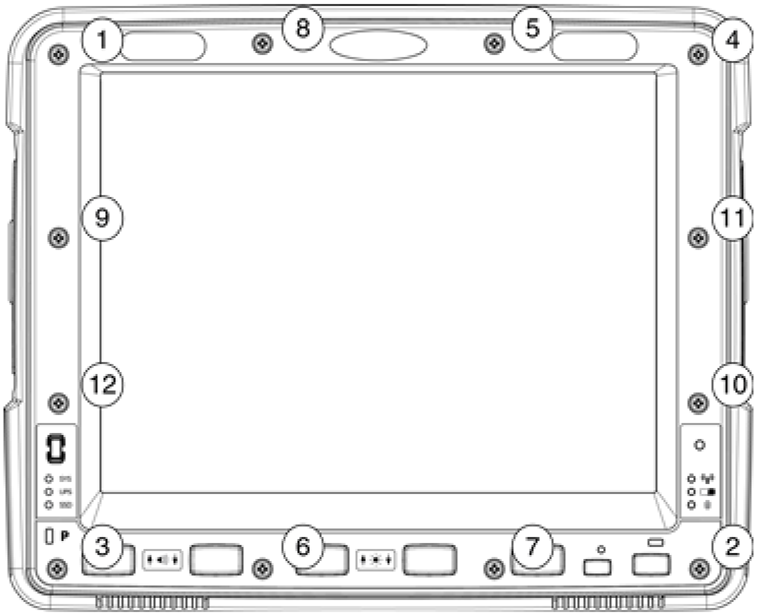
- Torquing tool capable of measuring inch pounds
- #2 Philips screwdriver bit

Caution ⚠	Before replacing the Thor VM2 front panel, the internal UPS battery must be disconnected.

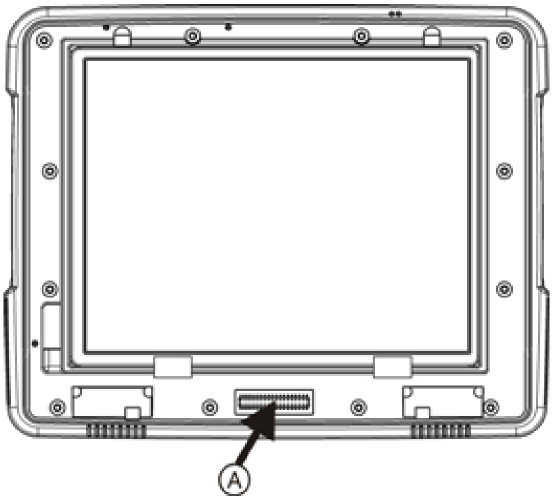
The front panel of the Thor VM2 is field replaceable. The front panel assembly contains the integrated keypad and touch screen. Should either of these components fail, the front panel assembly can easily be replaced to reduce downtime.

Replace Front Panel

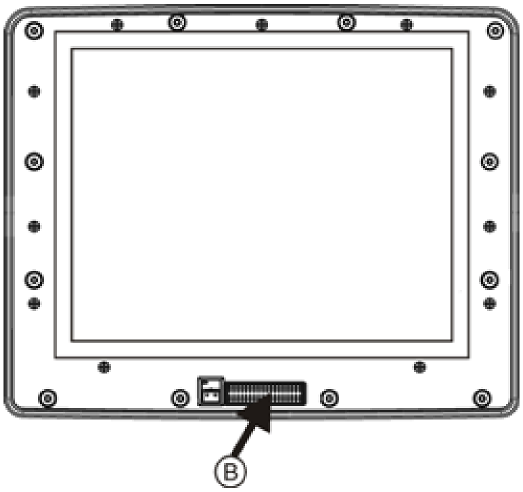
1. Place the Thor VM2 on a clean, well-lit surface before performing the front panel replacement.
2. Shutdown the Thor VM2 from the Windows menu.
3. Remove the Thor VM2 from the Quick Mount Smart Dock.
4. Disconnect the UPS.
5. Loosen the twelve (12) captive M3 screws holding the front panel. Use a #2 Philips bit.



5. Carefully lift the front panel away from the device.



A. Wiring connector on Thor VM2 body



B. Wiring connector on front panel

6. Position the replacement front panel so wiring connector on the back of the front (B in figure above) panel lines up with the connector (A in figure above) on the Thor VM2.
7. Gently press the front panel into place.
8. Tighten the twelve (12) captive M3 screws. In the order shown in the top figure above, use a #2 Philips bit and torque the screws to 6-7 inch pounds.
9. Reinstall the Thor VM2 in the Quick Mount Smart Dock.
10. When the Thor VM2 is placed in the powered dock, the UPS battery automatically reconnects.
11. Restart the Thor VM2.

Chapter 3 - 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.

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

The software loaded on the Thor VM2 computer consists of:

- BIOS
- Microsoft operating system (Windows Embedded Standard 2009)
- device drivers
- radio software
- touch screen software

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 Add or Remove Programs icon in the Windows Control Panel.

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. Please see Touch Screen Calibration for more information.

Programs Loaded on Drive C

Honeywell RFTerm (Optional)

Start > All Programs > Honeywell RFTerm

Terminal emulation software. The application can also be accessed by double-clicking the RFTerm desktop icon.

Summit Client Utility

Start > Control Panel > Wi-Fi

Manage wireless clients installed in the Thor VM2.

*Freefloat Link*One Wedge (Optional)*

Link*One bar code decoder configuration software is available on the Thor VM2. Click here for the Freefloat website.

*Freefloat Access*One TE (Optional)*

Access*One terminal emulation software is available on the Thor VM2. Click here for the Freefloat website.

*Freefloat Key*One*

Key*One input panel (soft keyboard) software is installed on the Thor VM2. Click here for the Freefloat website.

Control Panel

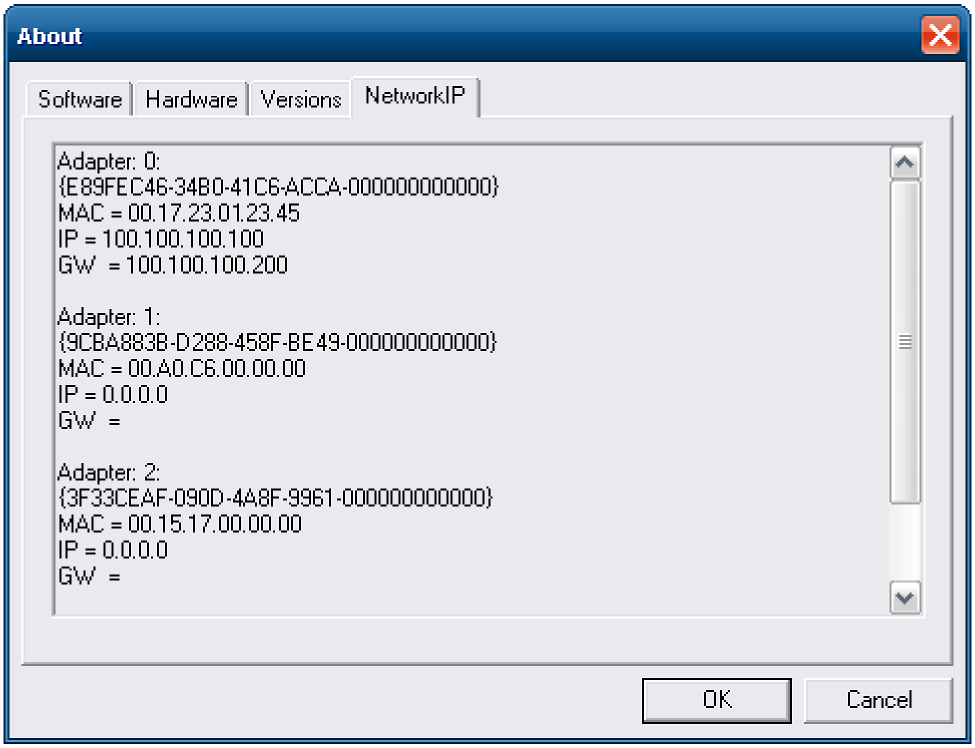
Most control panel applets on the Thor VM2 are standard Microsoft Windows items.

The control panels and other functions listed below may differ from a standard Microsoft Windows equipped PC or laptop.

About

Start > Control Panel > About (Classic view)

The Software, Hardware and Versions tabs displays hardware and software version information as stored in the registry.



```
Adapter: 0:
{E89FEC46-34B0-41C6-ACCA-000000000000}
MAC = 00.17.23.01.23.45
IP = 100.100.100.100
GW  = 100.100.100.200

Adapter: 1:
{9CBA883B-D288-458F-BE49-000000000000}
MAC = 00.A0.C6.00.00.00
IP = 0.0.0.0
GW  =

Adapter: 2:
{3F33CEAF-090D-4A8F-9961-000000000000}
MAC = 00.15.17.00.00.00
IP = 0.0.0.0
GW  =
```

The NetworkIP tab displays information on network connections, such as IP and MAC addresses.

Bluetooth

Start > Control Panel > Bluetooth

Note: Contact Technical Assistance for upgrade availability if your Bluetooth control panel is not the same as the control panel presented in this section.

Discover and manage pairing with nearby Bluetooth devices.

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
Printer Port on 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 reconnect	Enabled
Clear Pairing Table on Boot	Disabled
Auto Reconnect on Boot	Enabled
Auto Reconnect	Enabled

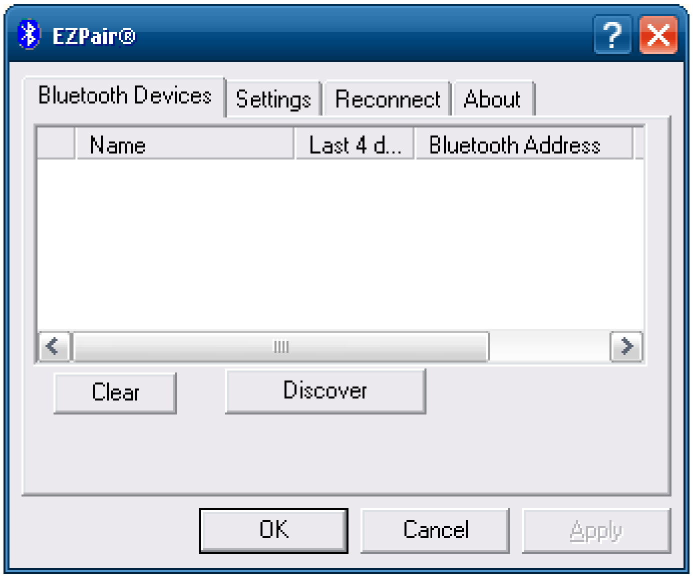
Bluetooth taskbar Icon state and Bluetooth device Icon states change as Bluetooth devices are discovered, paired, connected and disconnected. There may be audible or visual signals as paired devices re-connect with the Thor VM2.

- 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.

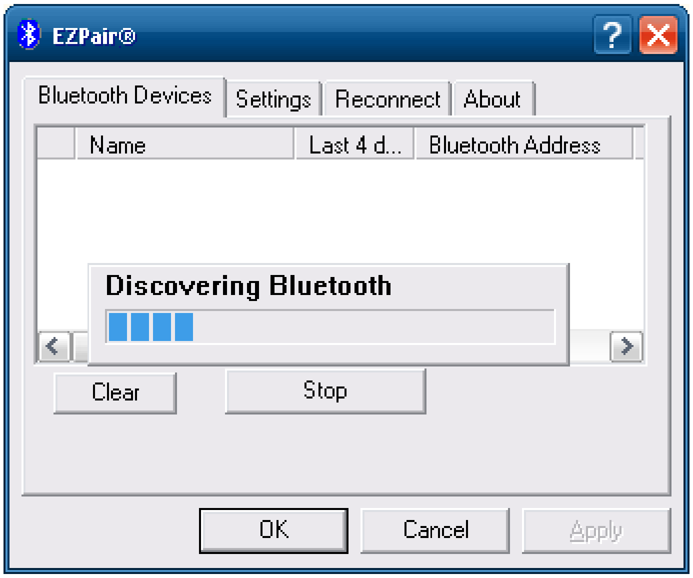
Bluetooth Devices

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.

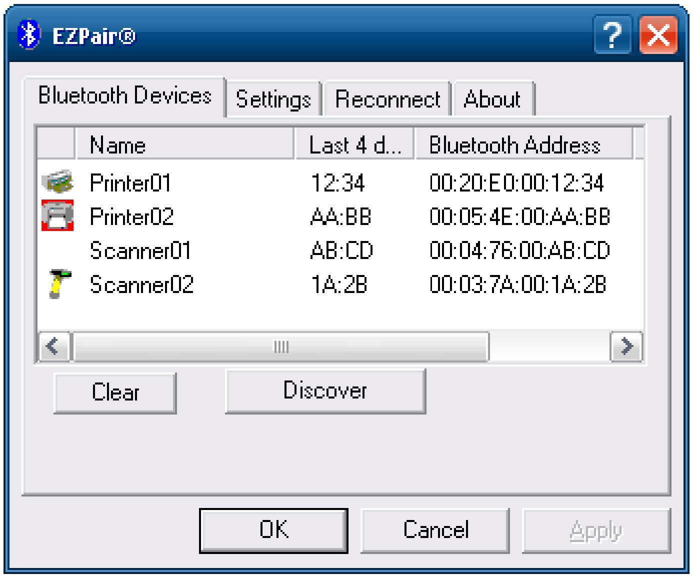


Stop Button

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



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

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.

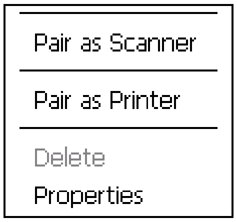
Clear Button

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

Pre-requisite: The Discover button has been clicked and there are Bluetooth devices listed.

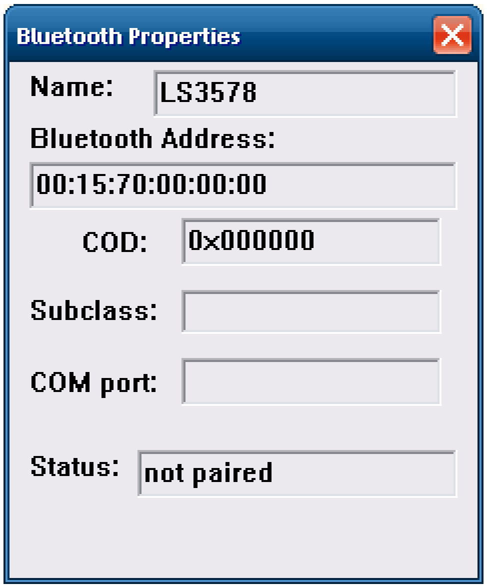
Click on a device in the list to highlight it. Double-click the highlighted device to display the Bluetooth Device **right-click menu** as shown below. The Bluetooth device does not need to be active.



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



Name: LS3578

Bluetooth Address: 00:15:70:00:00:00

COD: 0x000000

Subclass:

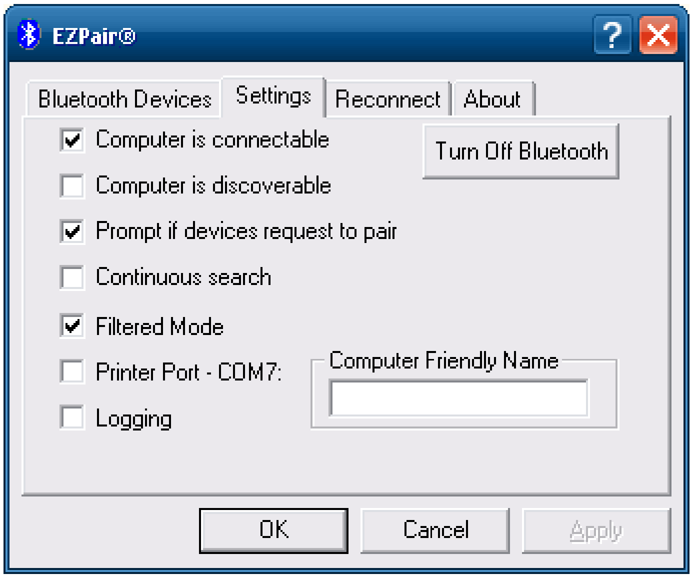
COM port:

Status: not paired

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



☑ Computer is connectable

□ Computer is discoverable

☑ Prompt if devices request to pair

□ Continuous search

☑ Filtered Mode

□ Printer Port - COM7:

□ Logging

Computer Friendly Name

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*.

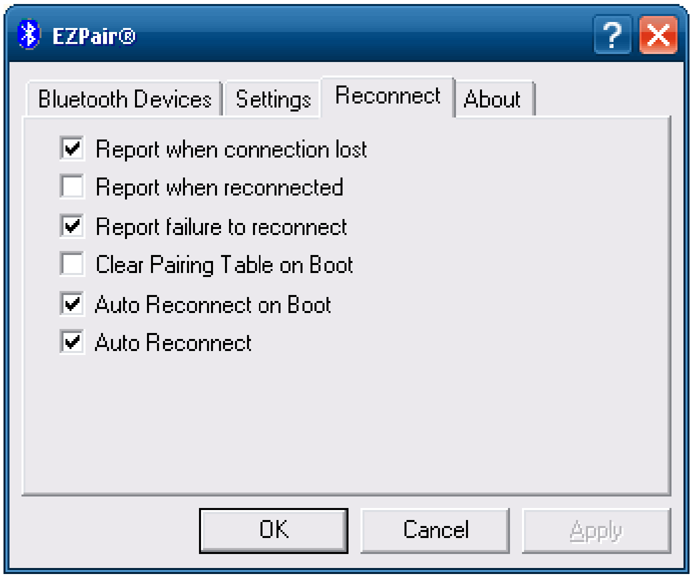
Default

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.
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



☑ Report when connection lost
☐ Report when reconnected
☑ Report failure to reconnect
☐ Clear Pairing Table on Boot
☑ Auto Reconnect on Boot
☑ Auto Reconnect

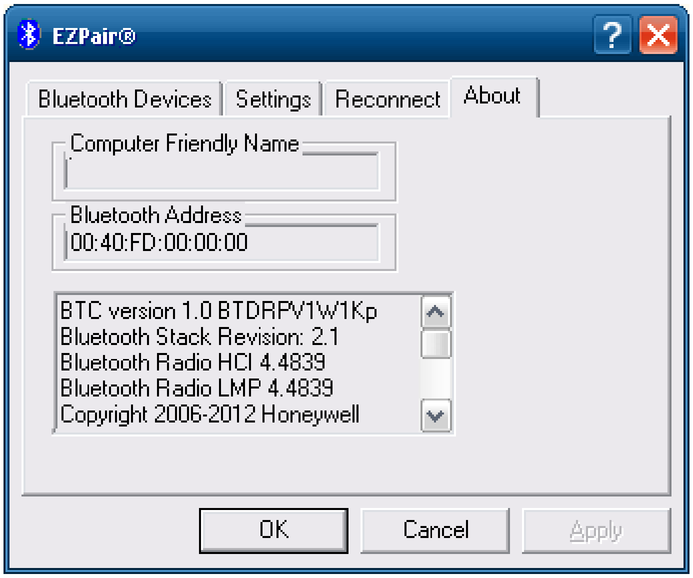
Note: These options can still be checked or unchecked whether Bluetooth connection is enabled or disabled.

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



Computer Friendly Name

Bluetooth Address
00:40:FD:00:00:00

BTC version 1.0 BTDRPV1W1Kp
Bluetooth Stack Revision: 2.1
Bluetooth Radio HCI 4.4839
Bluetooth Radio LMP 4.4839
Copyright 2006-2012 Honeywell

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

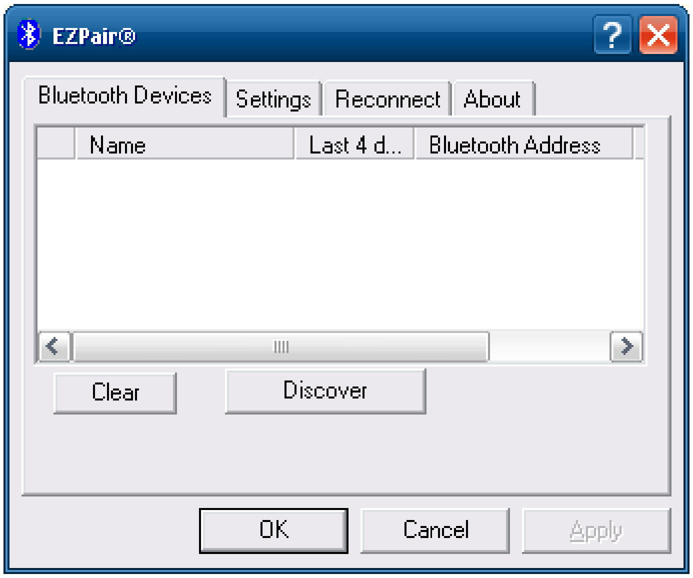
or Tap the Bluetooth icon in the taskbar to open the Bluetooth EZPair application.

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.

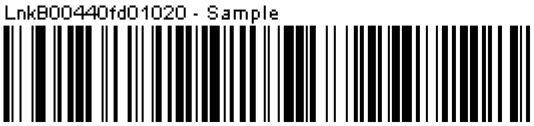
Bluetooth Bar Code Reader Setup

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

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

- The Thor VM2 has the Bluetooth hardware and software installed. An operating system upgrade may be required. Contact Technical Assistance for details.
- 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.



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.

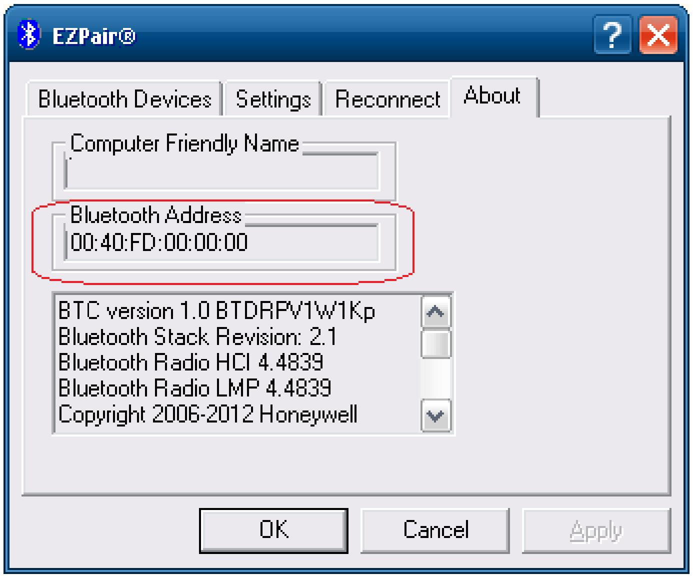
The devices are paired. The Bluetooth bar code reader responds with a series of beeps and an LED flashes. Refer to the following section titled "Bluetooth Beep and LED Indications".

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:

First, locate the Thor VM2 Bluetooth address by tapping Start > Control Panel > Bluetooth > About tab.



Computer Friendly Name

Bluetooth Address: 00:40:FD:00:00:00

BTC version 1.0 BTDRPV1W1Kp
Bluetooth Stack Revision: 2.1
Bluetooth Radio HCI 4.4839
Bluetooth Radio LMP 4.4839
Copyright 2006-2012 Honeywell

Next, create[1] 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 Also: "Bluetooth Beep and LED Indications"

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

Bluetooth Beep and LED Indications

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

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

Upon startup, if the 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 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.
4. 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).

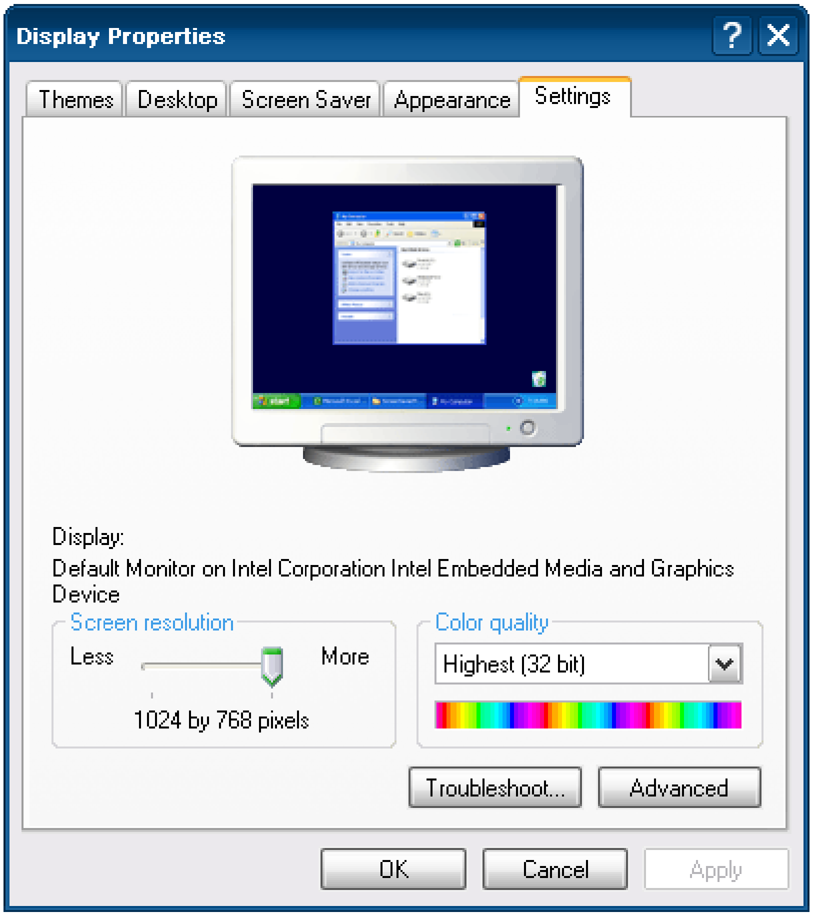
Note: Configuration elements are persistent and stored in the registry.

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

Display

Start > Control Panel > Display (Classic View)

Start > Control Panel > Appearance and Themes (Category View)



Display:
Default Monitor on Intel Corporation Intel Embedded Media and Graphics Device

Screen resolution
Less ... More
1024 by 768 pixels

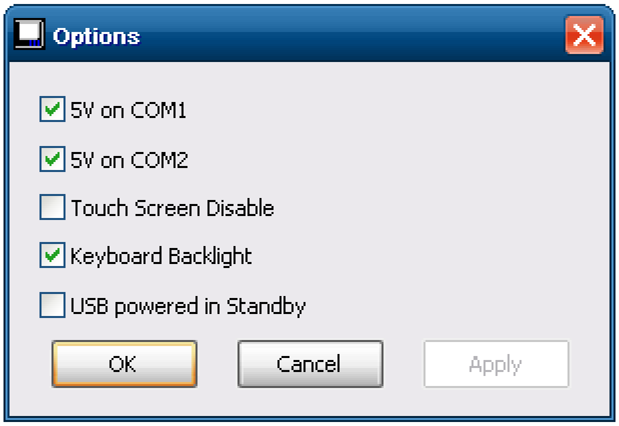
Color quality
Highest (32 bit)

The Thor VM2 supports a maximum 1024 x 768 pixel display resolution.

Screen rotation and other configuration options including Screen Blanking are configured on separate control panels.

Options

Start > Control Panel > Options (Classic view)



☑ 5V on COM1

☑ 5V on COM2

☐ Touch Screen Disable

☑ Keyboard Backlight

☐ USB powered in Standby

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

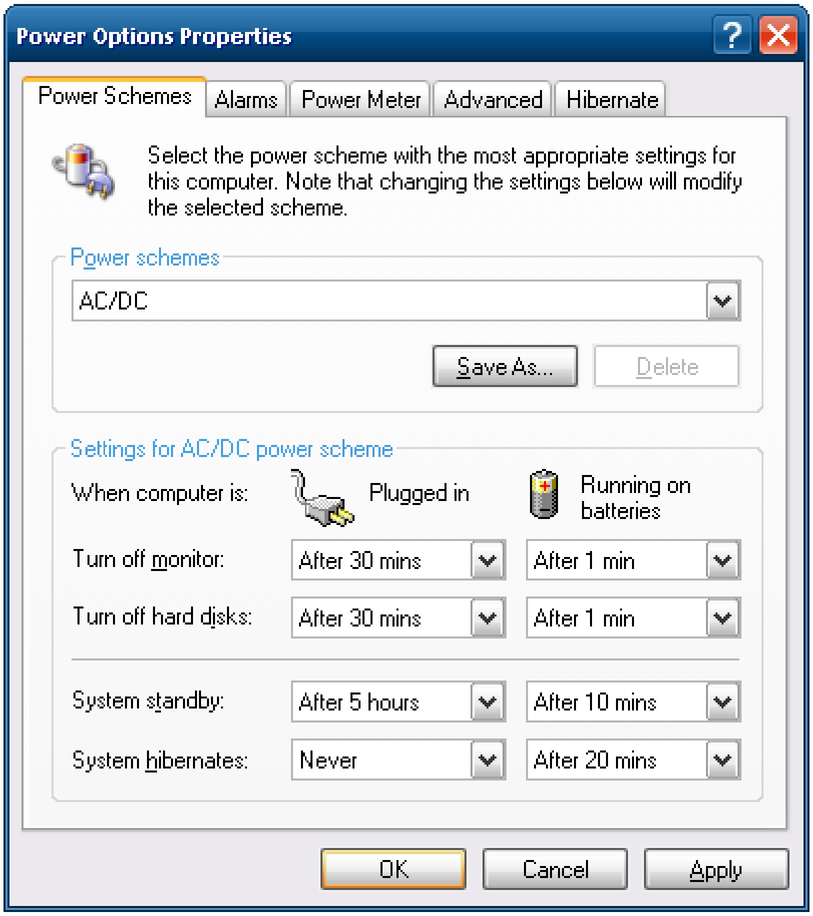
By default, power is removed from attached USB devices when the Thor VM2 is in Standby mode. Check this box to maintain power to attached USB devices in Standby.

Power Options

Start > Control Panel > Power Options (Classic View)

Start > Control Panel > Performance and Maintenance> Power Options (Category View)

Power Schemes



Select the power scheme with the most appropriate settings for this computer. Note that changing the settings below will modify the selected scheme.

Power schemes: AC/DC

Settings for AC/DC power scheme

When computer is:	Plugged in	Running on batteries
Turn off monitor:	After 30 mins	After 1 min
Turn off hard disks:	After 30 mins	After 1 min
System standby:	After 5 hours	After 10 mins
System hibernates:	Never	After 20 mins

The Thor VM2 has four power management schemes defined. The active Power Scheme depends on:

- The user selected Power Scheme
- And, for Ignition Control, the status of the ignition input signal.

Each power management scheme 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.

AC/DC

Select the AC/DC power scheme when manual control of the Thor VM2 power on process is desired.

This is the default power scheme. In AC/DC mode the Thor VM2 is turned on by a press of the Power button. Ignition input is ignored when AC/DC Mode is enabled.

The following default timeouts are used in the AC/DC power scheme.

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	5 hours	10 minutes
System hibernate	Never	20 minutes

When the AC/DC Power Scheme 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

Conditions

The Thor VM2 is **Off** and external power is available, such as:

- Thor VM2 is installed on a powered Quick Mount Smart Dock with the Dock power switch On
- Thor VM2 is already mounted to a Dock and external power is applied to the Dock

Result

The Thor VM2 boots when the Power button is pressed. Once booted the Thor VM2 follows the **AC/DC** power scheme with timers reset after bootup.

Thor VM2 is On

Conditions

The Thor VM2 is **On** (but powered by the UPS battery) 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 with the Dock power switch On and truck 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 the **AC/DC** power scheme with timers reset at power connection.

Ignition Control - Ignition On

Select either the Ignition Control - Ignition On or the Ignition Control - Ignition Off power scheme 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 depending on the state of the vehicle ignition input.

The following default timeouts are used in the Ignition Control - Ignition On power scheme.

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	5 hours	10 minutes
System hibernate	Never	20 minutes

The ignition input wire must be connected. If the user selects this power scheme but the ignition is Off, the Ignition Control - Ignition Off scheme is used instead.

When either Ignition Control Power Scheme 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 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 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 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 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.

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	1 hour	10 minutes
System hibernate	6 hours	20 minutes

The ignition input wire must be connected. If the user selects this power scheme but the ignition is On, the Ignition Control - Ignition On scheme is used instead.

When either Ignition Control Power Scheme 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 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 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 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.

The following default timeouts are used in the Auto-On power scheme.

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	5 hours	10 minutes
System hibernate	Never	20 minutes

When the Auto-On Power Scheme 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

Conditions

The Thor VM2 is **Off** and gets external power, such as

- Thor VM2 is installed on a powered Quick Mount Smart 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 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 Quick Mount Smart 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 with timers reset at the time power was connected.

UPS

When the Thor VM2 is operating on the UPS timeouts for any of the power schemes, the Thor VM2 behavior 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 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

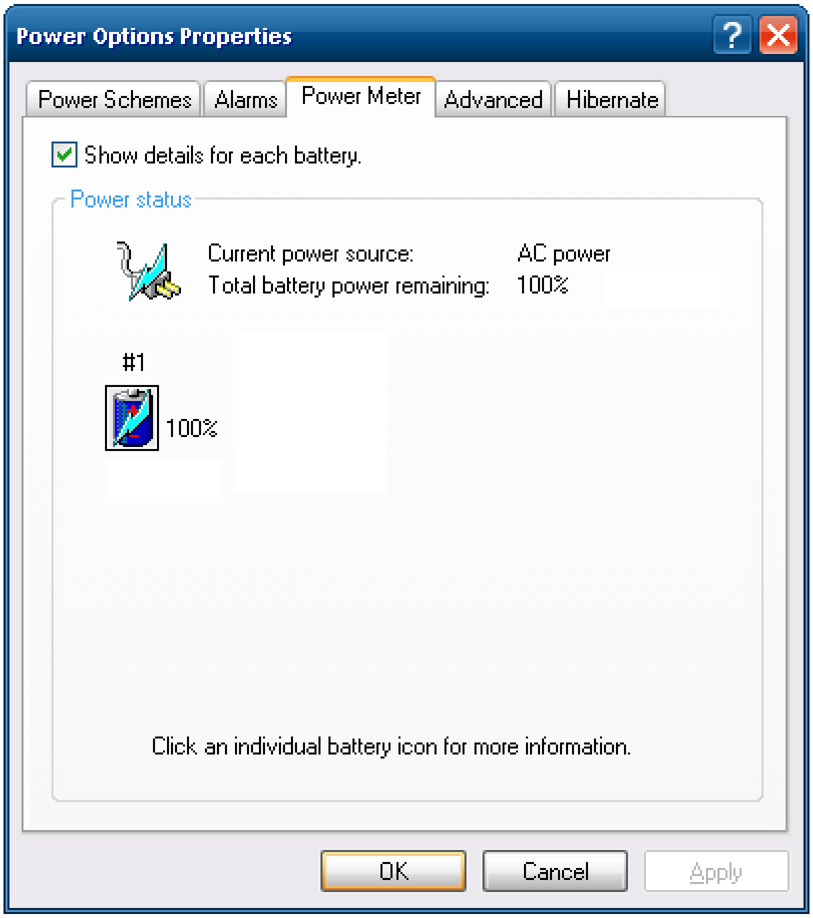
The Thor VM2 is On and external power is removed, such as:

- 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 timeouts with power management timers reset at the time of power removal. UPS charging is disabled.

Power Meter



☑ Show details for each battery.

Power status

Current power source: AC power

Total battery power remaining: 100%

#1

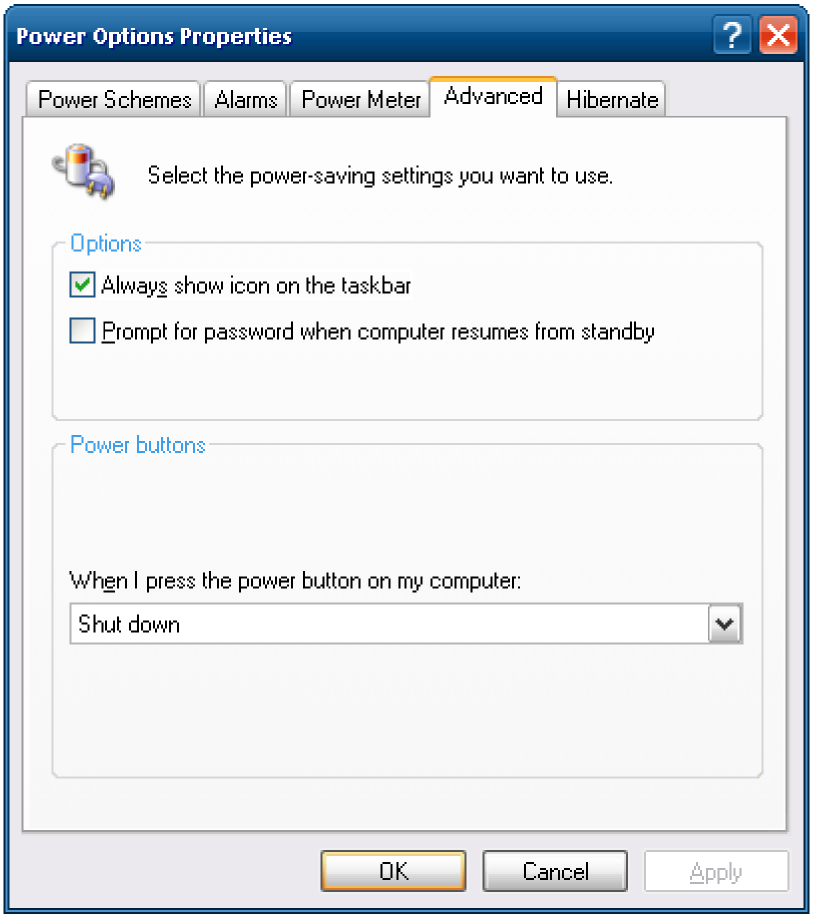
100%

Click an individual battery icon for more information.

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.

Advanced



Select the power-saving settings you want to use.

☑ Always show icon on the taskbar

□ Prompt for password when computer resumes from standby

When I press the power button on my computer:

Shut down

The **Advanced** panel allows setting the power button behavior when the unit is on and the power button is pressed. Options are:

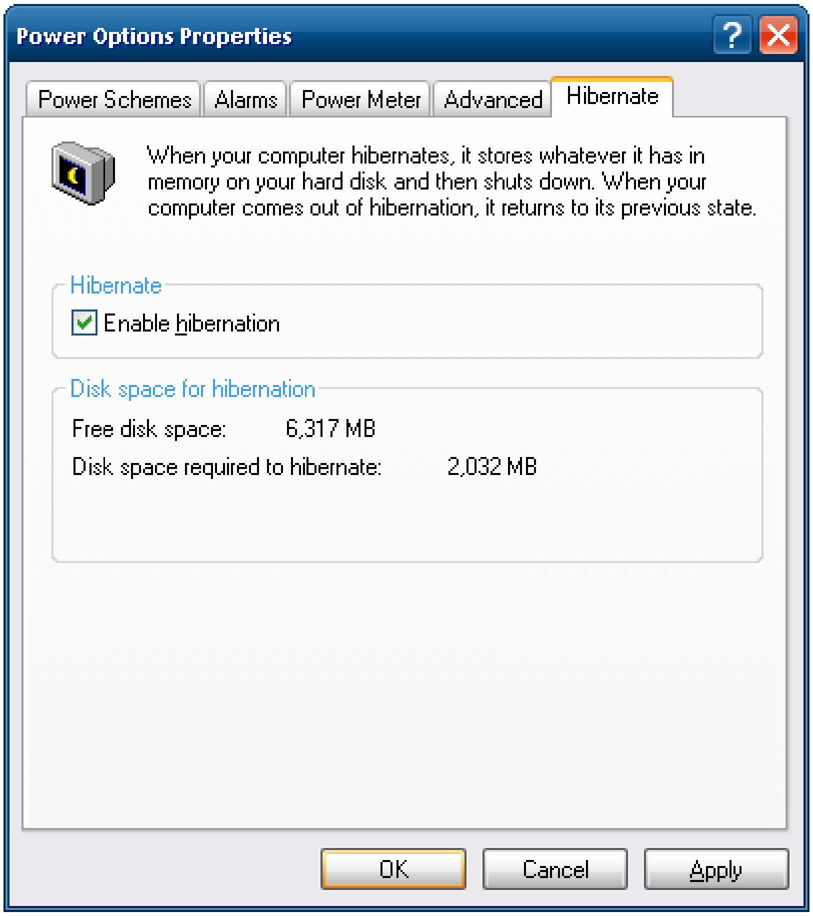
- Do nothing
- Ask me what to do
- Stand by
- Shut down.

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.

Hibernate

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.



When your computer hibernates, it stores whatever it has in memory on your hard disk and then shuts down. When your computer comes out of hibernation, it returns to its previous state.

Hibernate

☑ Enable hibernation

Disk space for hibernation

Free disk space: 6,317 MB

Disk space required to hibernate: 2,032 MB

Programmable Key

Start > Control Panel > programmable Key(Classic view)

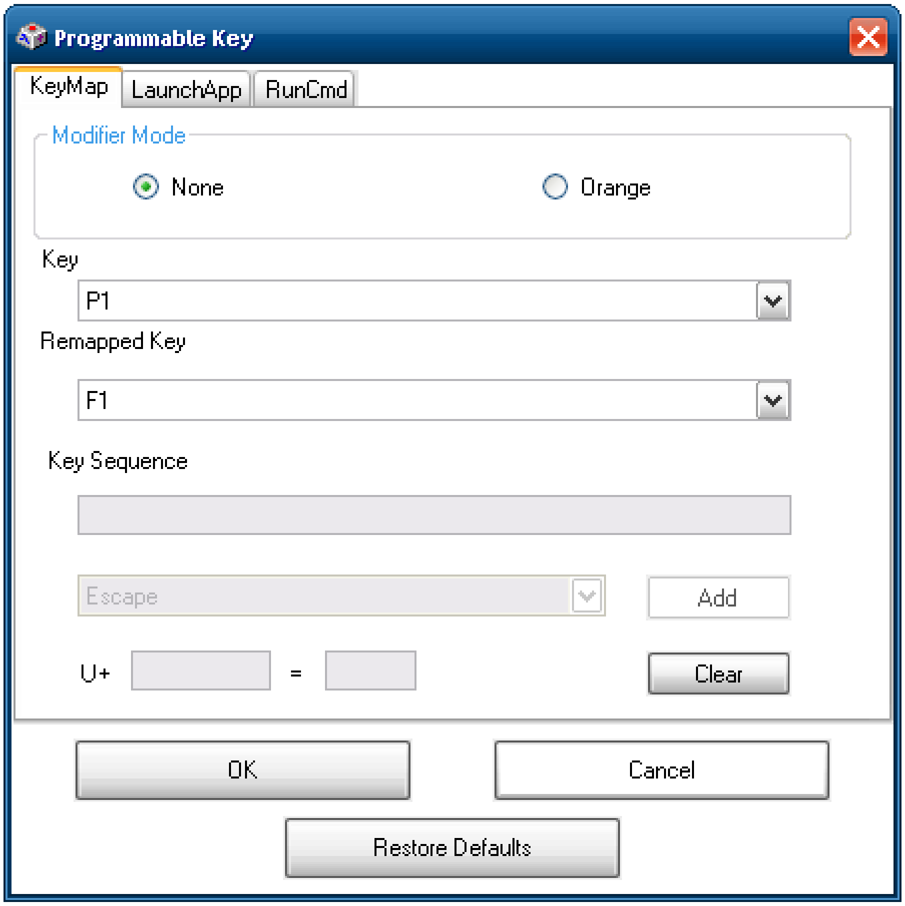
The Programmable Key panels can be used to perform the following functions:

- Remap a key to any single key
- Remap a key to a Unicode value
- Remap a key to a string of up to 16 keys or Unicode values in any combination
- Remap a key to launch a user-selected application
- Remap a key to run a command
- Remap a key to certain special functions

Factory Default Programmable Key Values

Programmable Key	Default Value	Programmable Key	Default Value
P1	F1	P6 (Orange + P1)	<no key>
P2	F2	P7 (Orange + P2)	<no key>
P3	F3	P8 (Orange + P3)	<no key>
P4	F4	P9 (Orange + P4)	<no key>
P5	F5	P10 (Orange + P5)	<no key>

KeyMap Tab



Modifier Mode

● None ○ Orange

Key: P1

Remapped Key: F1

Key Sequence

Escape

U+ =

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 Single Key

1. Select the modifier key from the Modifier Mode options.
2. Select the key to be remapped from the Key pulldown list.
3. Select the value from the remapped key from the Remapped Key pulldown 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 pulldown list.

3. Select **Unicode** from the Remapped Key pulldown list.
4. There are two Unicode text boxes located on the lower part of this tab. Enter the Unicode value in the left textbox and the Unicode character is displayed in the right textbox.
5. Click **OK** to save the result and close the control panel.

Remap 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 pulldown list.
3. Select **Key Sequence** from the Remapped Key pulldown list.
4. Select the first key for the multiple key sequence from the pulldown 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 pulldown list.
3. Select **Key Sequence** from the Remapped Key pulldown list.
4. Select **Unicode** from the Key Sequence pulldown list.
5. There are two Unicode text boxes located on the lower part of this tab. Enter the Unicode value in the left textbox and the Unicode character is displayed in the right textbox.
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 pulldown list.
3. Select the special function from the remapped key from the Remapped Key pulldown 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 an Application

1. Select the modifier key from the Modifier Mode options.
2. Select the key to be remapped from the Key pulldown list.
3. Select Launch **App1-4** from the remapped key from the Remapped Key pulldown list.
4. Click on the LaunchApp tab.
5. Make sure the **EXE** radio button is selected.
6. In the text box (App1-4) 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.

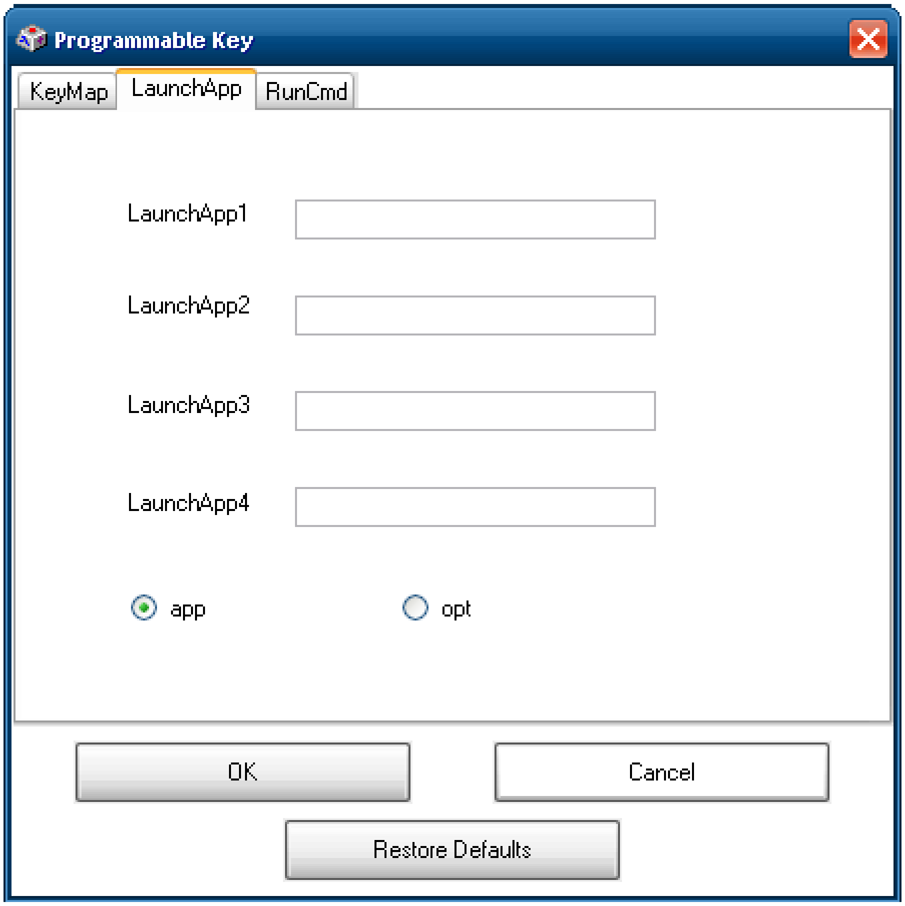
Remap a Command

1. Select the modifier key from the Modifier Mode options.
2. Select the key to be remapped from the Key pulldown list.
3. Select **RunCmd 1-4** from the remapped key from the Remapped Key pulldown list.
4. Click on the RunCmd tab.
5. Make sure the **FILE** radio button is selected.
6. In the text box (Cmd1-4) 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 Tab

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.



LaunchApp1

LaunchApp2

LaunchApp3

LaunchApp4

● app ○ opt

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 name of the executable file.
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.

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.

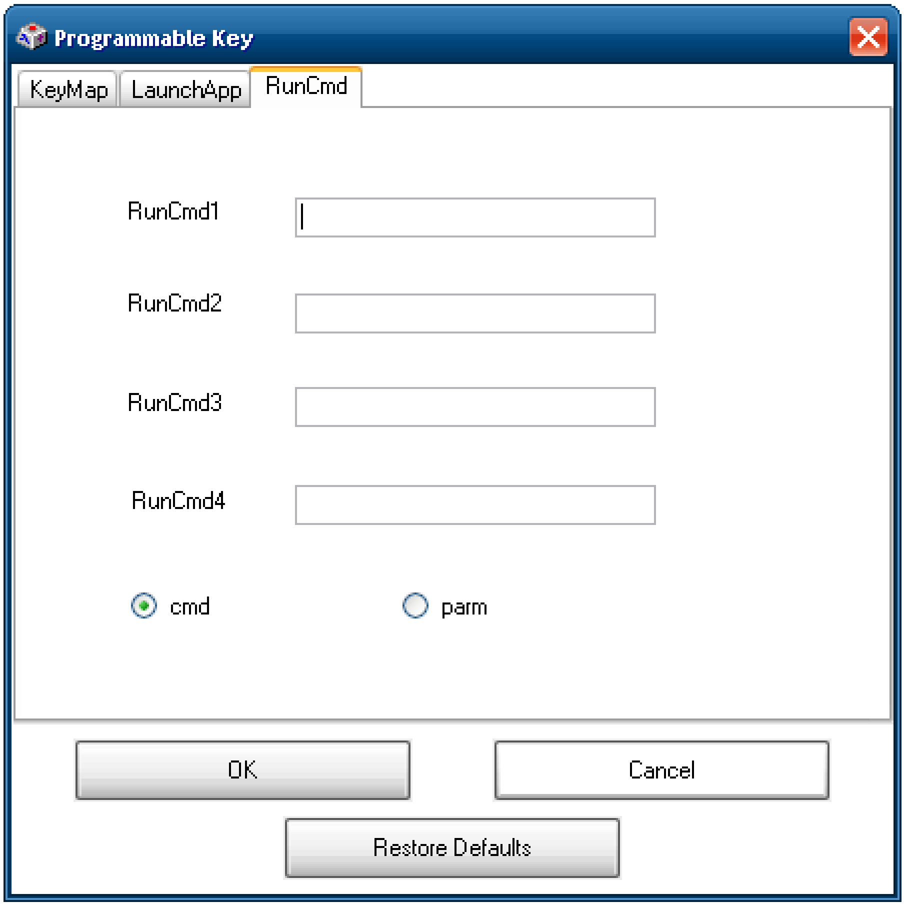
Tap the **Restore Defaults** to return all Programmable Keys to their default values and exit the Programmable Keys control panel.

The result of the application (**app**) and options (**opt**) entries are displayed on the KeyMap tab in the Key Sequence box when the key mapped to the LauchApp is selected.

RunCmd Tab

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.



● cmd ○ parm

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.

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.

Screen Control

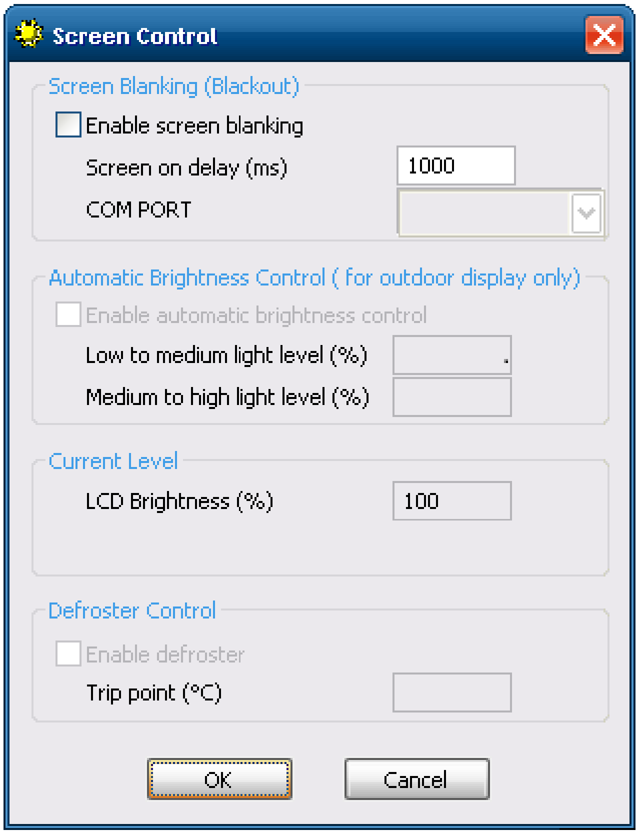
Start > Control Panel > Screen

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 (see note)

Note: There is no default value for Ambient Light % as it varies depending on the level of light where the Thor VM2 is located.


Screen Control
Screen Blanking (Blackout)
□ Enable screen blanking
Screen on delay (ms) 1000
COM PORT
Automatic Brightness Control (for outdoor display only)
□ Enable automatic brightness control
Low to medium light level (%)
Medium to high light level (%)
Current Level
LCD Brightness (%) 100
Defroster Control
□ Enable defroster
Trip point (°C)
OK
Cancel

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.

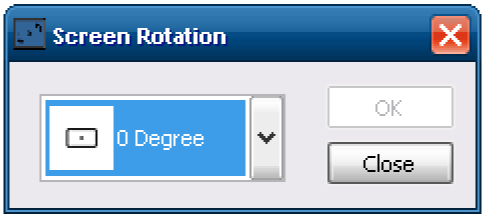
To disable screen blanking, uncheck the **Enable screen blanking** checkbox.

Screen blanking requires a serial cable and a screen blanking box or switch.

Please refer to the wiring instructions, including appropriate cautions and warnings, in the *Thor VM2 Vehicle Mounting Reference Guide*.

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.

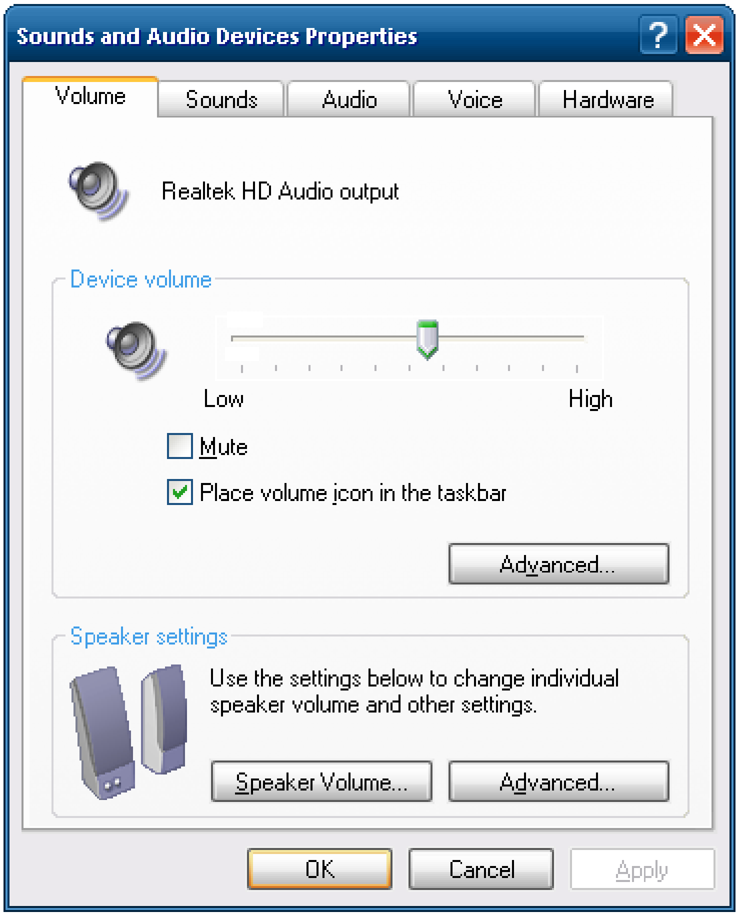
Select the desired rotation and tap **OK**. The screen may briefly go blank during the rotation process.

Tap **Close** to dismiss the panel and keep the current screen rotation.

Sounds

Start > Control Panel > Sounds and Audio Devices (Classic View)

Start > Control Panel > Sounds, Speech and Audio Devices (Category View)



Sounds and Audio Devices Properties

Realtek HD Audio output

Device volume

□ Mute

☑ Place volume icon in the taskbar

Speaker settings

Use the settings below to change individual speaker volume and other settings.

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 function keys - press the **2nd** key then **F9** to adjust volume up or **2nd** then **F10** to adjust volume down.

User Accounts

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 pre-configured 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 the Windows Certificate Store, 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 (SCU).

Bar Code Readers

The Thor VM2 can use the following external bar code readers:

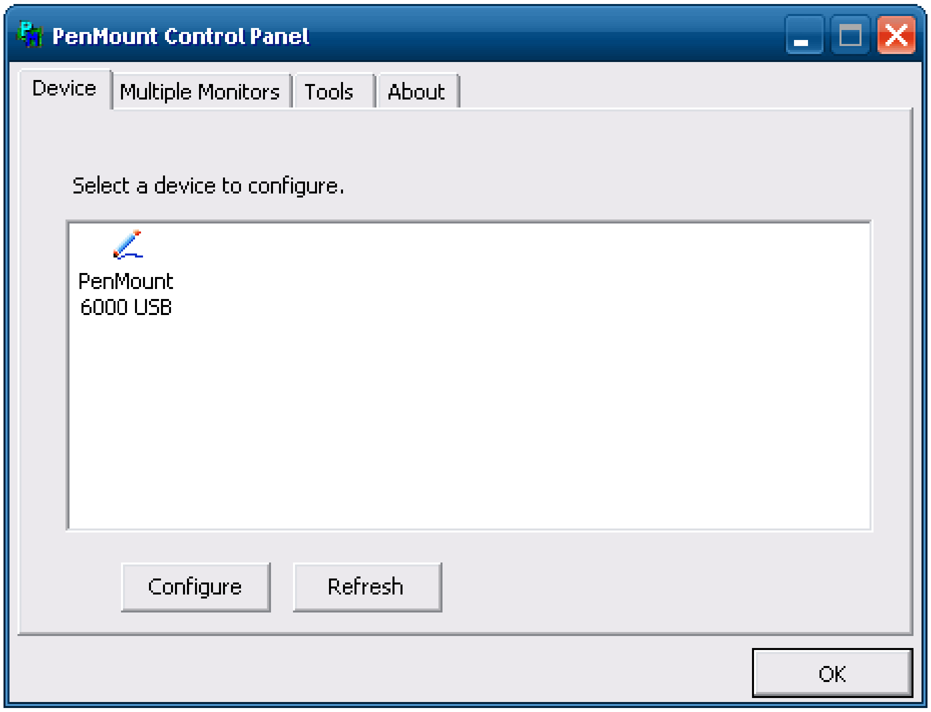
- Tethered hand-held scanners are tethered to a serial port or a USB host port (via a dongle cable) on the Thor VM2 Quick Mount Smart Dock and are configured by scanning the engine-specific bar codes in the scanner manufacturer's programming guide. The manufacturer's guides are usually shipped with the 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 when equipped with a Windows Embedded Standard operating system. Click here for the Freefloat website which contains 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 Embedded Standard 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.

Accessing the BIOS Setup

When the Embedded BIOS screen (Phoenix Technologies) is displayed press the **Del** key to enter BIOS setup.

Use the arrow keys to move around the screen.

To access and modify the BIOS on the Thor VM2, an external keyboard must be attached.

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 one of these options:

- Save Setting and Restart
- Exit Setup without Saving Changes
- Reload Factory-Defaults and Restart

The 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.

Contact Technical Assistance for information on the recovery DVD and for assistance installing other factory loaded software..

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.

Caution ⚠	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.

Chapter 4 - Wireless Network Connections

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.

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.

Security Options Supported are

- None
- WEP
- LEAP
- WPA-PSK
- WPA/LEAP
- PEAP-MSCHAP
- PEAP-GTC
- EAP-TLS
- EAP-FAST

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.
⚠	It may be necessary to upgrade radio software in order to use certain Summit Client Utility (SCU) features. Contact Technical Assistance for details.
⚠	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.

Help

Help is available by clicking the ? icon in the title bar on most SCU screens.

The SCU help may also be accessed by selecting Start > Help and tapping the Summit Client Utility link. The SCU does not have to be accessed to view the help information using this option.

Summit Tray Icon

- Tray icon is not shown when the Thor VM2 is running Windows Embedded Standard.

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

Windows XP and Windows Embedded
Standard devices

- The WZC utility has an icon in the toolbar (see above) 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.

How To: Use 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.

How 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.

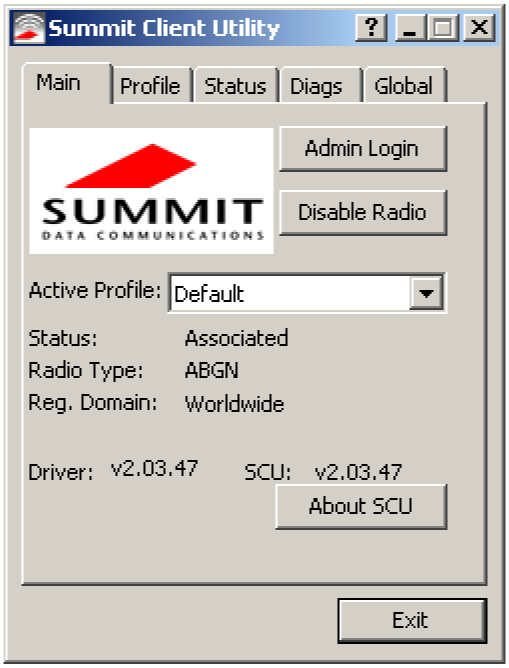
Radio control is passed to the SCU.

Main Tab

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



Active Profile: Default

Status: Associated

Radio Type: ABGN

Reg. Domain: Worldwide

Driver: v2.03.47 SCU: v2.03.47

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.

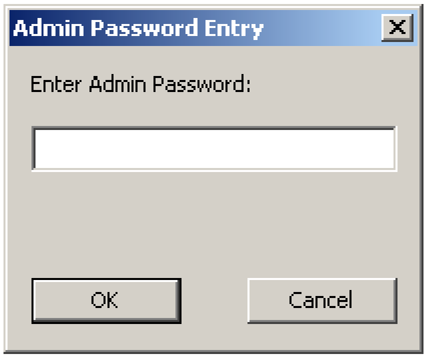
The password is case-sensitive.

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.

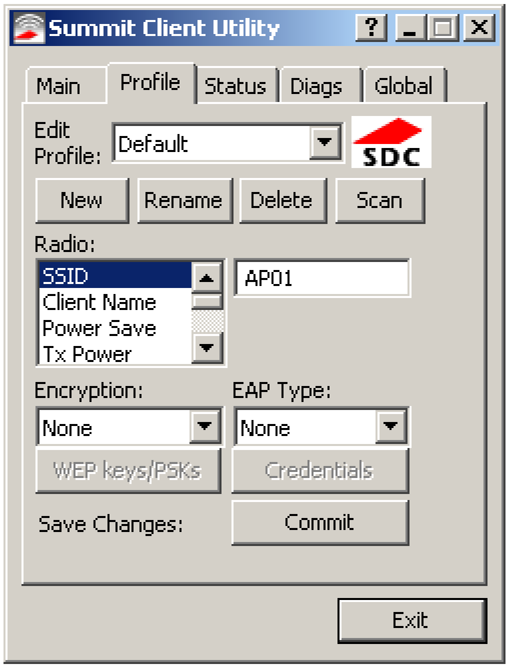
Profile Tab

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	See Profile Parameters for default
Auth Type	Open
EAP Type	None
Encryption	None



Edit Profile: Default

Radio:

SSID: AP01

Client Name

Power Save

Tx Power

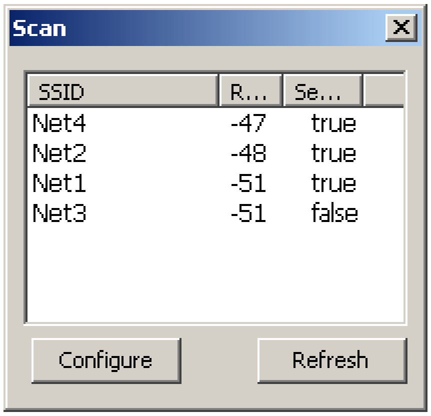
Encryption: None

EAP Type: None

Save Changes: Commit

When logged in as an Admin (see Admin Login), 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

<table>
<tr><th>Button</th><th>Function</th></tr>
<tr><td>Commit</td><td>Saves the profile settings made on this screen. Settings are saved in the profile.</td></tr>
<tr><td>Credentials</td><td>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.</td></tr>
<tr><td>Delete</td><td>Deletes the profile. The current active profile cannot be deleted and an error message is displayed if a delete is attempted.</td></tr>
<tr><td>New</td><td>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.</td></tr>
<tr><td>Rename</td><td>Assigns a new, unique name. If the new name is not unique, an error message is displayed and the profile is not renamed.</td></tr>
<tr><td>Scan</td><td>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.


<table><tr><th>SSID</th><th>R...</th><th>Se...</th></tr><tr><td>Net4</td><td>-47</td><td>true</td></tr><tr><td>Net2</td><td>-48</td><td>true</td></tr><tr><td>Net1</td><td>-51</td><td>true</td></tr><tr><td>Net3</td><td>-51</td><td>false</td></tr></table>
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).</td></tr>
<tr><td>WEP Keys / PSK Keys</td><td>Allows entry of WEP keys or pass phrase as required by the type of encryption.</td></tr>
</table>

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. *Note: 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)

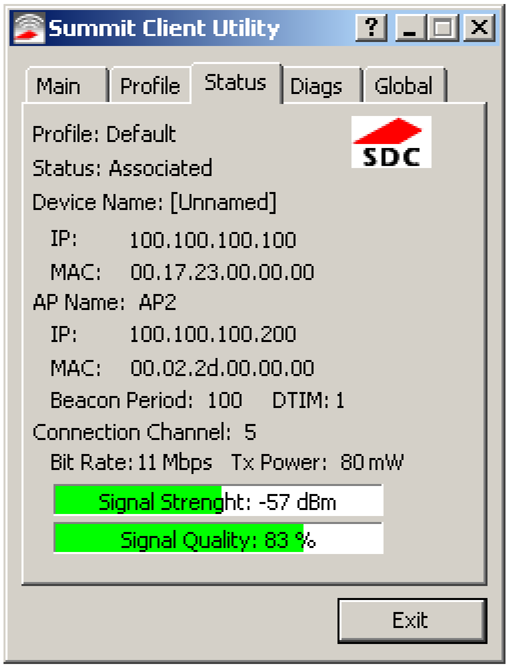
Parameter	Default	Explanation
		Ad Hoc (when connecting to another client device instead of an AP) Default: BGA Rates Full (for 802.11a/b/g/n radio)

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.

Contact Technical Assistance if you have questions about the antenna(s) installed on your Thor VM2.

Status Tab

Start > All Programs > Summit > Summit Client Utility > Status tab



Profile: Default
Status: Associated
Device Name: [Unnamed]
IP: 100.100.100.100
MAC: 00.17.23.00.00.00
AP Name: AP2
IP: 100.100.100.200
MAC: 00.02.2d.00.00.00
Beacon Period: 100 DTIM: 1
Connection Channel: 5
Bit Rate: 11 Mbps Tx Power: 80 mW
Signal Strenght: -57 dBm
Signal Quality: 83 %

This screen provides information on the radio:

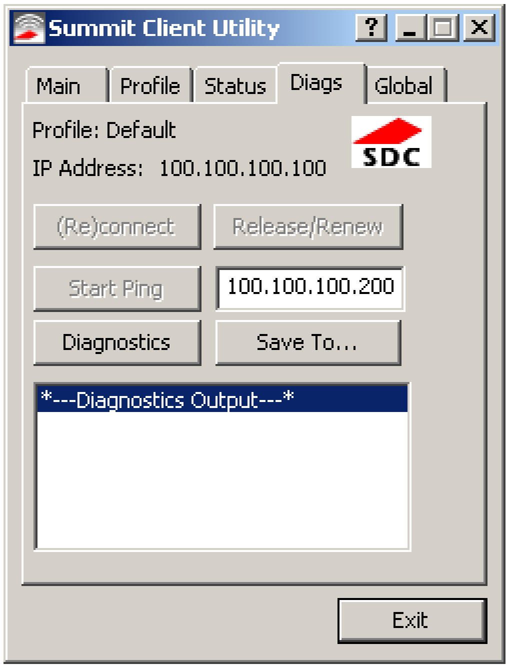
- The profile being used.
- The status of the radio card (down, associated, authenticated, etc.).
- Client information including device name, IP address and MAC address.
- Information about the Access Point (AP) maintaining the connection to the network including AP name, IP address and MAC address.
- 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 Tab

Start > All Programs > Summit > Summit Client Utility > Diags tab



Profile: Default

IP Address: 100.100.100.100

100.100.100.200

```
*---Diagnostics Output---*
```

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 Tab

Start > All Programs > Summit > Summit Client Utility > Global tab

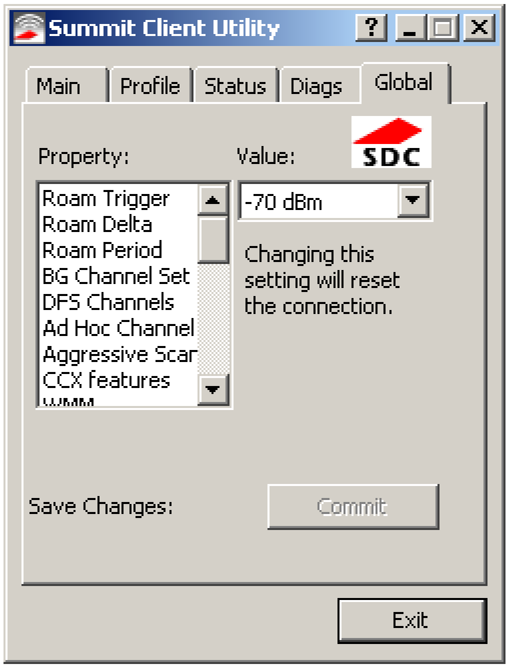
The parameters on this panel can only be changed when an Admin is logged in with a password. The current values for the parameters can be viewed by the general user without requiring a password.

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



Value: -70 dBm

Changing this setting will reset the connection.

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 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 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) Custom.
DFS Channels	Off	Support for 5GHZ 802.11a channels where support for DFS is required. Options are: On, Off, Optimized. *Note: 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.

Parameter	Default	Function
		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.
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).

Parameter	Default	Function
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 *Note: 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.
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 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.

Parameter	Default	Function
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. More info.

Note: Tap the Commit button to save changes. If this panel is closed before tapping the Commit button, changes are not saved!

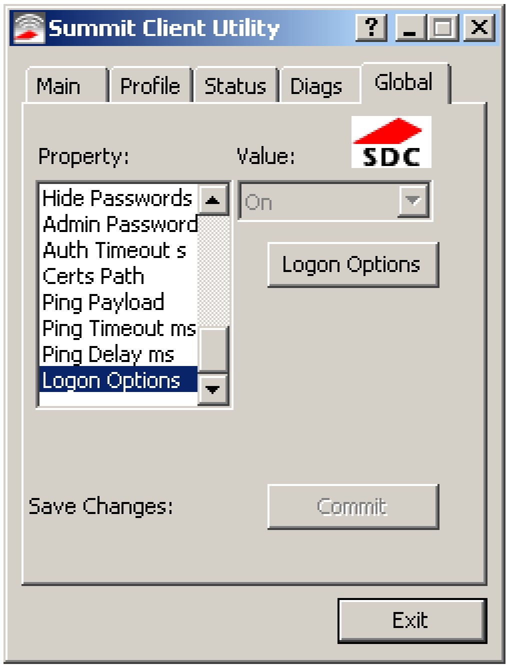
Logon Options

This option is only available on devices with a Windows XP Professional or Windows Embedded Standard operating system.

There are two options available, a single signon which uses the Windows username and password as the credentials for 802.1x authentication and pre-logon which uses saved credentials for 802.1x authentication before Windows logon.

If either option is enabled, the credentials entered here take precedence over any credentials entered on the Profile tab.

To use either option, select **Logon Options** from the **Property** list which activates the **Logon Options** button.



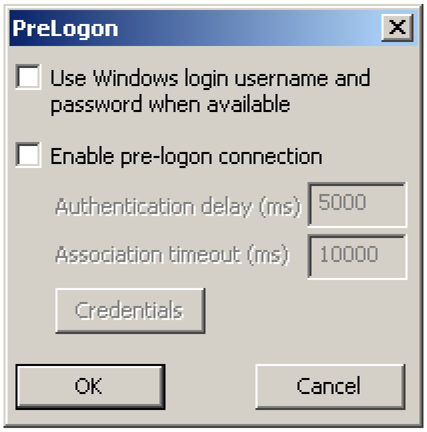
Property: Logon Options

Hide Passwords
Admin Password
Auth Timeout s
Certs Path
Ping Payload
Ping Timeout ms
Ping Delay ms
Logon Options

Value: On

Save Changes:

Click the **Logon Options** button.



□ Use Windows login username and password when available

□ Enable pre-logon connection

Authentication delay (ms) 5000

Association timeout (ms) 10000

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:

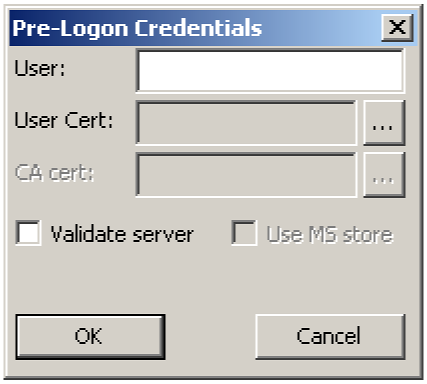
- EAP authentication is required for a WLAN connection
- Single Signon is configured, so the Windows username and password are used as credentials for EAP authentication
- The WLAN connection needs to be established before the Windows login.

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:

- Check the **Use MS store** checkbox. The default is to use the Full Trusted Store.
- To select an individual certificate, click on the **Browse** button.
- Uncheck the **Use full trusted store** checkbox.
- Select the desired certificate and click **Select**. You are returned to the Credentials screen.

If using the Certs Path option:

- Leave the Use MS store box unchecked.
- Enter the certificate filename in the CA Cert textbox.

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.

How 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.

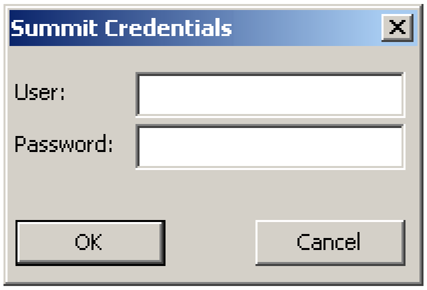
Note: See Configuring the Profile for more details.

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.

How to: Use Sign On Screen

1. After completing the other entries in the profile, click on the **Credentials** button. Leave the Username and Password blank. No entries are necessary on the Credentials screen for LEAP or 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 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 Diags Tab is clicked or
- the profile is modified and the **Commit** button is clicked.

How 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 wireless 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 Generating a User Certificate.
- To import the user certificate into the Windows certificate store, see Installing a User Certificate.
- A Root CA certificate is also needed. Refer to the section below.

Root CA Certificates

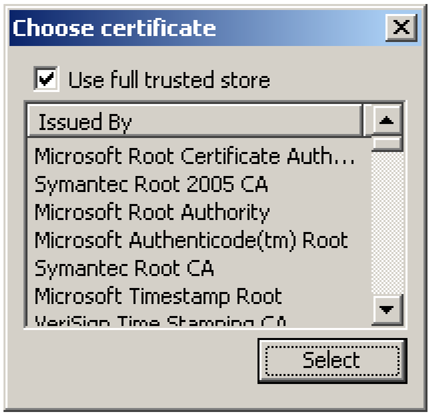
Root CA certificates are required for EAP/TLS, PEAP/GTC and PEAP/MSCHAP. Two options are offered for storing these certificates. They may be imported into the Windows certificate store or copied into the Certs Path directory.

How To: Use the Certs Path

1. See Generating 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 textbox.
5. Click **OK** to exit the Credentials screen and then **Commit** to save the profile changes.

How To: Use Windows Certificate Store

1. See Generating 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 Installing 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.



☑ Use full trusted store

Issued By
Microsoft Root Certificate Auth...
Symantec Root 2005 CA
Microsoft Root Authority
Microsoft Authenticode(tm) Root
Symantec Root CA
Microsoft Timestamp Root
VeriSign Time Stamping CA

6. Uncheck the **Use full trusted store** checkbox.
7. Select the desired certificate and click the **Select** button to return the selected certificate to the CA Cert textbox.
8. Click **OK** to exit the Credentials screen and then **Commit** to save the profile changes.

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.

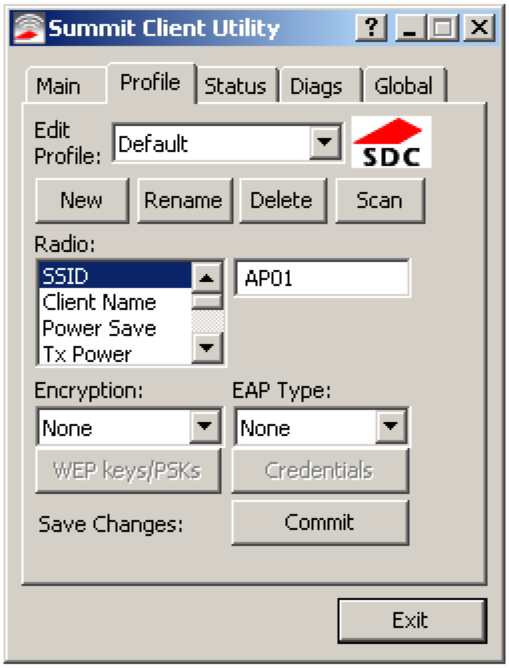
IMPORTANT – Remember to click the Commit button after making changes to ensure the changes are saved. Many versions of the SCU display a reminder if the Commit button is not clicked before an attempt is made to close or browse away from the tab in focus if there are unsaved changes.

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.

- Enter the **SSID** of the Access Point assigned to this profile
- Set **EAP Type** to **None**
- Set **Encryption** to **None**
- Set **Auth Type** to **Open**



Edit Profile: Default

Radio: SSID — AP01

Encryption: None

EAP Type: None

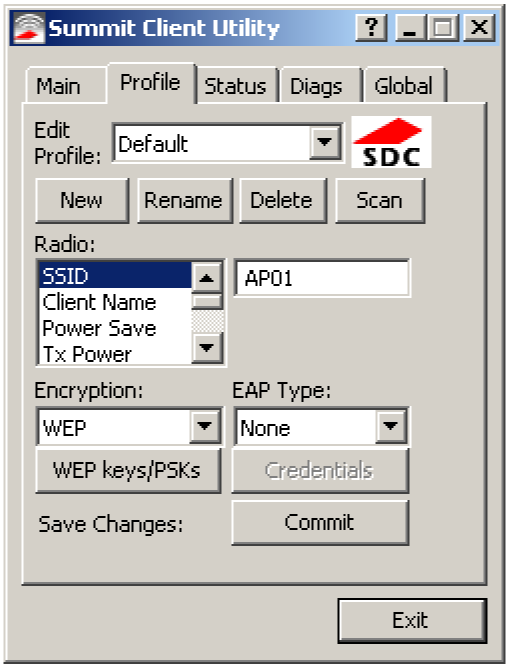
Once configured, click the **Commit** button.

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.

WEP

To connect using WEP, make sure the following profile options are used.

- Enter the **SSID** of the Access Point assigned to this profile
- Set **EAP Type** to **None**
- Set **Encryption** to **WEP** or **Manual WEP** (depending on SCU version)
- Set **Auth Type** to **Open**



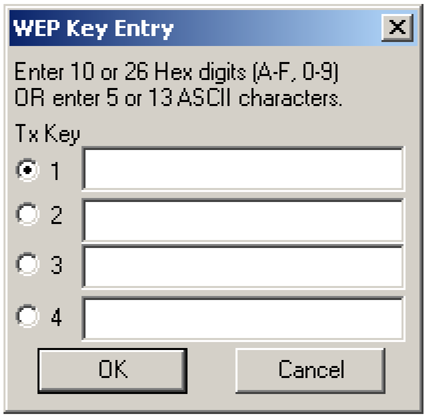
Edit Profile: Default

SSID: AP01

Encryption: WEP

EAP Type: None

Click the **WEP keys/PSKs** button.



Enter 10 or 26 Hex digits (A-F, 0-9)
OR enter 5 or 13 ASCII characters.

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**.

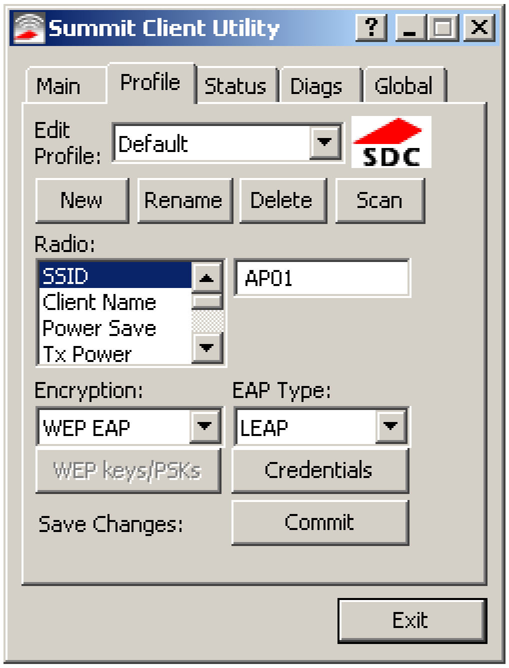
Once configured, click the **Commit** button.

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.

LEAP

To use LEAP (without WPA), make sure the following profile options are used.

- Enter the **SSID** of the Access Point assigned to this profile
- Set **EAP Type** to **LEAP**
- Set **Encryption** to **WEP EAP** or **Auto WEP** (depending on SCU version)
- 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**.


Edit Profile: Default

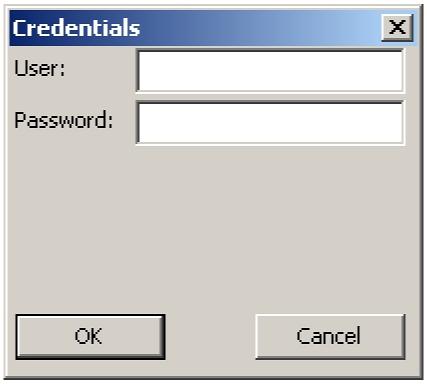
Radio: SSID: AP01

Encryption: WEP EAP

EAP Type: 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.**

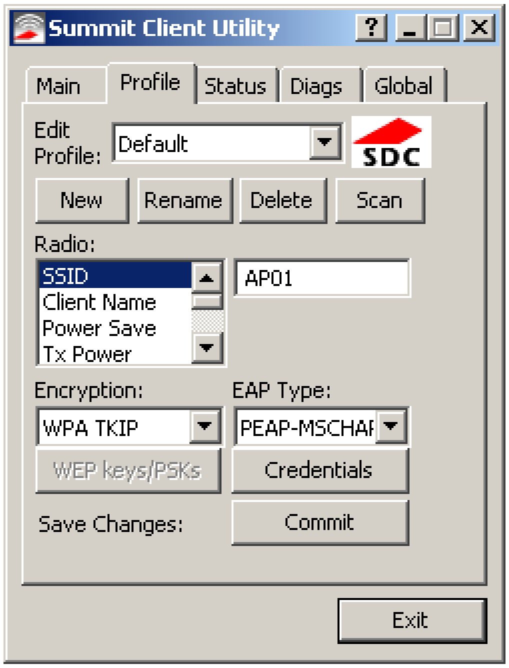
Ensure the correct Active Profile is selected on the Main tab and restart. The SCU Main tab shows the device is associated after the radio connects to the network.

PEAP/MSCHAP

To use PEAP/MSCHAP, make sure the following profile options are used.

- Enter the **SSID** of the Access Point assigned to this profile
- Set **EAP Type** to **PEAP-MSCHAP**
- Set **Encryption** to **WPA TKIP**
- Set **Auth Type** to **Open**

To use another encryption type, select WPA CCKM, WPA2 AES or WPA2 CCKM for encryption and complete other entries as detailed in this section.



Edit Profile: Default

Radio: SSID — AP01

Encryption: WPA TKIP

EAP Type: PEAP-MSCHAP

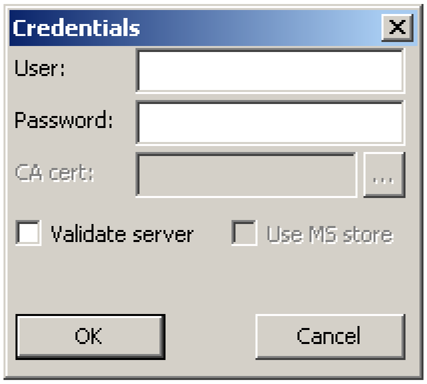
Save Changes:

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.


Credentials

User:

Password:

CA cert:

□ Validate server □ Use MS store

Enter the Domain\Username (if the Domain is required), otherwise enter the Username.

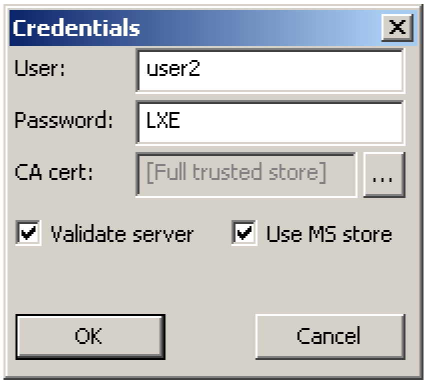
Enter the password.

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.


Credentials

User: user2

Password: LXE

CA cert: [Full trusted store]

☑ Validate server ☑ Use MS store

If using the Windows certificate store:

- Check the **Use MS store** checkbox. The default is to use the Full Trusted Store.
- To select an individual certificate, click on the **Browse** button.
- Uncheck the **Use full trusted store** checkbox.
- Select the desired certificate and click Select. You are returned to the Credentials screen.

If using the Certs Path option:

- Leave the **Use MS store** box unchecked.
- Enter the certificate filename in the CA Cert textbox.

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.

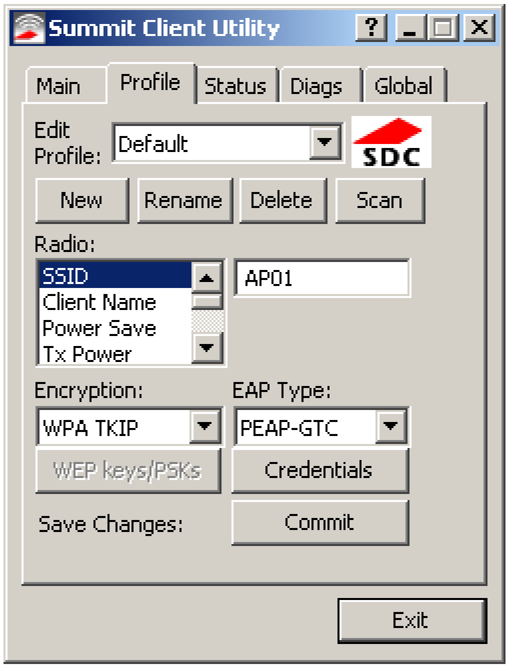
Note: The date must be properly set on the device to authenticate a certificate.

PEAP/GTC

To use PEAP/GTC, make sure the following profile options are used.

- Enter the **SSID** of the Access Point assigned to this profile
- Set **EAP Type** to **PEAP-GTC**
- Set **Encryption** to **WPA TKIP**
- Set **Auth Type** to **Open**

To use another encryption type, select WPA CCKM, WPA2 AES or WPA2 CCKM for encryption and complete other entries as detailed in this section.



Edit Profile: Default

SSID: AP01

Encryption: WPA TKIP

EAP Type: PEAP-GTC

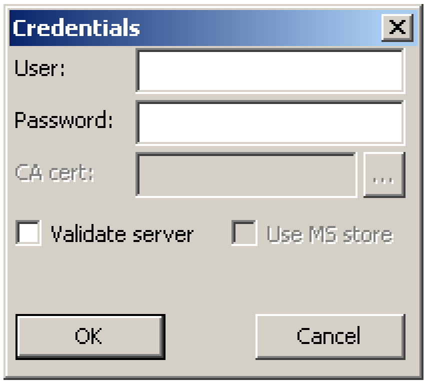
Save Changes:

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.



User:

Password:

CA cert:

□ Validate server □ Use MS store

Enter the Domain\Username (if the Domain is required), otherwise enter the Username.

Enter the password.

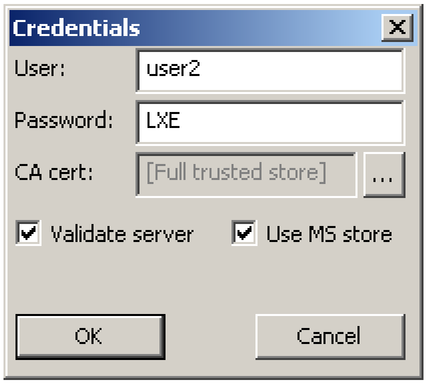
Leave the CA Certificate File Name blank for now.

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.



Credentials

User: user2

Password: LXE

CA cert: [Full trusted store]

☑ Validate server ☑ Use MS store

If using the Windows certificate store:

- Check the **Use MS store** checkbox. The default is to use the Full Trusted Store.
- To select an individual certificate, click on the **Browse** button.
- Uncheck the **Use full trusted store** checkbox.
- Select the desired certificate and click **Select**. You are returned to the Credentials screen.

If using the Certs Path option:

- Leave the **Use MS store box** unchecked.
- Enter the certificate filename in the CA Cert textbox.

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.

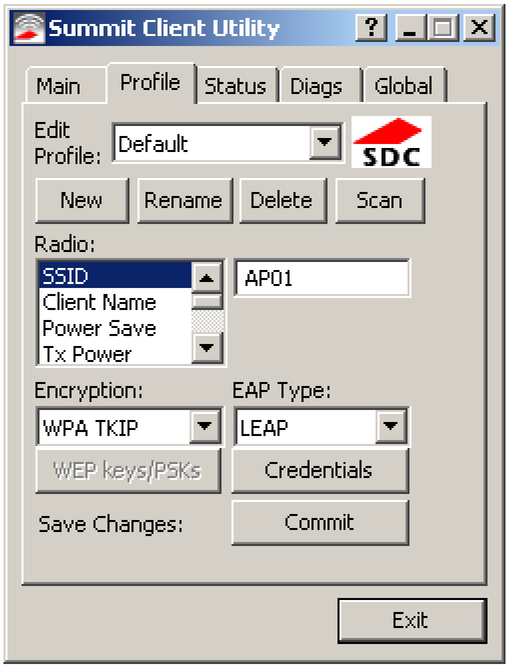
Note: The date must be properly set on the device to authenticate a certificate.

WPA/LEAP

To use WPA/LEAP, make sure the following profile options are used.

- Enter the **SSID** of the Access Point assigned to this profile
- Set **EAP Type** to **LEAP**
- Set **Encryption** to **WPA TKIP**
- Set **Auth Type** 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.



Summit Client Utility

Edit Profile: Default

Radio: SSID

AP01

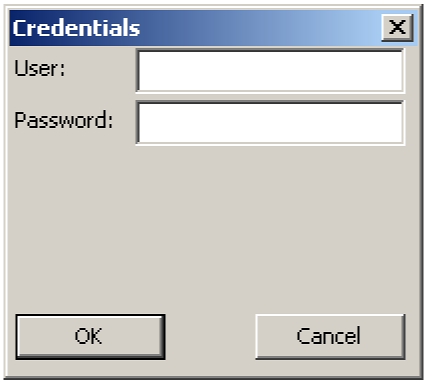
Encryption: WPA TKIP

EAP Type: LEAP

Save Changes:

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.

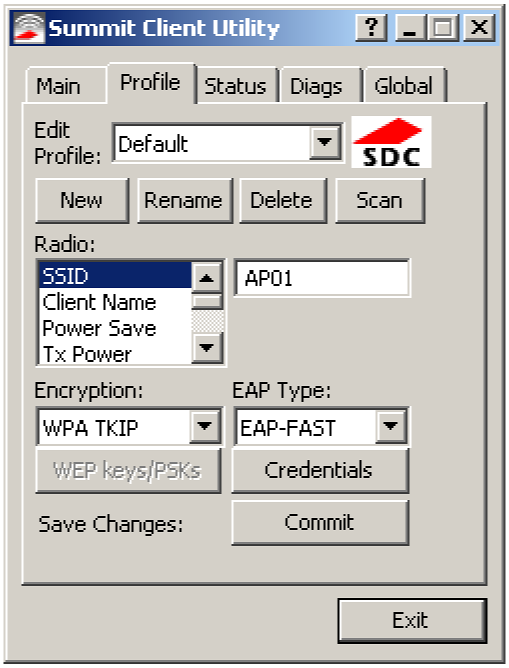
EAP-FAST

To use EAP-FAST, make sure the following profile options are used.

- Enter the **SSID** of the Access Point assigned to this profile
- Set **EAP Type** to **EAP-FAST**
- Set **Encryption** to **WPA TKIP**
- Set **Auth Type** to **Open**

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.



Edit Profile: Default

SSID: AP01

Encryption: WPA TKIP

EAP Type: EAP-FAST

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.

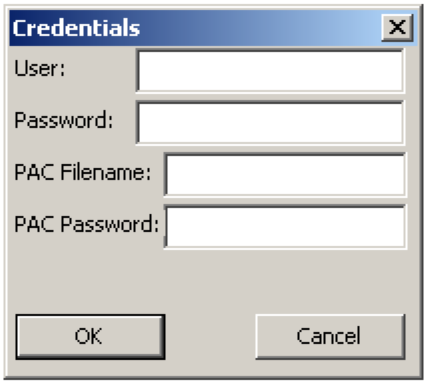
For manual PAC provisioning, the PAC filename and Password must be entered.

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.

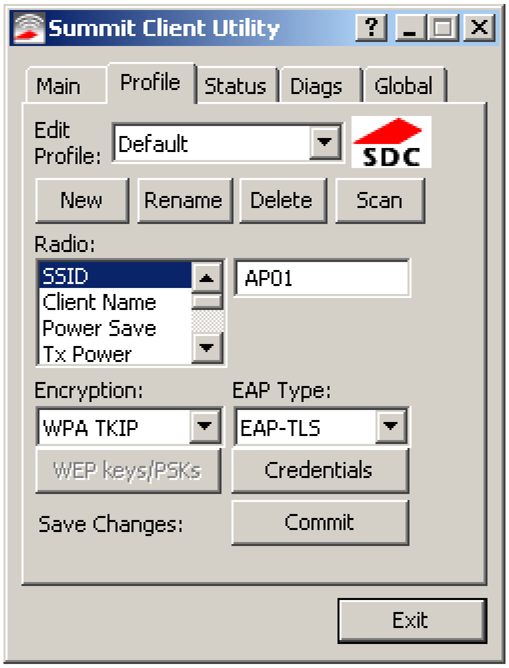
Note: When using Automatic PAC Provisioning, once authenticated, there is a file stored in the C:\Program Files\Summit\certs directory with the PAC credentials. If the username is changed, that file must be deleted. The filename is autoP.00.pac.

EAP-TLS

To use EAP-TLS, make sure the following profile options are used.

- Enter the **SSID** of the Access Point assigned to this profile
- Set **EAP Type** to **EAP-TLS**
- Set **Encryption** to **WPA TKIP**
- Set **Auth Type** to **Open**

To use another encryption type, select WPA CCKM, WPA2 AES or WPA2 CCKM for encryption and complete other entries as detailed in this section.



Edit Profile: Default

Radio: SSID: AP01

Encryption: WPA TKIP

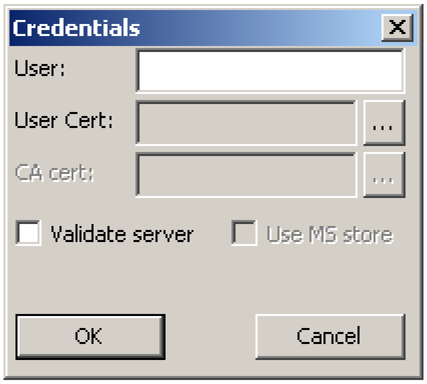
EAP Type: EAP-TLS

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.

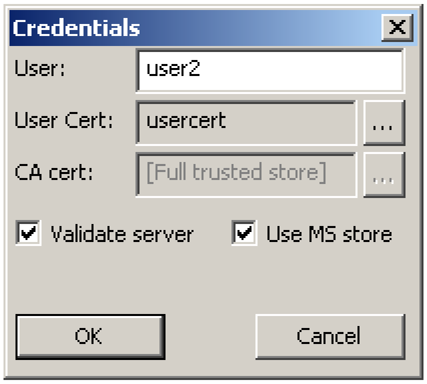
Select a user certificate from the Windows certificate store. Use the **Browse** button to locate the User Cert from the certificate store. Highlight the desired certificate and press the **Select** button. The name of the certificate is displayed in the User Cert box.

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 to generate and install the user certificate.

See Windows Certificate Store vs. Certs Path for more information on CA certificate storage.

Check the **Validate server** checkbox.



Credentials

User: user2

User Cert: usercert

CA cert: [Full trusted store]

☑ Validate server ☑ Use MS store

If using the Windows certificate store:

- Check the **Use MS store** checkbox. The default is to use the Full Trusted Store.
- To select an individual certificate, click on the **Browse** button.
- Uncheck the **Use full trusted store** checkbox.
- Select the desired certificate and click **Select**. You are returned to the Credentials screen.

If using the Certs Path option:

- Leave the Use MS store box unchecked.
- Enter the certificate filename in the CA Cert textbox.

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.

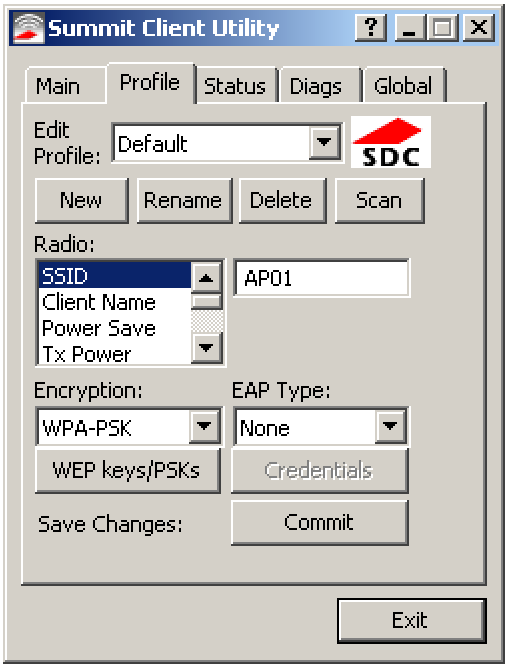
See Certificates for information on generating a Root CA certificate or a User certificate.

Note: The date must be properly set on the device to authenticate a certificate.

WPA PSK

To connect using WPA/PSK, make sure the following profile options are used:

- Enter the **SSID** of the Access Point assigned to this profile
- Set **EAP Type** to **None**
- Set **Encryption** to **WPA PSK** or **WPA2 PSK**
- Set **Auth Type** to **Open**



Edit Profile: Default

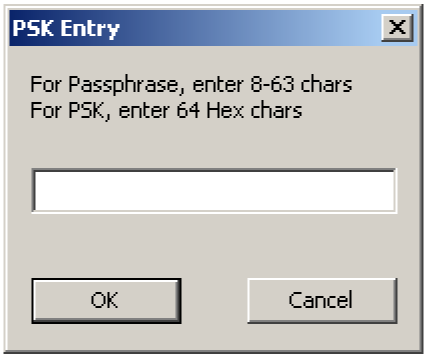
Radio: SSID AP01

Encryption: WPA-PSK

EAP Type: None

Save Changes:

Click the **WEP keys/PSKs** button.



For Passphrase, enter 8-63 chars
For PSK, enter 64 Hex chars

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 the wireless credentials 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 the 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 the User Certificate.

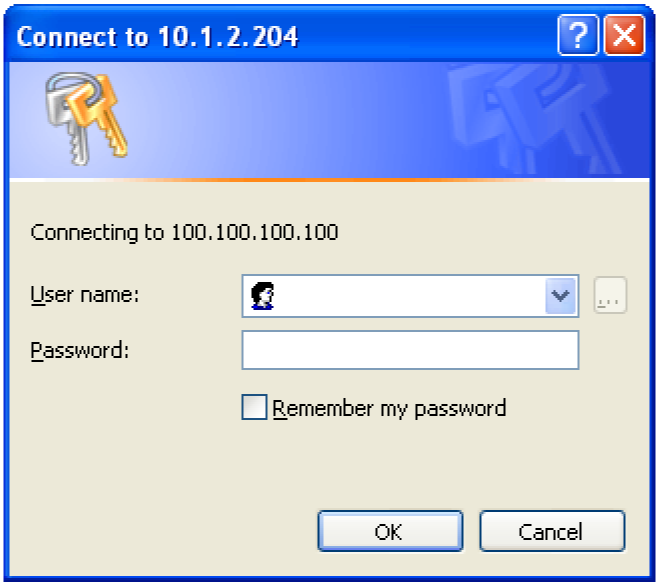
Generating a Root CA Certificate

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

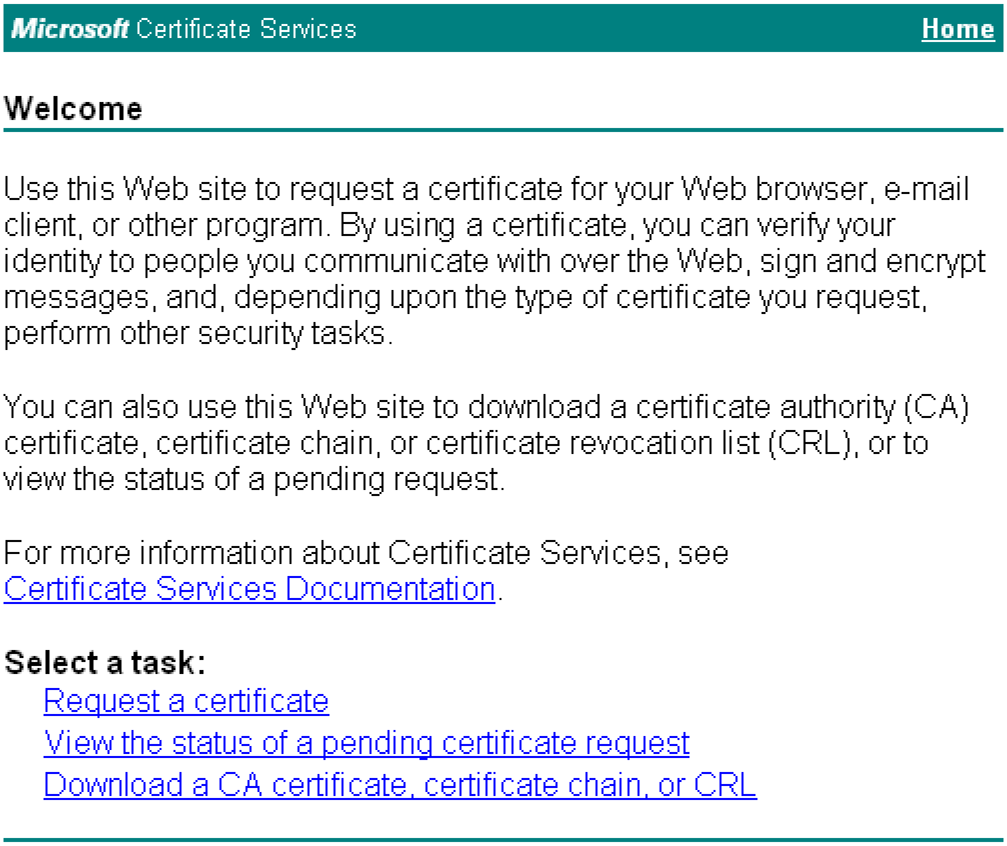
http://<CA IP address>/certsrv.

Sign into the CA with any valid username and password.



Connect to 10.1.2.204

Connecting to 100.100.100.100



Microsoft Certificate Services

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.

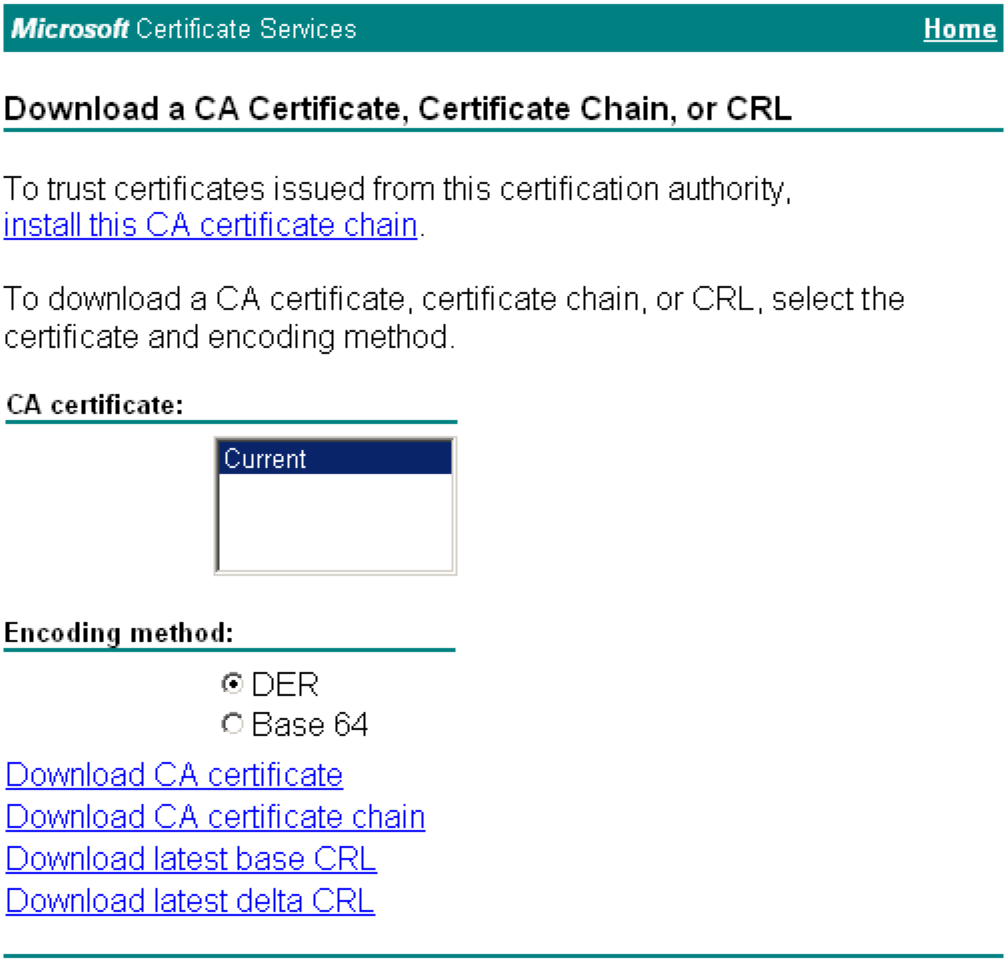
For more information about Certificate Services, see Certificate Services Documentation.

Select a task:

- Request a certificate
- View the status of a pending certificate request
- Download a CA certificate, certificate chain, or CRL

Click the **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

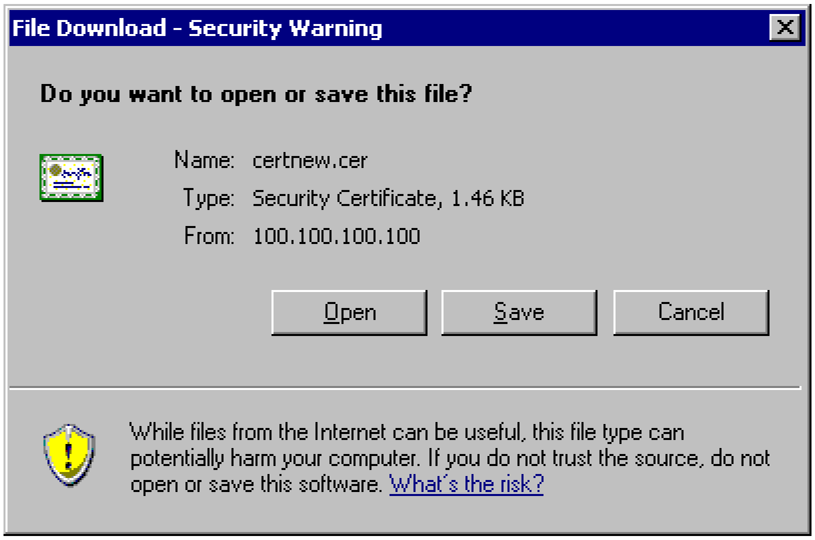
Encoding method:

● 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.



File Download - Security Warning

Do you want to open or save this file?

Name: certnew.cer
Type: Security Certificate, 1.46 KB
From: 100.100.100.100

While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not open or save this software. What's the risk?

Click the **Save** button and save the certificate. Make sure to keep track of the name and location of the certificate.

Install the certificate on the Thor VM2.

Installing a Root CA Certificate

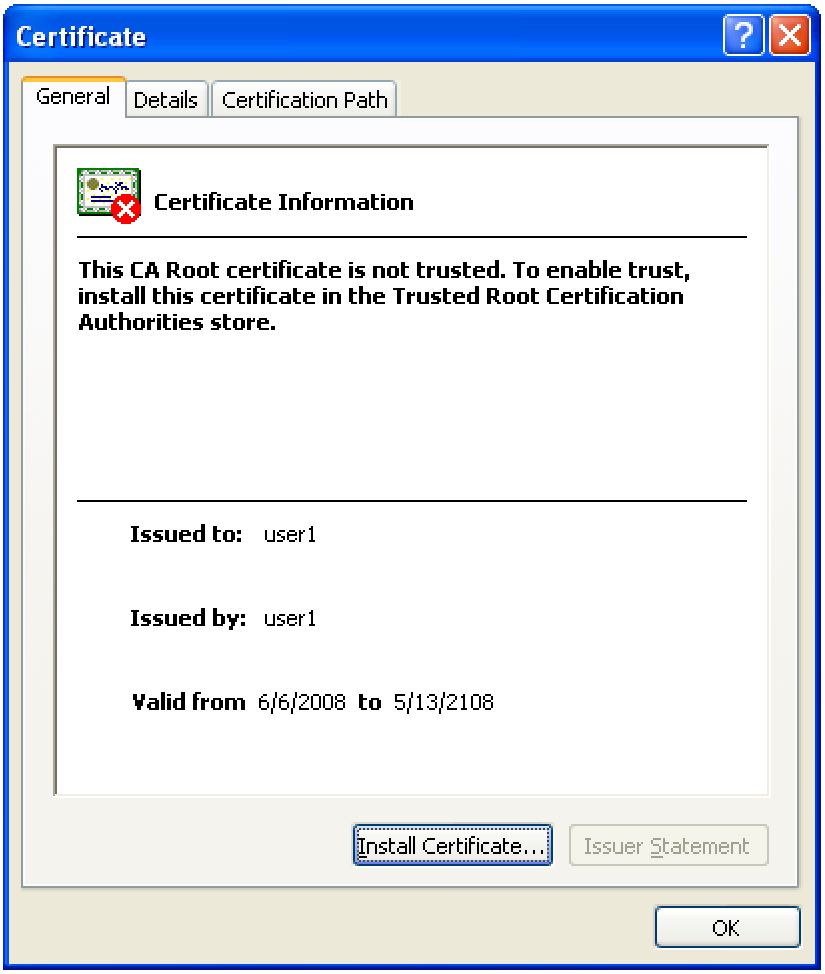
Note: This section is only if the Windows certificate store is used. If the certificate store is not used, copy the certificate to the C:\Program Files\Summit\certs folder or other path specified in the Summit Certs global parameter.

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.

Troubleshooting: 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**.
2. In the left pane, right-click **Trusted Root Certificate Authorities** and select **All Tasks > Import**.
3. The Certificate Import Wizard starts.
4. Tap **Next** and use the **Browse...** button to locate the Root certificate copied to the Thor VM2 then tap **Open**.
5. The certificate filename and path are displayed. Tap **Next**.



Certificate Information

This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: user1

Issued by: user1

Valid from 6/6/2008 **to** 5/13/2108

Tap the **Install Certificate** button.

The certificate import wizard starts. Tap **Next**.

Allow Windows to automatically select the certificate store.

Tap **Next** and **Finish**.

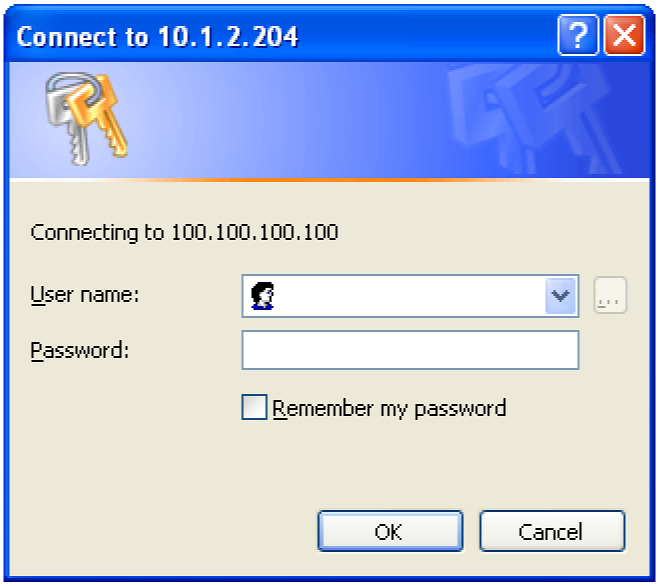
An import successful message is displayed.

Generating 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.

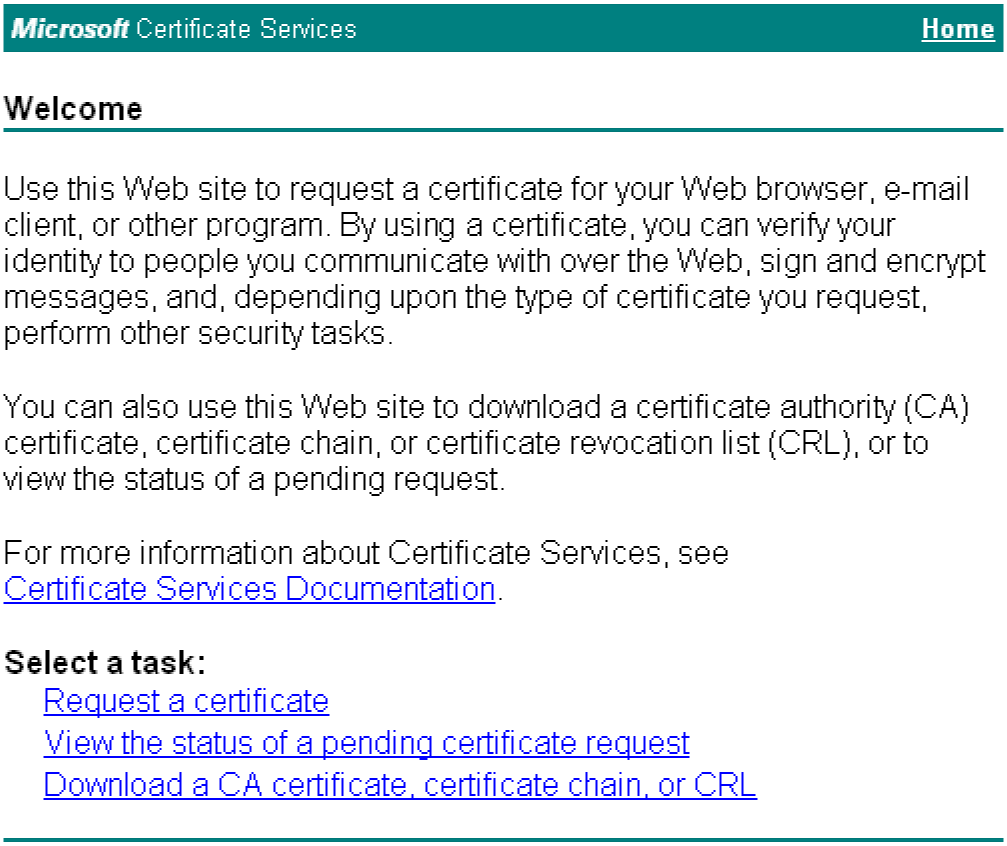
Sign into the CA with the username and password of the person who will be logging into the mobile device.



Connect to 10.1.2.204

Connecting to 100.100.100.100

This process saves a user certificate file. There is no separate private key file as used on Windows CE devices.



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.

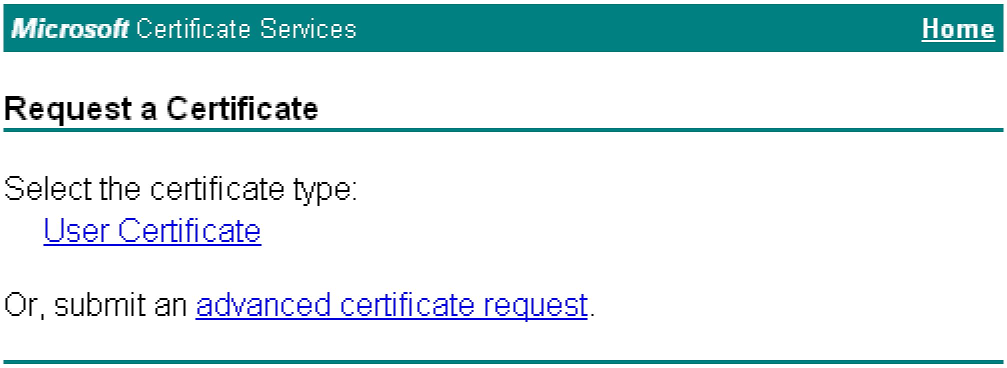
You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

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.

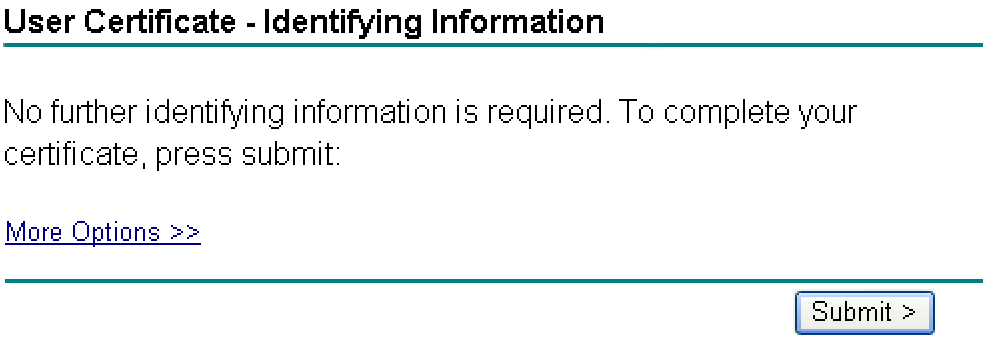


Request a Certificate

Select the certificate type:
User Certificate

Or, submit an advanced certificate request.

Click on the **User Certificate** link.

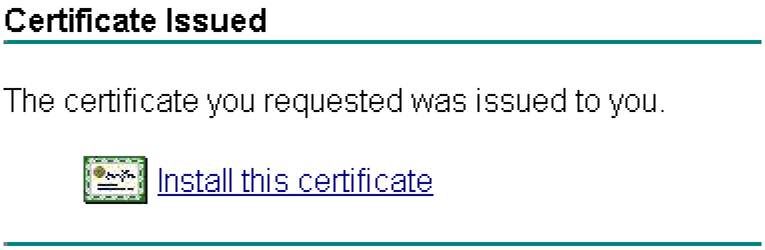


User Certificate - Identifying Information

No further identifying information is required. To complete your certificate, press submit:

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

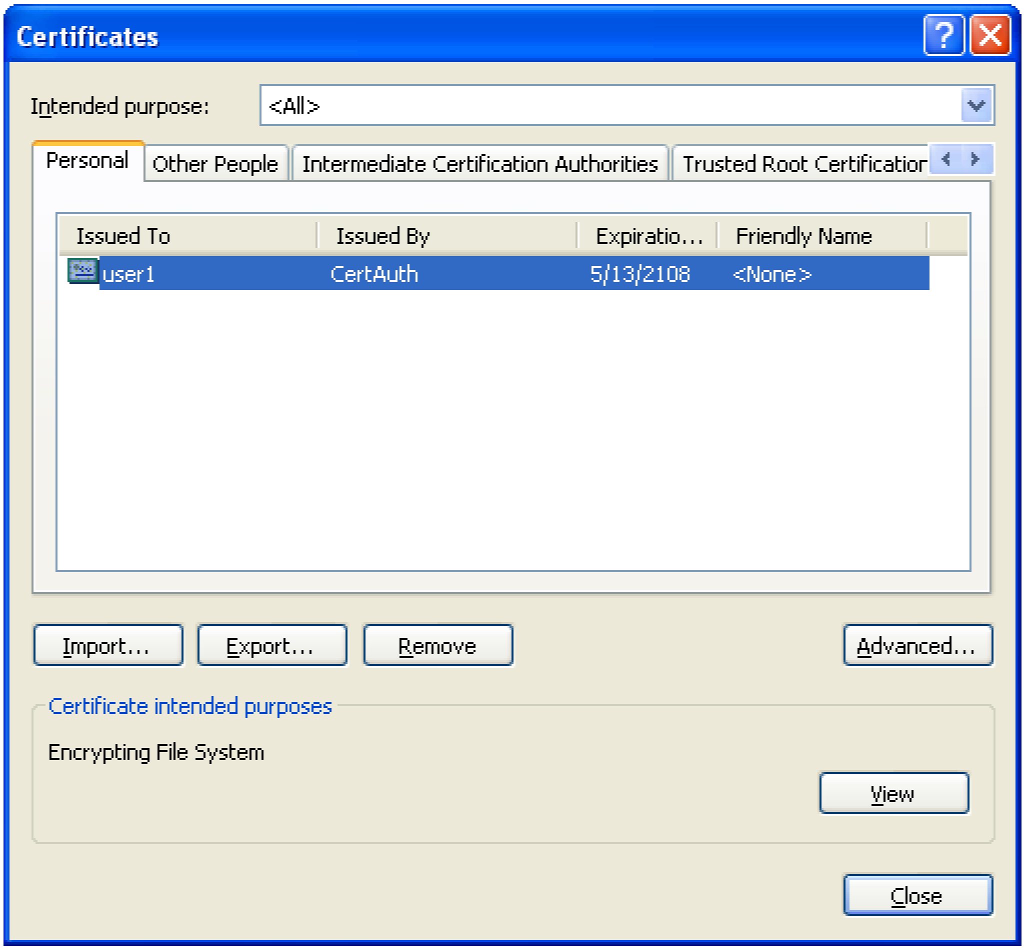
The certificate you requested was issued to you.

Install the user certificate on the requesting computer by clicking the **Install this certificate** 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.



Intended purpose: <All>

Issued To	Issued By	Expiratio...	Friendly Name
user1	CertAuth	5/13/2108	<None>

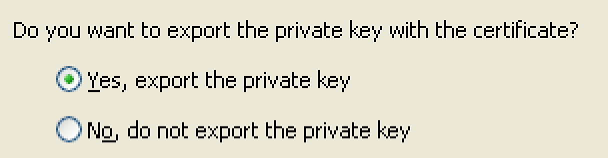
Certificate intended purposes

Encrypting File System

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.

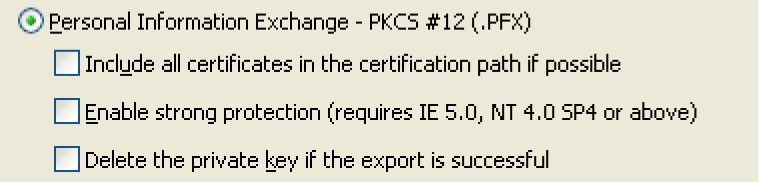


Do you want to export the private key with the certificate?

● Yes, export the private key

○ No, do not export the private key

Uncheck **Enable strong protection** and check **Next**. The certificate type must be PKCS #12 (.PFX).



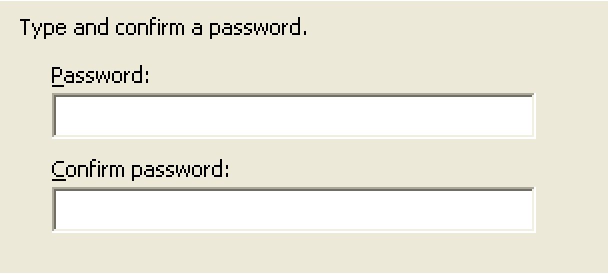
● Personal Information Exchange - PKCS #12 (.PFX)

□ Include all certificates in the certification path if possible

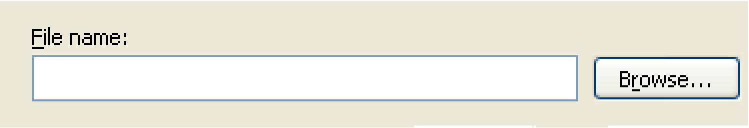
□ Enable strong protection (requires IE 5.0, NT 4.0 SP4 or above)

□ Delete the private key if the export is successful

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.

Installing a User Certificate

After generating and exporting the user certificate, copy it from the PC to the Thor VM2. Copy the certificate to a location on the Thor VM2.

Locate the certificate file (it has a .PFX extension) and double-click on it.

Troubleshooting: If the Certificate Wizard does not start automatically when you double-tap the certificate .PFX file:

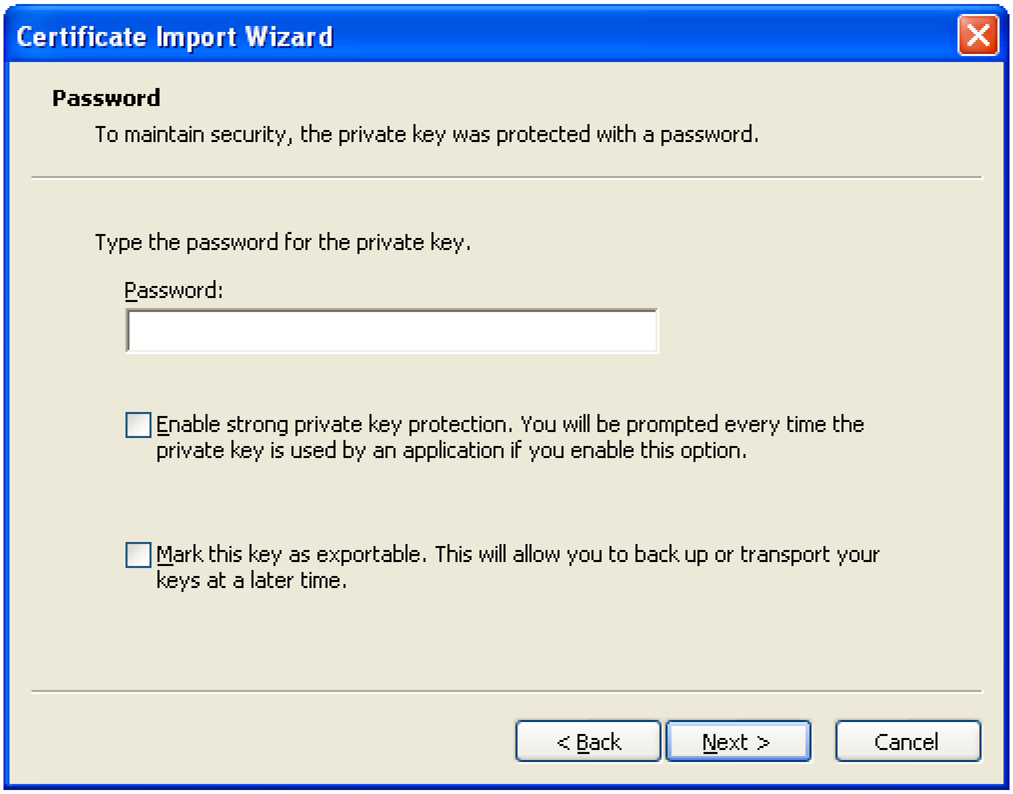
1. Select **Start > Run** and type **certmgr.msc** in the text box and tap **OK**.
2. In the left pane, right-click **Personal** and select **All Tasks > Import**.
3. The Certificate Import Wizard starts.
4. Tap **Next** and use the **Browse...** button to locate the User certificate copied to the Thor 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**.
5. The certificate filename and path are displayed. Tap **Next**.
6. Follow the instructions that follow starting with the prompt for password.

The certificate import wizard starts. Tap **Next**.

Confirm the certificate file name and location.

Tap **Next**.

You are prompted for the password that was assigned when the certificate was exported.



Certificate Import Wizard

Password

To maintain security, the private key was protected with a password.

Type the password for the private key.

Password:

□ Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.

□ Mark this key as exportable. This will allow you to back up or transport your keys at a later time.

It is not necessary to select either of the checkboxes displayed above.

Enter the password and tap **Next**.

On the next screen, allow Windows to automatically select the certificate store, then click **Next** and **Finish**. An import successful message is displayed.

OneClick Internet

This section contains the User Manual for the customized version of WebToGo's OneClick 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 on the Thor VM2 while the WWAN connection is active. When exiting standby, 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, the touch screen may remain inactive for 10-15 seconds after the Thor VM2 resumes from standby.

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 a 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.

Tap the **Settings** button and select the **Firmware** tab. Select the firmware for your carrier from the list and tap **Change**.

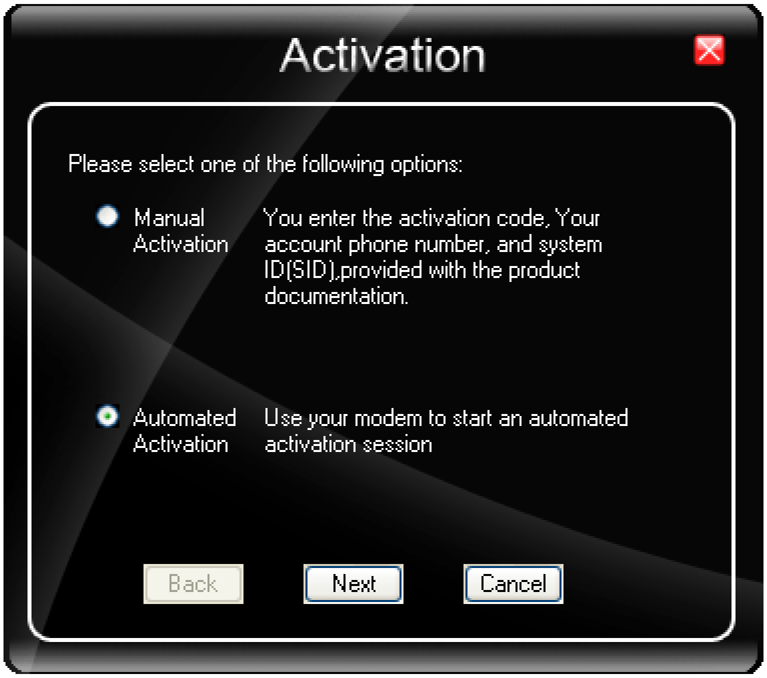
For more details, see OneClick Internet Connection Manager and the Firmware tab.

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 Settings > 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.

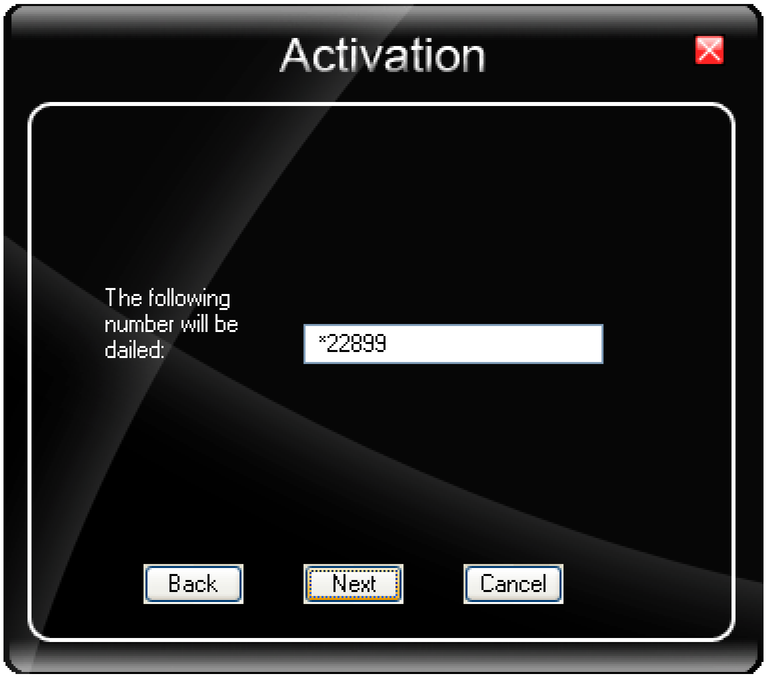


Please select one of the following options:

○ Manual Activation — You enter the activation code, Your account phone number, and system ID(SID),provided with the product documentation.

● Automated Activation — Use your modem to start an automated activation session

Make sure **Automated Activation** is selected and tap **Next**.



The following number will be dailed: *22899

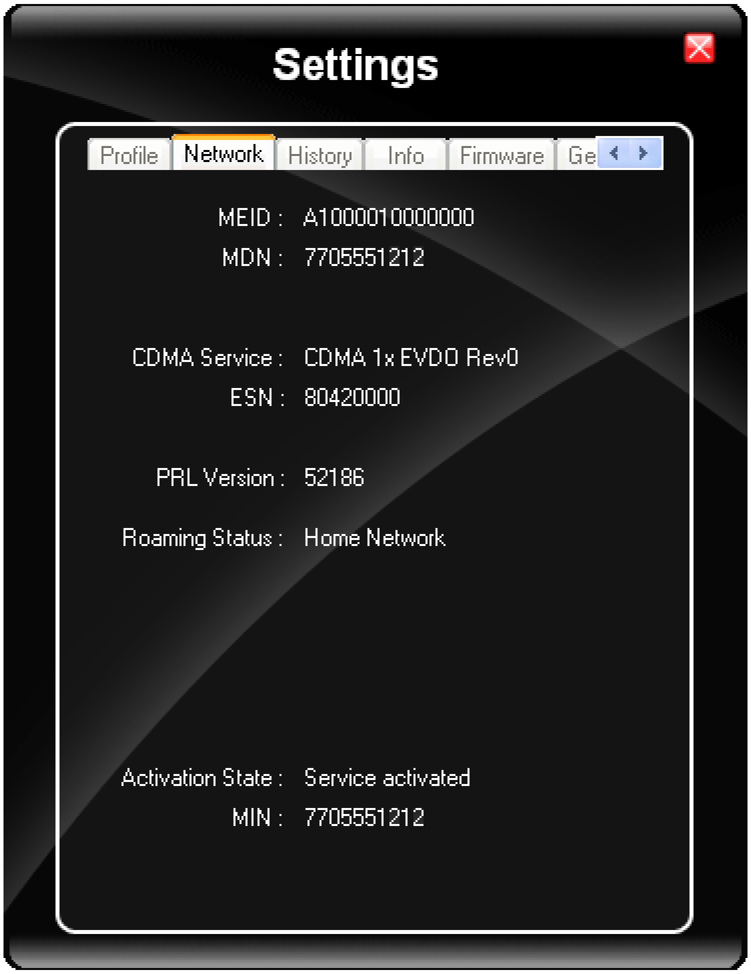
Tap **Next** to complete the activation.

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.



MEID : A1000010000000

MDN : 7705551212

CDMA Service : CDMA 1x EVDO Rev0

ESN : 80420000

PRL Version : 52186

Roaming Status : Home Network

Activation State : Service activated

MIN : 7705551212

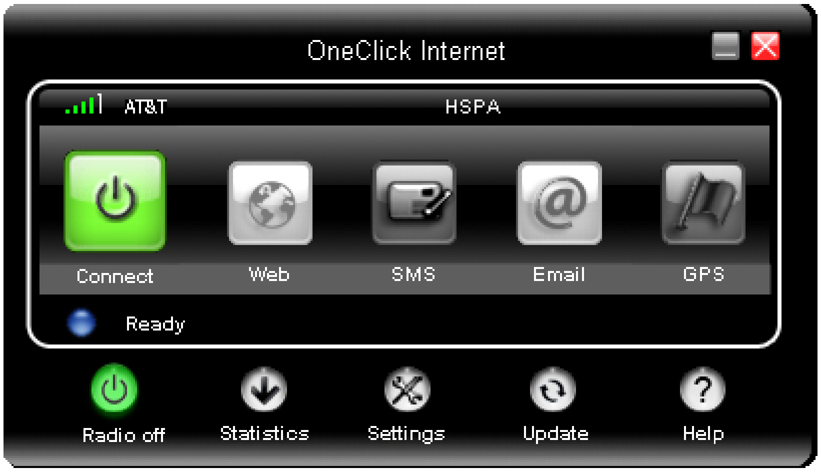
This screen contains the settings including the telephone number from the provider, in this case Verizon.

Using OneClick Internet

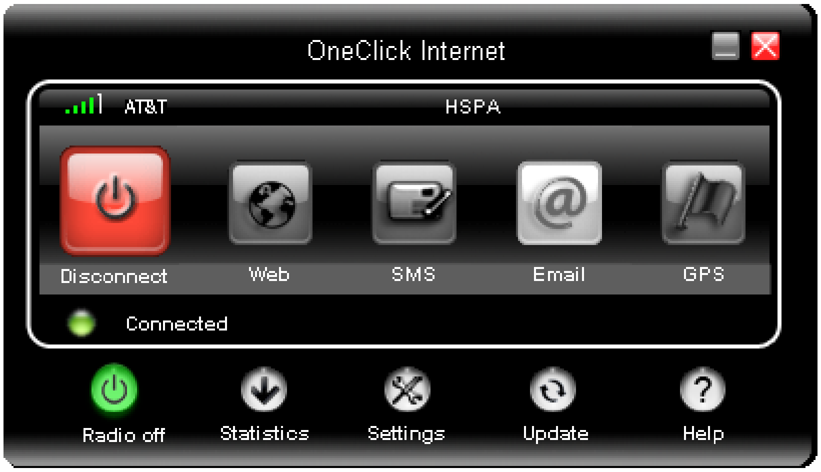
If OneClick Internet is not loaded, double-tap the desktop icon to load it. If OneClick Internet is loaded but minimized to the system tray, tap the OneClick Internet icon in the system tray to maximize it.

How To: 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

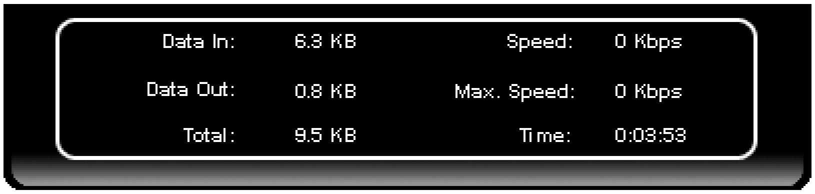
The Radio button allows you to switch the WWAN radio on and off to save power or to disable the radio in instances where it is not desired (such as during airplane travel).

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:    6.3 KB        Speed:   0 Kbps
Data Out:    0.8 KB   Max. Speed:   0 Kbps
   Total:    9.5 KB         Time:   0:03:53
```

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

One Click 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 for 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.

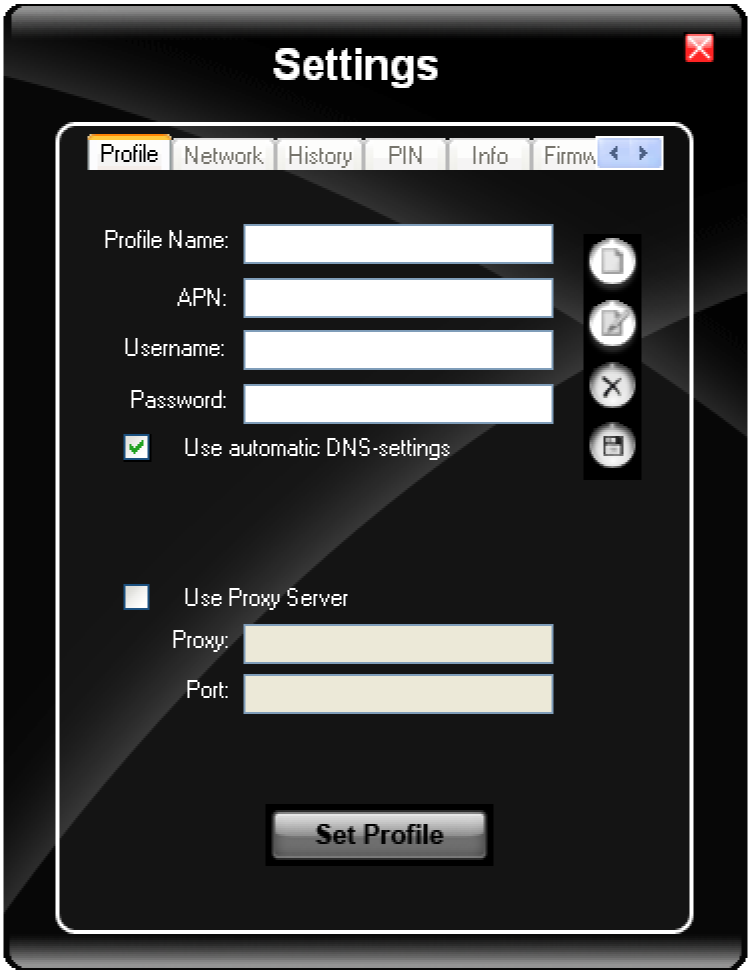
Settings Button

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 Tab



☑ Use automatic DNS-settings

□ Use Proxy Server

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 textbox 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.

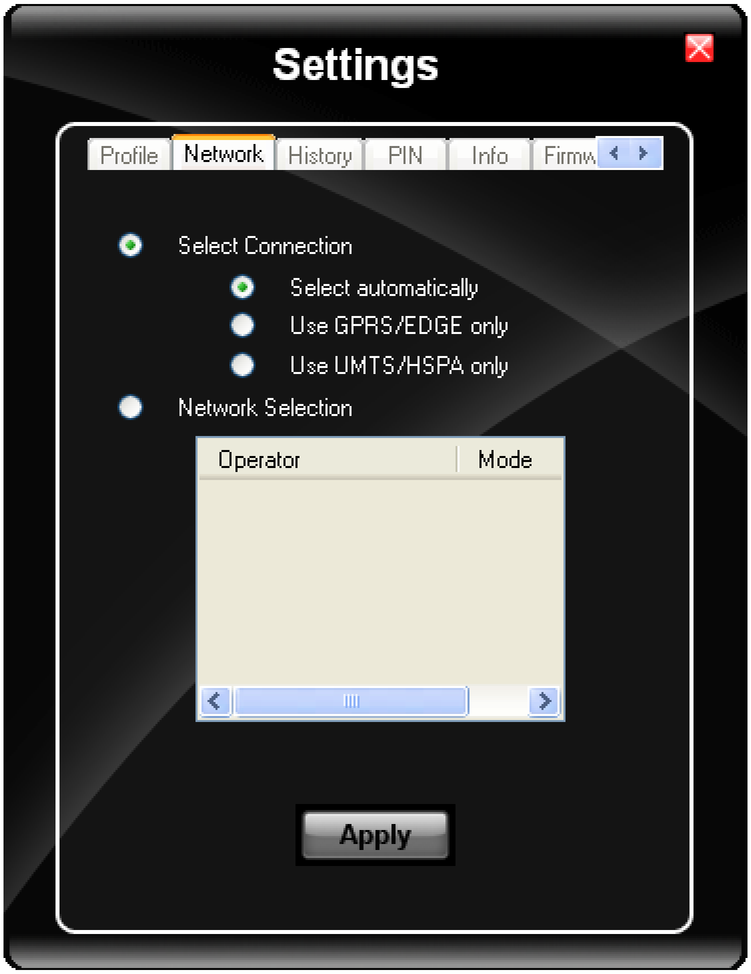
Parameters

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 Tab

The appearance of the network tab depends on the type of firmware selected.

Network with SIM Card



● Select Connection

● Select automatically

○ Use GPRS/EDGE only

○ Use UMTS/HSPA only

○ Network Selection

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".

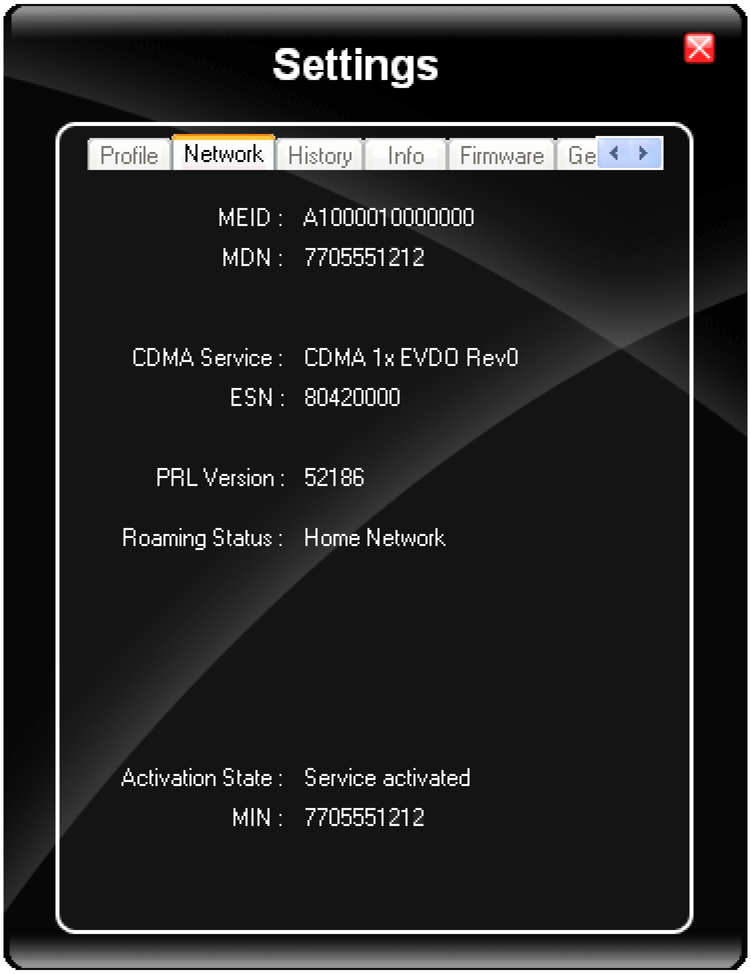
This item is useful when traveling . Automatic mode selects the preferred network of your network operator.

If enabled, Network Selection displays a list of network options.

1. Automatic Selection
2. Retrieving Networks...

The currently registered network is marked.

CDMA Network



MEID : A1000010000000

MDN : 7705551212

CDMA Service : CDMA 1x EVDO Rev0

ESN : 80420000

PRL Version : 52186

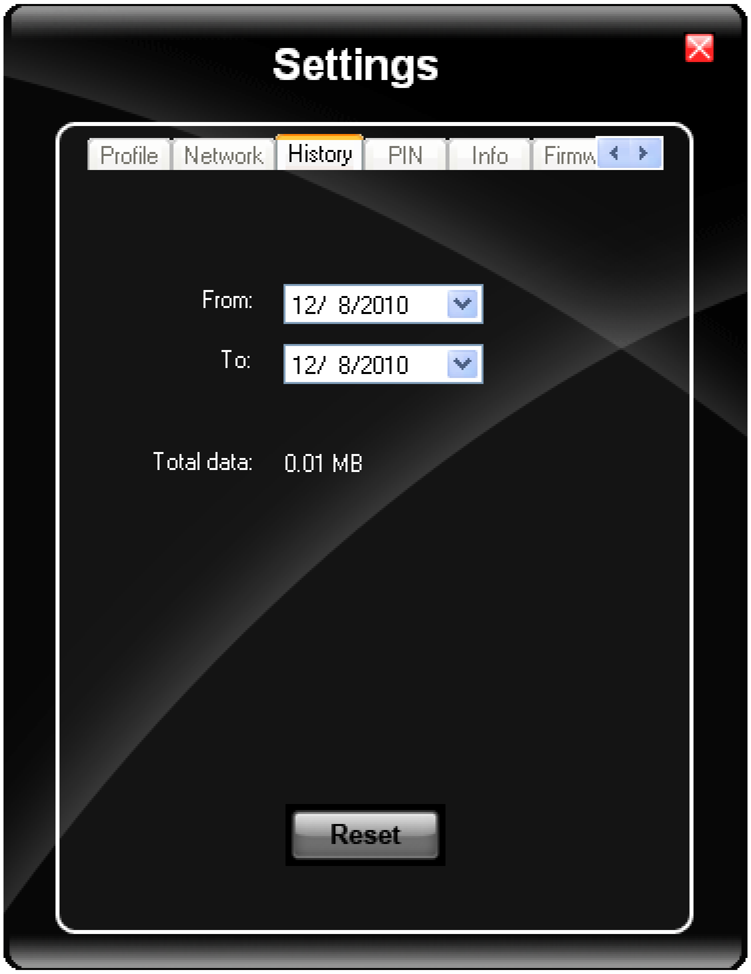
Roaming Status : Home Network

Activation State : Service activated

MIN : 7705551212

Information on the CDMA network is displayed. There are no editable parameters on this screen.

History Tab



From: 12/ 8/2010

To: 12/ 8/2010

Total data: 0.01 MB

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.

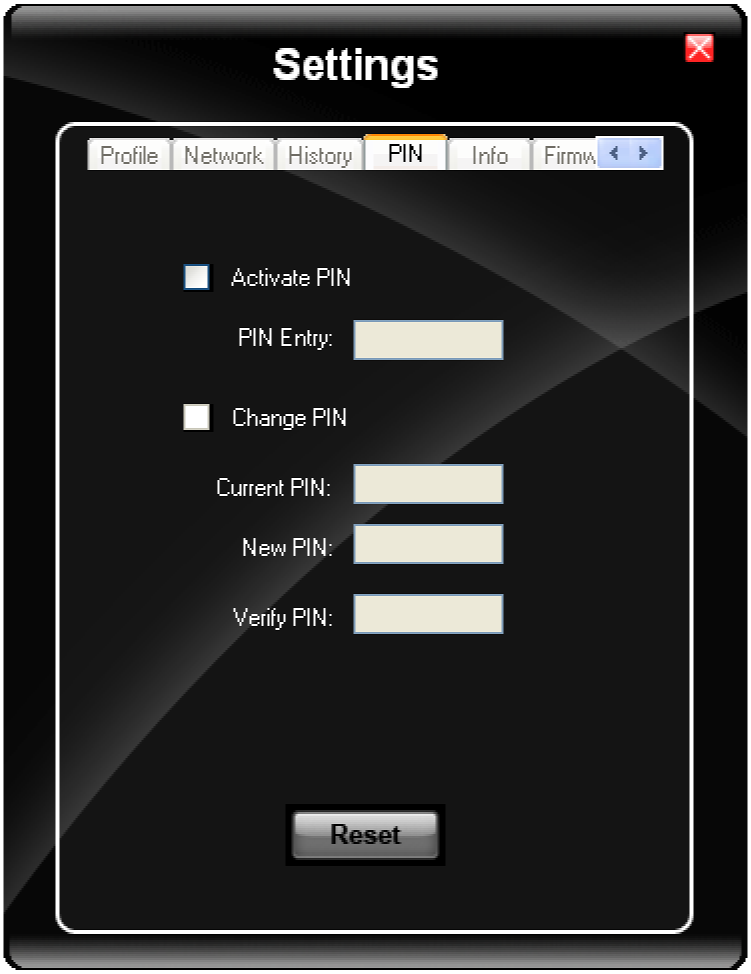
PIN Tab

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.



Settings

Profile | Network | History | PIN | Info | Firmw

□ Activate PIN

PIN Entry:

□ Change PIN

Current PIN:

New PIN:

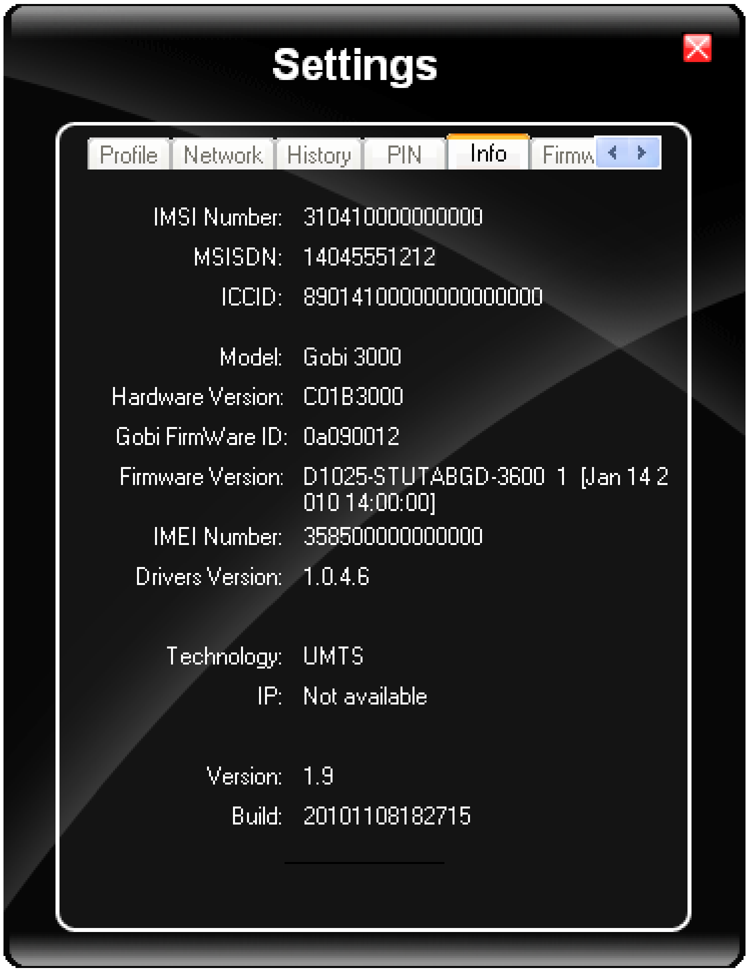
Verify PIN:

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 Tab



IMSI Number: 310410000000000
MSISDN: 14045551212
ICCID: 89014100000000000000

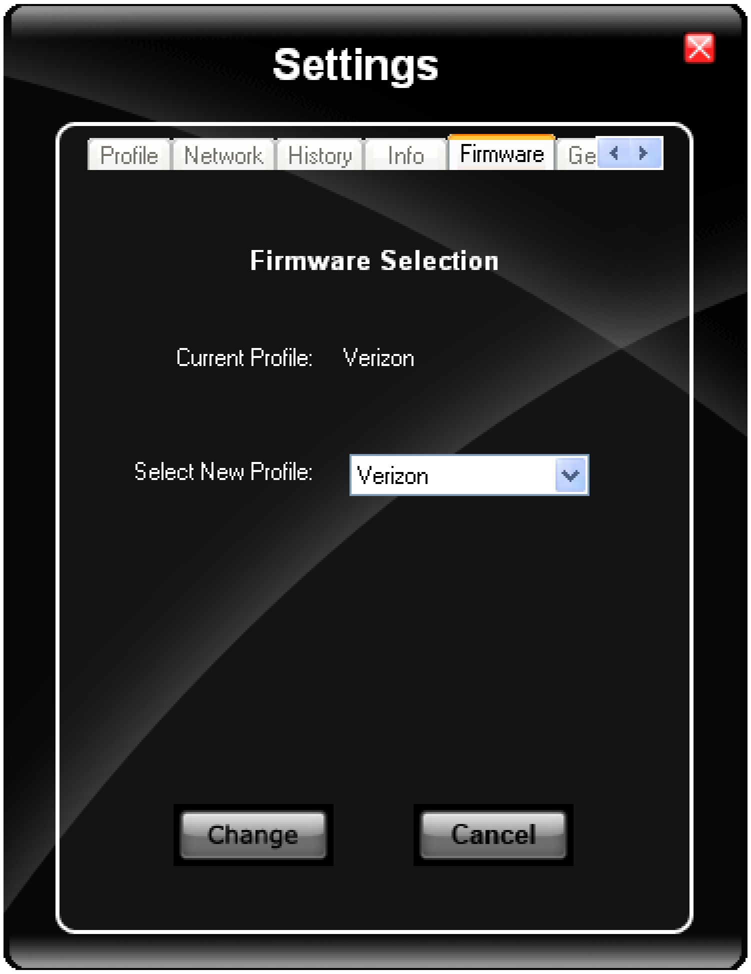
Model: Gobi 3000
Hardware Version: C01B3000
Gobi FirmWare ID: 0a090012
Firmware Version: D1025-STUTABGD-3600 1 [Jan 14 2010 14:00:00]
IMEI Number: 358500000000000
Drivers Version: 1.0.4.6

Technology: UMTS
IP: Not available

Version: 1.9
Build: 20101108182715

This tab displays SIM card, modem and system Information.

Firmware Tab



Current Profile: Verizon

Select New Profile: Verizon

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 clicking 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.

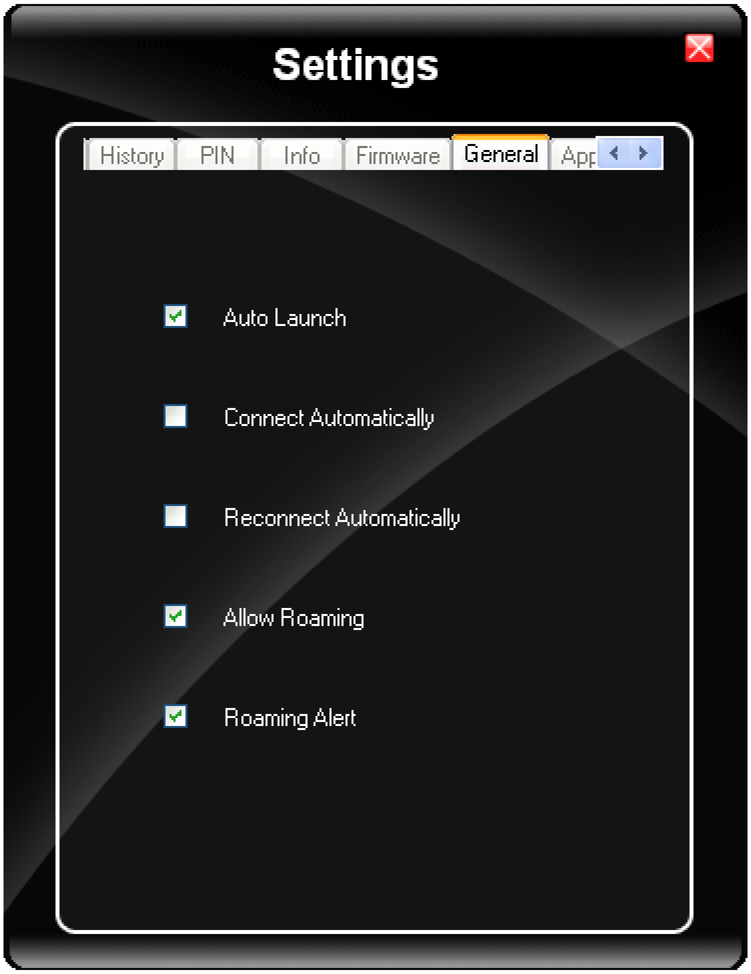
Activation on CDMA

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 window 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 Tab



☑ Auto Launch

□ Connect Automatically

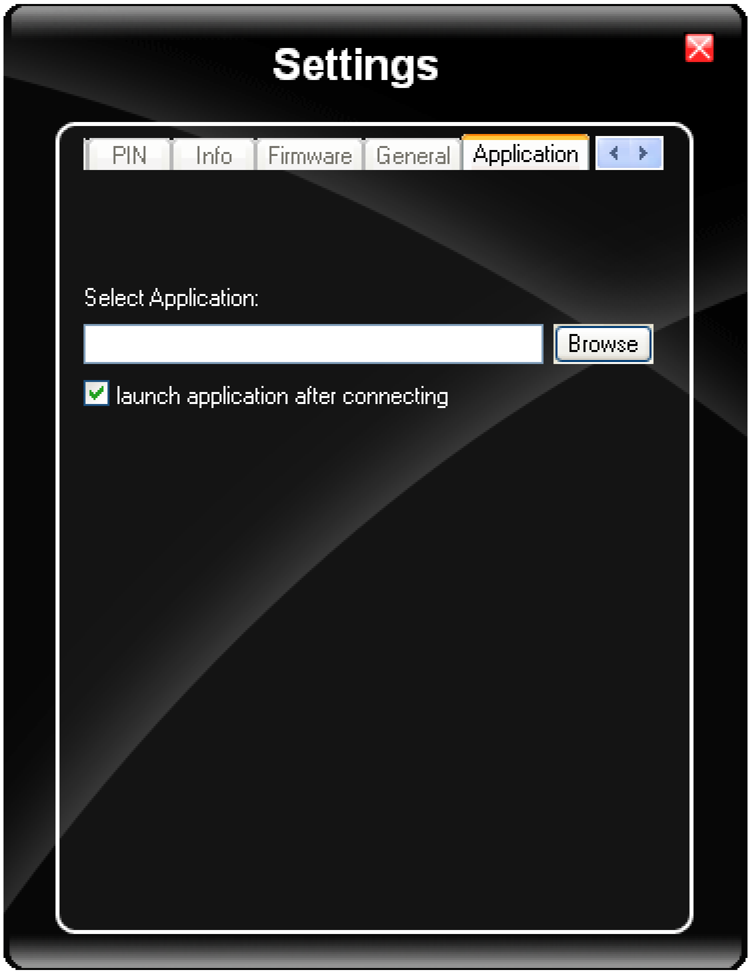
□ Reconnect Automatically

☑ Allow Roaming

☑ Roaming Alert

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 or hibernate.
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 Tab



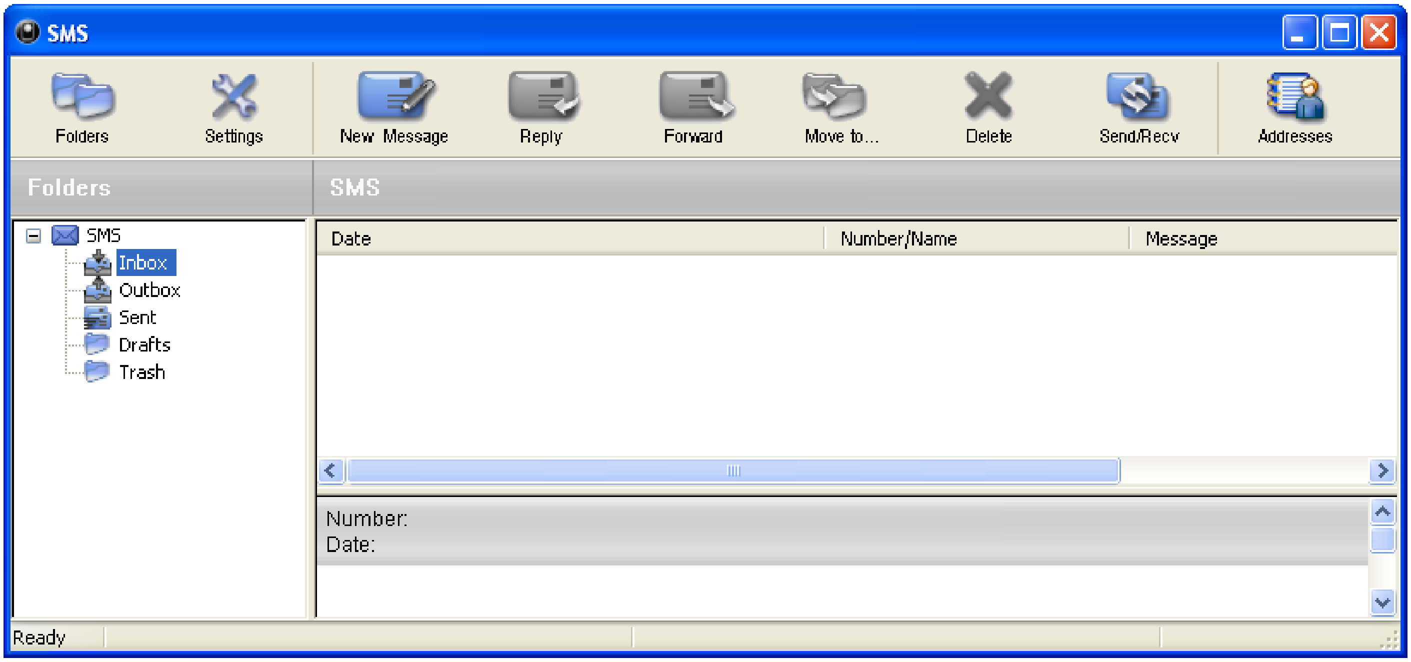
Select Application:

☑ launch application after connecting

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



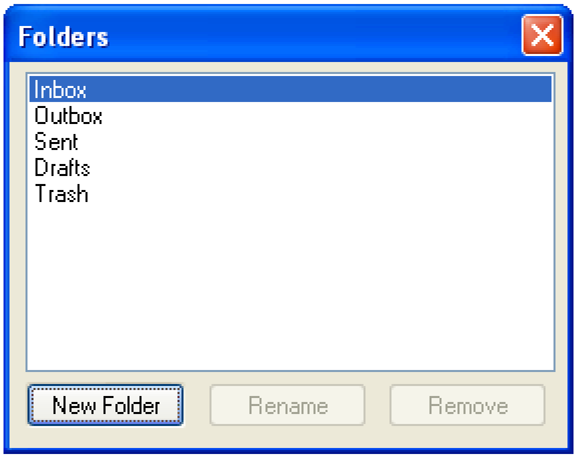
The SMS Center window is split into menu bar, folder view, folder content and preview window. To manage your short messages you may:

Button	Description
Folders	Manage SMS folders
Settings	Change SMS settings
New Message	Create new SMS/MMS messages
Reply	Reply to SMS
Forward	Forward SMS

Button	Description
Move to...	Move SMS to a folder
Delete	Delete SMS
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.

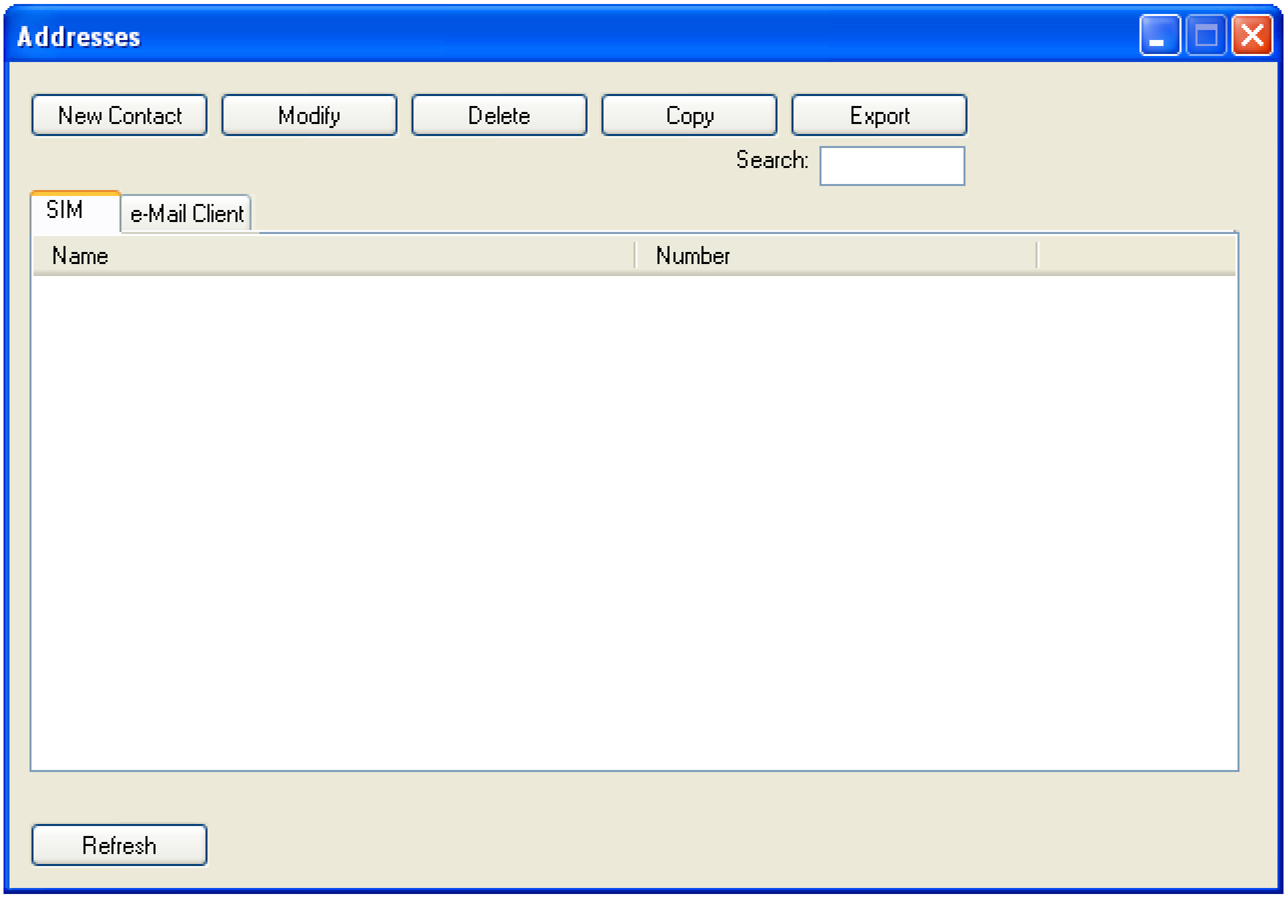
Send/Receive

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

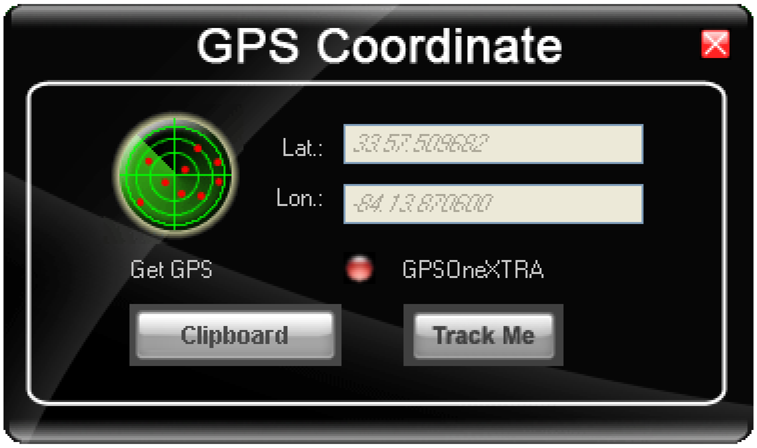
Clicking this button opens the Web Browser and allows the user to surf the Internet once the connection is established. The default browser is used, which is Internet Explorer by default on the Thor VM2.

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.



Lat.: 33 57.509682

Lon.: -84 13.870600

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 3000 3G Module (preinstalled by Honeywell)
- Gobi 3000 Driver package (loaded by Honeywell)

OneClick Internet for Gobi 3000 is compatible with

- Windows Embedded Standard 2009 on the Thor VM2

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.

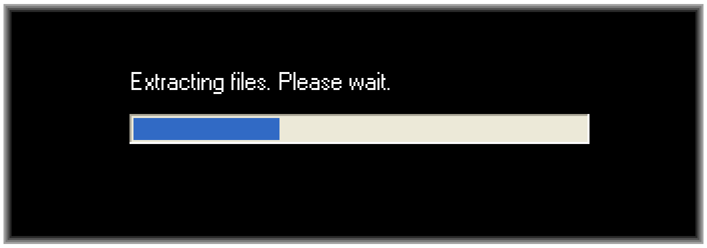
One Click Internet is pre-installed before the Thor VM2 is shipped.

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** and select **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.

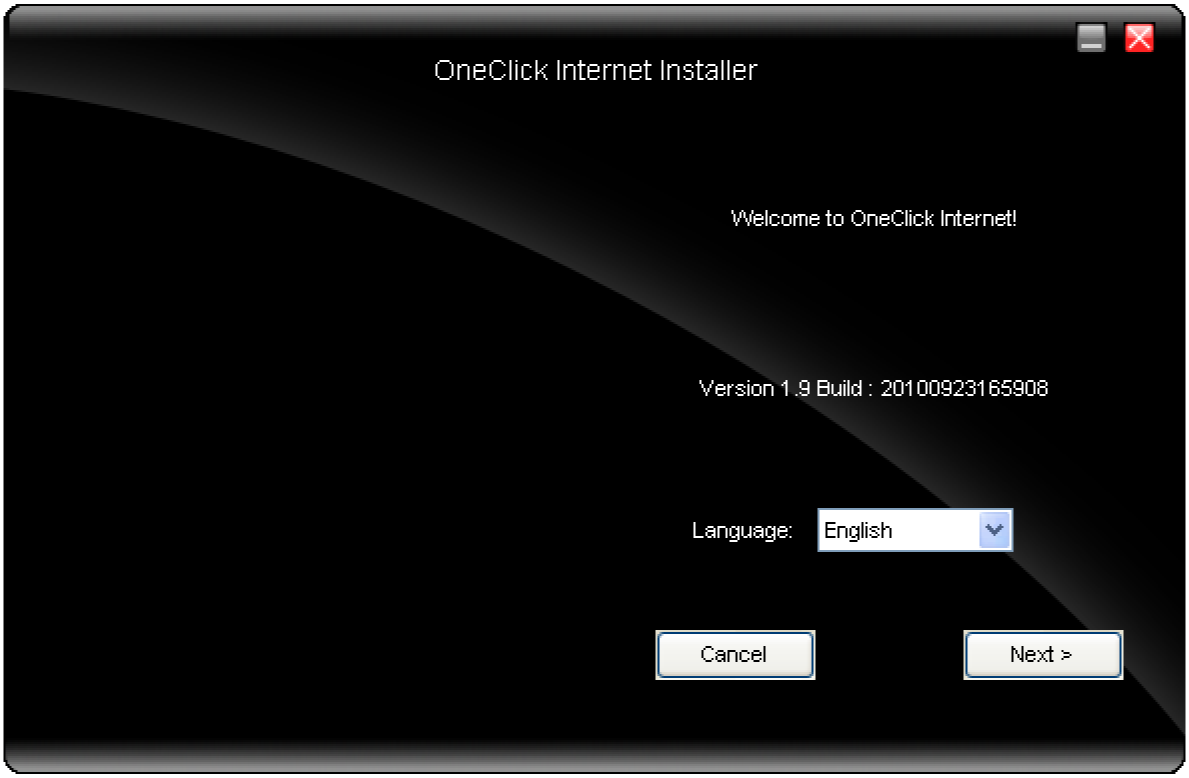
Installation

When you double-click the Installer file for OneClick Internet, it extracts the files to install.



Extracting files. Please wait.

Next, select the application language. By default, the language of the OS is used (if available).



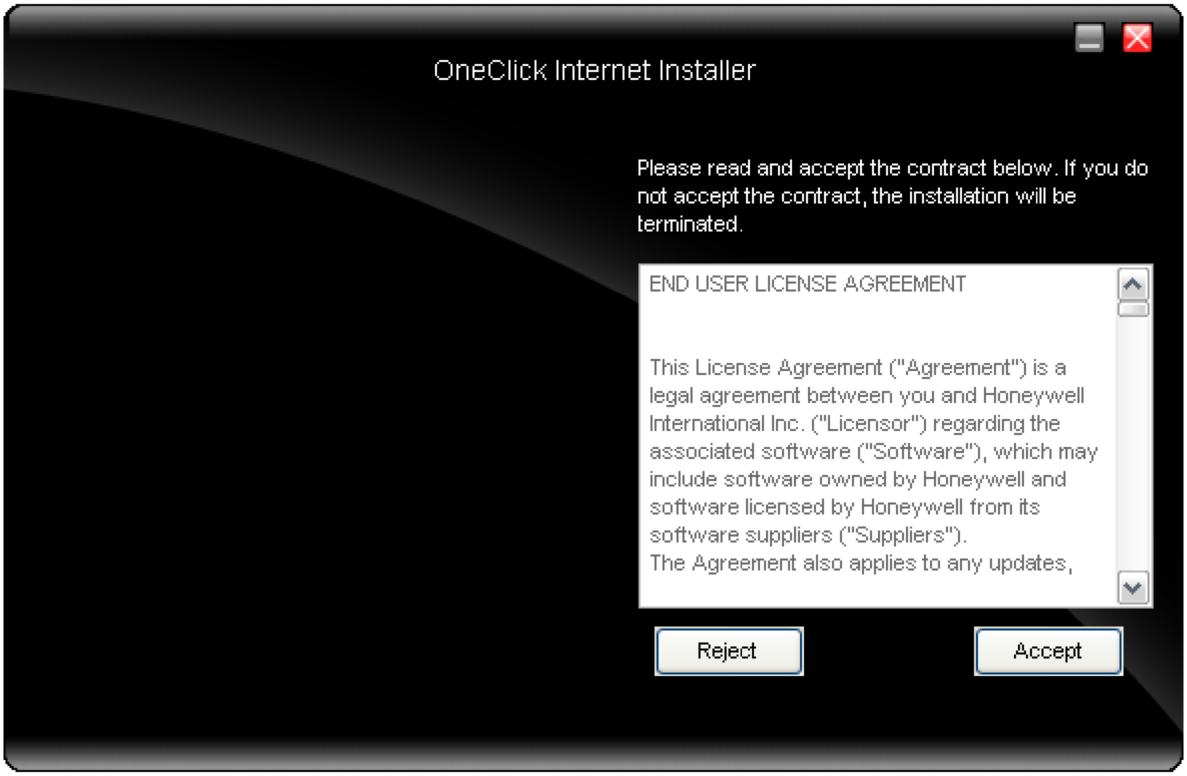
OneClick Internet Installer

Welcome to OneClick Internet!

Version 1.9 Build : 20100923165908

Language: English

Review and accept the license agreement. Click **Accept**, if you agree. Otherwise please click **Reject** to cancel installation.



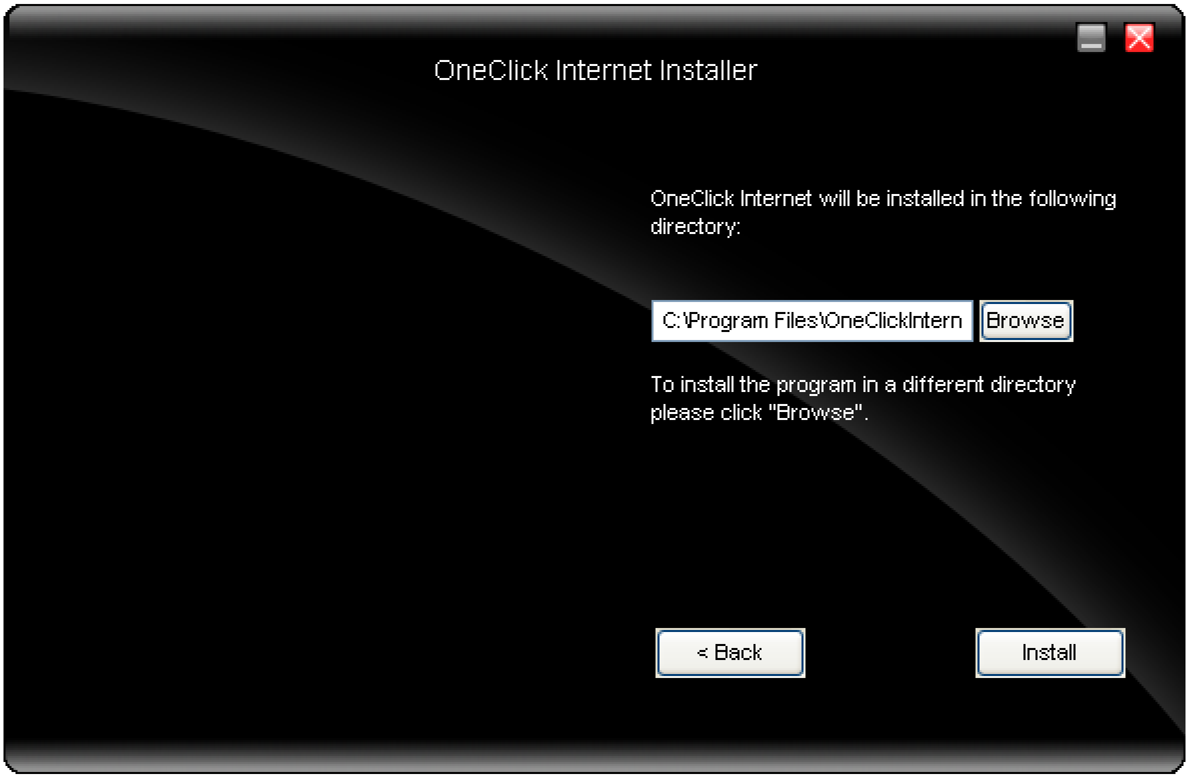
OneClick Internet Installer

Please read and accept the contract below. If you do not accept the contract, the installation will be terminated.

END USER LICENSE AGREEMENT

This License Agreement ("Agreement") is a legal agreement between you and Honeywell International Inc. ("Licensor") regarding the associated software ("Software"), which may include software owned by Honeywell and software licensed by Honeywell from its software suppliers ("Suppliers").
The Agreement also applies to any updates,

Next the installer asks for the installation directory. Use the **Browse** button to specify a location other than the default.



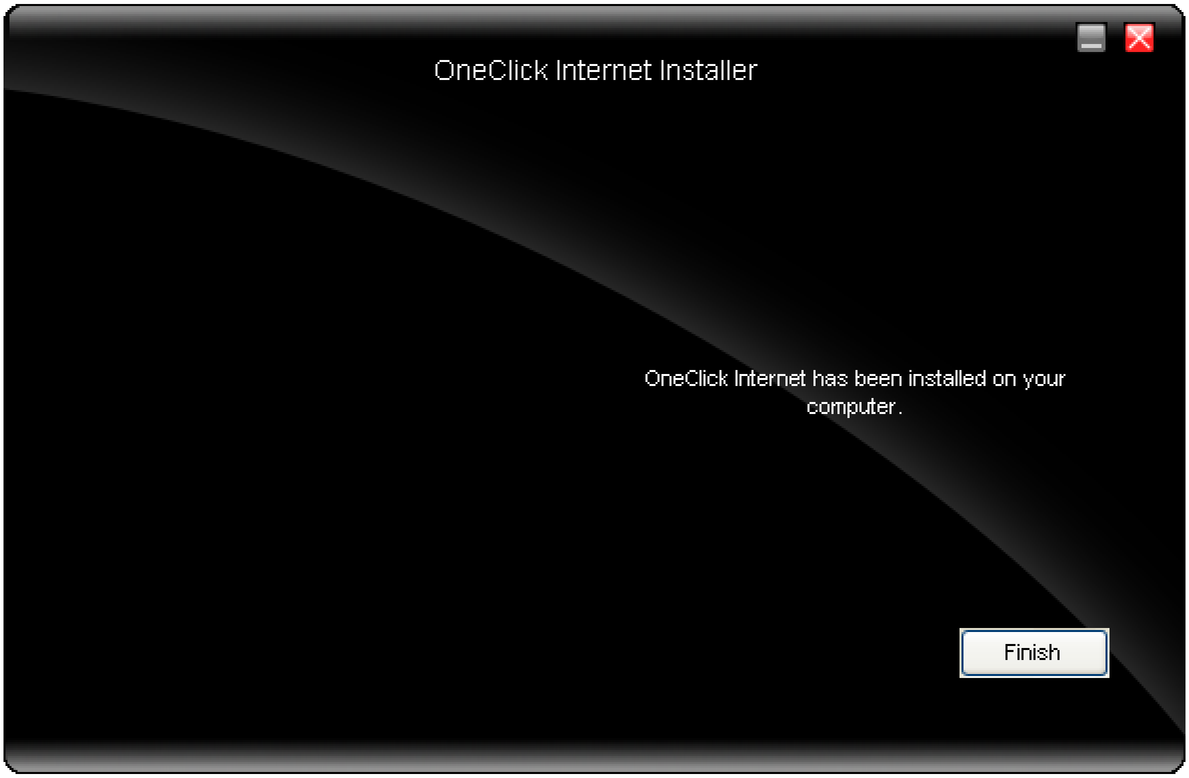
OneClick Internet Installer

OneClick Internet will be installed in the following directory:

C:\Program Files\OneClickIntern

To install the program in a different directory please click "Browse".

Installation process is indicated on screen. When completed. click the **Finish** button to exit the installer.



OneClick Internet Installer

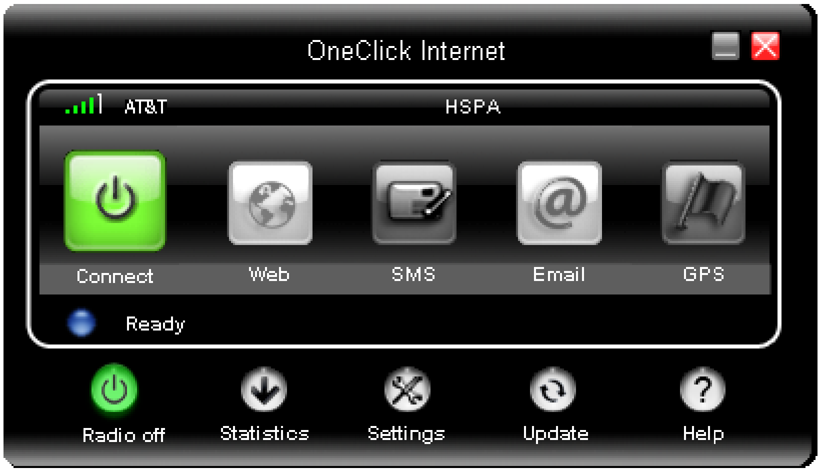
OneClick Internet has been installed on your computer.

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	**Connect / Cancel / Disconnect** Tap this button to connect or disconnect. The color of this button also indicates the status of the connection: Connect The radio is disconnected. Tap the button to connect. Cancel The radio is currently connecting. Disconnect The radio is connected. Tap the button to disconnect.

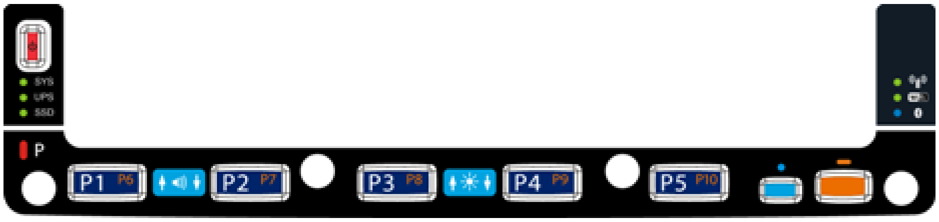
Icon	Description
✉	**SMS** The SMS button is enabled if no Internet connection is active. When this button is active, tapping it accesses the integrated SMS application.
🌐	**Web** Tap this button to launch the default browser.
@	**Email** Tap this button to launch the default Email application.
⚑	**GPS** 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. ⬆ Tap the button to hide the connection statistics.
✂	**Settings** Tap this button to access connection settings. Select from several tabs to configure the connection settings.
🔄	**Update** Tap this button to access OneClick Internet updates.
?	**Help** Click this button to view the on-line 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.

Chapter 5 - 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.

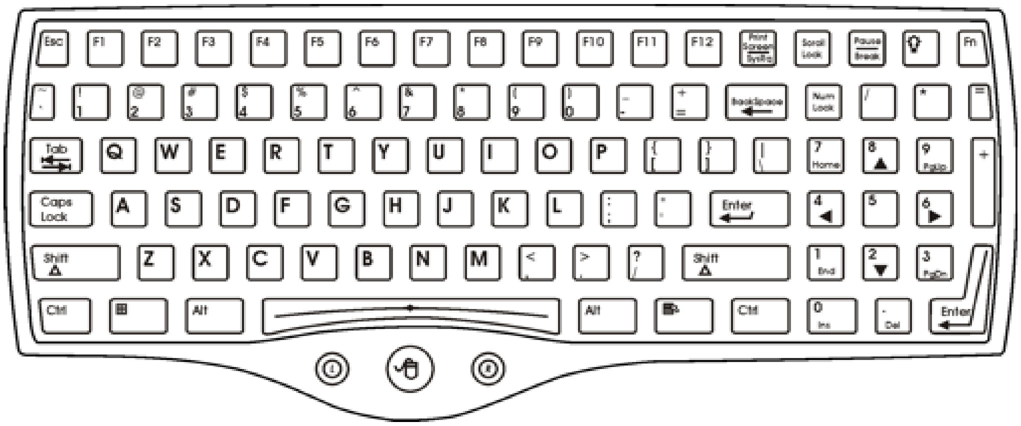
To get this Programmable Key	Press These Keys in this Order		Default Key Value
P1 (Programmable key 1)	P1		F1
P2 (Programmable key 2)	P2		F2
P3 (Programmable key 3)	P3		F3
P4 (Programmable key 4)	P4		F4
P5 (Programmable key 5)	P5		F5
P6 (Programmable key 6)	Orange	P1	<none>>
P7 (Programmable key 7)	Orange	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
Decrease display brightness	Blue	P4

The Blue plus P5 keypress sequence causes no action.

External 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 CE 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)

Chapter 6 - Technical Specifications

Thor VM2

Processor	Atom CPU operating at 1.6 GHz.
Memory	2GB SDRAM
Mass Storage	4 or 8GB CompactFlash
Storage Expansion	User installable, supports 1 to 4GB SD card
Operating System	Microsoft Windows Embedded Standard 2009
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	Controller: SVGA compatible controller 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
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 Quick Mount Smart Dock, see below.
Beeper	Minimum loudness greater than 95dBm at 10 cm in front of unit
Uninterruptible Power Supply	Internal UPS battery
Backup Battery (RCT)	Internal lithium Battery maintains Real Time Clock

Quick Mount Smart Dock

External Connectors	Two external RS-232 serial ports, COM1 and COM2, with switchable power CANbus/Audio connector supports either audio/microphone via adapter cable or J1939 Female and J1939 Male connectors via CANbus cable USB Host Port via adapter cable (USB Client Port not available)
Power Connector	5-pin connector. 10-60V DC input power
Power Switch	Sealed power switch
External Power Supply	External power supply. AC Adapter. 120-240VAC to 12VDC
Input Power	DC Input Voltage: 10- 60 VDC Input Current: 4.6 Amps Input Fuse: 10A Time Delay

Dimensions

Thor VM2

Width	10.6” (26.8 cm)
Height	8.4” (21.4 cm)
Depth	2.1” (5.3 cm)
Weight	4.8 lb. (2.2 kg)

Quick Mount Smart 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)
Weight	3.2 lb. (1.5 kg)

Environmental Specifications

Thor VM2 and Quick Mount Smart 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	Standard: Up to 90% non-condensing at 104°F (40°C) Extended temperature: 100%
Water and Dust	IEC 60529 compliant to IP66
ESD	15 kV
Vibration	MIL-STD-810F, composite wheeled vehicles.
Crash	SAE-J 1455

Network Card Specifications

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
Operating Temperature	Same as Thor VM2 Operating Temperature
Storage Temperature	Same as Thor VM2 Storage Temperature
Connectivity	TCP/IP, Ethernet, ODI
Diversity	Yes

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

Chapter 7 - Technical Assistance

If you need assistance installing or troubleshooting your device, please contact us by using one of the methods below:

Knowledge Base: www.hsmknowledgebase.com

Our Knowledge Base provides thousands of immediate solutions. If the Knowledge Base cannot help, our Technical Support Portal (see below) provides an easy way to report your problem or ask your question.

Technical Support Portal: www.hsmsupportportal.com

The Technical Support Portal not only allows you to report your problem, but it also provides immediate solutions to your technical issues by searching our Knowledge Base. With the Portal, you can submit and track your questions online and send and receive attachments.

Web form: www.hsmcontactsupport.com

You can contact our technical support team directly by filling out our online support form. Enter your contact details and the description of the question/problem.

Telephone: www.honeywellaidc.com/locations

For our latest contact information, please check our website at the link above.

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, please visit www.honeywellaidc.com and select **Support > Contact Service and Repair** to see your region's instructions on how to obtain a Return Material Authorization number (RMA #). You should do this prior to returning the product.

Limited Warranty

Honeywell International Inc. ("HII") warrants its products to be free from defects in materials and workmanship and to conform to HII's published specifications applicable to the products purchased at the time of shipment. This warranty does not cover any HII product which is (i) improperly installed or used; (ii) damaged by accident or negligence, including failure to follow the proper maintenance, service, and cleaning schedule; or (iii) damaged as a result of (A) modification or alteration by the purchaser or other party, (B) excessive voltage or current supplied to or drawn from the interface connections, (C) static electricity or electro-static discharge, (D) operation under conditions beyond the specified operating parameters, or (E) repair or service of the product by anyone other than HII or its authorized representatives.

This warranty shall extend from the time of shipment for the duration published by HII for the product at the time of purchase ("Warranty Period"). Any defective product must be returned (at purchaser's expense) during the Warranty Period to HII factory or authorized service center for inspection. No product will be accepted by HII without a Return Materials Authorization, which may be obtained by contacting HII. In the event that the product is returned to HII or its authorized service center within the Warranty Period and HII determines to its satisfaction that the product is defective due to defects in materials or workmanship, HII, at its sole option, will either repair or replace the product without charge, except for return shipping to HII.

EXCEPT AS MAY BE OTHERWISE PROVIDED BY APPLICABLE LAW, THE FOREGOING WARRANTY IS IN LIEU OF ALL OTHER COVENANTS OR WARRANTIES, EITHER EXPRESSED OR IMPLIED, ORAL OR WRITTEN, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT.

HII'S RESPONSIBILITY AND PURCHASER'S EXCLUSIVE REMEDY UNDER THIS WARRANTY IS LIMITED TO THE REPAIR OR REPLACEMENT OF THE DEFECTIVE PRODUCT WITH NEW OR REFURBISHED PARTS. IN NO EVENT

SHALL HII BE LIABLE FOR INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, AND, IN NO EVENT, SHALL ANY LIABILITY OF HII ARISING IN CONNECTION WITH ANY PRODUCT SOLD HEREUNDER (WHETHER SUCH LIABILITY ARISES FROM A CLAIM BASED ON CONTRACT, WARRANTY, TORT, OR OTHERWISE) EXCEED THE ACTUAL AMOUNT PAID TO HII FOR THE PRODUCT. THESE LIMITATIONS ON LIABILITY SHALL REMAIN IN FULL FORCE AND EFFECT EVEN WHEN HII MAY HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH INJURIES, LOSSES, OR DAMAGES. SOME STATES, PROVINCES, OR COUNTRIES DO NOT ALLOW THE EXCLUSION OR LIMITATIONS OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

All provisions of this Limited Warranty are separate and severable, which means that if any provision is held invalid and unenforceable, such determination shall not affect the validity of enforceability of the other provisions hereof. Use of any peripherals not provided by the manufacturer may result in damage not covered by this warranty. This includes but is not limited to: cables, power supplies, cradles, and docking stations. HII extends these warranties only to the first end-users of the products. These warranties are non-transferable.

The duration of the limited warranty for the Thor VM2 is 1 year.

The duration of the limited warranty for the Thor VM2 Quick Mount Smart Dock is 1 year.

The duration of the limited warranty for the Thor VM2 Vehicle Mount Assembly is 1 year.

The duration of the limited warranty for the Thor VM2 internal UPS battery is 1 year.

The duration of the limited warranty for the Thor VM2 AC power supply and cables is 1 year.

The duration of the limited warranty for the Thor VM2 DC-DC Converter is 1 year.

The duration of the limited warranty for the Thor VM2 cables (USB, Serial, Communication, Power) is 1 year.

Honeywell Scanning & Mobility
9680 Old Bailes Road
Fort Mill, SC 29707
www.honeywellaidc.com