

Thor™ VM1

Vehicle-Mounted Computer

Microsoft® Windows® Embedded CE 6 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.

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

© 2011-2012 Honeywell International Inc. All rights reserved.

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.

Wavelink®, the Wavelink logo and tagline, Wavelink Studio™, Avalanche Management Console™, Mobile Manager™, and Mobile Manager Enterprise™ are trademarks of Wavelink Corporation, Kirkland.

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

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

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

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

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

Acrobat® Reader © 2012 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	1-1
About this Guide	1-1
End User License Agreement (EULA)	1-2
Components	1-3
Front View	1-3
Back View with Quick Mount Smart Dock	1-4
Access Panels	1-4
Chapter 2: Hardware	2-1
System Hardware	2-1
802.11a/b/g Wireless Client	2-1
Central Processing Unit	2-1
Input/Output Components	2-2
System Memory	2-2
Video Subsystem	2-2
Audio Interface	2-2
Card Slots	2-2
CompactFlash (CF) Slot	2-2
Secure Digital (SD) Slot	2-2
Bluetooth LXEZ Pair	2-3
WWAN	2-3
GPS	2-3
Power	2-4
Vehicle DC Power Supply	2-4
External AC Power Supply	2-4
Uninterruptible Power Supply	2-4
Backup Battery	2-5
Fuse	2-5
Power Management Modes	2-6
On Mode (D0)	2-6
User Idle / Backlight Off Mode (D1)	2-6
System Idle / Display Off Mode (D2)	2-6
Suspend mode (D3)	2-6
Shutdown / Off Mode (D4)	2-6
Primary Events	2-7
User Primary Events	2-7
System Primary Events	2-7
Wake Source Events	2-7

Power Controls.....	2-9
Power Switch.....	2-9
Thor VM1 Power Button.....	2-9
Vehicle Ignition Monitoring.....	2-10
Auto On Behavior.....	2-10
Auto-On Enabled.....	2-10
Auto-On Disabled.....	2-10
External Connectors.....	2-11
Serial Connector (COM1 and COM2).....	2-12
Pinout.....	2-12
Screen Blanking.....	2-13
Serial Cable.....	2-13
Screen Blanking Box.....	2-14
Screen Blanking with Switch.....	2-14
USB Connector.....	2-15
USB Dongle Cable.....	2-16
D9 Male Connector.....	2-16
USB Host Connector.....	2-17
USB Client Connector.....	2-17
Power Supply Connector.....	2-18
CANbus / Audio Connector.....	2-19
Headset Adapter Cable.....	2-20
D15 Female Connector.....	2-20
Quick Connect Headset Connector.....	2-21
CANbus Cable.....	2-22
D15 Female Connector.....	2-22
9-Pin J1939 (Deutsch) Connectors.....	2-23
Antenna Connections.....	2-24
Antenna Connector.....	2-24
Internal WiFi Antenna.....	2-24
Vehicle Remote Antenna.....	2-24
Keyboard Options.....	2-25
64-Key QWERTY Keyboard.....	2-25
IBM 3270 Overlay.....	2-26
IBM 5250 Overlay.....	2-27
12-Key Keyboard.....	2-28
Keyboard LEDs.....	2-29
Shift LEDs.....	2-29
Secondary Keys LED.....	2-29
Ctrl and Alt Key LEDs.....	2-29

USB Keyboard / Mouse	2-29
LED Functions	2-30
System LEDs	2-31
SYS (System Status) LED	2-31
UPS Status LED	2-32
External Power Present	2-32
External Power Not Present	2-32
SSD (Solid State Drive) LED	2-32
Connection LEDs	2-33
WWAN LED	2-33
WiFi LED	2-33
Bluetooth LED	2-33
Keyboard LEDs	2-34
2nd LED	2-34
Shift LEDs	2-34
Ctrl LED	2-34
Alt LED	2-35
Display	2-36
Touch Screen	2-36
Touch Screen Defroster	2-36
Screen Blanking	2-36
Display Backlight Control	2-36
Disconnect UPS Battery	2-37
Install SD Card	2-39
Install SIM Card	2-41
Field Replaceable Front Panel	2-43
Replace Front Panel	2-43
Field Replaceable UPS Battery	2-45
Replace UPS Battery	2-45
Chapter 3: Software	3-1
Introduction	3-1
Operating System	3-1
Windows CE Operating System	3-1
General Windows CE Keyboard Shortcuts	3-2
Rebooting the Thor VM1	3-3
Warmboot	3-3
Restart	3-3
Clearing Persistent Storage / Reset to Default Settings	3-3
Folders Copied at Startup	3-3

Saving Changes to the Registry.....	3-4
Software Load.....	3-5
Software Applications.....	3-5
ActiveSync.....	3-5
Bluetooth.....	3-5
LXE RFTerm (Optional).....	3-6
Avalanche.....	3-6
Software Development.....	3-6
Thor VM1 Utilities.....	3-6
LAUNCH.EXE.....	3-6
LAUNCH.EXE and Persistent Storage.....	3-7
REGEDIT.EXE.....	3-8
REGLOAD.EXE.....	3-8
REGDUMP.EXE.....	3-8
WARMBOOT.EXE.....	3-8
WAVPLAY.EXE.....	3-8
Thor VM1 Command-line Utilities.....	3-8
PrtScn.EXE.....	3-8
Desktop.....	3-9
Desktop Icons.....	3-9
Taskbar.....	3-10
My Device Folders.....	3-10
Wavelink Avalanche Enabler (Optional).....	3-11
Internet Explorer.....	3-11
Start Menu Program Options.....	3-12
Communication.....	3-12
ActiveSync.....	3-12
Connect and LXEConnect.....	3-13
Start FTP Server / Stop FTP Server.....	3-13
Summit.....	3-13
Certs.....	3-13
Command Prompt.....	3-14
eXpress Scan.....	3-14
Internet Explorer.....	3-14
Media Player.....	3-14
File Viewers.....	3-15
Microsoft WordPad.....	3-15
Remote Desktop Connection.....	3-15
Settings.....	3-15
Transcriber.....	3-15

Windows Explorer.....	3-16
Taskbar.....	3-17
General Tab.....	3-17
Advanced Tab.....	3-17
Expand Control Panel.....	3-17
Clear Contents of Document Folder.....	3-18
Taskbar Icons.....	3-18
Thor VM1 OS Upgrade.....	3-19
Introduction.....	3-19
Preparation.....	3-19
Procedure.....	3-19
BIOS.....	3-20
Accessing the BIOS Setup.....	3-20
Boot Order.....	3-20
Exiting BIOS Setup.....	3-20
Control Panel.....	3-21
About.....	3-23
Version Tab and the Registry.....	3-23
Languages.....	3-23
Identifying Software Versions.....	3-24
MAC Address.....	3-24
Accessibility.....	3-25
Administration (for AppLock).....	3-26
Factory Default Settings - AppLock.....	3-27
Setup a New Device.....	3-28
Administration Mode.....	3-28
End User Mode.....	3-29
Passwords.....	3-29
End-User Switching Technique.....	3-30
Using a Stylus Tap.....	3-30
Using the Switch Key Sequence.....	3-30
Hotkey (Activation hotkey).....	3-31
Application Configuration.....	3-32
Application Panel.....	3-33
Launch Button.....	3-35
Auto At Boot.....	3-36
Auto Re-Launch.....	3-37
Manual (Launch).....	3-38
Allow Close.....	3-38
End User Internet Explorer (EUIE).....	3-39

Security Panel.....	3-40
Options Panel.....	3-41
Status Panel.....	3-42
View.....	3-42
Log.....	3-43
Save As.....	3-43
AppLock Help.....	3-44
AppLock Error Messages.....	3-44
Battery.....	3-52
Bluetooth.....	3-53
Bluetooth Devices.....	3-54
Discover.....	3-55
Stop Button.....	3-55
Bluetooth Device List.....	3-56
Clear Button.....	3-56
Bluetooth Device Menu.....	3-57
Right-Click Menu Options.....	3-57
Bluetooth Device Properties.....	3-58
Settings.....	3-59
Turn Off Bluetooth.....	3-59
Options.....	3-60
Reconnect.....	3-61
Options.....	3-62
About.....	3-64
Using Bluetooth.....	3-65
Initial Configuration.....	3-65
Subsequent Use.....	3-66
Bluetooth Indicators.....	3-67
Bluetooth Bar Code Reader Setup.....	3-68
Thor VM1 with Label.....	3-68
Thor VM1 without Label.....	3-69
Bluetooth Beep and LED Indications.....	3-70
Bluetooth Printer Setup.....	3-70
Easy Pairing and Auto-Reconnect.....	3-71
Certificates.....	3-72
Data Collection Wedge Introduction.....	3-73
Bar Code Readers.....	3-74
Return to Factory Default Settings.....	3-74
Data Processing Overview.....	3-75
Factory Default Settings.....	3-76

Main Tab.....	3-77
COM1 Tab.....	3-78
Power on Pin 9.....	3-78
COM2 Tab.....	3-79
Power on Pin 9.....	3-79
Data Options Tab.....	3-80
Enable Code ID.....	3-80
Buttons.....	3-81
Data Options - Symbology Settings.....	3-82
Clear Button.....	3-83
Enable, Min, Max.....	3-84
Strip Leading/Trailing Control.....	3-85
Bar Code Data Match List.....	3-86
Bar Code Data Match Edit Buttons.....	3-86
Match List Rules.....	3-87
Add Prefix/Suffix Control.....	3-88
Symbologies.....	3-88
Ctrl Char Mapping.....	3-89
Translate All.....	3-89
Parameters.....	3-89
Translate All.....	3-89
Character.....	3-90
Replacement.....	3-90
List Box.....	3-90
Assign Button.....	3-90
Delete Button.....	3-90
Custom Identifiers.....	3-91
Parameters.....	3-91
Buttons.....	3-92
Control Code Replacement Examples.....	3-93
Bar Code Processing Examples.....	3-94
Processing Tab.....	3-95
About Tab.....	3-96
Length Based Bar Code Stripping.....	3-97
Hat Encoding.....	3-99
Date / Time.....	3-101
Dialing.....	3-102
Display.....	3-103
Background.....	3-103
Appearance.....	3-104

Backlight.....	3-104
Gobi Connection Manager.....	3-105
Initial Use.....	3-105
SIM Card Installation.....	3-105
Activate.....	3-106
Home.....	3-107
CDMA.....	3-108
Activation Type.....	3-108
Autoconnect.....	3-109
Data Connection Test.....	3-109
UTMS.....	3-110
Autoconnect.....	3-110
Data Connection Test.....	3-110
GPS.....	3-110
About.....	3-112
Input Panel.....	3-113
Transcriber.....	3-113
Internet Options.....	3-114
Keyboard.....	3-117
KeyPad.....	3-118
KeyMap Tab.....	3-119
Remap a Single Key.....	3-119
Remap a Key to a Unicode Value.....	3-119
Remap a Key Sequence.....	3-120
Remap a Key to a Sequence of Unicode Values.....	3-120
Remap an Application.....	3-120
Remap a Command.....	3-121
LaunchApp Tab.....	3-122
RunCmd Tab.....	3-123
License Viewer.....	3-124
Mixer.....	3-125
Output Panel.....	3-125
Input Panel.....	3-126
Mouse.....	3-127
Network and Dialup Options.....	3-128
Create a New Connection.....	3-128
Network Capture.....	3-129
Netlog.....	3-129
NDISLog.....	3-131
Options.....	3-132

Communication	3-133
Enable TCP/IP Version 6	3-133
Allow Remote Desktop Autologon	3-133
Autolaunch TimeSync	3-133
Misc	3-134
CapsLock	3-134
Touch Screen Disable	3-134
Enable Keypad Backlight	3-134
Enable Auto-On	3-134
Status Popup	3-135
Owner	3-136
Password	3-138
PC Connection	3-139
Peripherals	3-140
Power	3-141
Regional and Language Settings	3-143
Registry	3-145
Remove Programs	3-146
Screen Control	3-147
Screen Blanking	3-149
Current Level	3-149
Automatic Brightness Control	3-149
Stylus	3-150
Double-Tap	3-150
Calibration	3-150
System	3-151
General Tab	3-151
Memory Tab	3-152
Device Name Tab	3-152
Copyrights Tab	3-153
Terminal Server Client Licenses	3-154
Volume and Sounds	3-155
Good Scan and Bad Scan Sounds	3-156
WiFi Control Panel	3-157
Chapter 4: ActiveSync	4-1
Introduction	4-1
Initial Setup	4-2
Connect via USB	4-2
Cable for USB ActiveSync Connection:	4-2

Explore	4-3
Backup Data Files using ActiveSync	4-3
Prerequisites	4-3
Connect	4-3
Disconnect	4-4
Thor VM1 with a Disabled Touch Screen	4-4
Reset and Loss of Host Re-connection	4-4
Troubleshooting ActiveSync	4-5
Configuring the Thor VM1 with LXEConnect	4-6
Install LXEConnect	4-6
Using LXEConnect	4-7
Chapter 5: Enabler Installation and Configuration	5-1
Introduction	5-1
Installation	5-1
Installing the Enabler on Mobile Devices	5-1
Enabler Uninstall Process	5-2
Stop the Enabler Service	5-2
Update Monitoring Overview	5-3
Mobile Device Wireless and Network Settings	5-4
Preparing a Device for Remote Management	5-5
Using Wavelink Avalanche to Upgrade System Baseline	5-6
Part 1 – Bootstrapping the RMU	5-6
Part 2 – Installing Packages	5-6
Version Information on Mobile Devices	5-6
User Interface	5-7
Enabler Configuration	5-7
File Menu Options	5-8
Avalanche Update using File > Settings	5-9
Menu Options	5-9
Connection	5-10
Server Contact	5-11
Data	5-12
Preferences	5-13
Display	5-15
Taskbar	5-16
Execution	5-17
Scan Config	5-18
Shortcuts	5-19
SaaS	5-20

Adapters.....	5-21
Status.....	5-24
Exit.....	5-25
Using Remote Management.....	5-25
Using eXpress Scan.....	5-26
Step 1: Create Bar Codes.....	5-26
Step 2: Scan Bar Codes.....	5-26
Step 3: Process Completion.....	5-28
Chapter 6: Wireless Network Connections.....	6-1
Summit Wireless Network Configuration.....	6-1
Important Notes.....	6-1
Summit Client Utility.....	6-2
Help.....	6-2
Summit Tray Icon.....	6-2
Wireless Zero Config Utility and the Summit Radio.....	6-3
How To: Use the Wireless Zero Config Utility.....	6-3
How to: Switch Control to SCU.....	6-3
Main Tab.....	6-4
Auto Profile.....	6-5
Admin Login.....	6-5
Profile Tab.....	6-7
Buttons.....	6-8
Profile Parameters.....	6-9
Status Tab.....	6-11
Diags Tab.....	6-12
Global Tab.....	6-13
Custom Parameter Option.....	6-14
Global Parameters.....	6-15
Sign-On vs. Stored Credentials.....	6-19
How to: Use Stored Credentials.....	6-19
How to: Use Sign On Screen.....	6-19
Windows Certificate Store vs. Certs Path.....	6-21
User Certificates.....	6-21
Root CA Certificates.....	6-21
How To: Use the Certs Path.....	6-21
How To: Use Windows Certificate Store.....	6-21
Configuring the Profile.....	6-23
No Security.....	6-24
WEP.....	6-25

LEAP.....	6-26
PEAP/MSCHAP.....	6-27
PEAP/GTC.....	6-29
WPA/LEAP.....	6-31
EAP-FAST.....	6-33
EAP-TLS.....	6-35
WPA PSK.....	6-37
Certificates.....	6-38
Generating a Root CA Certificate.....	6-39
Installing a Root CA Certificate.....	6-42
Generating a User Certificate.....	6-44
Installing a User Certificate.....	6-50
Verify Installation.....	6-52
Chapter 7: Technical Specifications	7-1
Thor VM1.....	7-1
Quick Mount Smart Dock.....	7-2
Dimensions.....	7-2
Thor VM1.....	7-2
Quick Mount Smart Dock.....	7-2
Environmental Specifications.....	7-3
Thor VM1 and Quick Mount Smart Dock.....	7-3
Network Card Specifications.....	7-4
Summit 802.11a/b/g.....	7-4
Bluetooth.....	7-4
Chapter 8: Key Maps	8-1
64-Key QWERTY Keypad Key Map.....	8-1
12-Key Keypad Key Map.....	8-6
IBM Terminal Emulation.....	8-8
IBM 3270.....	8-8
IBM 5250.....	8-9
Chapter 9: Technical Assistance	9-1

Chapter 1: Introduction

The Thor VM1 Vehicle Mount Computer (VMC) is a rugged, vehicle mounted computer running a Microsoft® Windows® CE 6 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.

<p>Caution</p> 	<p>Before shipping the Thor VM1, the internal UPS battery must be disconnected.</p>
--	---

The Thor VM1 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 VM1. Peripheral connections are on the dock. The Thor VM1 is designed to easily be removed from the dock with a latch on the lower rear of the Thor VM1 housing. Since the dock remains attached to the vehicle, the Thor VM1 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 VM1 contains a UPS battery which, when fully charged, can power the Thor VM1 for a minimum of 30 minutes. This can be when the Thor VM1 is not attached to a Quick Mount Smart Dock or when the Thor VM1 is attached to a dock but the vehicle power is interrupted, such as when the vehicle battery is being changed.

Contact [Technical Assistance](#) for information on the latest upgrades for your Thor VM1.



About this Guide

This Thor VM1 Reference Guide provides instruction for the system administrator to follow when configuring a Thor VM1. This reference guide has been developed for a Thor VM1 with a Microsoft® Windows® Embedded CE 6 operating system.

End User License Agreement (EULA)

When a new Thor VM1 starts up a EULA is displayed on the touch screen. It remains on the screen until the Accept or Decline button is tapped with a stylus.

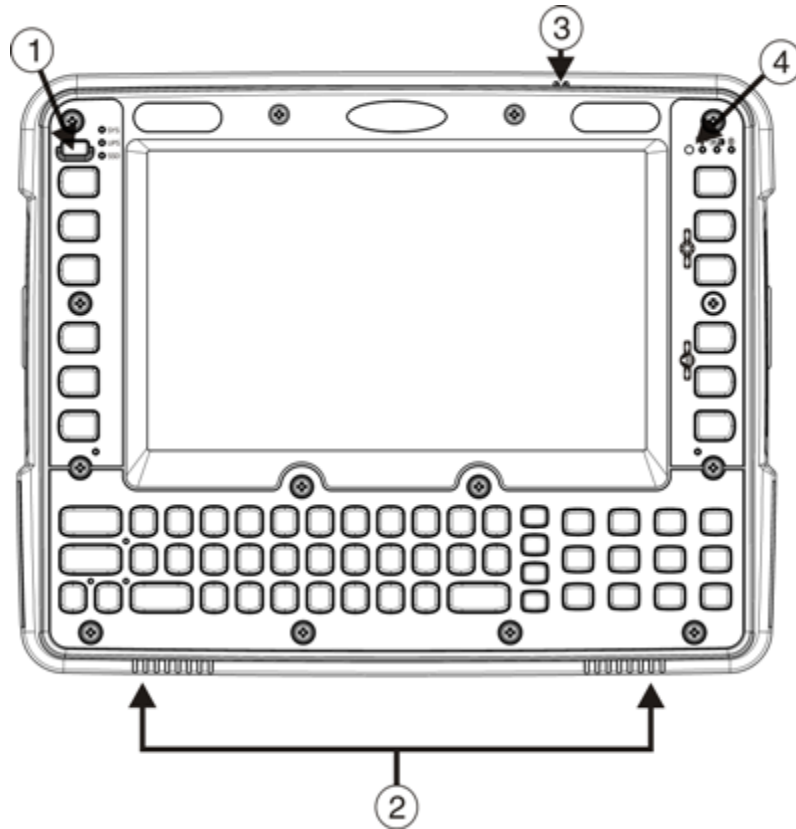
Tap the Accept button to accept the EULA terms and the Thor VM1 continues the startup process. The EULA is not presented to the user again.

Tap the Decline button to decline the EULA and the Thor VM1 will reboot. It will continue to reboot until the Accept button is tapped with the stylus.

Note: The EULA will be presented after any operating system upgrade or re-installation, including language-specific operating systems.

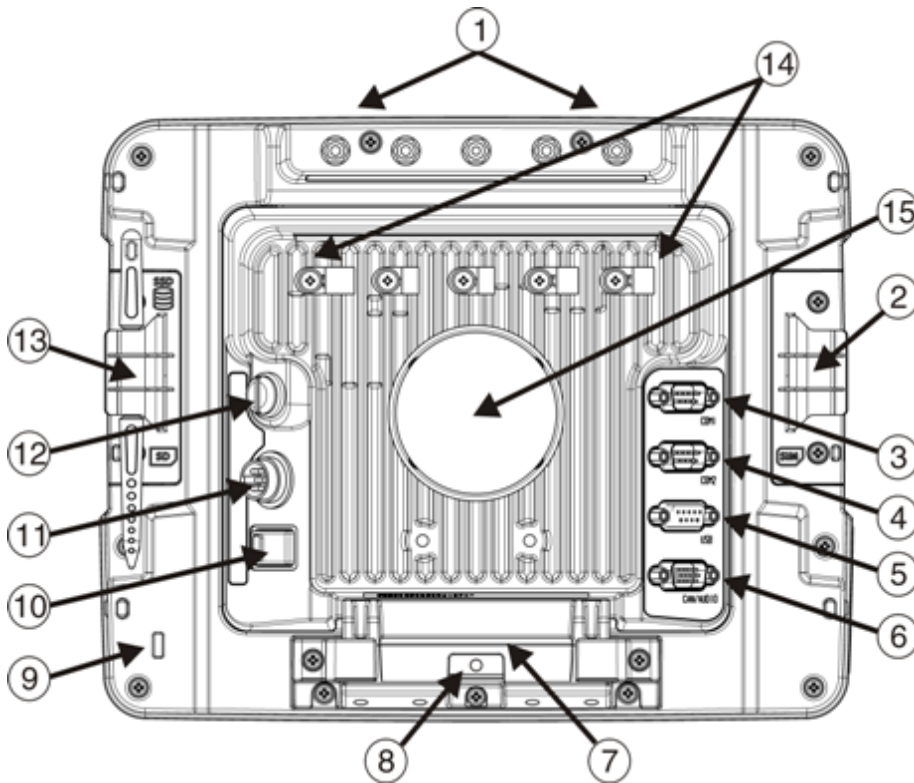
Components

Front View



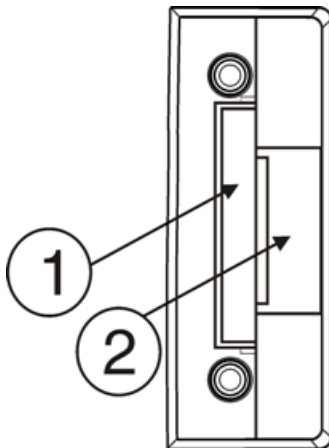
1. Power Button
2. Speakers
3. Microphone
4. Ambient Light Sensor

Back View with Quick Mount Smart Dock



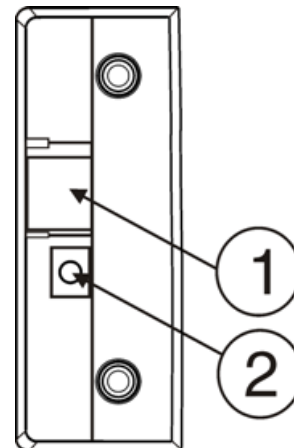
1. Antenna Connectors (on Thor VM1)
2. SIM card Access Panel (on Thor VM1)
3. COM1 Connector (on Dock)
4. COM2 Connector (on Dock)
5. USB Connector (on Dock)
6. CAN/Audio Connector (on Dock)
7. Quick Release Handle (On Thor VM1)
8. Provision for Padlock (on Thor VM1)
9. Provision for Laptop Security Cable (on Thor VM1)
10. Power Switch (on Dock)
11. Power Connector (on Dock)
12. Fuse (on Dock)
13. SD Card Access Panel (On Thor VM1)
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

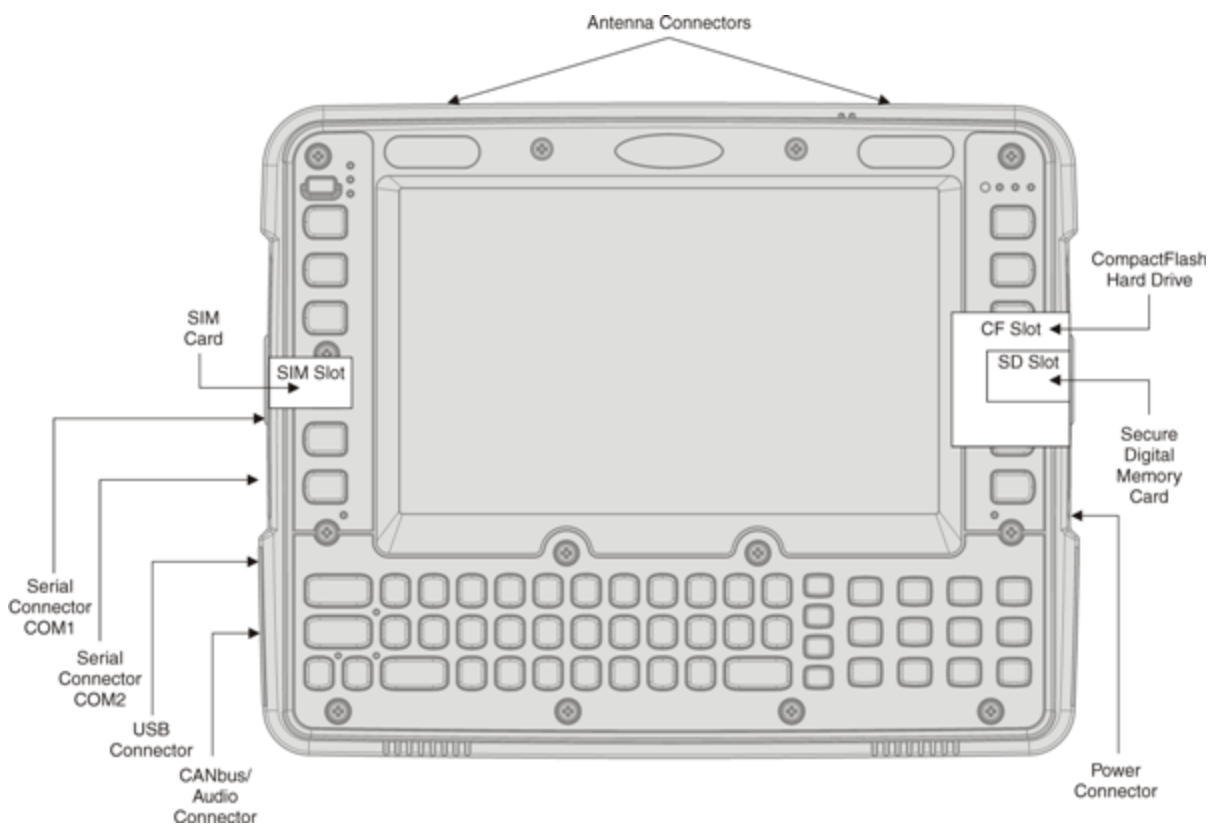


Access Panel Door is labeled with **SIM**.

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

Chapter 2: Hardware

System Hardware



802.11a/b/g Wireless Client

The Thor VM1 has an 802.11a/b/g 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 CE 6.0. The OS image is stored on an internal CompactFlash card and is loaded into DRAM for execution.

Input/Output Components

The Thor VM1 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.
- Ports available via dongle cable:
 - USB Host port
 - USB Client port
 - CANbus
 - Audio

System Memory

Main system memory is 1GB SDRAM.

Video Subsystem

The Thor VM1 video subsystem consists of a color TFT display. The video subsystem complies with the VESA VL bus standard. The resolution of this display is 800 x 480 pixels. This resolution complies with the WVGA 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 VM1. An 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 VM1 display, near the Thor VM1 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 VM1 must be powered down to insert or remove an ATA card. Since the operating system is stored on the CF ATA card, the Thor VM1 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 LXEZ Pair

The Thor VM1 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 VM1. However, the Thor VM1 supports authentication requests from pairing devices. If a pairing device requests authentication or encryption, the Thor VM1 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 is manipulated by the settings in the Thor VM1 Data Collection control panel applet.
- 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 VM1 during final bar code data manipulation.

WWAN

WWAN (Wireless Wide Area Networking) is available on the Thor VM1. A slot is provided for a SIM card.

GPS

GPS (Global Positioning System) is available on the Thor VM1.

Power

Vehicle DC Power Supply

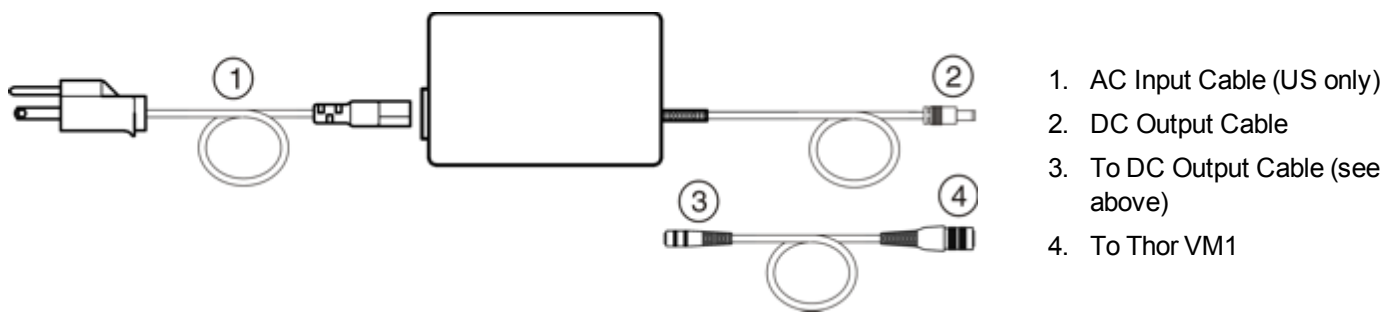
Vehicle power input for the Thor VM1 dock is 10V to 60V DC and is accepted without the need to perform any manual operation within the Thor VM1 dock. The dock provides a conditioned power output for the Thor VM1. By using a specified DC-to-DC adapter, input voltage of 72-144V DC nominal can be accepted.

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 VM1 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.



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 VM1 User Guide*.

Uninterruptible Power Supply

The Thor VM1 contains an internal UPS battery.

The UPS battery is automatically charged when the Thor VM1 is placed in a powered dock.

- A fully discharged UPS battery recharges in under 4 hours when the Thor VM1 is in a powered dock.
- Charging of the UPS battery continues during power management of the Thor VM1.
- 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 VM1 to a different location to charge the UPS battery.

When external power is removed, the UPS automatically powers the Thor VM1 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 VM1 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 VM1 for a minimum of 30 minutes at temperatures of -20°C (-4°F) or greater. For the extended temperature version of the Thor VM1, the UPS provides a minimum of 10 minutes of operation below -20°C (-4°F), up to -30°C (-22°F).

If operating on UPS power and the UPS battery becomes critically low, the Thor VM1 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 VM1 does not power on.

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

The UPS battery can be [replaced by the user](#).

Backup Battery

The Thor VM1 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 five years with normal use before it requires replacement.

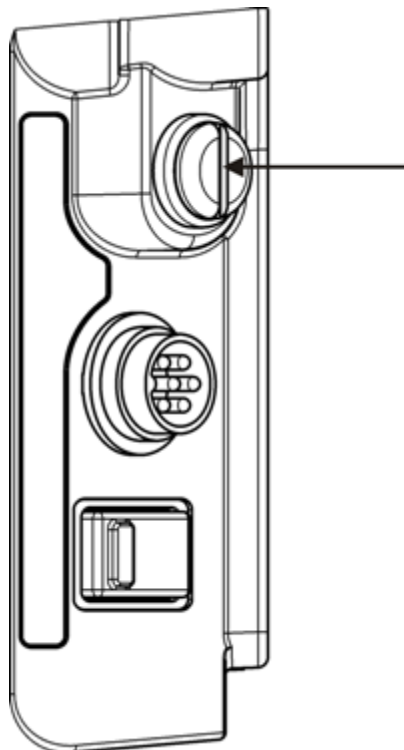
Note: The backup battery should only be changed by authorized service personnel.

Fuse

The Thor VM1 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 VM1 supports the standard Microsoft Windows CE power management modes: On (D0), Backlight Off (D1), Display Off (D2) and Suspend (D3).

On Mode (D0)

When the Thor VM1 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 VM1 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 backlight timer (if enabled) expires.

User Idle / Backlight Off Mode (D1)

Backlight is dimmed, but display is readable. The Thor VM1 transitions to this mode from On after the User Idle timeout period has passed without a primary event occurring.

System Idle / Display Off Mode (D2)

Backlight and display are off. The status LED is solid green. The Thor VM1 transitions to this mode from User Idle after the System Idle timeout period has passed without a primary event occurring.

Suspend mode (D3)

All devices that are not configured as wakeup events are powered off. The status LED is blinking green if external power is connected and off if external power is not connected. The Thor VM1 transitions to this mode from System Idle after the Suspend timeout period has passed without a primary event occurring.

Additionally the power button can be used to enter or exit Suspend mode:

- If the Thor VM1 is On, pressing the power button immediately transitions the unit to Suspend.
- If the Thor VM1 is in Suspend mode, pressing the power button transitions the unit to On.

Shutdown / Off Mode (D4)

The Thor VM1 shuts down when the Thor VM1 is operating on power and the UPS battery becomes critically low regardless of the current power management state. The Thor VM1 remains Off until external power is applied. The Thor VM1 may restart automatically when external power is applied or may require the user to press the Power button depending on installation and configuration.

A Real Time Clock (RTC) powered by an internal battery maintains the date and time while the Thor VM1 is off.

Primary Events

The Primary Events described below are the default behavior. Primary events can be modified using the LXEPowerMgrPrimaryEvents API.

Please refer to the *CE API Programming Guide* for API details.

User Primary Events

A User Primary Event transitions the Thor VM1 to D0 (On) mode. When no user event happens for the specified time period, the Thor VM1 transitions to D1 (User Idle), then D2 (System Idle) and then D3 (Suspend). Timeout periods are set via the Schemes tab in the Power control panel.

User primary events include:

- Any key press on the keypad
- Touch on the touch screen
- USB data entry (from a USB keyboard or mouse)

System Primary Events

A System Primary Event allows the Thor VM1 to transition to D2 (System Idle) but the Thor VM1 does not enter D3 (Suspend) as long the system event occurs.

System primary events include:

- Serial data transfer
- USB data transfer

Wake Source Events

These events wake the Thor VM1 from suspend:

- Power button
- Touch on the touch screen
- Any keypress on the keyboard
- USB connect / disconnect
- Truck power on or off (i.e. ignition key)
- RTC
- Bluetooth connection
- External power connection
- Serial port CTS control line
- Headset connection (this is not enabled by default, but can be configured to wake the Thor VM1)

Events generated by these actions are not processed. For example, the key press or touch screen tap that wakes the Thor VM1 is ignored.

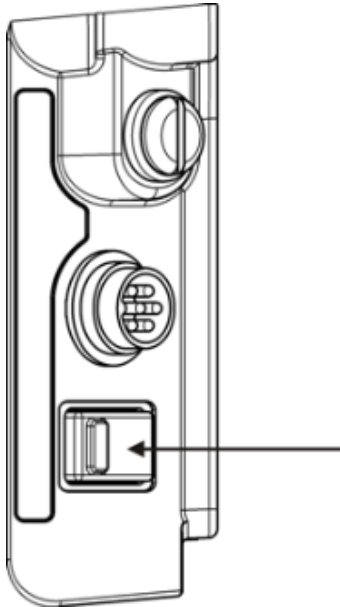
The following events DO NOT wake the Thor VM1 from suspend:

- Bluetooth keyboard or mouse
- USB host data (unless enabled via API)
- USB host connection

-
- SDIO interrupt
 - Serial data
 - 802.11 radio
 - External power disconnect

Power Controls

Power Switch

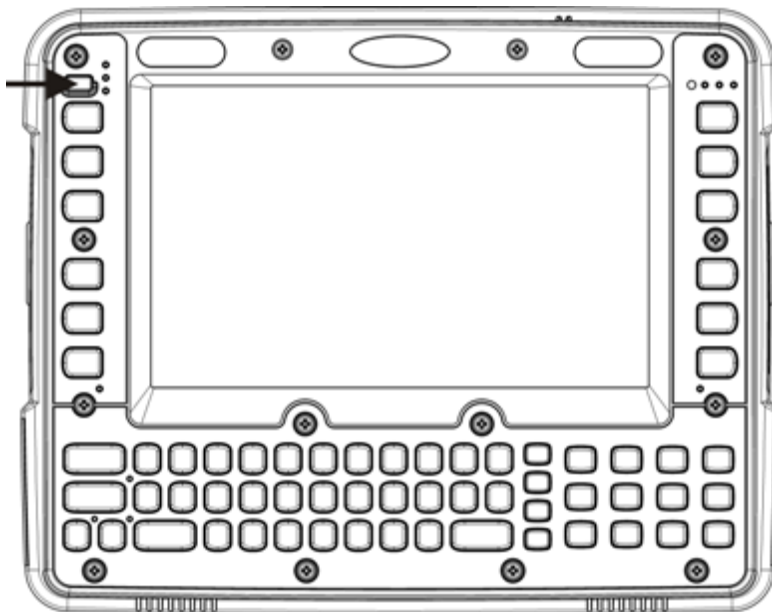


After all cables are connected, the Thor VM1 can be powered on.

There is a power switch located on the back of the Quick Mount Smart Dock. The power switch is a rocker switch.

The power switch has a raised bump to identify the switch position even when it is hidden from view. When the side of the switch with the raised bump is pressed, the power switch is On. If the Dock is connected to external power, the Dock delivers power to the Thor VM1.

Thor VM1 Power Button



The [power button](#) is located at the bottom left of the Thor VM1.

If the Thor VM1 is Off, pressing the power button starts the power up sequence.

Note: This assumes that the Thor VM1 is docked in a powered Quick Mount Smart Dock or that the internal UPS battery has a sufficient charge to power the Thor VM1. If no external power is available and the UPS battery does not have a charge, pressing the power button causes no action.

If the Thor VM1 is On, pressing the power button places the unit in Suspend.

Vehicle Ignition Monitoring

When Auto-On is disabled (see below) and the ignition input wire is connected, the Thor VM1 monitors the ignition input signal and adjusts modes as described below.

Auto On Behavior

The Thor VM1 can be configured for Auto-On using the [Options](#) control panel.

For information on the Ignition input signal please see the power cable instructions in the *Thor VM1 Vehicle Mounting Reference Guide*.

Auto-On Enabled

When Auto-On is enabled, the Ignition Input signal, if connected via the Thor VM1 vehicle power supply cable, is ignored.

When Auto-On is enabled, the Thor VM1 boots when external power is applied, such as when:

- The Thor VM1 is placed in a powered Smart Dock, with the dock's power switch set to On.
- The Thor VM1 is in a Smart Dock and truck power is applied to the dock
- The Thor VM1 is in a powered Smart Dock and the dock's power switch is turned from Off to On.

If the Thor VM1 is already on and one of the above events occurs, the Thor VM1 continues to run, however the power management scheme may change based on the connection to external power.

Auto-On Disabled

When Auto-On is disabled, the Ignition Input signal, if connected via the Thor VM1 vehicle power supply cable, is monitored.

When the Ignition Input wire is connected:

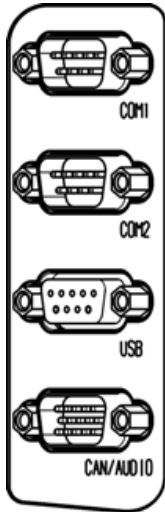
- If the Thor VM1 is **Off** and Ignition Input is **Inactive**, the Thor VM1 remains **Off**.
- If the Thor VM1 is **Off** and Ignition Input changes from **Inactive** to **Active**, the Thor VM1 **boots**.
- If the Thor VM1 is **On** and Ignition Input changes from **Inactive** to **Active**, the Thor VM1 remains **On**. If, for example, a Thor VM1 is running on the UPS and is placed into a Dock connected to a truck when the truck ignition is On, the power management scheme may change based on the availability of external power.
- If the Thor VM1 is **On** and Ignition Input changes from **Active** to **Inactive**, this event is treated the same as a **Power button press**, which places the Thor VM1 in Suspend.

If the Ignition Input wire is not connected, the Thor VM1 only powers on when the Power button is pressed.

External Connectors

Power the Thor VM1 off before attaching a cable to any port (serial, USB, Audio/CAN, etc.).

Most external connectors for the Thor VM1 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.
- [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 VM1.

Serial Connector (COM1 and COM2)

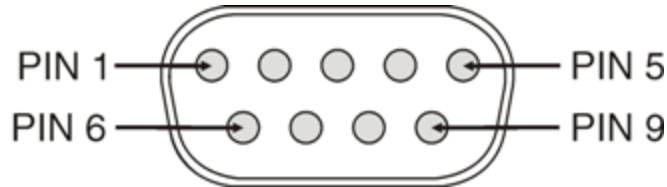
The COM1 and COM2 connectors are D-9 male connectors located on the back of the Quick Mount Smart Dock.

Power the Thor VM1 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.

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

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 or RI	Bar Code Scanner Power - 500mA max or Ring Indicator - Input
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:

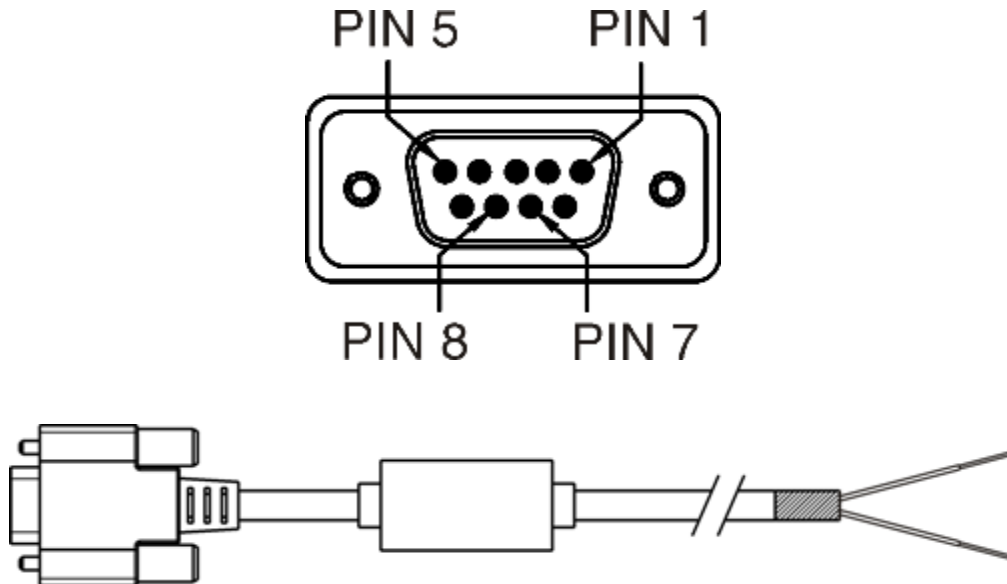
- An optional Screen Blanking Box Cable is available from Honeywell, or
- A user supplied serial cable can be used. The cable must provide wires from pins 7 and 8 of the connector. No other wires are used.



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 > Settings > Control Panel > Screen Control](#).

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 VM1) and the display on the Thor VM1 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 VM1 screen is displayed.

Please refer to the wiring instructions, including appropriate cautions and warnings, in the *Thor VM1 Vehicle Mounting Reference Guide*.

Screen Blanking with Switch

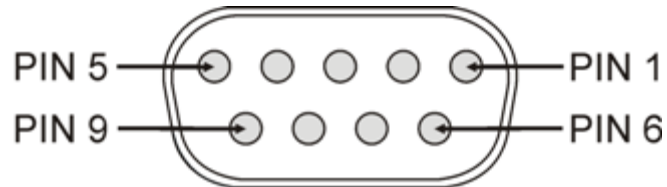
In applications where it is impractical to use the screen blanking box due to vehicle voltage or lack of a motion sensing signal, screen blanking can be controlled via a user supplied switch or relay that provides an electrical conductive connection between the wires connected to Pins 7 and 8 of the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

Please refer to the wiring instructions, including appropriate cautions and warnings, in the *Thor VM1 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.

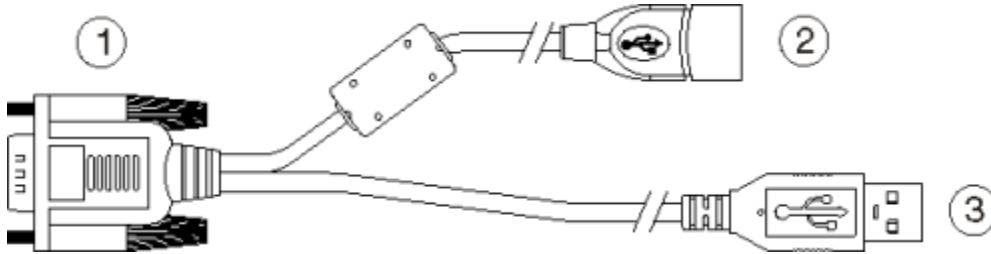
Power the Thor VM1 off before attaching a cable to any port (serial, USB, Audio/CAN, etc.).



Pin	Signal	Description
1	GND	Common ground
2	USBC_D+	USB client data signal
3	USBC_D-	USB client data signal
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

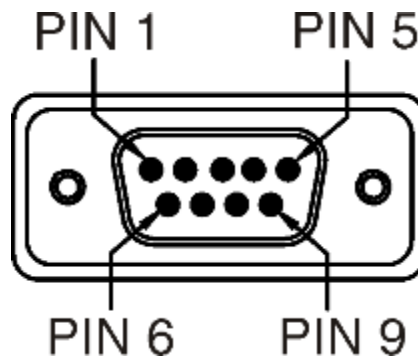
USB Dongle Cable

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



1. D9 Connector
2. USB Host Connector(s)
3. USB Client Connector

D9 Male Connector



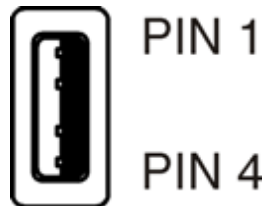
Pin	Signal	Description
1	GND	Common ground
2	USBC_D+	USB client data signal
3	USBC_D-	USB client data signal
4	USB_H1_PWR	USB host 5V output power
5	GND	Common ground
6	GND	Common ground
7	USB_H1_D+	USB host 1 data signal
8	USB_H1_D-	USB host 1 data signal
9	USBC_VBUS	USB client 5V detect from attached host

USB Host Connector



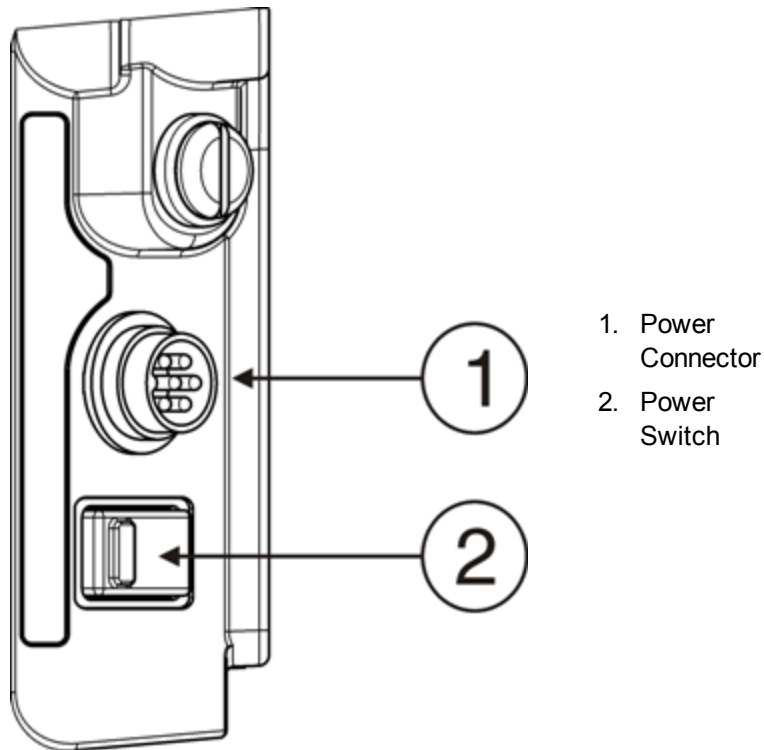
Pin	Signal	Description
1	5V_USB	USB Power, Current Limited
2	USB_H1_D-	USB D-
3	USB_H1_D+	USB D+
4	GND	USB Power Return
Shell	CGND	Chassis Ground

USB Client Connector



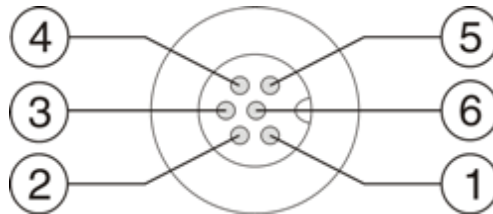
Pin	Signal	Description
1	5V_USB	USB Power, Current Limited
2	USB_H1_D-	USB D-
3	USB_H1_D+	USB D+
4	GND	USB Power Return
Shell	CGND	Chassis Ground

Power Supply Connector



Power is supplied to the Thor VM1 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 VM1 internal power supply can accept DC input voltages in the range of 10 to 60 Volts DC.

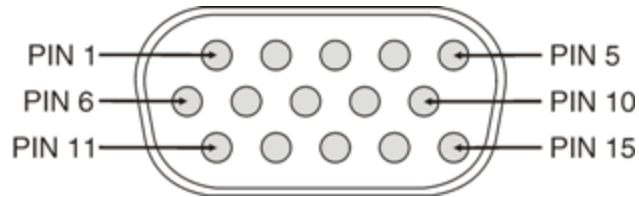


Pin	Signal	Description
1	V In+	10-60V DC input +
2	V In+	10-60V DC input +
3	V In-	input -
4	V In-	input -
5	GND	Chassis ground
6	Ignition	+0V to 60V to start terminal

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 VM1 does not support connecting audio and CANbus simultaneously.



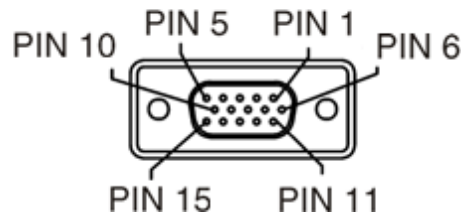
Pin	Signal Name	Description
1	-	CAN reserved
2	CAN_L	CAN_L bus line dominant low
3	CAN_GND	CAN Ground
4	-	CAN reserved
5	GND	Optional ground
6	Audio return	Headset return
7	Audio output	Headset output
8	Mic input	Microphone input
9	Mic return	Microphone return
10	Audio Return	
11	GND	Optional ground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

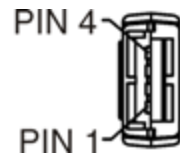


D15 Female Connector



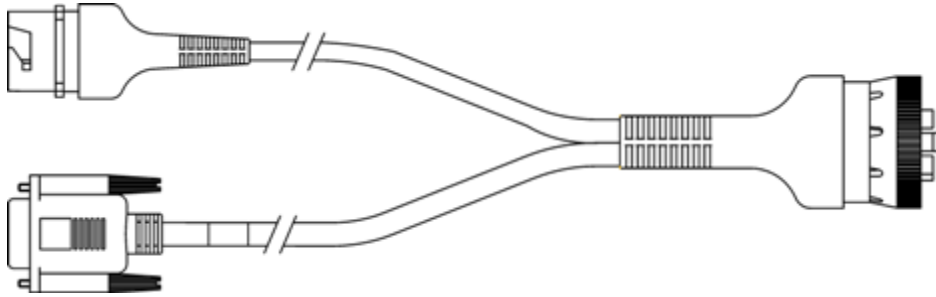
Pin	Signal	Description
1	-	Not used
2	-	Not used
3	-	Not used
4	-	Not used
5	-	Not used
6	Audio return	Headset return
7	Audio output	Headset output
8	Mic input	Microphone input
9	Mic return	Microphone return
10	-	Not used
11	-	Not used
12	-	Not used
13	-	Not used
14	-	Not used
15	-	Not used

Quick Connect Headset Connector



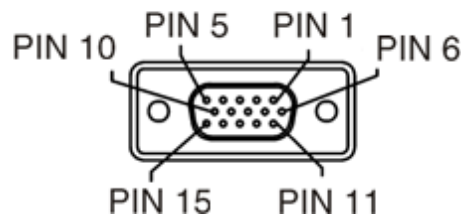
Pin	Signal	Description
1	Mic input	Microphone input
2	Mic return	Microphone return
3	Audio output	Headset output
4	Audio return	Headset return

CANbus Cable



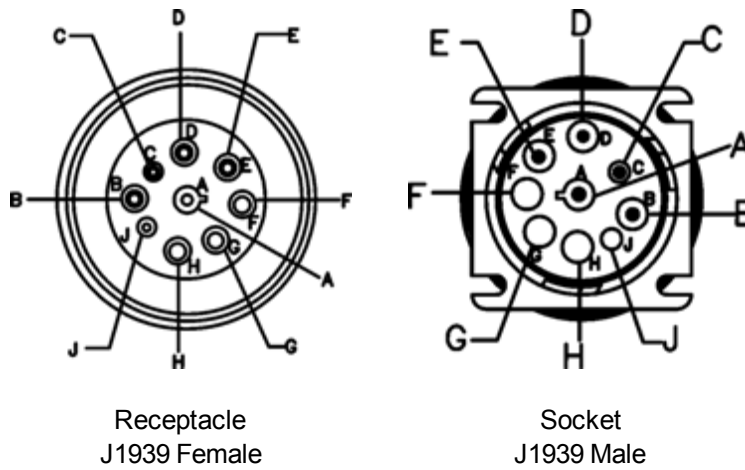
The CANbus interface is a virtual COM9 port. This port can be accessed using standard Windows API calls.

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

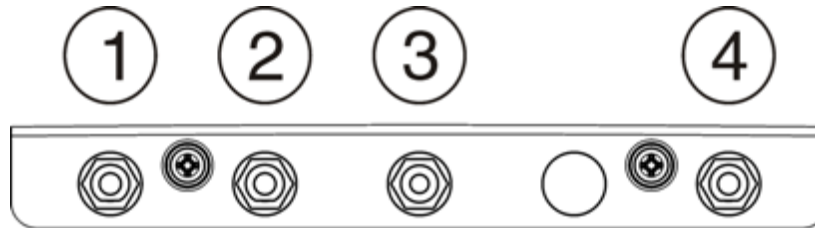
9-Pin J1939 (Deutsch) Connectors



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 VM1 is equipped with an 802.11 radio and can be ordered with internal antennas or external remote mount antennas. When the Thor VM1 is ordered with internal antennas, the external antenna connectors are not used. GPS and WWAN are optional on the Thor VM1 and require external remote mount antennas.



1. WI-FI (MAIN) (Red label) 802.11 Main External Antenna Connector
2. WI-FI (AUX) (Yellow label) 802.11 Auxiliary External Antenna Connector
3. GPS (Green label) GPS Antenna Connector
4. MOBILE NET (Blue label) WWAN Antenna Connector

Antenna Connector

When the Thor VM1 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 VM1. The internal antenna is not user accessible.

Vehicle Remote Antenna

The external antennas can be remotely mounted on the vehicle. See the *Thor VM1 Vehicle Mounting Reference Guide* for instruction. External antenna kits are available for the 802.11 WiFi radio, GPS and WWAN.

Keyboard Options

The 2nd, ALT, CTRL and Shift keys (when present) are sticky keys. The [keyboard LED behavior](#) identifies the active sticky modifier mode state of the keyboard.

64-Key QWERTY Keyboard



The Thor VM1 has a QWERTY keyboard, available with a standard overlay, an IBM 3270 overlay or an IBM 5250 overlay.

- Because the keyboard only has 64 keys, all functions are not visible (or printed on the keyboard). Therefore the Thor VM1 keyboard supports what is called hidden keys – keys that are accessible but not visible on the keyboard.
- A key or combination of 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 KeyPad option in the Control Panel ([Start > Settings > Control Panel > KeyPad](#)).
- Remapped keys persist across a warmboot or power cycle.
- The keyboard does not have a NumLock indicator or key. NumLock is always On.
- The warmboot behavior of CapsLock can be set via the Misc tab in [Start > Settings > Control Panel > Options](#).

The Thor VM1 keyboard keys are backlit.

- By default, the keyboard backlight follows the display backlight. When the display backlight is on, the keyboard backlight is on.
- If the display backlight brightness is increased (or decreased) the keyboard backlight brightness is increased (or decreased).

-
- The keyboard backlight and the display share the same timer, which is configured in [Start > Settings > Control Panel > Power](#).
 - The keyboard backlight can be disabled. See [Start > Settings > Control Panel > Options > Misc](#) tab.

IBM 3270 Overlay



IBM 5250 Overlay



12-Key Keyboard

The 12-key keyboard is available on the Thor VM1 running Windows CE 6.0.



- Because the keyboard only has 12 keys, all functions are not visible (or printed on the keyboard). Therefore the Thor VM1 keyboard supports what is called hidden keys -- keys that are accessible but not visible on the keyboard.
- A key or combination of 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 keyboard option in the Control Panel ([Start > Settings > Control Panel > KeyPad](#)).
- Remapped keys persist across a warmboot or power cycle.
- The keyboard does not have a NumLock indicator or key. NumLock is always On.
- The warmboot behavior of CapsLock can be set via the Misc tab in [Start > Settings > Control Panel > Options](#).

The Thor VM1 keyboard keys are backlit.

- By default, the keyboard backlight follows the display backlight. When the display backlight is on, the keyboard backlight is on.
- If the display backlight brightness is increased (or decreased) the keyboard backlight brightness is increased (or decreased).
- The keyboard backlight and the display share the same timer, which is configured in [Start > Settings > Control Panel > Power](#).
- The keyboard backlight can be disabled. See [Start > Settings > Control Panel > Options > Misc](#) tab.

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

Keyboard LEDs

Shift LEDs

Note: The 64-key Thor VM1 has two Shift keys with an LED beside each key. The 12-key Thor VM1 has a single Shift key and LED.

The Shift LEDs indicate the state of the keyboard Shift mode. If Shift is enabled the Shift LEDs beside both Shift keys (64-key only) blink green. When CapsLock is enabled, both Shift LEDs (64-key only) are lit solid green. When Shift and CapsLock are both off, the LEDs are off.

Press either Shift key to toggle Shift On and Off. press 2nd plus either Shift key to toggle CapsLock On or Off.

Secondary Keys LED

The Thor VM1 keyboard is equipped with several secondary keys. These keys are identified by the superscript text found on the keyboard keys.

The secondary keys are accessible by using two (2) keystrokes: the 2nd key followed by the superscript key.

Once the 2nd state is enabled (by pressing the 2nd key) the Secondary Mode LED is illuminated and the 2nd state is enabled until another key is pressed.

The 2nd key is toggled on with a 2nd key press and then immediately off with another 2nd key press.

For example:

Press 2nd and F1 to generate F11.

Ctrl and Alt Key LEDs

Note: Ctrl and Alt keys and the associated LEDs are not present on the 12-key version.

When the modifier keys (Ctrl or Alt) are active, the LED located next to the key is illuminated. The modifier key remains active until:

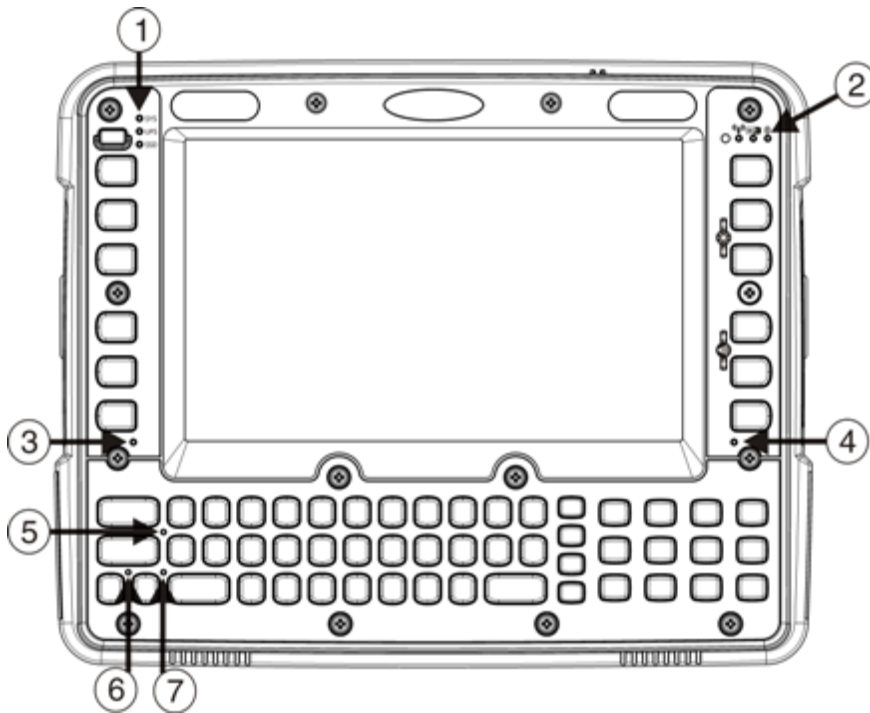
- The modifier key is pressed again, or
- A non-modifier key is pressed.

USB Keyboard / Mouse

A standard USB keyboard or mouse can be attached to the Thor VM1 using the appropriate dongle cable.

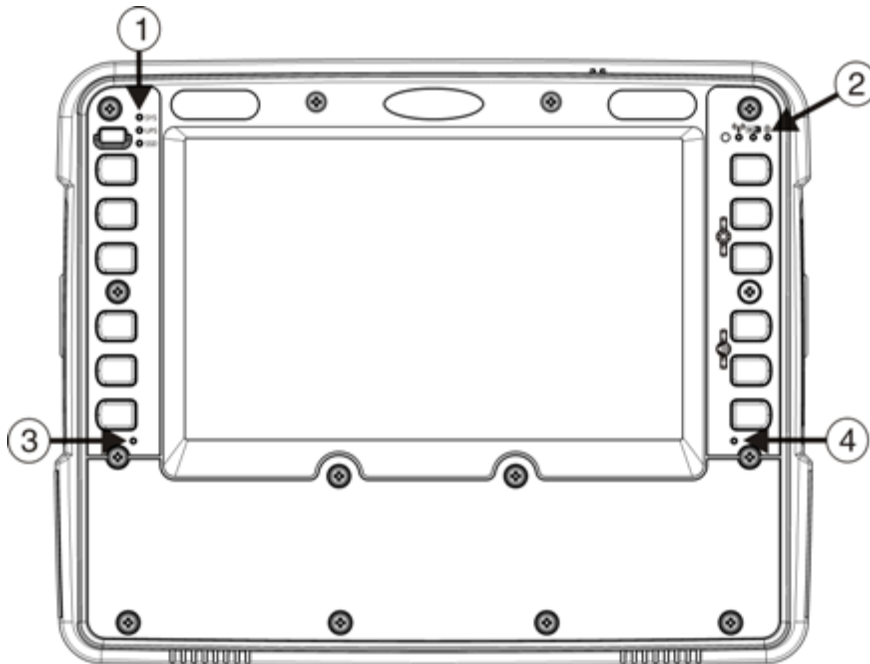
The dongle cable attaches to the Thor VM1 and provides a USB connector. Please refer to documentation provided with the USB keyboard or mouse for more information on their operation.

LED Functions

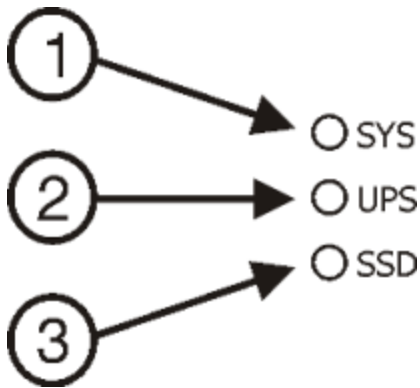


1. [System LEDs](#)
2. [Connection LEDs](#)
3. 2nd LED
4. Shift/CapsLock LED
5. Shift/CapsLock LED *
6. Ctrl LED *
7. Alt LED *

* 64-key keyboards only



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	<ul style="list-style-type: none">• On• On but Backlight Off• On but Display Off
Green blinking very slowly External power present (1/2 sec. on, 4 1/2 sec. off)	<ul style="list-style-type: none">• Suspend
Off External power not present	<ul style="list-style-type: none">• Off• Suspend
Green blinking slowly External power present (1/2 sec. on, 1 1/2 sec. off)	CPU temperature less than -20°C, Heater warming CPU for 30 seconds
Green blinking slowly External power not present (1/2 sec. on, 1 1/2 sec. off)	CPU temperature less than -20°C, Need to move unit to warmer environment

UPS Status LED

The behavior of the UPS LED depends if external power is connected or not.

External Power Present

LED Behavior	Status
Off	<ul style="list-style-type: none">• No UPS charging,• UPS charged
Solid Green	UPS charging
Solid Amber	<ul style="list-style-type: none">• Any charging fault,• Out of charging temperature range,• No UPS present,• Charge timeout

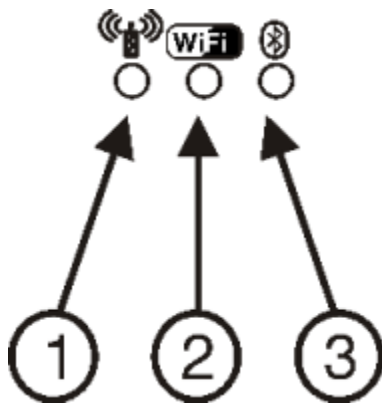
External Power Not Present

LED Behavior	Status
Off	<ul style="list-style-type: none">• Unit off,• UPS not present
Solid Amber	UPS supplying power and discharging
Solid Red	Approximately 2 minutes runtime until shutdown

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.

2nd LED

LED Behavior	Status
Solid Green	<ul style="list-style-type: none">Indicates the 2nd modifier key is active. 2nd mode is invoked for the next keypress only.Pressing the 2nd key a second time exits this modifier mode and turns off the LED.
Off	2nd mode is not invoked.

Shift LEDs

For the 64 key keyboard, there is one LED next to each **Shift** key. Both LEDs indicate the status of Shift mode and Caps Lock mode.

For the 12-key keyboard, there is a single **Shift** key and a single LED.

LED Behavior	Status
Blinking Green	<ul style="list-style-type: none">Indicates the keypad is in Shift mode. Shift mode is invoked for one keypress.Pressing the Shift key places the system in Shift mode.To exit Shift mode, press the Shift key again.
Solid Green	<ul style="list-style-type: none">When solid Green, indicates the keypad is in Caps Lock mode. Caps Lock mode is invoked until canceled.Pressing the 2nd key followed by the Shift key places the system in Caps Lock mode.To exit Caps Lock mode, press 2nd + Shift again.
Off	Neither Shift or Caps Lock mode is invoked.

Ctrl LED

The **Ctrl** key is not present on the 12-key keypad.

LED Behavior	Status
Solid Green	<ul style="list-style-type: none">Indicates the Ctrl modifier key is active. Ctrl mode is invoked for the next keypress only.Pressing the Ctrl key a second time exits this modifier mode and turns off the LED.
Off	Ctrl mode is not invoked.

Alt LED

The **Alt** key is not present on the 12-key keypad.

LED Behavior	Status
Solid Green	<ul style="list-style-type: none">• Indicates the Alt modifier key is active. Alt mode is invoked for the next keypress only.• Pressing the Alt key a second time exits this modifier mode and turns off the LED.
Off	Alt mode is not invoked.

Display

The display is a thin-film transistor display capable of supporting WVGA graphics modes. Display size is 800 x 480 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 VM1 is used in an abrasive environment. Contact [Technical Assistance](#) for availability.

Note: If the touch screen is disabled or loses calibration on a Thor VM1 with the 12 key keypad, you must use a USB mouse or keyboard attached to the Thor VM1 to access the control panel to re-enable or recalibrate the touch screen.

Touch Screen Defroster

Extended temperature versions of the Thor VM1 contain a touch screen defroster. The touch screen defroster can be disabled when not needed ([Start > Settings > Control Panel > Peripherals](#)). The defroster trip point is configurable. The defroster is always disabled when the device is operating from UPS battery power.

Screen Blanking

Screen blanking (blackout) can be enabled when the vehicle is in motion. A [serial cable](#) must be attached to the Thor VM1 and the Thor VM1 must be configured to enable screen blanking ([Start > Settings > Control Panel > Screen Control](#)). 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 on a Thor VM1 equipped with an outdoor display can be configured to automatically adjust depending on the ambient light level ([Start > Settings > Control Panel > Screen Control](#)).

Note: When automatic brightness control is enabled, the manual display brightness controls described below have no effect.


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

- Use the **2nd + F7** keypress to increase backlight brightness and the **2nd + F8** keypress to decrease backlight brightness.

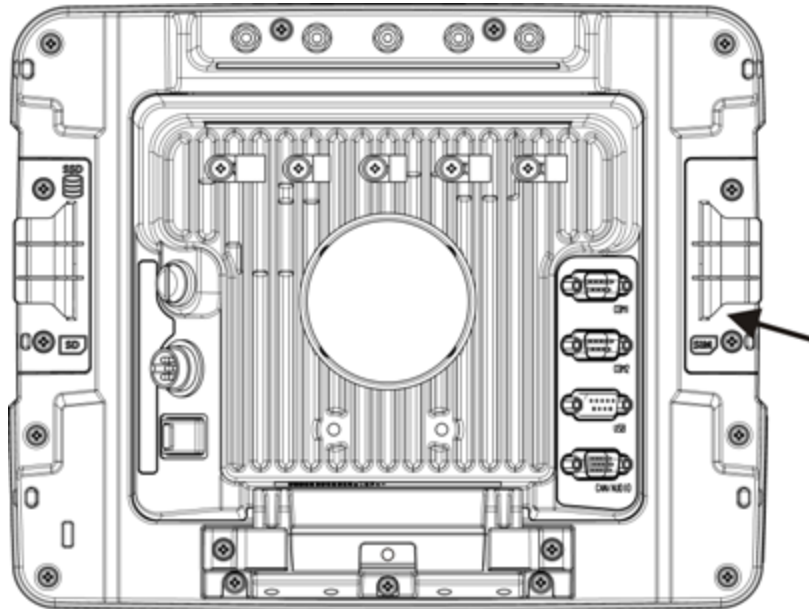
Disconnect UPS Battery

Equipment Required- User Supplied:

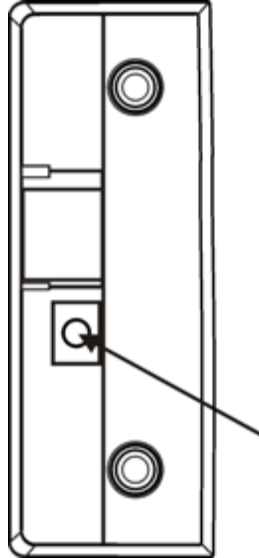
- Torquing tool capable of measuring inch pounds
- #2 Philips screwdriver bit

Caution 	The UPS battery must be disconnected before shipping the Thor VM1, replacing the UPS battery or replacing the front panel .
--	---

1. For convenience, the Thor VM1 can be removed from the Quick Mount Vehicle Dock, though it is not necessary.
2. If the Thor VM1 remains in the Dock, disconnect the power cable from the Dock.
3. Place the Thor VM1 in Suspend.
4. Place the Thor VM1 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 VM1 is face down with the top away from the user.



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

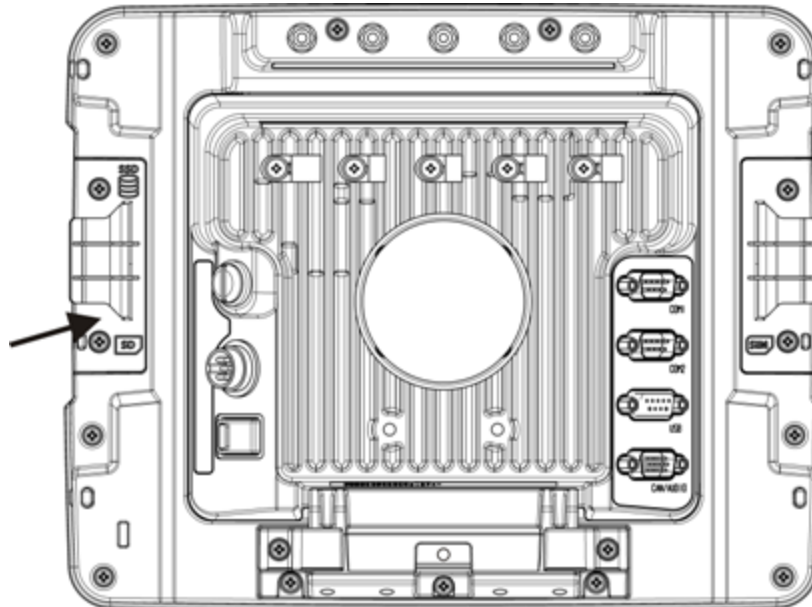


7. Press the push button to disconnect the UPS. The UPS battery maintains its charge but is disconnected from the power circuitry of the Thor VM1.
8. Reattach the access panel, torquing the M3 screws to 4-5 inch pounds using a #2 Philips bit.
9. When the Thor VM1 is attached to external power, the UPS battery is automatically reconnected.

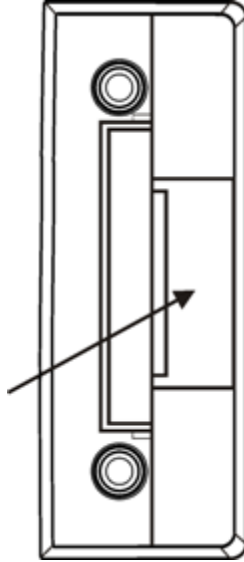
Install SD Card

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 VM1 can be removed from the Quick Mount Vehicle Dock, though it is not necessary.
 2. Place the Thor VM1 in Suspend by pressing the Power button.
 3. Place the Thor VM1 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 VM1 is face down with the top away from the user.



5. Locate the SD card installation slot.

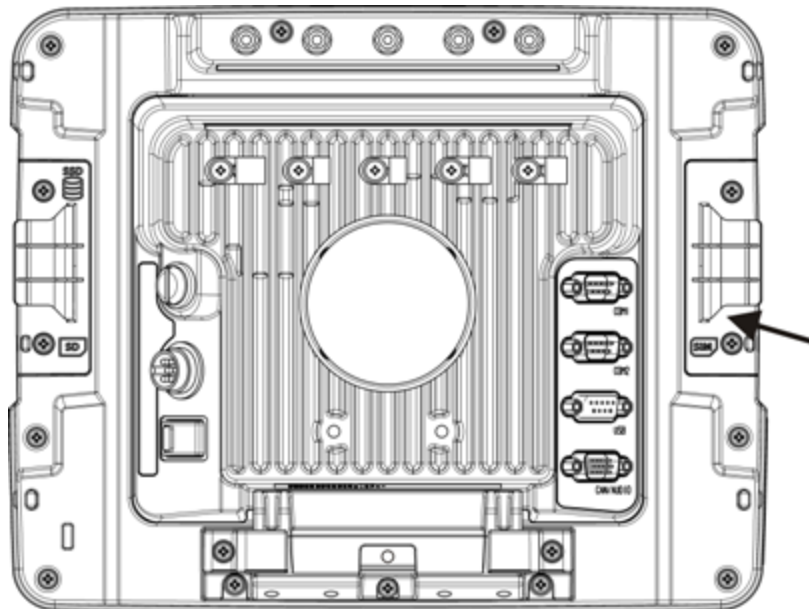


6. Slide the SD card into the slot. The label side (front) of the SD card faces toward the back of the Thor VM1.
7. Reattach the access panel, torquing the screws to 4-5 inch pounds.
8. If removed, reinstall the Thor VM1 in the Dock.
9. Resume the Thor VM1 from suspend.
10. When using Windows explorer to view **My Device**, the SD card is identified as **SD Card**. Some versions may label it **Storage Card** instead.

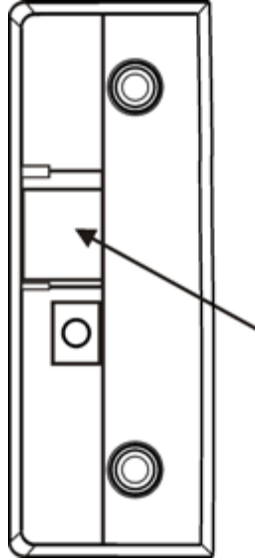
Install SIM Card

Equipment Required - User Supplied:

- Torquing tool capable of measuring inch pounds
 - #2 Phillips screwdriver bit
1. For convenience, the Thor VM1 can be removed from the Quick Mount Vehicle Dock, though it is not necessary.
 2. Place the Thor VM1 in Suspend by pressing the Power button.
 3. Place the Thor VM1 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 VM1 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 VM1 in the Dock.
9. Resume the Thor VM1 from suspend.

Field Replaceable Front Panel

Equipment Required - User Supplied:

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

Caution



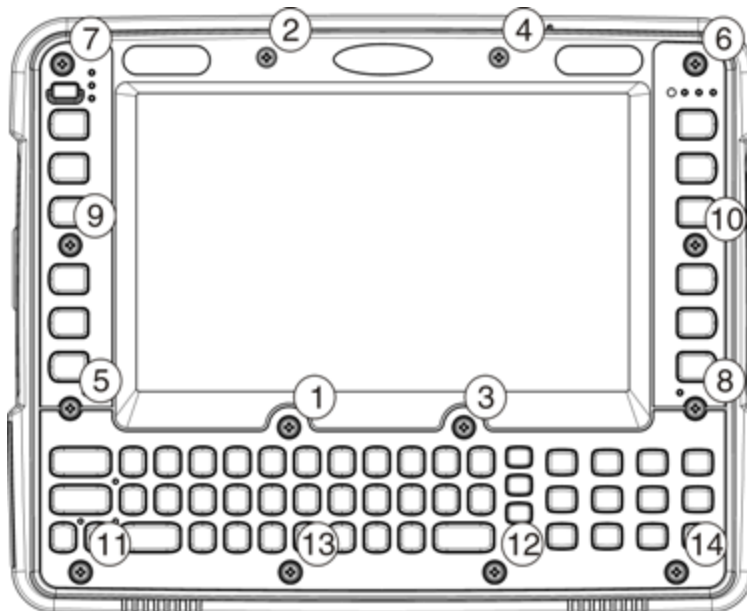
Before replacing the Thor VM1 front panel, the internal [UPS battery must be disconnected](#).

The front panel of the Thor VM1 is field replaceable. The front panel assembly contains the keyboard, touch screen and optional defroster. Should any of these components fail, the front panel assembly can easily be replaced to reduce downtime. The replacement front panel is available in several configurations:

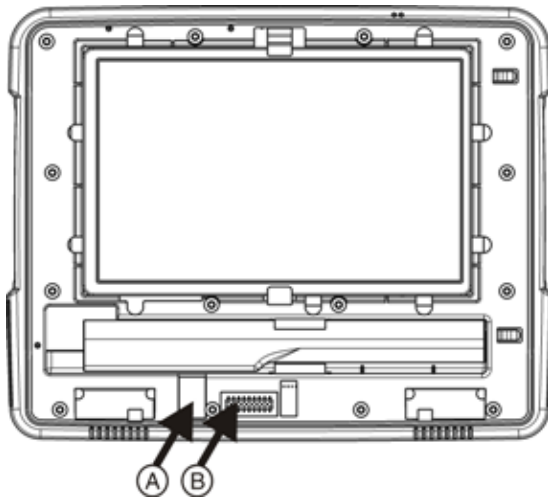
- 64-key ANSI keyboard with standard touch screen or cold storage touch screen
- 64-key 3270 keyboard with standard touch screen or cold storage touch screen
- 64-key 5250 keyboard with standard touch screen or cold storage touch screen
- 12-key keyboard with standard touch screen or cold storage touch screen

Replace Front Panel

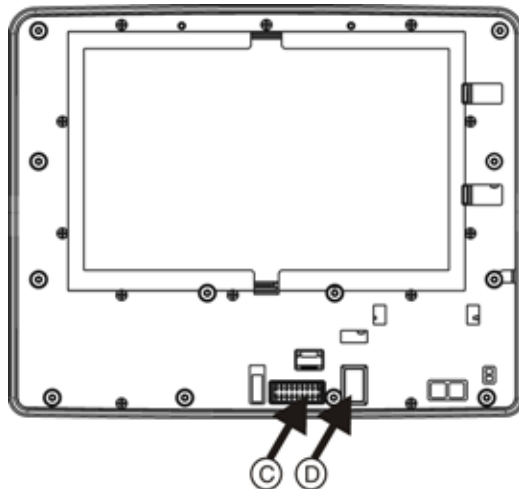
1. Place the Thor VM1 on a clean, well-lit surface before performing the front panel replacement.
2. Place the Thor VM1 in Suspend by pressing the Power button.
3. Remove the Thor VM1 from the Quick Mount Smart Dock.
4. [Disconnect the UPS](#).
5. Loosen the fourteen (14) captive M3 screws holding the front panel. Use a #2 Philips bit.



- Carefully lift the front panel away from the device.



- A. Slot on Thor VM1 body
- B. Wiring connector on Thor VM1 body



- C. Wiring connector on front panel
- D. Tab on front panel

- Position the replacement front panel so the tab on the back of the front (D in figure above) panel lines up with the slot (A in figure above) on the Thor VM1. Be sure the two wiring connectors (B and C in figures above) are also aligned.
- Gently press the front panel into place.
- Tighten the fourteen (14) 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.
- Reinstall the Thor VM1 in the Quick Mount Smart Dock.
- When the Thor VM1 is placed in the powered dock, the UPS battery automatically reconnects.
- Restart the Thor VM1.
- When restarted, the Thor VM1 automatically recognizes the keyboard type (12 or 64 keys).
- If the defroster configuration has changed, use the Test button on the [Peripherals](#) control panel to update the Thor VM1 defroster configuration.

Field Replaceable UPS Battery

Requirements - User Supplied:

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

Caution

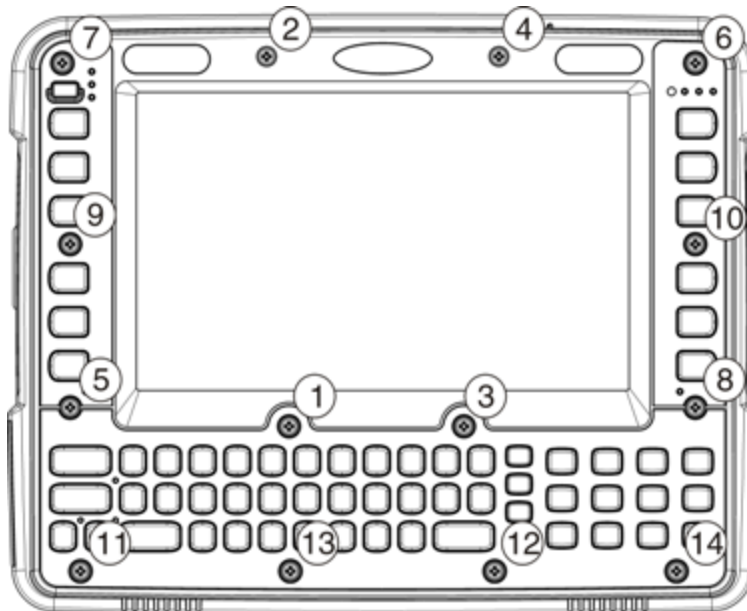


Before replacing the Thor VM1 UPS battery, the internal [UPS battery must be disconnected](#).

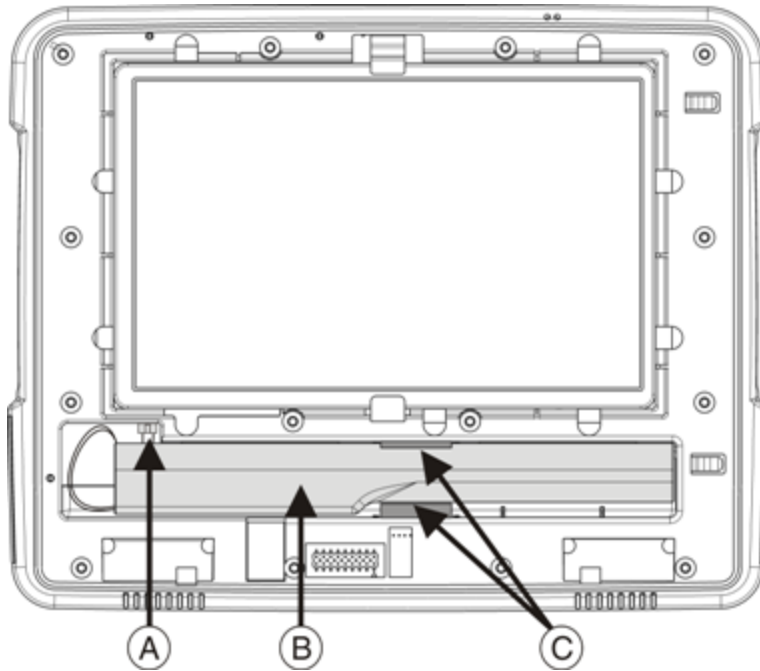
The UPS battery in the Thor VM1 is field replaceable. Should the UPS battery fail, it can easily be replaced to minimize downtime.

Replace UPS Battery

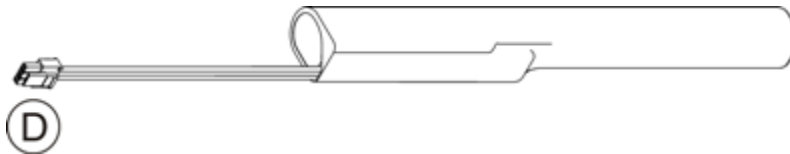
1. Place the Thor VM1 on a clean, well-lit surface before performing the UPS battery replacement.
2. Place the Thor VM1 in Suspend by pressing the Power button.
3. Remove the Thor VM1 from the Quick Mount Smart Dock.
4. [Disconnect the UPS](#).
5. Loosen the fourteen (14) captive M3 screws holding the front panel. Use a #2 Philips bit.



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

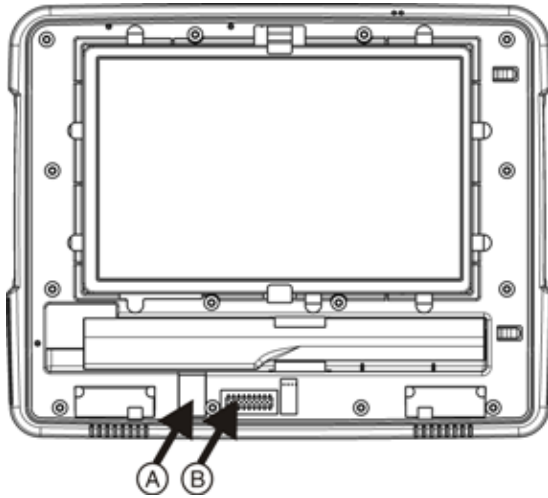


- A. Wiring Connector
- B. UPS Battery
- C. Foam Pads

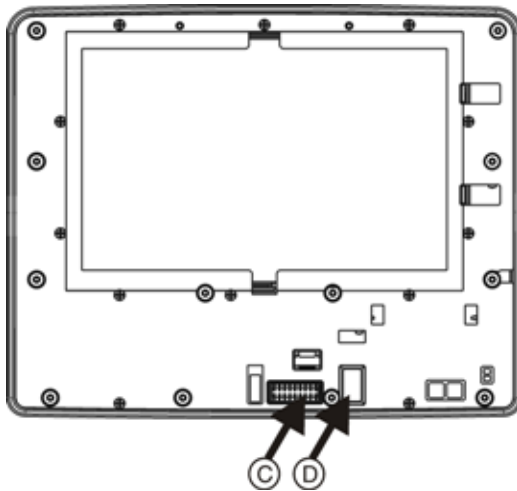


- D. Release Tab on Wiring Connector

- Note the orientation of the UPS battery. Lift the UPS battery out of the battery well and place it outside the well. Do not pull on the wires attaching the battery to the Thor VM1 while lifting the battery.
- Locate the retaining tab on the wiring connector for the UPS battery. Press on the tab and gently disconnect the UPS battery wiring from the Thor VM1.
- Remove the old battery and set it aside.
- Inspect the battery well to verify the two foam pads are still in place.
- Align the wiring connector on the new UPS battery with the connector on the Thor VM1. Gently press the connector into place until the retaining tab snaps into place.
- Place the UPS battery into the well. Note the orientation of the battery in the illustration below. The flat surface of the battery points toward the bottom of the Thor VM1. Make sure all wires are inside the battery well so they are not pinched when the front panel is reinstalled..



- A. Slot on Thor VM1 body
- B. Wiring connector on Thor VM1 body



- C. Wiring connector on front panel
- D. Tab on front panel

12. Position the front panel so the tab on the back of the front (D in figure above) panel lines up with the slot (A in figure above) on the Thor VM1. Be sure the two wiring connectors (B and C in figures above) are also aligned.
13. Gently press the front panel into place.
14. Tighten the fourteen (14) 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.
15. Reinstall the Thor VM1 in the Quick Mount Smart Dock.
16. When the Thor VM1 is placed in the powered dock, the UPS battery automatically reconnects. The UPS battery automatically begins charging from the powered dock.
17. Restart the Thor VM1.



Chapter 3: Software

Introduction

There are several different aspects to the setup, configuration and operation of the Thor VM1. Many of the setup and configuration settings are dependent upon the optional features such as hardware and software installed on the unit. The examples found in this section are to be used as examples only, the configuration of your specific Thor VM1 computer may vary. The following sections provide a general reference for the configuration of the Thor VM1 and some of its optional features.

Operating System

Your Thor VM1 operating system is Microsoft® Windows® Embedded CE 6. The Thor VM1 operating system revision is displayed on the Desktop. This is the default setting for the Desktop Display Background.

Windows CE Operating System

Note: For general use instruction, please refer to commercially available Windows CE user's guides or the Windows CE on-line Help application installed with the Thor VM1 operating system.

This segment assumes the system administrator is familiar with Microsoft Windows options and capabilities loaded on most standard Windows computers.

Therefore, the sections that follow describe only those Windows capabilities that are unique to the Thor VM1 and its Windows CE environment.

General Windows CE Keyboard Shortcuts

Use the keyboard shortcuts in the chart below to navigate with the Thor VM1 keyboard. These are standard keyboard shortcuts for Windows CE applications.

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

The touch screen provides equivalent functionality to a mouse:

- A touch on the touch screen is equivalent to a left mouse click.
- Many items can be moved by the “drag and drop” method, touching the desired item, moving the stylus across the screen and releasing the stylus in the desired location.
- A double stylus tap is equivalent to a double-click.
- A touch and hold is equivalent to a [right mouse click](#)¹.
- *Devices with Shift and Ctrl Keys* The Shift and Ctrl keys can be used with the touch screen for multiple selection of items.
 - To select disconnected items, press the Ctrl key and then touch each item to be selected in the set. Press the Ctrl key again to terminate this mode.
 - To select a connected set of items, press the Shift key, then touch the first item in the series. Touch the last item in the series. Press the Shift key again to terminate the selection mode.

¹Some applications may not support this right-click method. Please review documentation for the application to see if it provides for right mouse click configuration.

Rebooting the Thor VM1



If a USB drive, such as a thumb drive is attached to the Thor VM1, the device attempts to boot from the USB drive:

- If the USB drive contains a bootable sector, the Thor VM1 boots from the USB drive.
- If the USB drive does not contain a bootable sector, the Thor VM1 does not boot. Remove the USB drive and boot the Thor VM1 again.

Warmboot

A warmboot reboots the Thor VM1 without erasing any registry data. Configuration settings and data in RAM are preserved during a warmboot. Network sessions are lost and any data in running applications that has not been previously saved may be lost. CAB files already installed remain installed.

There are several warmboot methods available:

- Using the Registry, select Start > Settings > Control Panel > Registry and tap the Warmboot button. The Thor VM1 immediately warmboots.
- Using the Start menu, select Start > Run and type WARMBOOT in the text box. Press Enter. The Thor VM1 immediately warmboots. The WARMBOOT text command is not case-sensitive.
- For the 64-key keypad, use the **Ctrl + Alt + Del** keypress sequence to reboot the Thor VM1. The keys may be pressed in sequence; they do not need to be held down simultaneously.
- For the 12-key keypad, use the **2nd + F5 + Shift** keypress sequence to reboot the Thor VM1. The keys may be pressed in sequence; they do not need to be held down simultaneously. This reboot sequence also works on the 64-key keypad.

Restart

A restart reboots the Thor VM1 without erasing any registry data. Configuration settings are preserved during a restart. Network sessions are lost and any data in running applications that has not been previously saved may be lost. The contents of RAM are erased and the operating system and CAB files are reloaded.

To initiate a restart:

- Using the Registry, select Start > Settings > Control Panel > Registry and tap the Restart button. The Thor VM1 immediately restarts.
- Using the Start menu, select Start > Run and type RESTART in the text box. Press Enter. The Thor VM1 immediately restarts. The RESTART text command is not case-sensitive.

Clearing Persistent Storage / Reset to Default Settings

Use the Registry control panel **Load Factory Defaults** button to set the Thor VM1 registry back to factory defaults. No other clearing is available or necessary.

Folders Copied at Startup

If any of the following folders are created in the System folder, they are copied at startup:

System\Desktop	copied to	Windows\Desktop
System\Favorites	copied to	Windows\Favorites
System\Fonts	copied to	Windows\Fonts

System\Help	copied to	Windows\Help
System\Programs	copied to	Windows\Programs
AppMgr	copied to	Windows\AppMgr
Recent	copied to	Windows\Recent

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

The Windows\Startup folder is not copied on startup because copying this folder has no effect on the system or an incorrect effect.

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

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

Saving Changes to the Registry

The Thor VM1 saves the registry when you:

- Warmboot - either from the Registry control panel, the warmboot command or the reboot keypress sequence.
- Restart - from the Registry control panel
- Suspend/Resume - Either user initiated or upon Suspend timer expiration.
- Shutdown - The registry is saved during a controlled shutdown, such as when the UPS charge reaches a critically low level and external power is not available.

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

Software Load

The software loaded on the Thor VM1 consists of Microsoft® Windows® Embedded CE 6 OS, hardware-specific OEM Adaptation Layer, device drivers, Internet Explorer 6.0 for Windows CE browser and utilities. The software supported is summarized below:

- Full Operating System License: Includes all operating system components, including Microsoft® Windows® Embedded CE 6 kernel, file system, communications, connectivity (for remote APIs), device drivers, events and messaging, graphics, keyboard and touch screen input, window management, and common controls.
- Network and Device Drivers
- Bluetooth

Note: Please contact Honeywell Technical Assistance for software updates and CAB files as they are released by Honeywell.

Software Applications

The following applications are included:

- WordPad
- Data Collection Wedge (bar code result manipulation)
- ActiveSync
- Transcriber
- Internet Explorer
- Word Viewer
- Excel Viewer
- PDF Viewer
- PowerPoint Viewer

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

ActiveSync

ActiveSync is pre-loaded. Using Microsoft ActiveSync you can copy files from your Thor VM1 to your desktop/laptop, and vice versa. After an ActiveSync relationship (partnership) has been established with a desktop/laptop, ActiveSync will automatically startup each time the Thor VM1 is cabled to the desktop/laptop.

Bluetooth

Start > Settings > Control Panel > Bluetooth

Only installed on a Bluetooth equipped Thor VM1. The System Administrator can Discover and Pair targeted Bluetooth devices for each Thor VM1. The System Administrator can enable / disable Bluetooth settings and assign a Computer Friendly name for each Thor VM1.

The Bluetooth control panel can also be accessed by double-tapping the Bluetooth icon in the taskbar or on the desktop.

LXE RFTerm (Optional)

Start > Programs > LXE RFTerm

RFTerm is pre-loaded when ordered. The application can also be accessed by double-clicking the RFTerm desktop icon.

Avalanche

The Wavelink Avalanche Enabler installation file is loaded on the Thor VM1; however, the device is not configured to launch the installation file automatically. The installation application must be run manually the first time Avalanche is used. Following installation, the Wavelink Avalanche Enabler will be an auto-launch application. This behavior can be modified by accessing the Avalanche Update Settings panel through the Enabler Interface.

Software Development

See Also: *CE API Programming Guide*

The CE API Programming Guide documents Honeywell-specific API calls for the Thor VM1. It is intended as an addition to Microsoft Windows CE API documentation.

A Software Developers Kit (SDK) and additional information about software development can be found on the Developer Portal. Please Contact [Technical Assistance](#) for more information.

Thor VM1 Utilities

The following files are pre-loaded.

LAUNCH.EXE

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

```
HKEY_LOCAL_MACHINE \ Software \ LXE \ Persist
```

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

App Note

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

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

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

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

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

Order is used to force a sequence of events. Order=0 is first, and Order=99 is last. Order **must be greater than 4** for the Thor VM1. Two items which have the same order will be installed in the same pass, but not in a predictable sequence.

There are two optional fields that may be added:

1. Delay is used to add a delay after the item is loaded, before the next is loaded. The delay is given in seconds, and defaults to 0 if not specified. If the install fails (or the file to be installed is not found), the delay does not occur.
2. PCMCIA is used to indicate that the file (usually a CAB file) being loaded is a radio driver, and the PCMCIA slots should be started after this file is loaded. By default, the PCMCIA slots are off on powerup, to prevent the "Unidentified PCMCIA Slot" dialog from appearing. Once the drivers are loaded, the slot can be turned on. The value in the PCMCIA field is a DWORD, representing the number of seconds to wait after installing the CAB file, but before activating the slot (a latency to allow the thread loading the driver to finish installation). The default value of 0 means the slot is not powered on. The default values for the default radio drivers (listed below) is 1, meaning one second elapses between the CAB file loading and the slot powering up.

The auto-launch process proceeds as follows:

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

Note: Registry entries may vary depending on software revision level and options ordered with the Thor VM1.

LAUNCH.EXE and Persistent Storage

If any of the following directories are created in the System folder, Launch automatically copies all of the files in these directories:

- AppMgr
- Desktop
- Favorites
- Fonts
- Help

-
- Programs
 - Recent

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

REGEDIT.EXE

Registry Editor – Use caution when editing the Registry. Make a backup copy of the registry before changes are made.

REGLOAD.EXE

Double-tapping a registry settings file (e.g., REG) causes RegLoad to open the file and make the indicated settings in the registry.

REGDUMP.EXE

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

The Thor VM1 includes a Load User Defaults option in the [Registry](#) control panel. This is the preferred method for saving a backup of the registry. Save the registry file to the System folder on the Reference Guide (persistent storage) or copy the file to a PC.

WARMBOOT.EXE

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

WAVPLAY.EXE

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

Thor VM1 Command-line Utilities

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

PrtScrn.EXE

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

Desktop








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






The Thor VM1 Desktop appearance is similar to that of a desktop PC running a Windows operating system.

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

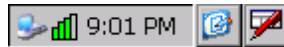
Desktop Icons

At a minimum, the desktop displays icons for My Device, Internet Explorer and the Recycle Bin. Following are a few of the other icons that may be on the Thor VM1 Desktop. Please Contact [Technical Assistance](#) about the latest updates and upgrades for your operating system.

Icon	Function
 My Device	Access files and programs.
 Recycle Bin	Storage for files that are to be deleted.
 Bluetooth	Discover and then pair with nearby discoverable Bluetooth devices.
 My Documents	Storage for downloaded files / applications.
 Internet Explorer	Connect to the Internet/intranet.
 Summit Client Utility	Used for accessing the appropriate wireless configuration, SCU (Summit Client Utility).
 eXpress Scan	The eXpress Scan utility allows an administrator to scan bar codes to provide the initial network and Avalanche Mobile Device Server address configuration. This eliminates the need to edit radio parameters manually on the Thor VM1. eXpress Scan uses bar codes created with eXpress Config.

Icon	Function
 LXE RFTerm	RFTerm is an optional terminal emulation program. When RFTerm is installed, this icon is displayed on the desktop.
 Remote Desktop Connection	A shortcut to the Remote Desktop Connection utility.
 Avalanche	Avalanche shortcut. Wavelink® Avalanche Mobility Center™ (Avalanche MC) is a remote client management system that is designed to distribute software and configuration updates to monitored devices. The enabler for Wavelink Avalanche is loaded on the Thor VM1 but not installed. When the enabler is installed the Avalanche icon is displayed on the desktop.
 TelnetCE	The demo version of Wavelink Telnet CE is installed on all devices. Please Contact Technical Assistance for licensing information. When installed, license details are maintained in the Wavelink tab in the License Viewer control panel.
	Start button. Access programs, select from the Favorites listing, documents last worked on, change/view settings for the control panel or taskbar, on-line help or run programs.

Taskbar



The number and type of icons displayed are based on the device type, installed options and configuration of the Thor VM1.

My Device Folders

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

Wavelink Avalanche Enabler (Optional)

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

The following features are supported by the Wavelink Avalanche Enabler when used in conjunction with the Avalanche Manager.

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

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

Related Manual: *Using Wavelink Avalanche*

The Thor VM1 has the Avalanche Enabler installation files loaded, but not installed, on the mobile device when it is shipped. The installation files are located in the System folder on CE devices. The installation application must be run manually the first time Avalanche is used.

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

The designation of the mobile device to the Avalanche CE Manager is LXE_THOR.

Internet Explorer

Start > Programs > Internet Explorer

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

Start Menu Program Options

The following list represents the factory default program installation. Your system may contain different items from those shown below, based on the software and hardware options purchased.

Communication	Stores Network communication options
Connect	Run this command after setting up a connection
Start (or Stop) FTP Server	Begin / end connection to FTP server
Command Prompt	The command line interface in a separate window
eXpress Scan	Option. Requires Wavelink Avalanche option eXpress Config.
Internet Explorer	Access web pages on the Internet/Intranet
File Viewers	
JETCET PDF Viewer	View Adobe PDF Documents
Office 2003 Excel Viewer	View Excel 2003 and compatible documents
Office 2003 PowerPoint Viewer	View PowerPoint 2003 and compatible documents
Office 2003 Word Viewer	View Word 2003 and compatible documents
Microsoft WordPad	Opens an ASCII notepad
Remote Desktop Connection	Log on to a Windows Terminal Server
LXE RFTerm	Option. Terminal emulation application.
Settings	Access to all Control Panels, a shortcut to the Network and Dialup Control Panel and access to Taskbar options.
Summit	Set Summit radio / network parameters
Transcriber	Enter data using the stylus on the touch screen
Wavelink Avalanche	Option. Remote management for networked devices
Windows Explorer	File management program
	<ul style="list-style-type: none">• If installed, RFTerm runs automatically at the conclusion of each reboot.• If installed and enabled, AppLock runs automatically at the conclusion of each reboot.• The wireless client connects automatically during each reboot.• Bluetooth re-connects to nearby paired devices automatically at the conclusion of each reboot.• If installed and pre-configured, Wavelink Avalanche connects remotely and downloads updates automatically during each reboot.

Communication

Start > Programs > Communication

ActiveSync

ActiveSync is pre-loaded on the Thor VM1.

Using Microsoft ActiveSync you can copy files from your Thor VM1 to your desktop computer, and vice versa.

Once an ActiveSync relationship (partnership) has been established with Connect (on a desktop computer), ActiveSync will synchronize using USB on the Thor VM1.

Connect and LXEConnect

Upon cabling your Thor VM1 to the desktop/laptop, and ActiveSync on the desktop/laptop opens, if the Connect or LXEConnect installation does not open on your host PC, Contact [Technical Assistance](#).

Start FTP Server / Stop FTP Server

Start > Programs > Communication > Start (or Stop) FTP Server

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

Summit

Start > Settings > Control Panel > Summit

Use this option to set up radio client profiles.

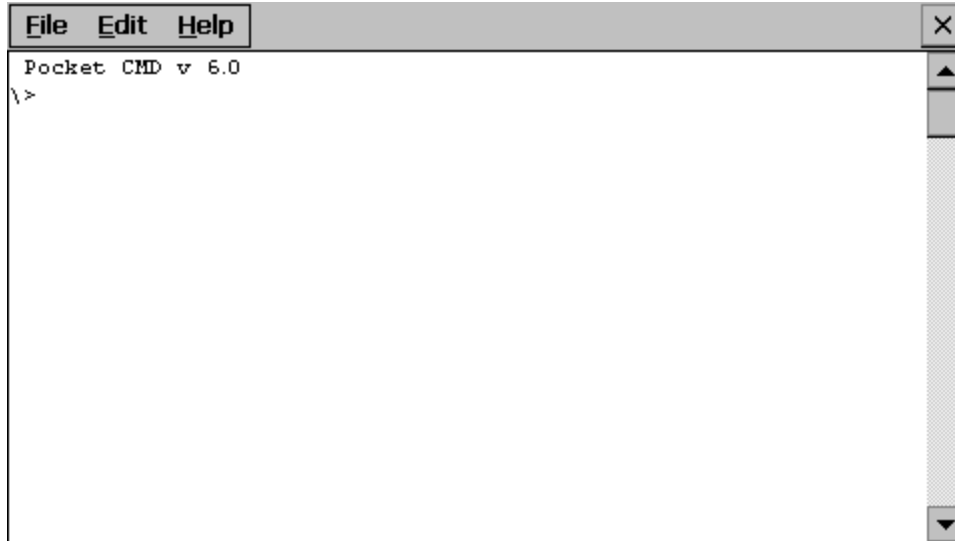
The Summit Control Panel can also be accessed by double-tapping the Summit icon in the taskbar or on the desktop.

Certs

The Certs option displays a readme file containing details on how the Summit Configuration Utility (SCU) handles certificates for WPA authentication.

Command Prompt

Start > Programs > Command Prompt



Type **help cmd** at the command prompt to view valid Pocket PC (Console) commands.

Exit the command prompt by typing **exit** at the command prompt or tap **File > Close**.

eXpress Scan

The eXpress Scan utility allows an administrator to scan bar codes to provide the initial network and Avalanche Mobile Device Server address configuration. This eliminates the need to edit radio parameters manually on the Thor VM1.

eXpress Scan uses bar codes created with eXpress Config.

Internet Explorer

Start > Programs > Internet Explorer

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

Media Player

Start > Programs > Media Player

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

After the Media Player application is running, click the ? button to access Media Player Help.

File Viewers

The following applications are included:

- JETCET PDF Viewer
- Office 2003 Excel Viewer
- Office 2003 PowerPoint Viewer
- Office 2003 Word Viewer

Note: The viewer applications allow viewing documents, but not editing them.

Microsoft WordPad

Start > Programs > Microsoft WordPad

Create and edit documents and templates in WordPad, using buttons and menu commands that are similar to those used in the desktop PC version of Microsoft WordPad.

By default WordPad files are saved as .PWD files. Documents can be saved in other formats e.g., .RTF or .DOC.

Tap the ? button to access WordPad Help.

Remote Desktop Connection

Start > Programs > Remote Desktop

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

If installed, Remote Desktop on the Thor VM1 can be accessed by **Start > Programs > Remote Desktop**.

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

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

Settings

Start > Settings

The Settings menu option may include the following:

Control Panel	All control panels
Network and Dialup Connections	Shortcut to control panel. Connect to a network, create a new connection, and adjust parameters for client connections.
Taskbar	Set Taskbar parameters

Transcriber

To make changes to the Transcriber application, tap the [keyboard](#) icon in the status bar. Select Transcriber from the pop-up menu. Then open the Input control panel and tap the Options button. Transcriber Options (Start > Settings > Control Panel >

Input Panel) are available only when Transcriber is selected as the active input method. Tap the “?” button or the Help button to access Transcriber Help.

Windows Explorer

Start > Programs > Windows Explorer

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

Taskbar

Start > Settings > Taskbar

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

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

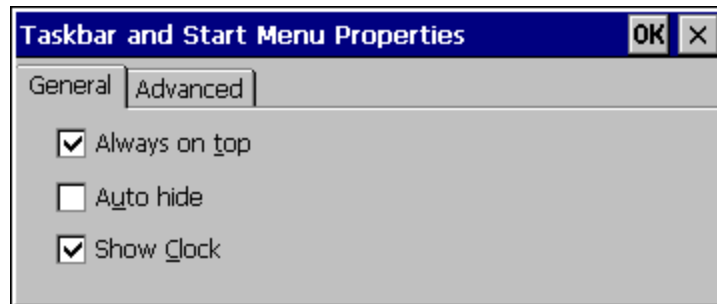
Clicking the Taskbar option on the Settings menu displays the Taskbar [General](#) tab and the Taskbar [Advanced](#) tab.

[See Also: "Taskbar Icons"](#)

General Tab

Factory Default Settings

Always on Top	Enabled
Auto hide	Disabled
Show Clock	Enabled



Advanced Tab



Expand Control Panel

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

Clear Contents of Document Folder














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

Taskbar Icons

As Thor VM1 devices and applications open and change state, icons are placed in the Taskbar. In most cases, tapping the icon in the Taskbar opens the related application.

Refer to **Start > Help** for an explanation of standard Windows CE taskbar icons.

Following are a few of the Thor VM1 taskbar icons that may appear in the Taskbar. These icons are in addition to the Windows CE taskbar icons.

	Wireless Zero Config Inactive / Connected / Not Connected. Clicking on the icon opens the Wireless Zero Config utility.
	Bluetooth connected / disconnected. Clicking the icon opens the Bluetooth control panel.
	ActiveSync Connection
	Cerdisp connected (displayed when LXEConnect is connected)
	Summit Client signal indicator no signal / excellent signal. Clicking on the icon opens the Summit Client Utility .
	Gobi Connection Manager (WWAN) signal indicator no signal / excellent signal. Clicking on the icon opens the Gobi Connection Manager .
	UPS battery charge indicator. Percent of battery charge is indicated.
	External power connected / connected and UPS battery charging.
	Current time. Clicking the time display opens the Date/Time control panel .
	Click this icon to return to the Desktop.
	AppLock switchpad.
	Input method, keyboard / input panel / transcriber
	CapsLock active


Thor VM1 OS Upgrade

Introduction

Depending on the size of the operating system, the total time required for a successful upgrade may require several minutes. The OS upgrade files are unique to your Thor VM1 physical configuration and date of manufacture. OS upgrade files designed for one device configuration should not be used on a different device configuration.

When upgrading the OS or firmware on a Thor VM1 with a 12-key keyboard, it is best to perform the upgrade using either Wavelink Avalanche or with an external USB keyboard attached.

There may be firmware and BIOS upgrades available for the Thor VM1. Contact [Technical Assistance](#) for upgrade information and instructions. In some cases, it may be necessary to upgrade firmware before upgrading the operating system.

<p>Caution</p> 	<p>The Thor VM1 must be connected to external power before upgrading the BIOS, firmware or operating systems.</p> <p>If the Thor VM1 is operating on UPS battery power, the upgrade process does not initiate and the Thor VM1 is not upgraded.</p>
--	---

Preparation

- Please Contact [Technical Assistance](#) to get the **OS upgrade files**.
- Honeywell Technical Assistance may advise you that additional upgrades such as BIOS or firmware are required before upgrading the OS. Please follow any additional upgrade instructions provided by Technical Assistance.
- Use ActiveSync to back up Thor VM1 user files and store them elsewhere before beginning an upgrade on the Thor VM1.
- Maintain an uninterrupted AC/DC power source to the Thor VM1 throughout this process.
- The CF card with the OS and systems files must be present for the Thor VM1 to boot. Removal or installation of SD or CF cards should be performed on a clean, well-lit surface.
- Always perform OS updates when the Thor VM1 has a dependable external power source connected to the Thor VM1.

Procedure

1. Verify a dependable power source is applied to the Thor VM1 and will stay connected during the upgrade procedure.
2. Warmboot the Thor VM1 before beginning the update process.
3. Establish an ActiveSync connection between the Thor VM1 and a desktop/laptop computer.
4. Download the OS files from the desktop/laptop to the Thor VM1's System folder.
5. During the file copy process to the Thor VM1 System folder, when asked "Overwrite ?", select Yes to All.
6. Review the files that were downloaded to the System folder.
7. Restart the Thor VM1.
8. Disconnect from ActiveSync.
9. When the OS finishes loading, check the OS update version by selecting **Start > Settings > Control Panel > About > Software** tab.

The touch screen may require calibration, however most Windows OS versions save the calibration data, eliminating the need to calibrate.


If the Thor VM1 won't boot up after the upgrade is finished, Contact [Technical Assistance](#) for re-imaging options.

BIOS

The Microsoft Windows CE 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.

<p>Caution:</p> 	<p>Be very careful when using this utility to modify BIOS Setup parameters. The Thor VM1 may generate unexpected results when incorrect or conflicting parameter values are entered. Selecting incorrect or invalid options may require the Thor VM1 to be returned for repairs.</p> <p>The parameters should only be modified by Information Services personnel or the system administrator.</p>
---	---

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 VM1 with 12-key keyboard, 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**.

	<p>If a USB drive, such as a thumb drive is attached to the Thor VM1, the device attempts to boot from the USB drive:</p> <ul style="list-style-type: none">• If the USB drive contains a bootable sector, the Thor VM1 boots from the USB drive.• If the USB drive does not contain a bootable sector, the Thor VM1 does not boot. Remove the USB drive and boot the Thor VM1 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

Control Panel

Start > Settings > Control Panel or **My Device > Control Panel link**

Tap the ? button for Help when changing Thor VM1 Control Panel options.

Option	Function
About	Software, hardware, versions and network IP. No user intervention allowed.
Accessibility	Customize the way the keyboard, audio, display or mouse function for users with hearing or viewing difficulties.
Administration	AppLock Administration utility.
Battery	View voltage and status of the internal UPS battery.
Bluetooth	Set the parameters for Bluetooth device connections.
Certificates	Manage digital certificates used for secure communication.
Data Collection (Wedge)	Wedge utility for data collected from bar code scans. Set data collection device, data stripping, and prefix/suffix options. Assign baud rate, parity, stop bits and data bits for COM1 and COM2 ports. Assign collected data manipulation parameters.
Date/Time	Set Date, Time, Time Zone, and Daylight Savings.
Dialing	Connection setup for modem attached to COM port or CompactFlash slot. . CompactFlash slot not available for modem use on Thor VM1.
Display	Set background graphic and scheme. Set touch screen and keypad backlight properties and timers.
Gobi Connection Manager	Set parameters for the Wireless Wide Area Network client, if installed.
Input Panel	Select the current key / data input method. Select custom key maps.
Internet Options	Set General, Connection, Security, Privacy, Advanced and Popups options for Internet connectivity.
Keyboard	Select a Key Map (or font). Set key repeat delay and key repeat rate.
KeyPad	Configure KeyMap keys, RunCmd and LaunchApp.
License Viewer	Displays license information for installed licensed applications.
Mixer	Adjust the input and output parameters – volume, sidetone, and record gain, for headphone, software and microphone.
Mouse	Set the double-tap sensitivity for stylus taps on the touch screen.
Network and Dial Up Options	Set network driver properties and network access properties.
Network Capture	Set network logging options.
Options	Set various device specific configuration options.
Owner	Set the mobile device owner details (name, phone, etc.). Enter notes. Enable / disable Owner display parameters. Enter Network ID for the device – user name, password, domain.
Password	Set OS access password properties for signon and/or screen saver.

Option	Function
PC Connection	Control the connection between the mobile device and a local desktop or laptop computer.
Peripherals	Enable or disable defroster, if installed.
Power	Set Power scheme properties. Review device status and properties.
Regional Settings	Set appearance of numbers, currency, time and date based on country region and language settings.
Registry	Load User Defaults, Save User Defaults, Load Factory Defaults, and Warmboot.
Remove Programs	Select to remove specific user installed programs in their entirety.
Screen Control	Configure screen blanking and automatic screen brightness control.
Stylus	Set double-tap sensitivity properties and/or calibrate the touch panel.
System	Review System and Computer data and revision levels. Adjust Storage and Program memory settings. Enter device name and description. Review copyright notices.
Terminal Server Client Licenses	Select a server client license from a drop down list.
Volume and Sounds	Enable / disable volume and sounds. Set volume parameters and assign sound WAV files to events.
WiFi	Set the parameters for a Summit client.

About

Start > Settings > Control Panel > About

The data cannot be edited by the Thor VM1 user on these panels.

Tab	Contents
Software	GUID, Serial Number, Windows CE Version, OAL Version, Compile Version, and Language. Language indicates localized version.
Hardware	CPU Type, Codec Type, Display, and DRAM memory
Versions	Revision level of software modules and .NET Compact Framework Version.
Network IP	Current network connection IP and MAC address. Only the first 2 adapters are shown (usually radio and ActiveSync). Bluetooth MAC address is shown.

Version window information is retrieved from the registry.

Version Tab and the Registry

Modify the Registry using the Registry Editor. Use caution when editing the Registry and make a backup copy of the registry before changes are made.

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

To add a user application to the Version panel, create a new string value under the HKLM\Software\LXE\Version key. The string name should be the Application name to appear in the Version window. The data for the value should be the version number to appear in the Version window.

Version strings can be equal to or less than 254 characters. Because the strings are displayed in a text box, any number can be accommodated, up to the 64K byte text box limitation.

Languages

The Software tab displays the localized language version of the OS image:

- English only – No additional languages are built into the OS
- Japanese
- Simplified Chinese
- Traditional Chinese
- Korean
- Spanish
- French
- German
- Thai

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

Identifying Software Versions

The Versions tab displays the versions of many of the software programs installed. Not all installed software is included in this list and the list varies depending on the applications loaded on the Thor VM1. The Image line displays the revision of the system software installed. Refer to the last three digits to determine the revision level.

MAC Address

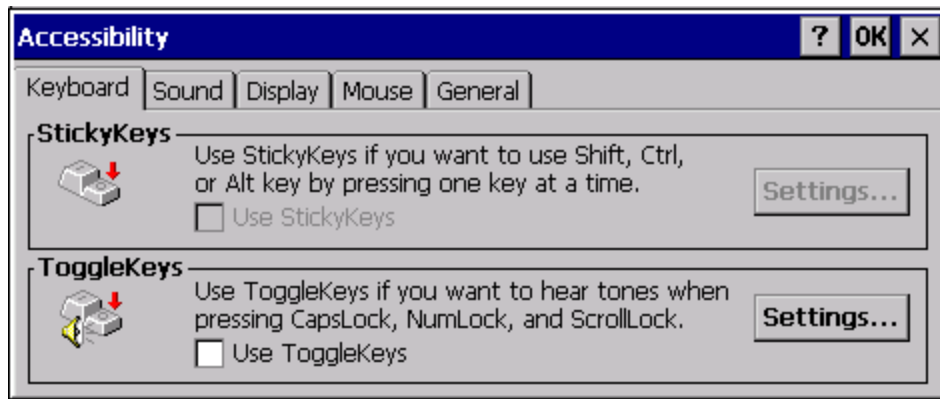
The Network IP tab displays the MAC address of the network card.

Accessibility

Start > Settings > Control Panel > Accessibility

Customize the way the Thor VM1 keyboard, sound, display, mouse, automatic reset and notification sounds function. There are a few changes from general Windows desktop Accessibility options.

Keyboard	Sticky Keys - Disabled (cannot be enabled). ToggleKeys - Disabled by default. Tap the <i>Use ToggleKeys</i> checkbox to enable this option. Tap the Settings button to view or change parameters.
Sound	SoundSentry is disabled by default. Tap the <i>Use SoundSentry</i> checkbox to enable this option. Tap the Settings button to view or change parameters.
Display	High Contrast is disabled by default. Tap the <i>Use High Contrast</i> checkbox to enable this option. Tap the Settings button to view or change parameters.
Mouse	MouseKeys is disabled by default. Tap the <i>Use MouseKeys</i> checkbox to enable this option. Tap the Settings button to view or change parameters.
General	Automatic reset is disabled by default. Tap the <i>Turn off accessibility features</i> checkbox to enable this option and use the dropdown option to assign a timer. Notification is enabled by default. Sounds are emitted when turning a feature on or off.



The following exceptions are due to a limitation in the Microsoft Windows CE operating system:

- If the ToggleKeys option is selected, please note that the ScrollLock key does not produce a sound as the CapsLock and NumLock keys do.
- If the SoundSentry option is selected, please note that ScrollLock does not produce a visual warning as the CapsLock and NumLock keys do.

Administration (for AppLock)

Start > Settings > Control Panel > Administration

AppLock is designed to be run on certain certified Windows CE based devices only. The AppLock program is installed as part of the default software load.

Configuration parameters are specified by the AppLock Administrator for the Thor VM1 end-user. AppLock is password protected by the Administrator.

End-user mode locks the end-user into the configured application or applications. The end user can still reboot the mobile device and respond to dialog boxes. The administrator-specified applications are automatically launched in the specified order and run in full screen mode when the device boots up.

When the mobile device is reset to factory default values, for example after a cold reset, the Administrator may need to reconfigure the AppLock parameters.

The assumption, in this section, is that the first user to power up a new mobile device is the system administrator.

Note: AppLock Administrator Control panel file Launch option does not inter-relate with similarly-named options contained in other Thor VM1 Control Panels.

Note: A few applications do not follow normal procedures when closing. AppLock cannot prevent this type of application from closing, but is notified that the application has closed. For these applications, AppLock immediately restarts the application (see Auto Re-Launch) which causes the screen to flicker. If this type of application is being locked, the administrator should close all other applications before switching to end-user mode to minimize the screen flicker.

AppLock is updated periodically as new options become available. Contact [Technical Assistance](#) for update availability.

Factory Default Settings - AppLock

Application Panel	
Filename	Blank
Title	Blank
Arguments	Blank
Order	1
Internet	Disabled
Global Key	Ctrl+Spc
Global Delay	10 sec
Input Panel	Disabled
Launch Button Panel	
Auto at Boot	Enabled
Auto at Boot Retries	0
Auto at Boot Delay	10 sec
Auto Re-launch	Enabled
Auto Re-launch Retries	0
Auto Re-launch Delay	0 sec
Manual Launch	Disabled
Allow Close	Disabled
Security Panel	
Hotkey (Activation key)	Shift+Ctl+A
Password	Blank
Options Panel	
Launch timeout	60000
Replace timeout	20000
Restart timeout	20000
Status Panel	
Filename	\System\applock.txt
View Level	None
Log Level	None

Setup a New Device

Devices with the AppLock feature are shipped to boot in Administration mode with no default password, thus when the Thor VM1 is first booted, the user has full access to the device and no password prompt is displayed. After the administrator specifies the applications to lock, a password is assigned and the device is rebooted or the hotkey is pressed, the device switches to end-user mode.

Briefly, the process to configure a new device is as follows:

1. Connect an external power source to the device and press the Power button.
2. Adjust screen display, audio volume and other parameters if desired. Install accessories.
3. Tap Start > Settings > Control Panel > Administration icon.
4. Assign applications on the Control (single application) or Application (dual application) tab screen.
5. Assign a password on the Security tab screen.
6. Select a view level on the Status tab screen, if desired.
7. Tap OK
8. Press the hotkey sequence to launch AppLock and lock the configured application(s)
9. The device is now in end-user mode.

Administration Mode

Administration mode gives full access to the mobile device, hardware and software configuration options.

The administrator must enter a valid password (when a password has already been assigned) before access to Administration mode and configuration options are allowed. The administrator can configure the following options:

- Create/change the keystroke sequence to activate administrator access.
- Create/change the password for administrator access.
- Assign the name of the application, or applications, to lock.
- Select the command line of the application to lock.

In addition to these configuration options, the administrator can view and manage the status logs of AppLock sessions.

Administrator default values for this device:

Administrator Hotkey

Shift+Ctrl+A

Note: You must use an external keyboard with the 12-key version of the Thor VM1 to enter the Administrator Hotkey.

Password

none

Application path and name

none

Application command line

none

End User Mode

End-user mode locks the end-user into the configured application or applications. The end user can still reboot and respond to dialog boxes. Each application is automatically launched and runs in full screen mode when the device boots up.

The user cannot unintentionally or intentionally exit the application nor can the end user execute any other applications. Normal application exit or switching methods and all Microsoft defined Windows CE key combinations, such as close (X) icon, File Exit, File Close, Alt-F4, Alt-Tab, etc. are disabled. The Windows CE desktop icons, menu bars, task bar and system trays are not visible or accessible. Task Manager is not available.

If the end-user selects File/Exit or Close from the applications menu bar, the menu is cleared and nothing else happens; the application remains active. Nothing happens when the end-user clicks on the Close icon on the application's title bar and the application remains active.

Note: A few applications do not follow normal procedures when closing. AppLock cannot prevent this type of application from closing, but is notified that the application has closed. For these applications, AppLock immediately restarts the application which causes the screen to flicker. If this type of application is being locked, the administrator should close all other applications before switching to end user mode to minimize the screen flicker.

Windows accelerator keys such as Alt-F4 are disabled.

Passwords

A password must be configured. If the password is not configured, a new device switches into Administration mode without prompting for a password. In addition to the hotkey press, a mode switch occurs if inaccurate information has been configured or if mandatory information is missing in the configuration.

There are several situations that display a password prompt after a password has been configured.

If the configured hotkey is pressed, the password prompt is displayed. In this case the user has 30 seconds to enter a password. If a valid password is not entered within 30 seconds, the password prompt is dismissed and the device returns to end-user mode.

All other situations that present the password prompt do not dismiss the prompt – this is because the other situations result in invalid end-user operation.

These conditions include:

- If inaccurate configuration information is entered by the administrator, i.e. an application is specified that does not exist.
- If the application name, which is mandatory for end-user mode, is missing in the configuration.
- Invalid installation of AppLock (e.g. missing DLLs).
- Corrupted registry settings.

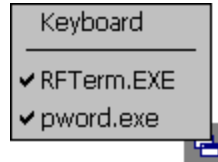
To summarize, if an error occurs that prevents AppLock from switching to user mode, the password will not timeout and AppLock will wait until the correct password is entered.

Forgotten password?

See: [AppLock help](#)

End-User Switching Technique

Note: The touch screen must be enabled.



A checkmark indicates applications currently active or available for Launching by the user. When Keyboard is selected, the Thor VM1 default input method (Input Panel, Transcriber, or custom input method) is activated.

The check to the left of the application name indicates that the application is active.

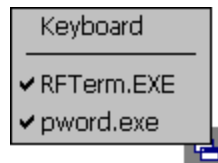
If the application is listed but does not have a checkmark to the left of the application name, this means the application is configured in AppLock and can be manually launched by clicking on the application name in the list.

Using a Stylus Tap

When the mobile device enters end-user mode, a Switchpad icon (it looks like three tiny windows one above the other) is displayed in the lower right corner of the display. The Switchpad is always visible on top of the application in focus. However, if only one application is configured in AppLock and the Input Panel is disabled the Switchpad is not visible.



When the user taps the Switchpad icon, a menu is displayed showing the applications available to the user. The user can tap an application name in the popup menu and the selected application is brought to the foreground. The previous application continues to run in the background. Stylus taps affect the application in focus only. When the user needs to use the Input Panel, they tap the Keyboard option. Input Panel taps affect the application in focus only.



See Also: Application Panel > Launch > [Manual \(Launch\)](#) and [Allow Close](#)

Using the Switch Key Sequence

One switch key sequence (or hotkey) is defined by the administrator for the end-user to use when switching between locked applications. This is known as the **Activation key**. The Activation key is assigned by the Administrator using the Global Key parameter. When the switch key sequence is pressed on the keypad, the next application in the AppLock configuration is moved to the foreground and the previous application moves to the background. The previous application continues to run in the background. End-user key presses affect the application in focus only.

See Also: Start > Settings > Administration > Application Panel > [Global Key](#)

Hotkey (Activation hotkey)

The default Hotkey (Activation key) is **Ctrl+Spc**. The key sequence switches the focus between one application and another. Data entry affects the application running in the foreground only. Note that the system administrator may have assigned a different key sequence to use when switching applications.

Note: You must use an external keyboard with the 12-key version of the Thor VM1 to use the Hotkey. If an external keyboard is not attached, use the Switchpad to switch between applications.

Application Configuration

Settings > Control Panel > Administration icon

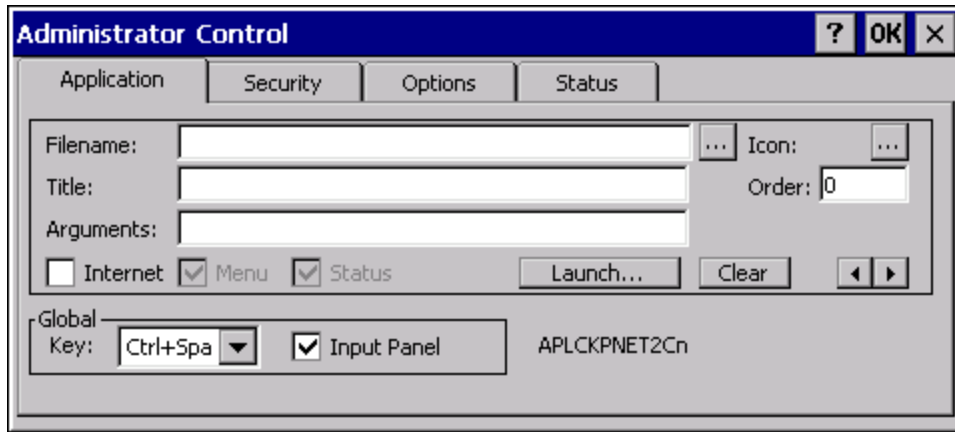
The default Administrator Hotkey sequence is **Shift+Ctrl+A**.

Administrator mode allows access to all features on the device. When the hotkey is pressed to switch into Administrator mode, a password prompt is displayed (if a password has been configured). A password must be entered within 30 seconds (and within three tries) or the password prompt is removed and the device remains in end-user mode with the focus returned to the locked application. Without entry of a valid password, the switch into Administrator mode will not occur.

The password prompt is displayed if a password has been configured. When the valid password is entered, the Administration Control panel is displayed. When a valid password is not entered within 30 seconds, the user is returned to the System Control Panel.

If a password has not been configured, the Administrator Control panel is displayed.

Application Panel



Use the Application tab options to select the applications to launch when the device boots up in End-user Mode.

If no application is specified when the Administrator Control Panel is closed, the mobile device reboots into Administrator mode. If a password has been set, but an application has not been specified, the user will be prompted for the password before entering administration mode. The password prompt remains on the display until a valid password is entered.

Option	Explanation
Filename	Default is blank. Move the cursor to the Filename text box and either type the application path or tap the Browse button (the ... button). The standard Windows CE Browse dialog is displayed. After selecting the application from the Browse dialog, tap OK.
Title	Default is blank. Enter the Title to be associated with the application. The assumption is that multiple copies of the same application may need unique titles in order to differentiate them in the Switchpad .
Arguments	Default is blank. Enter the command line parameters for the application in the Arguments text box.
Order	Default is 1. Enter the Order in which the application is to be loaded or presented to the end-user. Applications are launched in lowest to highest number order and do not need to be sequential.
Internet	Default is Disabled. Enable the Internet checkbox to use the End-user Internet Explorer (EUIE.EXE). When the checkbox is enabled, the Internet Menu and Internet Status are available. See the section titled End-user Internet Explorer (EUIE) for more details.
Launch Button	See following section titled Launch Button . <i>Note: AppLock Administrator Control panel file Launch option does not inter-relate with similarly-named options contained in other Control Panels.</i>
Global Key	Default is Ctrl+Spc. Select the Global Key key sequence the end-user is to press when switching between applications. The Global Key default key sequence must be defined by the AppLock Administrator. The Global key is presented to the end-user as the Activation key.
Global Delay	Default is 10 seconds. Enter the number of seconds that Applications must wait before starting to run after reboot. <i>Note: Delay (Global) may not be available in all versions of AppLock. You can simulate a Global Delay function by setting a delay for the first application (lowest Order) launched and setting the delay to 0 for all other applications. See Boot Options.</i>

Option	Explanation
Input Panel	Default is Disabled. Enable (check) to show the Keyboard option on the Switchpad menu. When enabled the input panel cannot be enabled or disabled for each individual application, and is available to the user for all configured applications.
Clear Button	Tap the Clear button to clear all currently displayed Filename or Application information. The Global settings are not cleared.
Scroll Buttons	Use the left and right scroll buttons to move from application setup screen to application setup screen. The left and right buttons update the information on the screen with the previous or next configured application respectively.

Launch Button

Note: The Launch button may not be available in all versions of Multi-AppLock. Contact [Technical Assistance](#) for and AppLock update availability.

When clicked, displays the Launch options panel for the Filename selected on the Administration panel.

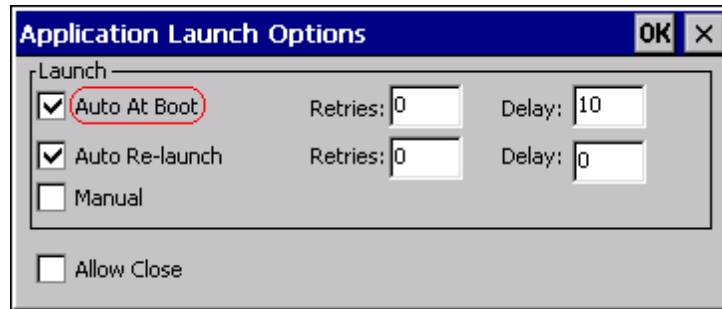
The screenshot shows a dialog box titled "Application Launch Options" with "OK" and "X" buttons in the top right corner. The dialog contains a "Launch" section with the following options:

- Auto At Boot Retries: 0 Delay: 10
- Auto Re-launch Retries: 0 Delay: 0
- Manual

Below the "Launch" section is an Allow Close checkbox.

Note: Launch order is determined by the Order specified in the Application tab. The Order value does not have to be sequential.

Auto At Boot



Default is Enabled.

Auto At Boot

When enabled, automatically launches (subject to the specified Delay in seconds) the application after the unit is rebooted. If a Delay in seconds is specified, AppLock waits for the specified period of time to expire before launching the application. The Delay default value is 10 seconds; valid values are between 0 “no delay” and a maximum of 999 seconds.

Retries

This is the number of times the application launch will be retried if a failure occurs when the application is automatically launched at bootup. Valid values are between 0 (no tries) and 99 tries or -1 for infinite. Infinite tries ends when the application successfully launches. The default is 0 retries.

Delay

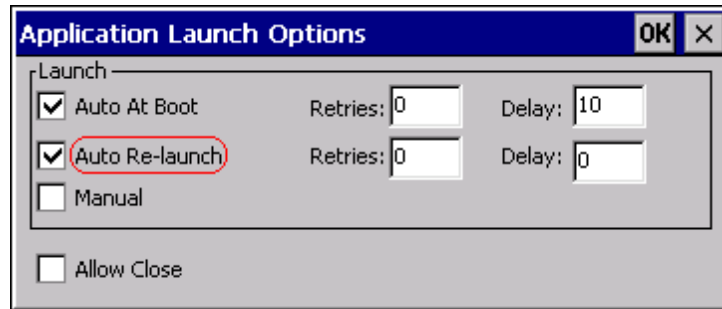
This timer is the time that AppLock waits prior to the initial launch of the selected application when it is automatically launched at bootup. Delay default is 10 seconds. Valid values are between 0 seconds (no delay) and 999 seconds.

The Auto At Boot delay is associated for each application; it will be either a value specified by the Administrator or it will be the delay default value. At startup, when a delay has been assigned for each application, AppLock waits for the delay associated with the first application to expire before launching the first application then AppLock waits for the delay associated with the second application to expire before launching the second application. AppLock continues in this manner until all applications are launched.

Note: A “Global Delay” can be accomplished by setting a timed delay for the first application to be launched (by lowest Order number) and no delay (0 seconds) for all other applications.

Note: Launch order is determined by the Order specified in the Application tab. The Order value does not have to be sequential.

Auto Re-Launch



Auto Re-Launch

Default is Enabled.

When enabled for a specific application, automatically re-launches it (subject to the specified Auto Re-Launch Delay in seconds) after it terminates. This option allows the Administrator to disable the re-launch operation. AppLock cannot prevent all applications from closing. When an application that AppLock cannot prevent from closing terminates, perhaps because of an error condition, AppLock re-launches the application when this option is enabled.

Note: If Allow Close is enabled and both Auto Re-launch and Manual (Launch) are disabled, the application cannot be restarted for the end-user or by the end-user after the application terminates.

Retries

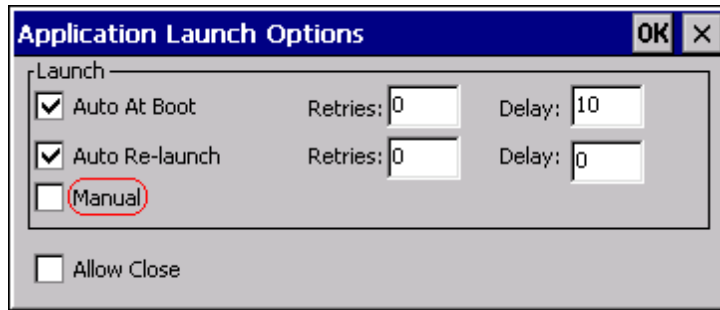
Default is 0 tries. Retries is the number of times AppLock will try to re-launch the application. The retry count is reset after an application is successfully launched and controlled by AppLock. Valid values are between 0 (no tries) and 99 tries or -1 for infinite. Infinite tries ends when the application successfully launches.

Delay

Default is 0 seconds (no delay). Delay is the amount of time AppLock waits prior to re-launching an application that has terminated. The delay is specified in seconds. Valid values are between 0 (no delay) and 99 seconds.

AppLock must also be configured to automatically re-launch an application. To AppLock, application termination by the end-user is indistinguishable from application termination for any other reason.

Manual (Launch)



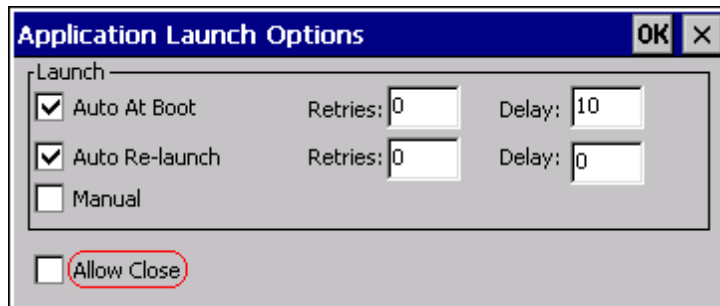
Default is Disabled. Enabling this option allows the end-user to launch the specified application(s). Upon bootup completion an application with Manual enabled is listed on the Switchpad accompanied by a checkmark that indicates the application is currently active or available for Launching. When an application name is tapped by the end-user, the application is launched (if inactive) and brought to the foreground.

Applications set up with Manual (Launch) enabled may or may not be launched at bootup. This function is based on the application's Auto At Boot setting. The applications have been listed as approved applications for end-user manual launch using the Switchpad menu structure. The approved applications are listed on the Switchpad. A checkmark indicates the applications active status.

When Manual (Launch) is disabled for an application, and Allow Close is enabled for the application, when the end-user closes the specific application it is no longer available (shown) on the Switchpad.

When Auto At Boot and Manual (Launch) are both disabled for a specific application, the application is 1) not placed on the list of approved applications for end-user manual launch and 2) never launched, and 3) not displayed on the Switchpad.

Allow Close



Default is Disabled. When enabled, the associated application can be closed by the end-user.

This option allows the administrator to configure applications that consume system resources to be terminated if an error condition occurs or at the end-user's request. Error conditions may generate a topmost popup requiring an end-user response, memory resource issues requiring an end-user response, etc. Also at the administrator's discretion, these types of applications can be started manually (see Manual [Launch]) by the end-user.

End User Internet Explorer (EUIE)

AppLock supports applications that utilize Internet Explorer, such as .HTML pages and JAVA applications. The end user can run an application by entering the application name and path in Internet Explorer's address bar.

To prevent the end user from executing an application using this method, the address bar and Options settings dialog are restricted in Internet Explorer. This is accomplished by creating an Internet Explorer that is used in end user mode: End-user Internet Explorer (EUIE.EXE). The EUIE executes the Internet Explorer application in full screen mode which removes the address bar and status bar. The Options Dialog is also removed so the end user cannot re-enable the address bar.

The administrator specifies the EUIE by checking the Internet checkbox in the Application tab of the Administrator applet. The internet application should then be entered in the Application text box.

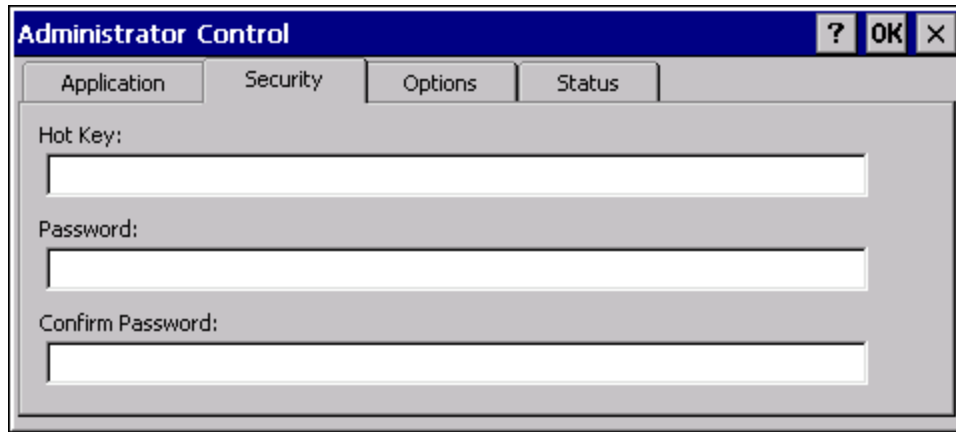
When the Internet checkbox is enabled, the Menu and Status check boxes are available.

Enabling the Menu checkbox displays the EUIE menu which contains navigation functions like Back, Forward, Home, Refresh, etc., functions that are familiar to most Internet Explorer users. When the Menu checkbox is blank, the EUIE menu is not displayed and Navigation functions are unavailable.

When the Status checkbox is enabled, the status bar displayed by EUIE gives feedback to the end-user when they are navigating the Internet.

If the standard Internet Explorer that is shipped with the mobile device is desired, it should be treated like any other application. This means that IEXPLORER.EXE should be specified in the Application text box and the internet application should be entered in the command line. In this case, do not check the Internet checkbox.

Security Panel



Hotkey

Specify the hotkey sequence that triggers AppLock to switch between administrator and user modes and the password required to enter Administrator mode. The default hotkey sequence is **Shift+Ctrl+A**.

A 2nd key keypress is an invalid keypress for a hotkey sequence.

Move the cursor to the Hot Key text box. Enter the new hot key sequence by first pressing the Shift state key followed by a normal key. The hotkey selected must be a key sequence that the application being locked does not use. The hotkey sequence is intercepted by AppLock and is not passed to the application.

Input from the keyboard or Input Panel is accepted with the restriction that the normal key must be pressed from the keyboard when switching modes. The hotkey sequence is displayed in the Hot key text box with "Shift", "Alt", and "Ctrl" text strings representing the shift state keys. The normal keyboard key completes the hotkey sequence. The hotkey must be entered via the keypad. Some hotkeys cannot be entered via the Input Panel. Also, hotkeys entered via the SIP are not guaranteed to work properly when switching operational modes.

For example, if the 'Ctrl' key is pressed followed by 'A', "Ctrl+A" is entered in the text box. If another key is pressed after a normal key press, the hotkey sequence is cleared and a new hotkey sequence is started.

A normal key is required for the hotkey sequence and is unlike pressing the normal key during a mode switch; this key can be entered from the SIP when configuring the key. However, when the hotkey is pressed to switch modes, the normal key must be entered from the keypad; it cannot be entered from the SIP.

Password

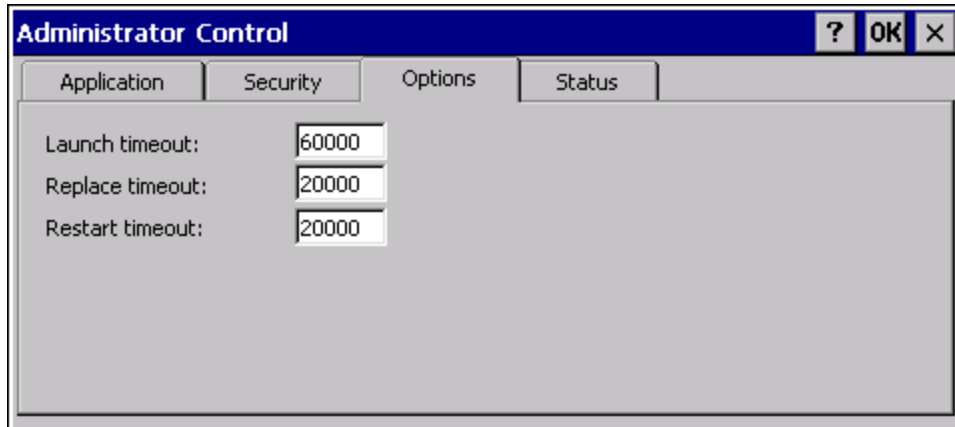
Move the cursor to the Password text box. The passwords entered in the Password and Confirm Password fields must match. Passwords are case sensitive.

When the user exits the Administrator Control panel, the two passwords are compared to verify that they match. If they do not match, a dialog box is displayed notifying the user of the error. After the user closes the dialog box, the Security Panel is displayed and the password can then be entered and confirmed again. If the passwords match, the password is encrypted and saved.

See Also: [Passwords](#) and [AppLock Help](#)

Options Panel

AppLock contains several types of delays and timeouts to accommodate different applications. Please note that the delays specified on the [Launch](#) panel are delays before AppLock attempts to start the specified application(s). The timeouts specified on this panel are delays after AppLock has attempted to launch the application.



Launch timeout

This timeout specifies the period of time for AppLock to wait for the application to initially launch after the application has been called. For example, if the application takes time to launch and then initialize before a display window is created, use this delay to specify the delay period.

Replace timeout

This timeout specifies the period of time for AppLock to wait after an initial screen (like a password prompt screen) is replaced by another application window.

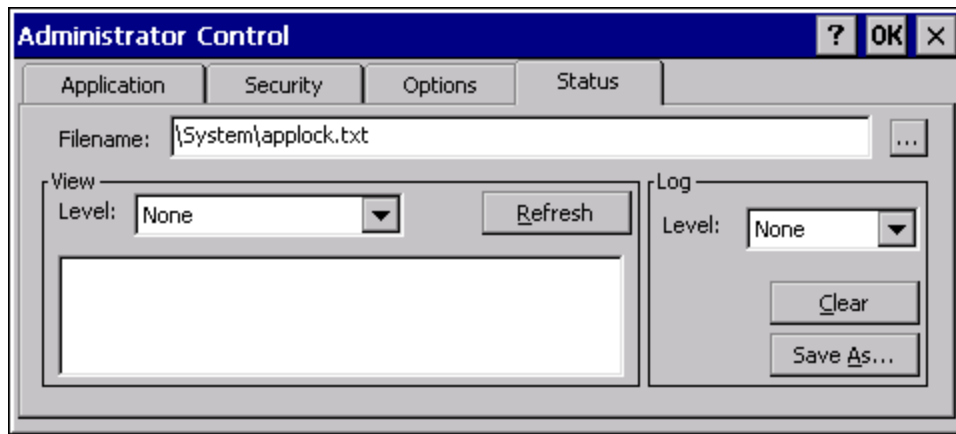
Restart timeout

This specifies the period of time for AppLock to wait for an application to restart. If the application fails to restart automatically, AppLock then proceeds according to the options selected when the application was configured on the [Application](#) and [Launch](#) panels.

Status Panel

Use the Status panel to view the log of previous AppLock operations and to configure which messages are to be recorded during AppLock operation.

Status information is stored in a specific location on the storage device and in a specific logfile specified by the Administrator. For this reason, the administrator can configure the type of status information that is logged, as well as clear the status information.



Move the cursor to the Filename text box and either type the logfile path or tap the Browse button (the ... button). The standard Windows CE Browse dialog is displayed. After selecting the logfile from the Browse dialog, tap OK.

Note: If your Status Panel does not look like the figure shown above, you may have the Single Application version which does not have as many options.

View

Error	Error status messages are logged when an error occurs and is intended to be used by the administrator to determine why the specified application cannot be locked.
Process	Processing status shows the flow control of AppLock components and is mainly intended for Customer Service when helping users troubleshoot problems with their AppLock program.
Extended	Extended status provides more detailed information than that logged by Process Logging.
All	All messages are displayed.

Tap the Refresh button after changing from one view level to another. The filtered records are displayed, all others are not displayed.

Log

Note: If a level higher than *Error* is selected, the status should be cleared frequently by the administrator.

In addition to the three view levels the administrator can select that all status information be logged or turn off all status information logging completely. The system default is 'None'; however to reduce registry use, the administrator may want to select 'None' after verifying the configuration. Tap the Clear button to clear the status information from the registry.

- None
- Error
- Processing
- Extended
- All

Save As

When the 'Save As'... button is selected, a standard 'Save As' dialog screen is displayed. Specify the path and filename. If the filename exists, the user is prompted whether the file should be overwritten. If the file does not exist, it is created.

See Also: [Error Messages](#)

AppLock Help

The mobile device won't switch from Administration mode to end-user mode.

- If the configuration is valid for one application but not the other, the switch to end-user mode fails. AppLock stays in Administration mode and is stopped until the Administrator password is entered.

The hotkey sequence needed is not allowed. What does this mean?

When the Administrator is selecting a hotkey sequence to use when switching user modes, they are not allowed to enter key combinations that are reserved by installed software applications. Only RFTerm key combinations are validated.

When RFTerm is installed on the mobile device and an RFTerm restricted key sequence is specified as a hotkey sequence by the Administrator, the following error message is displayed in a message box:

Selected hotkey is not allowed. Please reenter.

When RFTerm is not installed on the mobile device, the RFTerm keys are not restricted from use.

Can't locate the password that has been set by the administrator?

Contact [Technical Assistance](#) for password help.

AppLock Error Messages

Any messages whose first word is an 'ing' word is output prior to the action described in the message. For example, "Switching to admin-hotkey press" is logged after the administrator has pressed the hotkey but prior to starting the switch process.

For all operations that can result in an error, an Error level message is displayed when a failure occurs. These messages contain the word "failure". These messages have a partner Extended level message that is logged which contains the word "OK" if the action completed successfully rather than with an error.

For processing level messages, "Enter..." is logged at the beginning of the function specified in the message and "Exit..." is logged at the end (just before the return) of the function specified in the message.

Message	Explanation and/or corrective action	Level
Error reading hotkey	The hotkey is read but not required by AppLock.	LOG_EX
Error reading hotkey; using default	A hotkey is required. If there is a failure reading the hotkey, the internal factory default is used.	LOG_ERROR
App Command Line= <Command line>	Command line of the application being locked	LOG_PROCESSING
App= <Application name>	Name of the application being locked	LOG_PROCESSING
dwProcessID= <#>	Device ID of the application being locked	LOG_EX
Encrypt exported key len <#>	Size of encrypt export key	LOG_EX
Encrypt password length= <#>	The length of the encrypted password.	LOG_EX
Encrypted data len <#>	Length of the encrypted password	LOG_EX
hProcess= <#>	Handle of the application being locked	LOG_EX
Key pressed = <#>	A key has been pressed and trapped by the hotkey processing.	LOG_EX

Message	Explanation and/or corrective action	Level
*****	The status information is being saved to a file and the file has been opened successfully.	LOG_EX
Address of keyboard hook procedure failure	AppLock found the kbdhook.dll, but was unable to get the address of the initialization procedure. For some reason the dll is corrupted. Look in the Windows directory for kbdhook.dll. If it exists, delete it. Also delete AppLock.exe from the Windows directory and reboot the unit. Deleting AppLock.exe triggers the AppLock system to reload.	LOG_ERROR
Address of keyboard hook procedure OK	AppLock successfully retrieved the address of the keyboard filter initialization procedure.	LOG_EX
Alt pressed	The Alt key has been pressed and trapped by the HotKey processing.	LOG_EX
Alt	Processing the hotkey and backdoor entry	LOG_EX
Application handle search failure	The application being locked did not complete initialization.	LOG_ERROR
Application handle search OK	The application initialized itself successfully	LOG_ERROR
Application load failure	The application could not be launched by AppLock; the application could not be found or is corrupted.	LOG_ERROR
Backdoor message received	The backdoor keys have been pressed. The backdoor hotkeys provide a method for customer service to get a user back into their system without editing the registry or reloading the device.	LOG_PROCESSING
Cannot find kbdhook.dll	The load of the keyboard filter failed. This occurs when the dll is missing or is corrupted. Look in the Windows directory for kbdhook.dll. If it exists, delete it. Also delete AppLock.exe from the Windows directory and reboot the unit. Deleting AppLock.exe triggers the AppLock system to reload.	LOG_ERROR
Converted Pwd	Converted password from wide to mbs.	LOG_EX
Could not create event EVT_HOTKEYCHG	The keyboard filter uses this event at the Administrator Control panel. The event could not be created.	LOG_ERROR
Could not hook keyboard	If the keyboard cannot be controlled, AppLock cannot process the hotkey. This failure prevents a mode switch into user mode.	LOG_ERROR
Could not start thread HotKeyMon	The keyboard filter must watch for hot key changes. The watch process could not be initiated.	LOG_ERROR
Ctrl after L or X	Processing the backdoor entry.	LOG_EX
Ctrl pressed	The Ctrl key has been pressed and trapped by the HotKey processing.	LOG_EX
Ctrl	Processing the hotkey and backdoor entry.	LOG_EX
Decrypt acquire context failure	Unable to decrypt password.	LOG_ERROR
Decrypt acquired context OK	Decryption process ok.	LOG_EX
Decrypt create hash failure	Unable to decrypt password.	LOG_ERROR
Decrypt created hash OK	Decryption process ok.	LOG_EX
Decrypt failure	Unable to decrypt password.	LOG_ERROR
Decrypt import key failure	Unable to decrypt password.	LOG_ERROR
Decrypt imported key OK	Decryption process ok.	LOG_EX

Message	Explanation and/or corrective action	Level
Encrypt acquire context failure	Unable to encrypt password.	LOG_ERROR
Encrypt acquire encrypt context failure	Unable to encrypt password.	LOG_ERROR
Encrypt acquired encrypt context OK	Encrypt password process successful.	LOG_EX
Encrypt create hash failure	Unable to encrypt password.	LOG_ERROR
Encrypt create key failure	Unable to encrypt password.	LOG_ERROR
Encrypt created encrypt hash OK	Encrypt password process successful.	LOG_EX
Encrypt export key failure	Unable to encrypt password.	LOG_ERROR
Encrypt export key length failure	Unable to encrypt password.	LOG_ERROR
Encrypt exported key OK	Encrypt password process successful.	LOG_EX
Encrypt failure	The password encryption failed.	LOG_ERROR
Encrypt gen key failure	Unable to encrypt password.	LOG_ERROR
Encrypt generate key failure	Unable to encrypt password.	LOG_ERROR
Encrypt get user key failure	Unable to encrypt password.	LOG_ERROR
Encrypt get user key ok	Encrypt password process successful.	LOG_EX
Encrypt hash data failure	Unable to encrypt password.	LOG_ERROR
Encrypt hash data from pwd OK	Encrypt password process successful.	LOG_EX
Encrypt length failure	Unable to encrypt password.	LOG_ERROR
Encrypt out of memory for key	Unable to encrypt password.	LOG_ERROR
Encrypted data OK	The password has been successfully encrypted.	LOG_EX
Enter AppLockEnumWindows	In order for AppLock to control the application being locked so it can prevent the application from exiting, AppLock launches the application and has to wait until it has created and initialized its main window. This message is logged when the function that waits for the application initialization is entered.	LOG_EX
Enter DecryptPwd	Entering the password decryption process.	LOG_PROCESSING
Enter EncryptPwd	Entering the password encryption processing.	LOG_PROCESSING
Enter FullScreenMode	Entering the function that switches the screen mode. In full screen mode, the taskbar is hidden and disabled.	LOG_PROCESSING
Enter GetAppInfo	Processing is at the beginning of the function that retrieves the application information from the registry.	LOG_PROCESSING
Enter password dialog	Entering the password dialog processing.	LOG_PROCESSING

Message	Explanation and/or corrective action	Level
Enter password timeout	Entering the password timeout processing.	LOG_PROCESSING
Enter restart app timer	Some application shut down before AppLock can stop it. In these cases, AppLock gets notification of the exit. When the notification is received, AppLock starts a timer to restart the application. This message logs that the timer has expired and the processing is at the beginning of the timer function.	LOG_PROCESSING
Enter TaskbarScreenMode	Entering the function that switches the screen to non-full screen mode and enable the taskbar.	LOG_PROCESSING
Enter ToAdmin	Entering the function that handles a mode switch into admin mode.	LOG_PROCESSING
Enter ToUser	Entering the function that handles the mode switch to user mode	LOG_PROCESSING
Enter verify password	Entering the password verification processing.	LOG_PROCESSING
Exit AppLockEnumWindows-Found	There are two exit paths from the enumeration function. This message denotes the enumeration function found the application.	LOG_PROCESSING
Exit AppLockEnumWindows-Not found	There are two exit paths from the enumeration function. This message denotes the enumeration function did not find the application.	LOG_PROCESSING
Exit DecryptPwd	Exiting password decryption processing.	LOG_PROCESSING
Exit EncryptPwd	Exiting password encryption processing.	LOG_PROCESSING
Exit FullScreenMode	Exiting the function that switches the screen to full screen.	LOG_PROCESSING
Exit GetAppInfo	Processing is at the end of the function that retrieved the application information from the registry.	LOG_PROCESSING
Exit password dialog	Exiting password prompt processing.	LOG_PROCESSING
Exit password dialog-cancel	Exiting password prompt w/cancel.	LOG_PROCESSING
Exit password dialog-OK	Exiting password prompt successfully.	LOG_PROCESSING
Exit password timeout	Exiting password timeout processing.	LOG_PROCESSING
Exit restart app timer	Processing is at the end of the timer function	LOG_PROCESSING
Exit TaskbarScreenMode	Exiting the function that switches the screen mode back to normal operation for the administrator.	LOG_PROCESSING
Exit ToAdmin	Exiting the function that handles the mode switch into admin mode.	LOG_PROCESSING
Exit ToUser	Exiting the user mode switch function.	LOG_PROCESSING

Message	Explanation and/or corrective action	Level
Exit ToUser-Registry read failure	The AppName value does not exist in the registry so user mode cannot be entered.	LOG_PROCESSING
Exit verify password-no pwd set	Exiting password verification.	LOG_PROCESSING
Exit verify password-response from dialog	Exiting password verification.	LOG_PROCESSING
Found taskbar	The handle to the taskbar has been found so that AppLock can disable it in user mode.	LOG_PROCESSING
Getting address of keyboard hook init procedure	AppLock is retrieving the address of the keyboard hook.	LOG_PROCESSING
Getting configuration from registry	The AppLock configuration is being read from the registry. This occurs at initialization and also at entry into user mode. The registry must be re-read at entry into user mode in case the administration changed the settings of the application being controlled.	LOG_PROCESSING
Getting encrypt pwd length	The length of the encrypted password is being calculated.	LOG_EX
Hook wndproc failure	AppLock is unable to lock the application. This could happen if the application being locked encountered an error after performing its initialization and shut itself down prior to being locked by AppLock.	LOG_ERROR
Hook wndproc of open app failure	The application is open, but AppLock cannot lock it.	LOG_ERROR
Hot key event creation failure	The Admin applet is unable to create the hotkey notification.	LOG_ERROR
Hot key pressed	Processing the hotkey and backdoor entry	LOG_EX
Hot key pressed	Processing the hotkey and backdoor entry	LOG_EX
Hot key set event failure	When the administrator changes the hotkey configuration the hotkey controller must be notified. This notification failed.	LOG_ERROR
Hotkey press message received	The user just pressed the configured hotkey.	LOG_PROCESSING
In app hook:WM_SIZE	In addition to preventing the locked application from exiting, AppLock must also prevent the application from enabling the taskbar and resizing the application's window. This message traps a change in the window size and corrects it.	LOG_EX
In app hook:WM_WINDOWPOSCHANGED	In addition to preventing the locked application from exiting, AppLock must also prevent the application from enabling the taskbar and resizing the application's window. This message traps a change in the window position and corrects it.	LOG_EX
Initializing keyboard hook procedure	AppLock is calling the keyboard hook initialization.	LOG_PROCESSING
Keyboard hook initialization failure	The keyboard filter initialization failed.	LOG_ERROR
Keyboard hook loaded OK	The keyboard hook dll exists and loaded successfully.	LOG_EX
L after Ctrl	Processing the backdoor entry.	LOG_EX
Loading keyboard hook	When AppLock first loads, it loads a dll that contains the keyboard hook processing. This message is logged prior to the load attempt.	LOG_PROCESSING

Message	Explanation and/or corrective action	Level
Open failure	The status information is being saved to a file and the file open has failed. This could occur if the file is write protected. If the file does not exist, it is created.	LOG_ERROR
Open registry failure	If the Administration registry key does not exist, the switch to user mode fails because the AppName value in the Administration key is not available.	LOG_ERROR
Opened status file	The status information is being saved to a file and the file has been opened successfully.	LOG_EX
Out of memory for encrypted pwd	Not enough memory to encrypt the password.	LOG_ERROR
pRealTaskbarWndProc already set	The taskbar control has already been installed.	LOG_EX
Pwd cancelled or invalid-remain in user mode	The password prompt was cancelled by the user or the maximum number of failed attempts to enter a password was exceeded.	LOG_EX
Read registry error-hot key	The hotkey registry entry is missing or empty. This is not considered an error. The keyboard hook uses an embedded default if the value is not set in the registry.	LOG_ERROR
Read registry failure-app name	AppName registry value does not exist or is empty. This constitutes a failure for switching into user mode.	LOG_ERROR
Read registry failure- Cmd Line	AppCommandLine registry entry is missing or empty. This is not considered an error since command line information is not necessary to launch and lock the application.	LOG_ERROR
Read registry failure-Internet	The Internet registry entry is missing or empty. This is not considered an error since the Internet value is not necessary to launch and lock the application.	LOG_ERROR
Registering Backdoor MSG	The AppLock system communicates with the keyboard hook via a user defined message. Both AppLock.exe and Kbdhook.dll register the message at initialization.	LOG_PROCESSING
Registering Hotkey MSG	The AppLock system communicates with the keyboard hook via a user defined message. Both Applock.exe and Kbdhook.dll register the message at initialization.	LOG_PROCESSING
Registry read failure at reenter user mode	The registry has to be read when entering user mode is the AppName is missing. This user mode entry is attempted at boot and after a hotkey switch when the administrator has closed the application being locked or has changed the application name or command line.	LOG_ERROR
Registry read failure at reenter user mode	The registry has to be read when switching into user mode. This is because the administrator can change the settings during administration mode. The read of the registry failed which means the Administration key was not found or the AppName value was missing or empty.	LOG_ERROR
Registry read failure	The registry read failed. The registry information read when this message is logged is the application information. If the Administration key cannot be opened or if the AppName value is missing or empty, this error is logged. The other application information is not required. If the AppName value is not available, AppLock cannot switch into user mode.	LOG_ERROR
Reset system work area failure	The system work area is adjusted when in user mode to cover the taskbar area. The system work area has to be adjusted to exclude the taskbar area in administration mode. AppLock was unable to adjust this area.	LOG_ERROR
Shift pressed	The Shift key has been pressed and trapped by the HotKey processing.	LOG_EX
Shift	Processing the hotkey and backdoor entry	LOG_EX
Show taskbar	The taskbar is now being made visible and enabled.	LOG_PROCESSING

Message	Explanation and/or corrective action	Level
Switching to admin-backdoor	The system is currently in user mode and is now switching to admin mode. The switch occurred because of the backdoor key presses were entered by the administrator.	LOG_PROCESSING
Switching to admin-hotkey press	The system is currently in user mode and is now switching to admin mode. The switch occurred because of a hotkey press by the administrator.	LOG_PROCESSING
Switching to admin-kbdhook.dll not found	The keyboard hook load failed, so AppLock switches to admin mode. If a password is specified, the password prompt is displayed and remains until a valid password is entered.	LOG_PROCESSING
Switching to admin-keyboard hook initialization failure	If the keyboard hook initialization fails, AppLock switches to admin mode. If a password is specified, the password prompt is displayed and remains until a valid password is entered.	LOG_PROCESSING
Switching to admin-registry read failure	See the explanation of the "Registry read failure" above. AppLock is switching into Admin mode. If a password has been configured, the prompt will be displayed and will not be dismissed until a valid password is entered.	LOG_PROCESSING
Switching to TaskbarScreenMode	In administration mode, the taskbar is visible and enabled.	LOG_EX
Switching to user mode	The registry was successfully read and AppLock is starting the process to switch to user mode.	LOG_PROCESSING
Switching to user-hotkey press	The system is currently in admin mode and is now switching to user mode. The switch occurred because of a hotkey press by the administrator.	LOG_PROCESSING
Taskbar hook failure	AppLock is unable to control the taskbar to prevent the locked application from re-enabling it.	LOG_ERROR
Taskbar hook OK	AppLock successfully installed control of the taskbar.	LOG_EX
Timeout looking for app window	After the application is launched, AppLock must wait until the application has initialized itself before proceeding. The application did not start successfully and AppLock has timed out.	LOG_ERROR
ToUser after admin, not at boot	The user mode switch is attempted when the device boots and after the administrator presses the hotkey. The mode switch is being attempted after a hotkey press.	LOG_EX
ToUser after admin-app still open	The switch to user mode is being made via a hotkey press and the administrator has left the application open and has not made any changes in the configuration.	LOG_EX
ToUser after admin-no app or cmd line change	If user mode is being entered via a hotkey press, the administrator may have left the configured application open. If so, AppLock does not launch the application again unless a new application or command line has been specified; otherwise, it just locks it.	LOG_EX
Unable to move desktop	The desktop is moved when switching into user mode. This prevents them from being visible if the application is exited and restarted by the timer. This error does not affect the screen mode switch; processing continues.	LOG_ERROR
Unable to move taskbar	The taskbar is moved when switching into user mode. This prevents them from being visible if the application is exited and restarted by the timer. This error does not affect the screen mode switch; processing continues.	LOG_ERROR
Unhook taskbar wndproc failure	AppLock could not remove its control of the taskbar. This error does not affect AppLock processing	LOG_ERROR
Unhook wndproc failure	AppLock could not remove the hook that allows monitoring of the application.	LOG_ERROR
Unhooking taskbar	In administration mode, the taskbar should return to normal operation, so AppLock's control of the taskbar should be removed.	LOG_EX

Message	Explanation and/or corrective action	Level
Unhooking wndproc	When the administrator leaves user mode, the device is fully operational; therefore, AppLock must stop monitoring the locked application.	LOG_EX
WM_SIZE adjusted	This message denotes that AppLock has readjusted the window size.	LOG_EX
X after Ctrl+L	Processing the backdoor entry.	LOG_EX
Ret from password <#>	Return value from password dialog.	LOG_EX
Decrypt data len <#>	Length of decrypted password.	LOG_EX
Window handle to enumwindows=%x	The window handle that is passed to the enumeration function. This message can be used by engineering with other development tools to trouble shoot application lock failures.	LOG_EX
WM_WINDOWPOSCHG adjusted=%x	Output the window size after it has been adjusted by AppLock	LOG_EX

Battery

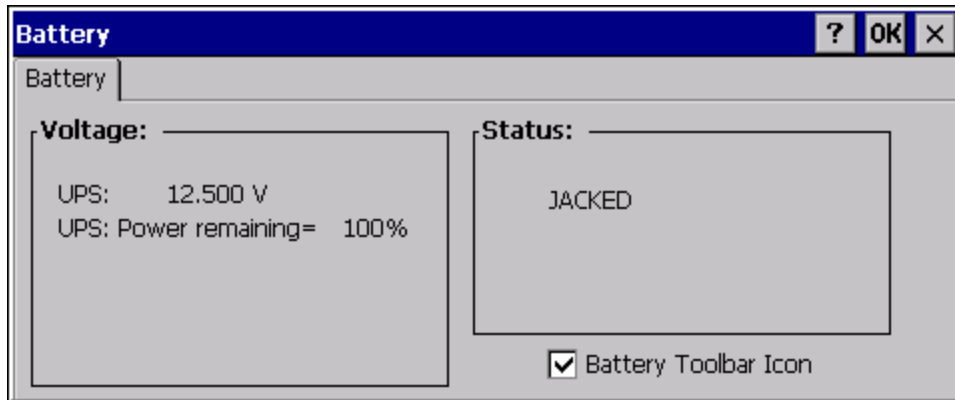
Start > Settings > Control Panel > Battery

This panel is used to view the status and percentage of power remaining in the Thor VM1 UPS battery.

The battery gas gauge icon resides in the system tray and shows four levels of charge – 100%, 75%, 50%, 25%. At a point below 25%, the system status LED will turn red and the gas gauge icon will turn red indicating the battery is low.



The battery gauge icon is enabled by default, but can be disabled on the Thor VM1 Battery control panel. Jacked is shown in the Status box when the UPS battery is receiving external power.



Bluetooth

Start > Settings > Control Panel > Bluetooth

Note: Contact [Technical Assistance](#) for upgrade availability if your Bluetooth control panel is not the same as the control panels presented in this section.

Discover and manage pairing with nearby Bluetooth devices.

Factory Default Settings

Discovered Devices	None
Settings	
Turn Off Bluetooth	Enabled
Computer is connectable	Enabled
Computer is discoverable	Disabled
Prompt if devices request to pair	Enabled
Continuous search	Disabled
Filtered Mode	Enabled
Printer Port on COM 7:	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 Device Name
Reconnect	
Report lost connection	Enabled
Report when reconnected	Disabled
Report failure to reconnect	Enabled
Clear Pairing Table on boot	Disabled
Auto Reconnect on Boot	Enabled
Auto Reconnect	Enabled

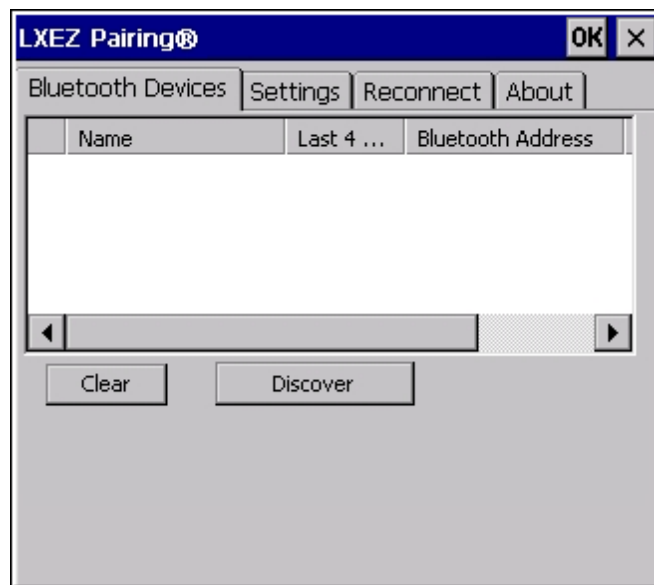
Bluetooth taskbar Icon state and Bluetooth device Icon states change as Bluetooth devices are discovered, paired, connected and disconnected. There may be audible or visual signals as paired devices re-connect with the Thor VM1.

- The default Bluetooth setting is On.
- The Thor VM1 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 VM1 can pair with one Bluetooth scanner and one Bluetooth printer.
- When **Filtered Mode** is disabled, the Thor VM1 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 VM1.
- The target Bluetooth device should be as close as possible (up to 32.8 ft (10 meters) Line of Sight) to the Thor VM1 during the pairing process.

Assumption: The System Administrator has Discovered and Paired targeted Bluetooth devices for the Thor VM1. The Thor VM1 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 VM1.



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.

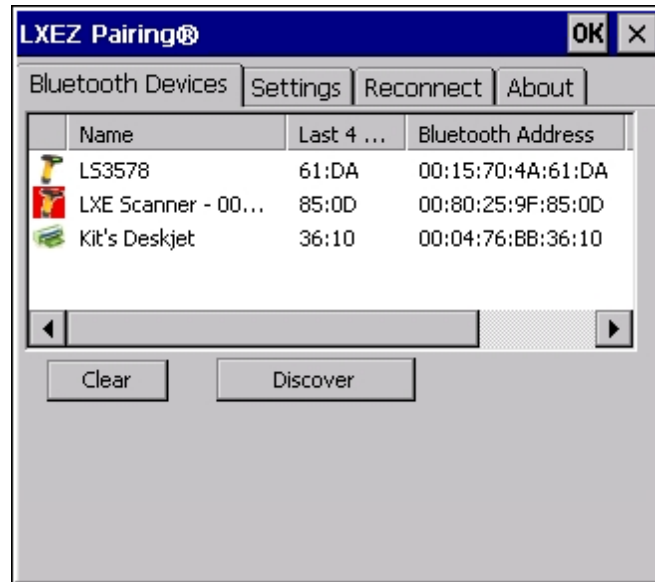


Stop Button

Tap Stop at any time to end the Discover and Query for Unique Identifier functions. Devices not paired are not shown after any reboot sequence.

Note: When an active paired device enters Suspend Mode, is turned Off or leaves the Thor VM1 Bluetooth scanning range, the Bluetooth connection between the paired device and the Thor VM1 is lost. There may be audible or visual signals as paired devices disconnect from the Thor VM1.

Bluetooth Device List



The discovered paired devices may or may not be identified with an icon. Discovered devices without an icon can be paired as a Scanner or a Printer. 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 VM1 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? Yes/No". Tap the Yes button to remove disconnected or deleted devices from the device table. The devices are removed from the Device table after any reboot sequence or after closing and reopening the Bluetooth panels. Tap the No button to make no changes. See [Clear Pairing Table on Boot](#).

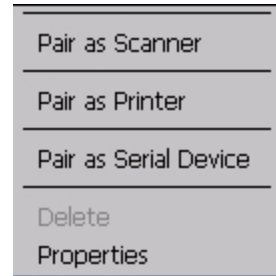
Bluetooth Device Menu

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. The Bluetooth device does not need to be active.



Filtered Mode Enabled

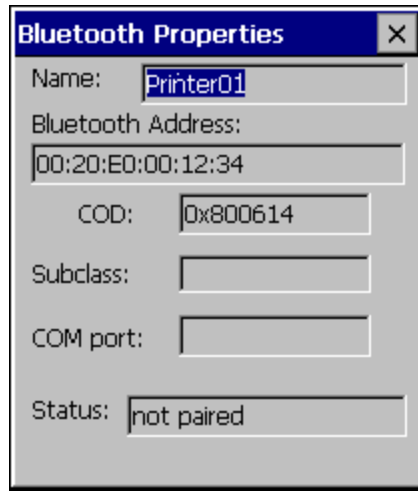


Filtered Mode Disabled

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.
Pair as Serial Device	Communicate with the highlighted serial Bluetooth device. This option is available when Filtered Mode is disabled.
Disconnect	Stop the connection between the Thor VM1 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 VM1 Bluetooth Devices panel after the user taps OK.
Properties	More information on the highlighted Bluetooth device.

Bluetooth Device Properties



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

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

Settings



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

Turn Off Bluetooth

Tap the button to toggle the Bluetooth client On or Off. The button title changes from *Turn Off Bluetooth* to *Turn On Bluetooth*.

Default

The default value is Bluetooth On.

Options

Option	Function
Computer is connectable	This option is Enabled by default. Disable this option to inhibit Thor VM1 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 VM1.
Prompt if devices request to pair	This option is Enabled by default. A dialog box appears on the Thor VM1 screen notifying the user a Bluetooth device requests to pair with the Thor VM1. The requesting Bluetooth device does not need to have been Discovered by the Thor VM1 before the pairing request is received. Tap the Accept button or the Decline button to remove the dialog box from the screen. <i>Note: 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.</i>
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 VM1 stops searching after 30 minutes. This option draws power from the Main Battery.
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 VM1 can pair with up to four Bluetooth devices. A Warmboot is required every time Filtered Mode is toggled on and off.
Printer Port - COM7	This option is Disabled by default. This option assigns Bluetooth printer connection to COM7 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 VM1 creates <i>bt_log.txt</i> and stores it in the /System folder. Bluetooth activity logging is added to the text file as activity progresses. A <i>bt_log_bak.txt</i> file contains the data stored by <i>bt_log.txt</i> prior to reboot. During a reboot process, the Thor VM1 renames <i>bt_log.txt</i> to <i>bt_log_bak.txt</i> . If a file already exists with that name, the existing file is deleted, the new <i>bt_log_bak.txt</i> file is added and a new <i>bt_log.txt</i> is created.
Computer Friendly Name	Default: Computer System Name (System Panel > Device Name tab). The name, or identifier, entered in this space by the System Administrator is used exclusively by Bluetooth devices and during Bluetooth communication.

Reconnect



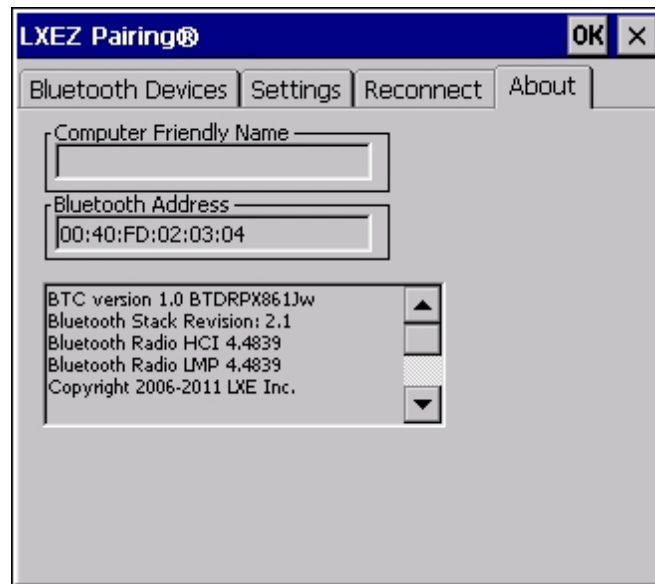
Note: These options can still be checked or unchecked whether Bluetooth connection is enabled or disabled.

Options

Option	Function
Report when connection lost	<p>This option is Enabled (checked) by default.</p> <p>There may be an audio or visual signal when a connection between a paired, active device is lost.</p> <p>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.</p>
Report when reconnected	<p>This option is Disabled (unchecked) by default.</p> <p>There may be an audio or visual signal when a connection between a paired, active device is made.</p> <p>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.</p>
Report failure to reconnect	<p>This option is Enabled (checked) by default.</p> <p>The default time delay is 30 minutes. This value cannot be changed by the user.</p> <p>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.</p> <p>Tap the X button or ok button to close the dialog box.</p> <p>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.</p>
Clear Pairing Table on Boot	<p>This option is Disabled (unchecked) by default.</p> <p>When enabled (checked), all previous paired information is deleted upon any reboot sequence and no devices are reconnected.</p> <p>When enabled (checked) "Auto Reconnect on Boot" is automatically disabled (dimmed).</p>
Auto Reconnect on Boot	<p>This option is Enabled (checked) by default. All previously paired devices are reconnected upon any reboot sequence.</p> <p>When disabled (unchecked), no devices are reconnected upon any reboot sequence.</p>

Option	Function
Auto Reconnect	<p>This option is Enabled (checked) by default. This option controls the overall mobile Bluetooth device reconnect behavior.</p> <ul style="list-style-type: none"> • When Auto Reconnect is disabled (unchecked), <i>Auto Reconnect on Boot</i> is automatically disabled and dimmed. • When Auto Reconnect is disabled (unchecked), no devices are reconnected in any situation. The status of <i>Auto Reconnect on Boot</i> is ignored and no devices are reconnected on boot. The status of <i>Clear Pairing Table on Boot</i> controls whether the pairing table is populated on boot. • When Auto Reconnect is enabled (checked) and <i>Auto Reconnect on Boot</i> 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 <i>Clear Pairing Table on Boot</i> 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 <i>Auto Reconnect on Boot</i> is ignored and the option is automatically disabled (unchecked) and dimmed.

About



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

Using Bluetooth

Start > Settings > Control Panel > Bluetooth or Bluetooth icon in taskbar or Bluetooth icon on desktop



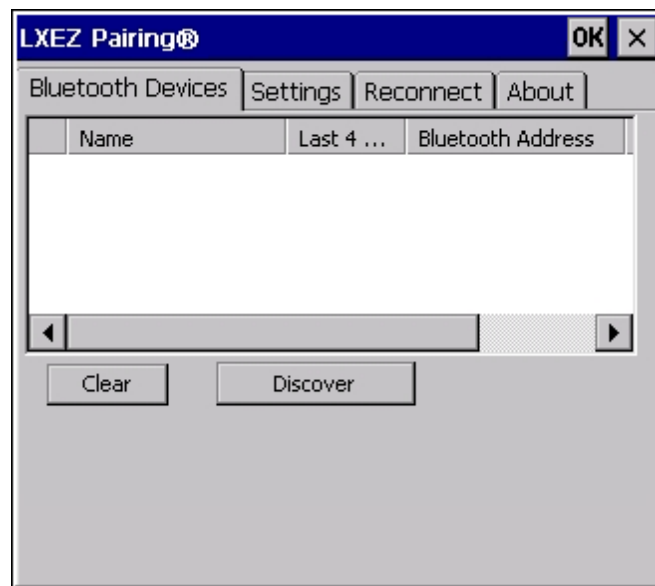
Bluetooth taskbar icon

The Thor VM1 default Bluetooth setting is Enabled.

The Thor VM1 Bluetooth® module is designed to Discover and pair with nearby Bluetooth devices.

Prerequisite: The 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 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 > Settings > Control Panel > Bluetooth** or tap the Bluetooth icon in the taskbar or on the desktop.
2. Tap the **Settings** Tab.
3. Change the **Computer Friendly Name** at the bottom of the Settings display. The Bluetooth Thor VM1 default name is determined by the factory installed software version. A unique name (up to 32 characters) should be assigned to every Thor VM1 before Bluetooth Discovery is initiated.
4. Check or uncheck the Thor VM1 Bluetooth options on the **Settings** and **Reconnect** tabs.
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 LXEZ Pair 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 VM1 to receive scanner data.
7. Tap **Pair as Printer** to set up the Thor VM1 to send data to the printer.
8. Tap **Serial Device** (when Filtered mode is disabled) to set up the Thor VM1 to communicate with a Bluetooth serial device.
9. Tap **Disconnect** to stop pairing with the device. Once disconnected, tap **Delete** to remove the device name and data from the Thor VM1 Bluetooth Devices list. The device is deleted from the list after the OK button is clicked.
10. 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 VM1 display.
11. Whenever the Thor VM1 is turned On, all previously paired, live, Bluetooth devices in the vicinity are paired, one at a time, with the Thor VM1. If the devices cannot connect to the Thor VM1 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

There may be audible or visual signals as paired devices re-connect with the Thor VM1.

Only printers or scanners are recognized and displayed in the Bluetooth panel. All other Bluetooth devices are ignored.

Taskbar Icon	Legend
	Thor VM1 is connected to one or more of the targeted Bluetooth device(s).
	Thor VM1 is not connected to any Bluetooth device. Thor VM1 is ready to connect with any Bluetooth device. Thor VM1 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 VM1 Bluetooth scan range, the Bluetooth connection between the paired device and the Thor VM1 is lost. There may be audible or visual signals as paired devices disconnect from the Thor VM1.

160;

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 VM1.

AppLock, if installed, does not stop the end-user from using Bluetooth applications, nor does it stop authorized Bluetooth-enabled devices from pairing with the Thor VM1 while AppLock is in control.

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.

Several different types of bar code readers are supported. This section describes the interaction and setup for a mobile Bluetooth laser scanner or laser imager connected to the Thor VM1 using Bluetooth functions.

Prerequisites

- The Thor VM1 has the Bluetooth hardware and software installed. An operating system upgrade may be required. Contact [Technical Assistance](#) for details.
- If the Thor VM1 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 VM1 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 LXEZ Pair program, tap **Start > Settings > 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 VM1. The label is the Bluetooth address identifier for the Thor VM1.

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

Important: The Thor VM1 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 VM1 with Label

If the Thor VM1 has a Bluetooth address bar code label attached, follow these steps:

1. Scan the Bluetooth address bar code label, attached to the Thor VM1, with the Bluetooth mobile scanner.
2. If this is the first time the Bluetooth scanner has scanned the Thor VM1 Bluetooth label, the devices are paired. See section titled "[Bluetooth Beep and LED Indications](#)". If the devices do not pair successfully, go to the next step.
3. Open the LXEZ Pair panel (Start > Settings > 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 VM1 with the Bluetooth mobile scanner.

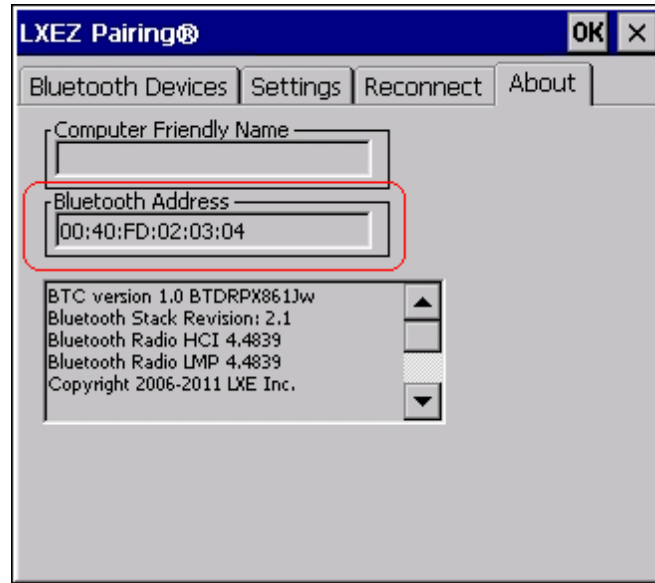
The devices are paired. The Bluetooth bar code reader responds with a series of beeps and an LED flashes. Refer to the following section titled "[Bluetooth Beep and LED Indications](#)".

Note: After scanning the Thor VM1 Bluetooth label, if there is no beep and no LED flash from the Bluetooth device, the devices are currently paired.

Thor VM1 without Label

If the Thor VM1 Bluetooth address bar code label does not exist, follow these steps to create a unique Bluetooth address bar code for the Thor VM1:

First, locate the Thor VM1 Bluetooth address by tapping Start > Settings > Control Panel > Bluetooth > About tab.



Next, [create](#)¹ a Bluetooth address bar code label for the Thor VM1.

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 VM1 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 VM1 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](#)"

¹Free 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 scanner sounds a long tone, this means the scanner has not passed its automatic Selftest and has entered isolation mode. If the scanner is reset, the sequence is repeated. Contact [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 VM1 during the pairing process.

1. Open the LXEZ Pair 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 VM1 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 VM1 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. [See Also: "Reconnect"](#)

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

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

AppLock, if installed, does not stop the end-user from using the Bluetooth application, nor does it stop other Bluetooth-enabled devices from pairing with the Thor VM1 while AppLock is in control.

Certificates

Start > Settings > Control Panel > Certificates

Manage digital certificates used for secure communication.

Note: Digital certificates are date sensitive. If the date on the Thor VM1 is incorrect, wireless authentication will fail.



The Certificates stores tab lists the certificates trusted by the Thor VM1 user.

These values may change based on the type of network security resident in the client, access point or the host system.

Tap the **Import** button to import a digital certificate file.

Tap the **View** button to view a highlighted digital certificate.

Tap the **Remove** button to remove highlighted certificate files.

Tap the ? button and follow the instructions in the Windows CE Help file when working with trusted authorities and digital certificates.

Data Collection Wedge Introduction

Start > Settings > Control Panel > Data Collection

This software component is the interface between data collection devices such as bar code scanners, or imagers, externally connected to a COM port on the Thor VM1 or bar code scanners wirelessly connected via Bluetooth to your Thor VM1. This software component collects the data from the varied sources and presents it to applications on your Thor VM1 in a transparent manner.

Note: When a HID enabled USB scanner is connected to the Thor VM1 the scanned data is transmitted to the active window as keystroke messages. The data bypasses the data collection wedge. Any data handling to be applied to the scanned data, for example strip leading or trailing characters, must be programmed into the scan engine via configuration bar codes or handled by the application accepting the data.

Use the options on the control panels to set Thor VM1 data collection keyboard wedge parameters, enable or disable allowed symbologies and assign scan key settings.

Assign baud rate, parity, stop bits and data bits for available COM ports.

Parameters on the Main tab and the COM tab(s) apply to this device only.

Bar code manipulation parameter settings on the [Data Options tab](#) are applied to the incoming data resulting from successful bar code scans received by the Thor VM1 for processing. The successful bar code scan data may be sent by

- a wireless Bluetooth Handheld Scanner,
- or a tethered serial scanner.

Bar Code Readers

The Thor VM1 can use the following external bar code readers:

- Tethered hand-held scanners are tethered to a [serial port](#) or a USB host port on the Thor VM1 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.

Return to Factory Default Settings

After scanning the engine-specific bar code to return the scanner/imager to factory default settings, the next step is to open the bar code wedge panel on the mobile device collecting the scanned data. Click the OK button to close the panel. This action will synchronize all scanner formats for your device.

Data Processing Overview

Bar code data processing involves several steps. Some steps may be skipped during the processing depending on user selections on the Data Options control panels. The steps are presented below in the order they are performed on the scanned data.

1. Scanned data is tested for a **code ID** and length (Min/Max). If it matches, it is processed per the rules in place for that symbology. If the scan does not meet the criteria for that symbology, it is processed based on the settings for All. If a code ID is not found, the bar code data is processed based on the settings for All.
 2. If the symbology is **disabled**, the scan is rejected.
 3. Strip **leading** data bytes unconditionally.
 4. Strip **trailing** data bytes unconditionally.
 5. Parse for, and strip if found, **Data Options** strings.
 6. Replace any **control characters** with string, as configured.
 7. Add **prefix** string to output buffer.
 8. If **Code ID** is *not* stripped, add saved **code ID** from above to output buffer.
 9. Add processed **data string** from above to output buffer.
 10. Add **suffix string** to output buffer.
 11. Add a terminating **NUL** to the output buffer, in case the data is processed as a string.
 12. If key output is enabled, start the process to output keys. If control characters are encountered:
 - If Translate All is set, key is translated to CTRL + char, and output.
 - If Translate All is not set, and key has a valid VK code, key is output.
 - Otherwise, key is ignored (not output).
 13. If key output is disabled, a windows message is broadcast to notify listening applications that data is available.
- The manipulated data is ready to be read by applications.

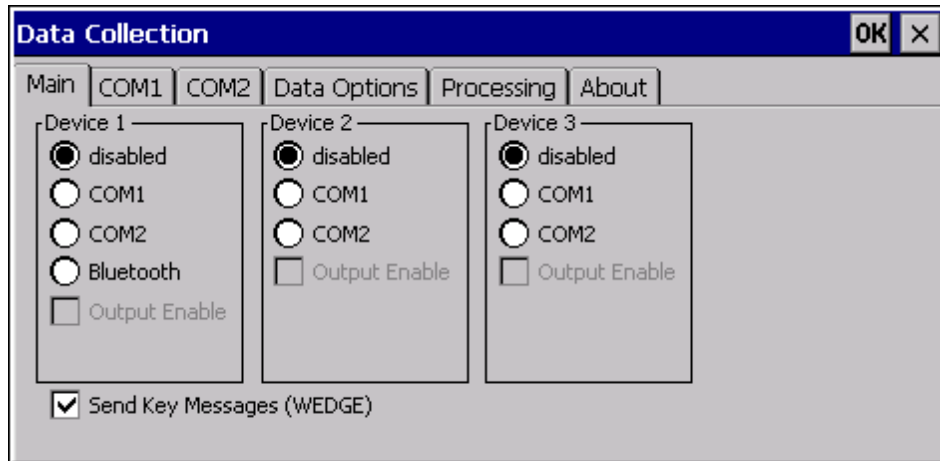
Factory Default Settings

Main Tab	
Device 1	Disabled
Device 2	Disabled
Device 3	Disabled
Send Key Message (WEDGE)	Enabled
COM1 Tab (External serial port)	
Baud Rate	9600
Stop Bits	1
Parity	None
Data Bits	8
Power on Pin 9	Enabled
COM2 Tab (External serial port)	
Baud Rate	9600
Stop Bits	1
Parity	None
Data Bits	8
Power on Pin 9	Enabled
Data Options Tab	
Enable Code ID	None
Symbology Settings	All
Control Character Translate All	Disabled
Custom IDs	Name blank
Processing Tab	
Enable buffered key output	Enabled
Same buffer limit	32
Delay between buffers	75 ms

Main Tab

Start > Settings > Control Panel > Data Collection > Main tab

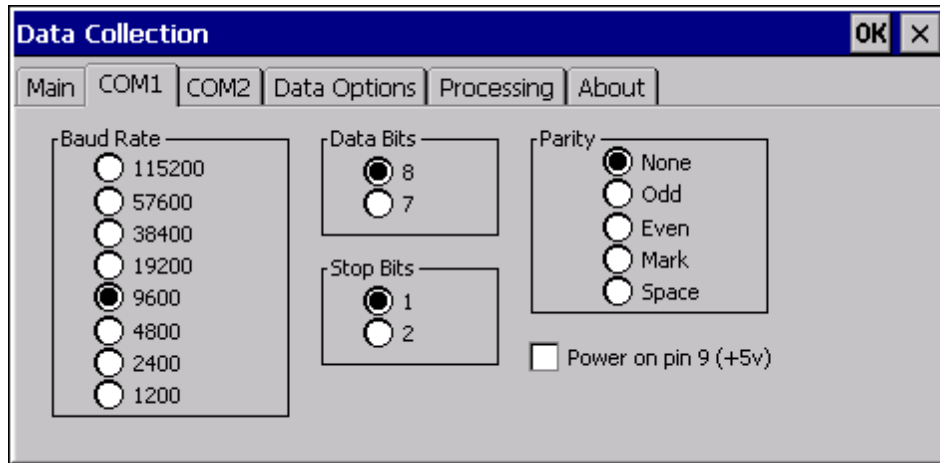
The parameters shown on these panels are only those that apply to the specific mobile device.



Parameter	Function
Device 1,2,3	1 - Default is Disabled 2 - Default is Disabled 3 - Default is Disabled The data collection device (laser scanner, laser imager, external, or wireless).
Send Key Messages (WEDGE)	Default: Enabled. When Send Key Messages (WEDGE) is checked any data collection scan is converted to keystrokes and sent to the active window. When this checkbox is not checked, the application will need to use the set of Scanner APIs to retrieve the data from the scanner driver. Note that this latter method is significantly faster than using Wedge.

COM1 Tab

Start > Settings > Control Panel > Data Collection > COM1



This panel sets communication parameters for any device connected to the external port.

Adjust the settings and click the OK button to save the changes. Any changes take effect immediately.

This panel does not configure the connected device. Please refer to the documentation for the external connected or wireless device for information on configuring the device.

Note: COM default values are restored after a cold boot or operating system upgrade. COM1 supports 5V switchable power on Pin 9 for tethered scanners.

Power on Pin 9

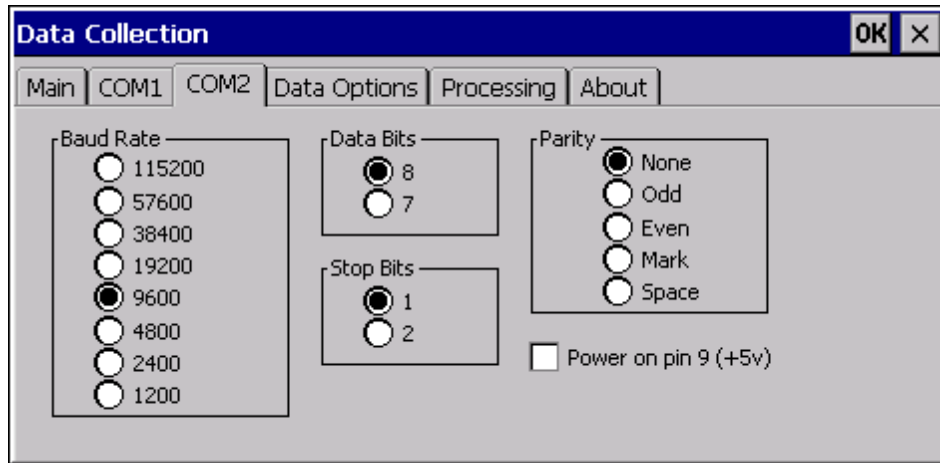
To configure the COM port to supply power to an external scanner tethered to the COM1 port, check the checkbox for Power on Pin 9 (+5V). The default is On (enabled).

The tethered external scanner is powered by the external device power source.

Wireless external scanners use their own power source.

COM2 Tab

Start > Settings > Control Panel > Data Collection > COM2



This panel sets communication parameters for any device connected to the external port.

Adjust the settings and click the OK button to save the changes. Any changes take effect immediately.

This panel does not configure the connected device. Please refer to the documentation for the external connected or wireless device for information on configuring the device.

Note: COM default values are restored after a cold boot or operating system upgrade. COM2 supports 5V switchable power on Pin 9 for tethered scanners.

Power on Pin 9

To configure the COM port to supply power to an external scanner tethered to the COM2 port, check the checkbox for Power on Pin 9 (+5V). The default is On (enabled).

The tethered external scanner is powered by the external device power source.

Wireless external scanners use their own power source.

Data Options Tab

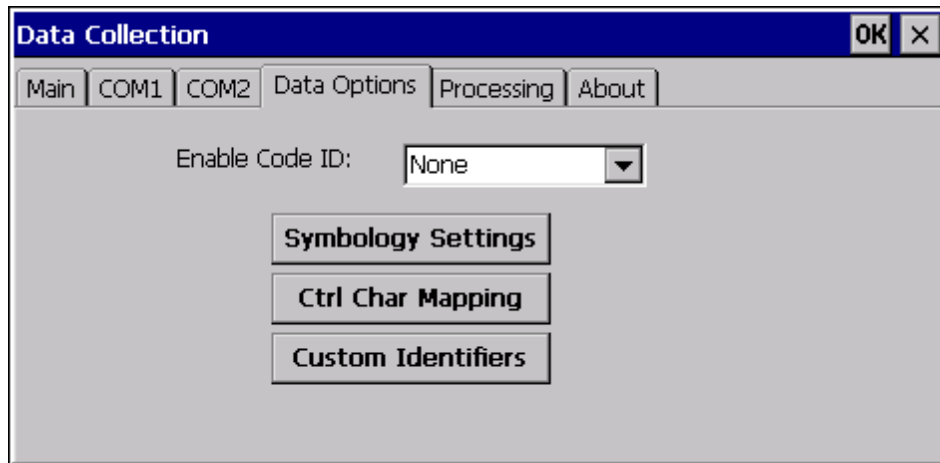
Start > Settings > Control Panel > Data Collection > Data Options tab

Bar code manipulation parameter settings on this tab are applied to the incoming data resulting from successful bar code scans sent to the Thor VM1 for processing.

Note: The Data Options tab contains only those options available for one type of decoding engine.

The Data Options tab contains several options to control bar code processing. Options include:

- Defining custom Code IDs
- Disable processing of specified bar code symbologies
- Rejecting bar code data that is too short or too long
- Stripping characters including Code ID, leading or trailing characters and specified bar code data strings
- Replacing control characters
- Adding a prefix and a suffix.



Enable Code ID

Choose an option in the Enable Code ID drop-down box:

None	Disables transmission of a Code ID. The only entry in the Symbology combo box is All .
Custom ID	Does not change the scanner's Code ID transmission setting. The combo box in the Symbology control panel is populated with any configured Custom code IDs.

Buttons

Symbology Settings	Individually enable or disable a bar code from being scanned, set the minimum and maximum size bar code to accept, strip Code ID, strip data from the beginning or end of a bar code, or (based on configurable Bar Code Data) add a prefix or suffix to a bar code before transmission.
Ctrl Char Mapping	Define the operations the Wedge performs on control characters (values less than 0x20) embedded in bar codes.
Custom Identifiers	Defines an identifier that is at the beginning of bar code data which acts as a Code ID. After a Custom Identifier is defined, Symbology Settings can be defined for the identifier just like standard Code IDs.

See Also: ["Data Processing Overview"](#)

Data Options - Symbology Settings

Start > Settings > Control Panel > Data Collection > Data Options > Symbology Settings button

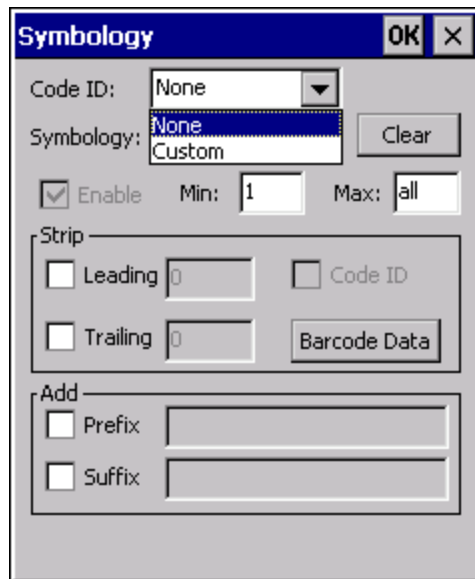
The Symbology selected in the Symbology drop-down list defines the symbology for which the data is being configured. The features available on the Symbology panel include the ability to

- individually enable or disable a bar code from scanning,
- set the minimum and maximum size bar code to accept,
- strip Code ID,
- strip data from the beginning or end of a bar code,
- or (based on configurable Bar Code Data) add a prefix or suffix to a bar code.

The Code ID drop-down box only filters the available symbologies in the Symbology drop down box by the selected Code ID. This Code ID box does not enable or disable the Code ID as that function is controlled by the Enable Code ID box on the Data Options tab.

The Symbology drop-down box contains all symbologies supported based on the Code ID selected above. An asterisk appears in front of symbologies that have already been configured or have been modified from the default value.

Each time a Symbology is changed, the settings are saved as soon as the ok button is tapped. Settings are also saved when a new Symbology is selected from the Symbology drop-down list.



The screenshot shows a dialog box titled "Symbology" with an "OK" button and a close "X" button. It contains the following fields and controls:

- Code ID:** A dropdown menu currently set to "None".
- Symbology:** A dropdown menu with "None" selected and "Custom" visible below it. A "Clear" button is to its right.
- Enable:** A checked checkbox.
- Min:** A text input field containing "1".
- Max:** A text input field containing "all".
- Strip:** A section containing:
 - Leading:** A checkbox (unchecked) and a text input field containing "0".
 - Trailing:** A checkbox (unchecked) and a text input field containing "0".
 - Code ID:** A checkbox (unchecked).
 - Barcode Data:** A button.
- Add:** A section containing:
 - Prefix:** A checkbox (unchecked) and a text input field.
 - Suffix:** A checkbox (unchecked) and a text input field.

The order in which these settings are processed are:

- Min / Max
- Code ID
- Leading / Trailing
- Bar Code Data
- Prefix / Suffix

*Note: When **Enable Code ID** is set to **None** on the Data Options tab and when **All** is selected in the Symbology field, **Enable** and **Strip Code ID** on the Symbology panel are grayed and the user is not allowed to change them, to prevent deactivating the scanner completely.*

When **All** is selected in the Symbology field and the settings are changed, the settings in this dialog become the defaults, used unless overwritten by the settings for individual symbologies. This is also true for Custom IDs, where the code IDs to be stripped are specified by the user.

*Note: In Custom mode on the Data Options tab, any Code IDs **not** specified by the user will not be stripped, because they will not be recognized as Code IDs.*

If a specific symbology's settings have been configured, a star (*) will appear next to it in the Symbology drop-down box, so the user can tell which symbologies have been modified from their defaults.

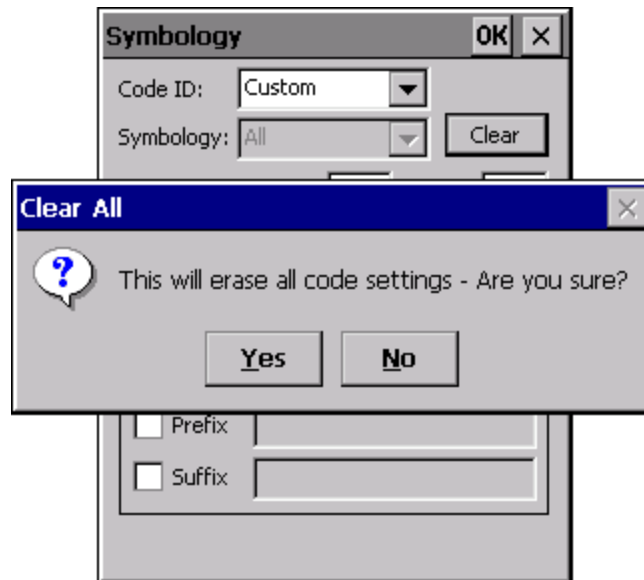
If a particular symbology has been configured, the entire set of parameters from that symbologies screen are in effect for that symbology. In other words, either the settings for the configured symbology will be used, or the default settings are used, not a combination of the two.

If a symbology has not been configured (does not have an * next to it) the settings for **All** are used which is not necessarily the default.

Clear Button

Clicking this button will erase any programmed overrides, returning to the default settings for the selected symbology.

If **Clear** is pressed when **All** is selected as the symbology, a confirmation dialog appears:



then all symbologies are reset to their factory defaults, and all star (*) indications are removed from the list of Symbologies.

Click the Yes button or the No button.

Enable, Min, Max

Enable

This checkbox enables (checked) or disables (unchecked) the symbology field.

The scanner driver searches the beginning of the bar code data for the type of ID specified in the Data Options tab -- Enable Code ID field plus any custom identifiers.

When a code ID match is found as the scanner driver processes incoming bar code data, if the symbology is disabled, the bar code is rejected. Otherwise, the other settings in the dialog are applied and the bar code is processed.

If the symbology is disabled, all other fields on this dialog are dimmed.

If there *are customized settings*, uncheck the Enable checkbox for the All symbology. This results in disabling all symbologies *except* the customized ones.

Min

This field specifies the minimum length that the bar code data (not including Code ID) must meet to be processed.

Any bar code scanned that is less than the number of characters specified in the Min field is rejected. The default for this field is 1.

Max

This field specifies the maximum length that the bar code data (not including Code ID) can be processed. Any bar code scanned that has more characters than specified in the Max field is rejected. The default for this field is All (9999).

If the value entered is greater than the maximum value allowed for that symbology, the maximum valid length is used instead.

Strip Leading/Trailing Control

Start > Settings > Control Panel > Data Collection > Data Options tab > Symbology button

This group of controls determines what data is removed from the collected data before the data is buffered for the application. When all values are set, Code ID takes precedence over Leading and Trailing; Bar Code Data stripping is performed last. Stripping occurs before the Prefix and Suffix are added, so does not affect them.



The screenshot shows a control panel titled "Strip". It contains four controls: a checkbox for "Leading" with a numeric input field set to "0", a checkbox for "Trailing" with a numeric input field set to "0", a checkbox for "Code ID", and a button labeled "Barcode Data".

If the total number of characters being stripped is greater than the number of characters in the collected data, it becomes a zero byte data string.

If, in addition, Strip Code ID is enabled, and no prefix or suffix is configured, the processing will return a zero-byte data packet, which will be rejected.

The operation of each type of stripping is defined below:

Leading

This strips the number of characters specified from the beginning of the collected data (not including Code ID). The data is stripped unconditionally. This action is disabled by default.

Trailing

This strips the number of characters specified from the end of the collected data (not including Code ID). The data is stripped unconditionally. This action is disabled by default.

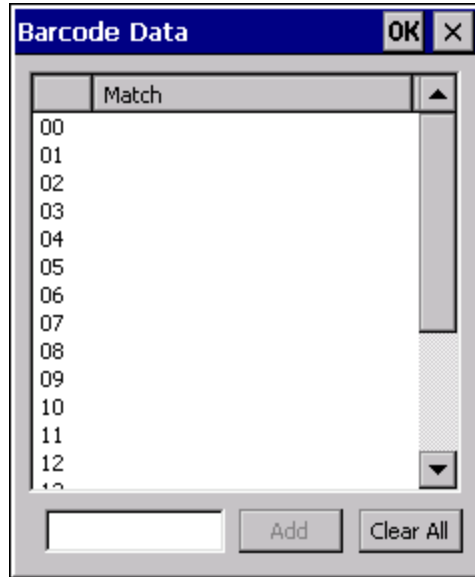
Code ID

Strips the Code ID based on the type code ID specified in the Enable Code ID field in the Data Options tab. By default, Code ID stripping is enabled for every symbology (meaning code IDs will be stripped, unless specifically configured otherwise).

Bar Code Data Match List

Bar Code Data Panel

This panel is used to strip data that matches the entry in the Match list from the bar code. Enter the data to be stripped in the text box and tap the Insert or Add button. The entry is added to the Match list.



To remove an entry from the Match list, highlight the entry in the list and click the Remove button. Click the OK button to store any additions, deletions or changes.

Bar Code Data Match Edit Buttons

Add	Entering data into the text entry box enables the Add button. Click the Add button and the data is added to the next empty location in the Custom ID list.
Insert	Click on an empty line in the Custom ID list. The Add button changes to Insert . Enter data into both the Name and ID Code fields and click the Insert button. The data is added to the selected line in the Custom IDs list.
Edit	Double-click on the item to edit. Its values are copied to the text boxes for editing. The Add button changes to Replace . When Replace is clicked, the values for the current item in the list are updated.
Clear All	When no item in the Custom IDs list is selected, clicking the Clear All button clears the Custom ID list and any text written (and not yet added or inserted) in the Name and ID Code text boxes.
Remove	The Clear All button changes to a Remove button when an item in the Custom IDs list is selected. Click the desired line item and then click the Remove button to delete it. Line items are Removed one at a time. Contents of the text box fields are cleared at the same time.

Notes

-
- **Prefix** and **Suffix** data is always added on after stripping is complete, and is not affected by any stripping settings.
 - If the stripping configuration results in a 0 length bar code, a good beep will still be emitted, since bar code data was read from the scanner.

Match List Rules

The data in the match list is processed by the rules listed below:

- Strings in the list will be searched in the order they appear in the list. If the list contains **ABC** and **AB**, in that order, incoming data with **ABC** will match first, and the **AB** will have no effect.
- When a match between the first characters of the bar code and a string from the list is found, that string is stripped from the bar code data.
- Processing the list terminates when a match is found or when the end of the list is reached.
- If the wildcard * is not specified, the string is assumed to strip from the beginning of the bar code data. The string **ABC*** strips off the prefix **ABC**. The string ***XYZ** will strip off the suffix **XYZ**. The string **ABC*XYZ** will strip both prefix and suffix together. More than one * in a configuration string is not allowed. (The User Interface will not prevent it, but results would not be as expected, as only the first * is used in parsing to match the string.)
- The question mark wildcard ? may be used to match any single character in the incoming data. For example, the data **AB?D** will match **ABCD**, **ABcD**, or **AB0D**, but not **ABDE**.
- The data collected is saved per symbology configured. The Symbology selected in the Symbologies dialog defines the symbology for which the data is being configured.
- Note that the Code ID (if any are configured) is ignored by this dialog, regardless of the setting of **Strip: Code ID** in the Symbologies dialog. According to the sequence of events (specified above), the Code ID must not be included in the bar code data being matched, because when the matching test occurs, the Code ID has already been stripped. If Strip Code ID is disabled, then the bar code data to match must include the Code ID. If Strip Code ID is enabled, the data should not include the Code ID since it has already been stripped.

Add Prefix/Suffix Control

Start > Settings > Control Panel > Data Collection > Symbology button

Use this option to specify a string of text, hex values or hat encoded values to be added to the beginning (prefix) or the end (suffix) of the bar code data.



The image shows a control panel titled 'Add'. It contains two rows. The first row has a checkbox labeled 'Prefix' followed by a text input field. The second row has a checkbox labeled 'Suffix' followed by a text input field.

Up to 19 characters can be included in the string. The string can include any character from the keyboard plus characters specified by hex equivalent or entering in hat encoding. Please see [Hat Encoding](#) for a list of characters with their hex and hat-encoded values.

Use the **Escape** function to enter literal hex and hat values.

Add Prefix	To enable a prefix, check the Prefix checkbox and enter the desired string in the textbox. The default is disabled (unchecked) with a blank text string. When bar code data is processed, the Prefix string is sent to the output buffer before any other data. Because all stripping operations have already occurred, stripping settings do not affect the prefix. The prefix is added to the output buffer for the Symbology selected from the pull down list. If 'All' is selected, the prefix is added for any symbology that has not been specifically configured.
Add Suffix	To enable a suffix, check the Suffix checkbox and enter the desired string in the textbox. The default is disabled (unchecked) with a blank text string. When bar code data is processed, the Suffix string is sent to the output buffer after the bar code data. Because all stripping operations have already occurred, stripping settings do not affect the suffix. The suffix is added to the output buffer for the Symbology selected from the pull down list. If 'All' is selected, the suffix is added for any symbology that has not been specifically configured.

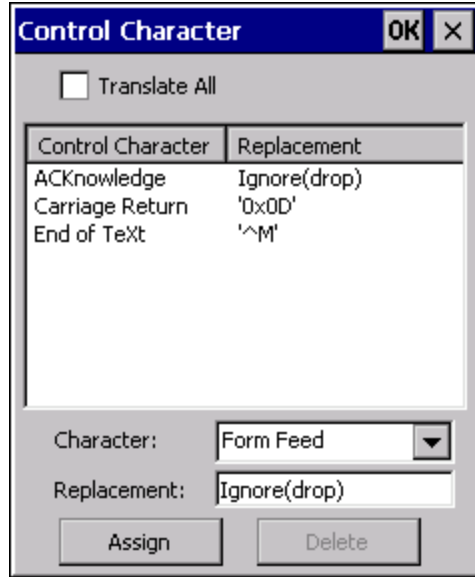
Note: Non-ASCII equivalent keys in Key Message mode are unavailable in this option. Non-ASCII equivalent keys include the function keys (e.g. F1), arrow keys, Page up, Page down, Home, and End.

Symbologies

The Thor VM1 supports only Custom IDs.

Ctrl Char Mapping

The Ctrl Char Mapping button (Control Character Mapping) activates a dialog to define the operations the Data Collection Wedge performs on control characters (values less than 0x20) embedded in bar codes.



Control characters can be replaced with user-defined text which can include hat encoded or hex encoded values. In key message mode, control characters can also be translated to their control code equivalent key sequences.

Translate All

When **Translate All is checked**, unprintable ASCII characters (characters below 20H) in scanned bar codes are assigned to their appropriate CTRL code sequence when the bar codes are sent in Character mode.

The wedge provides a one-to-one mapping of control characters to their equivalent control+character sequence of keystrokes. If control characters are translated, the translation is performed on the bar code data, prefix, and suffix before the keystrokes are simulated.

Parameters

Translate All

This option is grayed unless the user has Send Key Messages (WEDGE) on the Main tab selected.

In Key Message mode, when this option is enabled, control characters embedded in a scanned bar code are translated to their equivalent control key keystroke sequence (13 [0x0d] is translated to Control+M keystrokes as if the user pressed the CTRL, SHIFT, and m keys on the keypad).

Additionally, when Translate All is disabled, any control code which has a keystroke equivalent (enter, tab, escape, backspace, etc.) is output as a keystroke.

Any control code without a keystroke equivalent is dropped.

Character

This is a drop down combo box that contains the control character name. Refer to the Character drop down box for the list of control characters and their names.

When a character name is selected from the drop down box, the default text *Ignore (drop)* is shown and highlighted in the Replacement edit control. *Ignore (drop)* is highlighted so the user can type a replacement if the control character is not to be ignored.

Once the user types any character into the Replacement edit control, reselecting the character from the Character drop down box redisplay the default *Ignore (drop)* in the Replacement edit control.

Replacement

The edit control where the user types the characters to be assigned as the replacement of the control character.

Replacements for a control character are assigned by selecting the appropriate character from the Character drop down box, typing the replacement in the Replacement edit control (according to the formats defined above) and then clicking the button. The assigned replacement is then added to the list box above the Assign button.

For example, if Carriage Return is replaced by Line Feed (by specifying ^J or 0x0A) in the configuration, the value 0x0d received in any scanned bar code (or defined in the prefix or suffix) will be replaced with the value 0x0a.

The Wedge then sends Ctrl+J to the receiving application, rather than Ctrl+M.

List Box

The list box shows all user-defined control characters and their assigned replacements.

All replacements are enclosed in single quotes to delimit white space that has been assigned.

Assign Button

Click this button when you want to assign the characters in the Replacement text box to the character in the Character drop down box.

Delete Button

This button is grayed unless an entry in the list box is highlighted.

When an entry (or entries) is highlighted, and the Delete button is clicked, the highlighted material is deleted from the list box.

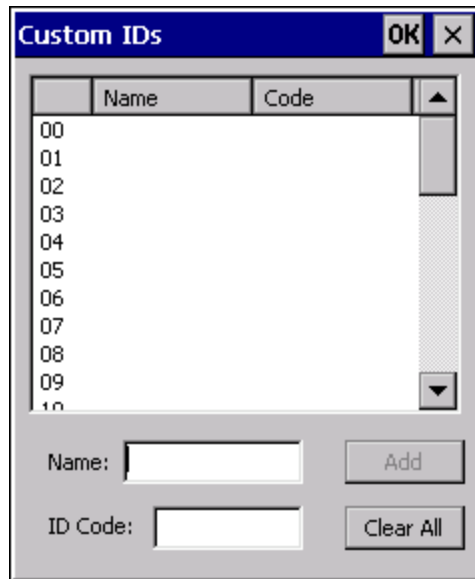
Custom Identifiers

Code IDs are defined by the user for external bar code scanners. These are called **custom Code IDs** and are included in the Symbology drop down box in the Symbology dialog, unless **Enable Code ID** is set to **None**. When the custom Code ID is found in a bar code, the configuration specified for the custom Code ID is applied to the bar code data.

When **Enable Code ID** is set to **None**, custom code IDs are ignored.

*Note: When **Strip: Code ID** is enabled, the entire custom Code ID string is stripped (i.e., treated as a Code ID).*

The dialog box shown below allows the custom Code IDs to be configured. When incoming data is checked for a custom ID code, the list is compared in the order displayed in this dialog box.



After adding, changing and removing items from the Custom IDs list, click the OK button to save changes and return to the Bar Code panel.

Parameters

Name text box

Name is the descriptor that is used to identify the custom Code ID. Names must be unique from each other; however, the Name and ID Code may have the same value. Name is used in the Symbology drop down box to identify the custom Code ID in a user-friendly manner. Both Name and ID Code must be specified in order to add a custom Code ID to the Custom IDs list.

ID Code text box

ID Code defines the data at the beginning of a bar code that acts as an identifier (the actual Code ID). Both Name and ID Code must be specified in order to add a custom Code ID to the Custom IDs list.

Buttons

Add

Entering data into both the Name and ID Code fields enables the Add button. Click the Add button and the data is added to the next empty location in the Custom ID list.

Insert

Click on an empty line in the Custom ID list. The Add button changes to Insert. Enter data into both the Name and ID Code fields and click the Insert button. The data is added to the selected line in the Custom IDs list.

Edit

Double-click on the item to edit. Its values are copied to the text boxes for editing. The Add button changes to Replace. When Replace is clicked, the values for the current item in the list are updated.

Clear All

When no item in the Custom IDs list is selected, clicking the Clear All button clears the Custom ID list and any text written (and not yet added or inserted) in the Name and ID Code text boxes.

Remove

The Clear All button text changes to a Remove button when an item in the Custom IDs list is selected. Click the desired line item and then click the Remove button to delete it. Line items are Removed one at a time. Contents of the text box fields are cleared at the same time.

Control Code Replacement Examples

Configuration Data	Translation	Example Control Character	Example Configuration	Translated Data
Ignore (drop)	The control character is discarded from the bar code data, prefix and suffix	ESCAPE	Ignore (drop)	0x1B in the bar code is discarded.
Printable text	Text is substituted for Control Character.	Start of TeXt	STX	0x02 in a bar code is converted to the text STX.
Hat-encoded text	The hat-encoded text is translated to the equivalent hex value.	Carriage Return	^M	Value 0x0d in a bar code is converted to the value 0x0d.
Escaped hat-encoded text	The hat-encoding to pass through to the application.	Horizontal Tab	^I	Value 0x09 in a bar code is converted to the text ^I.
Hex-encoded text	The hex-encoded text is translated to the equivalent hex value.	Carriage Return	0x0A	Value 0x0D in a bar code is converted to a value 0x0A.
Escaped hex-encoded text	The hex-encoding to pass through to the application.	Vertical Tab	\0x0A or 0\x0A	Value 0x0C in a bar code is converted to text 0x0A

See Also: ["Hat Encoding"](#)

Bar Code Processing Examples

The following table shows examples of stripping and prefix/suffix configurations.

	Symbology				
	All	EAN-128(JC1)	EAN-13(JE0)	Intrlv 2 of 5(JIO)	Code93
Enable	Enabled	Enabled	Enabled	Enabled	Disabled
Min length	1	4	1	1	
Max length	all	all	all	10	
Strip Code ID	Enabled	Enabled	Disabled	Enabled	
Strip Leading	3	0	3	3	
Strip Bar Code Data		*123	1*	456	
Strip Trailing	0	0	3	3	
Prefix	aaa	bbb	ccc	ddd	
Suffix	www	xxx	yyy	zzz	

Provided that the wedge is configured with the above table, below are examples of scanned bar code data and results of these manipulations.

Bar Code Symbology	Raw Scanner Data	Resulting Data
EAN-128	JC11234567890123	bbb1234567890xxx
EAN-128	JC111234567890123	bbb11234567890xxx
EAN-128	JC1123	< rejected > (too short)
EAN-13	JE01234567890987	cccJE04567890yyy
EAN-13	JE01231234567890987	cccJE0234567890yyy
EAN-13	JE01234	cccJE0yyy
I2/5	J104444567890987654321	< rejected > (too long)
I2/5	J104444567890123	ddd7890zzz
I2/5	J10444	dddzzz
I2/5	J1022245622	ddd45zzz
Code-93	JG0123456	< rejected > (disabled)
Code-93	JG0444444	< rejected > (disabled)
Code-39	JA01234567890	aaa4567890www
Code-39 full ASCII	JA41231234567890	aaa1234567890www
Code-39	JA4	< rejected > (too short)

Note: Rejected bar codes generate a bad scan beep. In some cases, the receipt of data from the scanner triggers a good scan beep (from the external scanner), and then the rejection of scanned bar code data by the processing causes a bad scan beep on the same data.

Processing Tab

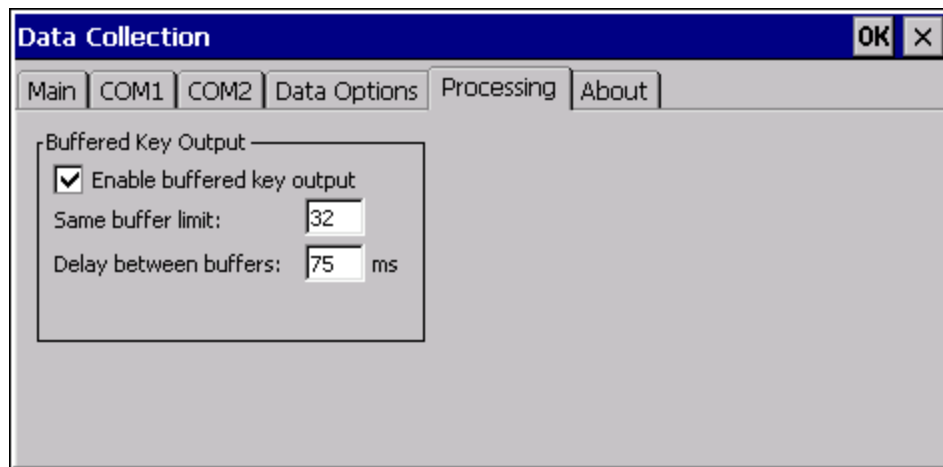
Start > Settings > Control Panel > Data Collection > Processing tab

The Processing tab contains a user configurable key delay that applies to scanned bar codes as they are input when Remote Desktop is the application with the input focus.

Factory Default Settings

Enable buffered key output	Enabled
Same buffer limit (characters)	32
Delay between (key) buffers	75 ms

Note: Settings on this panel have no effect when RFTerm is the application with the input focus.



Enable buffered key output

Default is enabled (checked). Click the checkbox to turn off buffered key output.

Same buffer limit

Default is 32 ms. Raise or lower this value as desired.

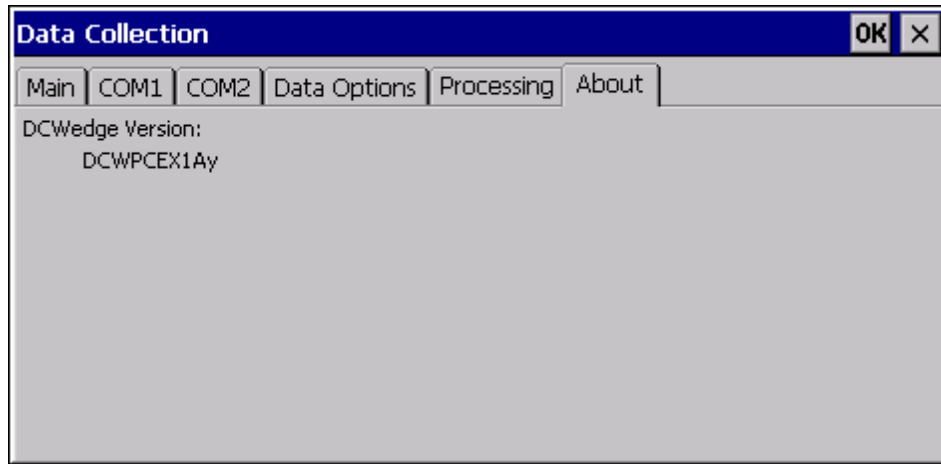
Delay between (key) buffers

Specifies the number of milliseconds to delay after each character in the scanned bar code is processed as a keystroke. This value may need to be adjusted depending on the network traffic in the environment. The default value is 75 ms. Valid value is from 0 to 9999. A zero value is No Delay between characters.

About Tab

Start > Settings > Control Panel > Data Collection > About tab

This tab displays the Data Collection Wedge driver version installed in the Thor VM1. The version number shown in the image below is used only as an example, your version number will be different.



Length Based Bar Code Stripping

Use this procedure to create symbology rules for two bar codes with the same symbology but with different discrete lengths. This procedure is not applicable for bar codes with variable lengths (falling between a maximum value and a minimum value).

Example:

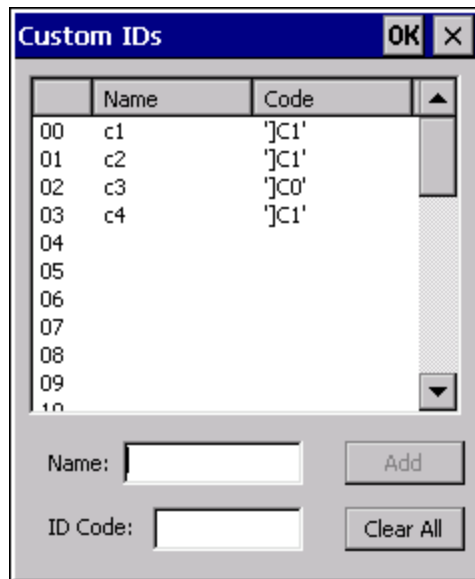
For the purposes of this example, the following sample bar code parameters will be used – EAN 128 and Code 128 bar codes. Some of the bar codes start with '00' and some start with '01'. The bar codes are different lengths.

- 34 character length with first two characters = "01" (strip first 2 and last 18)
- 26 character length with first two characters = "01" (strip first 2 and last 10)
- 24 character length with first two characters = "01" (strip first 2 and last 8). This 24 character bar code is Code 128.
- 20 character length with first two characters = "00" (strip first 0 (no characters) and last 4)

On the Data Options tab, set Enable Code ID to Custom.

Create four custom IDs, using 1 for EAN 128 bar code and 0 for Code 128 bar code.

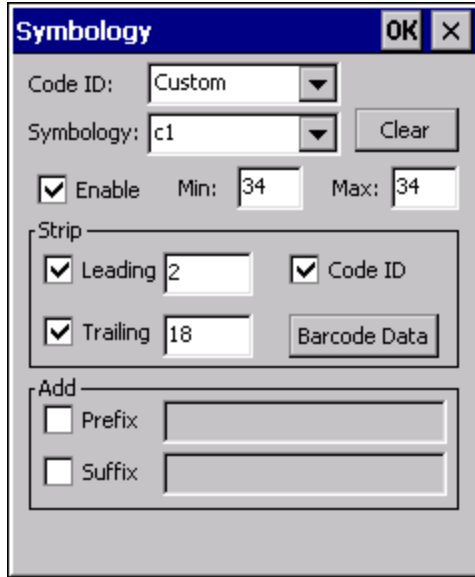
- c1 = Code = ']C1'
- c2 = Code = ']C1'
- c3 = Code = ']C0' (24 character bar code is Code 128)
- c4 = Code = ']C1'



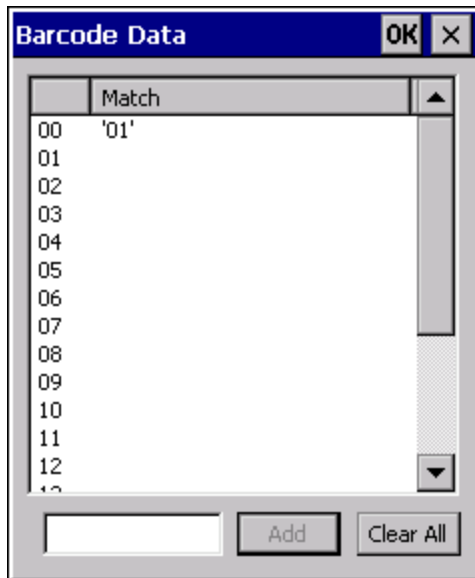
Custom symbology setup is assigned in the following manner:

- c1 min length = 34, max length = 34, strip leading 2, strip trailing 18, Code ID enabled, Bar Code Data = "01"
- c2 min length = 26, max length = 26, strip leading 2, strip trailing 10, Code ID enabled, Bar Code Data = "01"
- c3 min length = 24, max length = 24, strip leading 2, strip trailing 8, Code ID enabled, Bar Code Data = "01"
- c4 min length = 20, max length = 20, strip leading 0, strip trailing 4, Code ID enabled, Bar Code Data = "00"

Add the custom symbologies. Refer to the previous section *Symbology Settings* for instruction.



- Click the Bar Code Data button.
- Click the Add button.
- Add the data for the match codes.



- Refer to the previous section [Bar Code Data Match List](#) for instruction.
- Scan a bar code and examine the result.

Hat Encoding

Desired ASCII	Hex Value	Hat Encoded
NUL	0X00	^@
SOH	0X01	^A
STX	0X02	^B
ETX	0X03	^C
EOT	0X04	^D
ENQ	0X05	^E
ACK	0X06	^F
BEL	0X07	^G
BS	0X08	^H
HT	0X09	^I
LF	0X0A	^J
VT	0X0B	^K
FF	0X0C	^L
CR	0X0D	^M
SO	0X0E	^N
SI	0X0F	^O
DLE	0X10	^P
DC1 (XON)	0X11	^Q
DC2	0X12	^R
DC3 (XOFF)	0X13	^S
DC4	0X14	^T
NAK	0X15	^U
SYN	0X16	^V
ETB	0X17	^W
CAN	0X18	^X
EM	0X19	^Y
SUB	0X1A	^Z
ESC	0X1B	^[
FS	0X1C	^\
GS	0X1D] ^
RS	0X1E	^^
US	0X1F	^ (Underscore)
	0X7F	^?
	80	~@
	81	~A
	82	~B
	83	~C
IND	84	~D
NEL	85	~E
SSA	86	~F
®	AE	~. (Period)
-	AF	~/
°	B0	~0 (Zero)
±	B1	~1

Desired ASCII	Hex Value	Hat Encoded
ESA	87	~G
HTS	88	~H
HTJ	89	~I
VTS	8A	~J
PLD	8B	~K
PLU	8C	~L
RI	8D	~M
SS2	8E	~N
SS3	8F	~O
DCS	90	~P
PU1	91	~Q
PU2	92	~R
STS	93	~S
CCH	94	~T
MW	95	~U
SPA	96	~V
EPA	97	~W
	98	~X
	99	~Y
	9A	~Z
CSI	9B	~[
ST	9C	~\
OSC	9D	~]
PM	9E	~^
APC	9F	~_ (Underscore)
(no-break space)	A0	~ (Tilde and Space)
¡	A1	~!
¢	A2	~"
£	A3	~#
¤	A4	~\$
¥	A5	~%
¦	A6	~&
§	A7	~'
-	A8	~(
©	A9	~)
*	AA	~*
«	AB	~+
-	AC	~,
(soft hyphen)	AD	~- (Dash)
×	D7	~W
Ø	D8	~X
Ù	D9	~Y
Ú	DA	~Z

Desired ASCII	Hex Value	Hat Encoded
²	B2	~2
³	B3	~3
´	B4	~4
µ	B5	~5
¶	B6	~6
·	B7	~7
¸	B8	~8
¹	B9	~9
º	BA	~:
»	BB	~;
¼	BC	~<
½	BD	~=
¾	BE	~>
¿	BF	~?
À	C0	~@
Á	C1	~A
Â	C2	~B
Ã	C3	~C
Ä	C4	~D
Å	C5	~E
Æ	C6	~F
Ç	C7	~G
È	C8	~H
É	C9	~I
Ê	CA	~J
Ë	CB	~K
Ì	CC	~L
Í	CD	~M
Î	CE	~N
Ï	CF	~O
Ð	D0	~P
Ñ	D1	~Q
Ò	D2	~R
Ó	D3	~S
Ô	D4	~T
Õ	D5	~U
Ö	D6	~V

Desired ASCII	Hex Value	Hat Encoded
Û	DB	~[
Ü	DC	~\
Ý	DD	~]
Þ	DE	~^
ß	DF	~_ (Underscore)
à	E0	~`
á	E1	~a
â	E2	~b
ã	E3	~c
ä	E4	~d
å	E5	~e
æ	E6	~f
ç	E7	~g
è	E8	~h
é	E9	~i
ê	EA	~j
ë	EB	~k
ì	EC	~l
í	ED	~m
î	EE	~n
ï	EF	~o
ð	F0	~p
ñ	F1	~q
ò	F2	~r
ó	F3	~s
ô	F4	~t
õ	F5	~u
ö	F6	~v
÷	F7	~w
ø	F8	~x
ù	F9	~y
ú	FA	~z
û	FB	~{
ü	FC	~
ý	FD	~}
þ	FE	~
ÿ	FF	~?

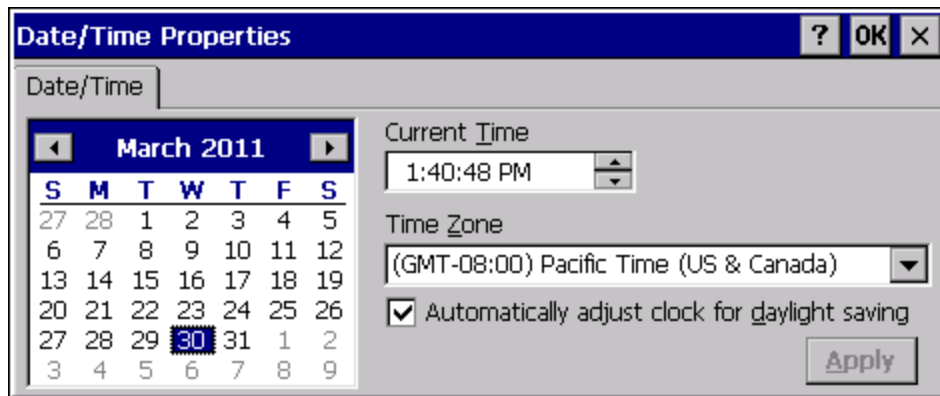
Date / Time

Start > Settings > Control Panel > Date/Time - or - Time in Desktop Taskbar

Use this Thor VM1 panel to set Date, Time, Time Zone, and assign a Daylight Savings location.

Factory Default Settings

Current Time	Midnight
Time Zone	GMT-05:00
Daylight Savings	Enabled



There is very little functional change from general desktop or laptop Date/Time Properties options.

Double-tapping the time displayed in the Desktop Taskbar causes the Date/Time Properties screen to appear.

The Sync button (if available) activates a utility that will set the clock using a network time server.

Dialing

Start > Settings > Control Panel > Dialing

Set dialup properties for internal modems (not supplied or supported on the Thor VM1).

Factory Default Settings

Location	Work
Area Code	425
Tone Dialing	Enabled
Country/Region	1
Disable Call Waiting	Disabled (blank)



Display

Start > Settings > Control Panel > Display

The display might also called the touch screen.

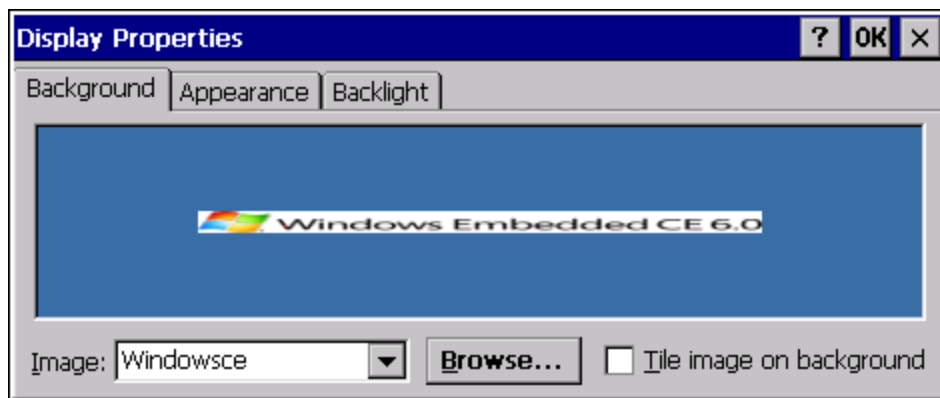
Select the desktop background image and appearance scheme for the Thor VM1. Using the options on the Backlight tab, set the display backlight and keypad backlight timers when running on battery or external power.

Adjust the settings and tap the OK button to save the changes. Saved changes take effect immediately.

Factory Default Settings

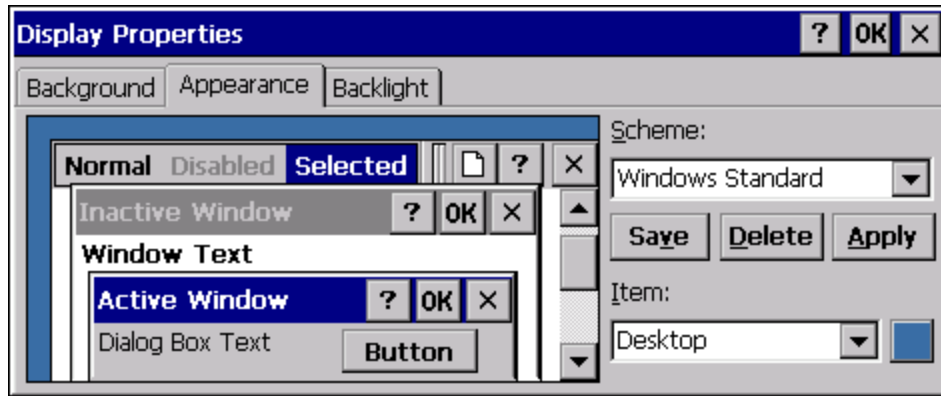
Background tab	
Image	Windows CE
Image on background	Disabled
Appearance tab	
Schemes	Windows Standard
Backlight tab	
Battery power	30 seconds
External power	2 minutes

Background



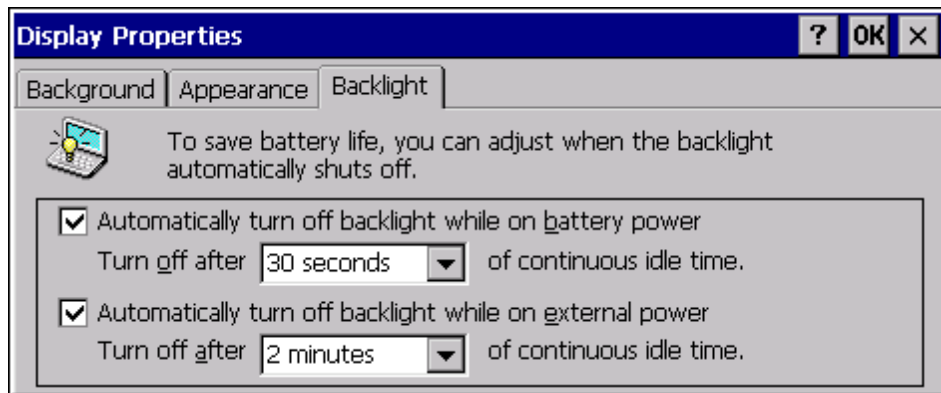
There is very little change from general desktop PC Display Properties / Background options. Select an image from the dropdown list (or tap the Browse button to select an image from another folder) to display on the Desktop, and then tap the OK button to save the change. The change takes effect immediately.

Appearance



There is very little change from general desktop PC Appearance options. Select a scheme from the dropdown list and make changes to the parameters. The default is High Contrast White for monochrome displays and Windows Standard for color displays. Tap the Save button to save any changes, renaming the scheme if desired. Tap the Delete button to delete schemes. Tap the Apply button to apply the selected scheme to the display.

Backlight



When the backlight timer expires, the touch screen backlight is dimmed, not turned off. When both checkboxes are unchecked, the backlight never turns off (or dims).

The default values are 2 minutes for external power and 30 seconds when operating on the internal UPS battery.

Gobi Connection Manager

Start > Settings > Control Panel > Gobi Connection Manager or

Tap the Gobi Connection Manager Desktop Icon or

Tap the Gobi Connection Manager icon in the system tray or

Tap Start > Programs > GobiCM > GobiCMExe






Note: Earlier versions may be labeled LXEGobiCM > LXEGobiCMExe.

Set parameters for optional internal WWAN module.

Home	View connection status and select firmware.
CDMA	Use this tab to activate a CDMA carrier such as Verizon.
UMTS	Use this tab to test and save connection parameters.
GPS	View GPS statistics.
About	View information on the WWAN card.

The Gobi Connection Manager tray icon indicates the status of the connection in dark blue bars. If you hover the mouse pointer over the Connection Manager Taskbar icon, the current signal level and radio interface are displayed.

Note: The similar Summit wifi icon in the task bar uses red, yellow and green bars.

	There is no WWAN connection present.
	-105 dbm to -86 dbm signal strength
	-85 dbm to -66 dbm signal strength
	-65 dbm to -46 dbm signal strength
	-45 dbm or higher signal strength

Initial Use

Some carriers such as AT&T and T-Mobile require a SIM card for use on their networks. Other carriers such as Verizon use a CDMA network and must be activated. Please refer to the sections below for more details.

SIM Card Installation

Depending on the carrier, a SIM card may be necessary for WWAN connection. To install a SIM card:

1. Place the Thor VM1 in Suspend.
2. Remove the Thor VM1 from the Quick Mount Vehicle Dock.
3. Place the Thor VM1 face down on a stable surface.
4. Use 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 VM1 is face down with the top away from the user.
5. Install the SIM card in the slot.
6. Reattach the access panel, torquing the screws to 4 to 5 inch pounds.

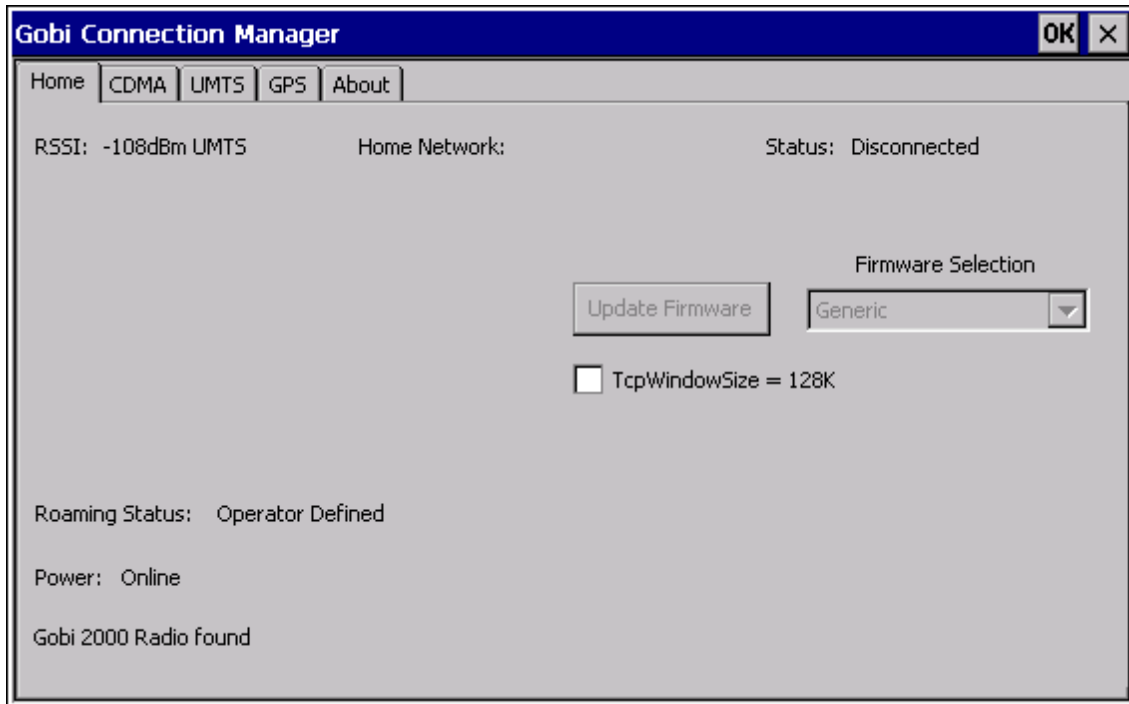
-
7. Reinstall the Thor VM1 in the Dock.
 8. Resume the Thor VM1 from suspend.

Activate

To activate service for a CDMA carrier such as Verizon, complete the necessary entries on the [CDMA tab](#).

Home

Use the **Home** tab to update firmware and view the status of the connection.



To update firmware:

1. Select the firmware for the desired carrier from the **Firmware Selection** pull down list.
2. If no firmware files are found, an error message is displayed. Contact [Technical Assistance](#) for information.
3. Tap the **Update Firmware** button.
4. The update process may take a minute or so to complete.

The status of the Gobi 2000 radio is displayed in the lower left corner of this tab. An error message is displayed in this location if the firmware selected requires a SIM card and no SIM card is installed in the Thor VM1.

Connection status is at the top of this tab.

CDMA

Use the **CDMA** tab to activate the Thor VM1 for use with a CDMA carrier such as Verizon. This step is not necessary for carriers using a SIM card.

The Serial Number, IMEI (International Mobile Equipment Identity) and MEID (Mobile Equipment ID) numbers are displayed on this tab as the carrier may request this information when setting up an account.

The screenshot shows the 'Gobi Connection Manager' window with the 'CDMA' tab selected. The window title bar includes 'OK' and 'X' buttons. The interface is divided into several sections:

- Home** | **CDMA** | UMTS | GPS | About
- S/N**: 803EB555
- IMEI**: 980030000000000
- MEID**: A1000000000000
- Activation Type**: Automatic, Manual
- Autoconnect**: Enable
- Activate** button
- Service not activated** message
- Authentication ***: PAP, CHAP
- Data Connection Test ***: **Connect** and **Disconnect** buttons
- Activation Code**: [Text box]
- Service Programming Code**: [Text box] **Validate SPC** button
- System Identification Number**: [Text box]
- Mobile Directory Number**: [Text box]
- Mobile Identification Number**: [Text box]
- User Name ***: [Text box]
- Password ***: [Text box]
- (*) Data Connection test only** label
- Save Connection Data** button

Activation Type

There are two activation methods, Automatic and Manual.

Automatic Activation

1. Select the **Automatic** radio button for **Activation Type**.
2. Automatic activation requires an Activation Code. Enter the Activation Code in the **Activation Code** text box and tap **Activate**.
3. All other text boxes are grayed out as no additional entries are required for automatic activation.
4. Verify the activation process is successful by reviewing the message below the **Activation Type** group.

Manual Activation

1. Select the **Manual** radio button for **Activation Type**.
2. Enter the Service Programming Code, System Identification number, Mobile Directory number and Mobile Identification Number in the appropriate text boxes.
3. The **Activation Code** text box is not used.

4. Tap **Activate**.

5. Verify the activation process is successful by reviewing the message below the **Activation Type** group.

Autoconnect

When checked, Autoconnect is enabled. The Connection Manager automatically connect when necessary, such as when Internet Explorer is launched.

Data Connection Test

Tap the **Connect** button to make a temporary test connection to validate the carrier account.

Entries identified with an asterisk (*) are used to configure the test connection.

Tap the **Save Connection Data** button to save the connection parameters.

UTMS

Use the **UTMS** tab to configure the session parameters.

The screenshot shows the 'Gobi Connection Manager' application window with the 'UTMS' tab selected. The interface includes a menu bar with 'Home', 'CDMA', 'UTMS', 'GPS', and 'About'. The main area is divided into two columns. The left column contains text labels and input fields for: APN, User Name, Password, IP Address, Primary DNS, Secondary DNS, Primary NetBIOS Name Server *, and Secondary NetBIOS Name Server *. A note at the bottom left states '(*) Data Connection test only'. The right column contains: an 'Autoconnect' section with an 'Enable' checkbox; a 'Disconnected' status indicator; an 'Authentication' section with 'PAP' and 'CHAP' radio buttons; a 'Data Connection Test *' section with 'Connect' and 'Disconnect' buttons; and a 'Save Connection Data' button at the bottom right. The window title bar includes 'OK' and 'X' buttons.

Autoconnect

When checked, Autoconnect is enabled. The Connection Manager automatically connect when necessary, such as when Internet Explorer is launched.

Data Connection Test

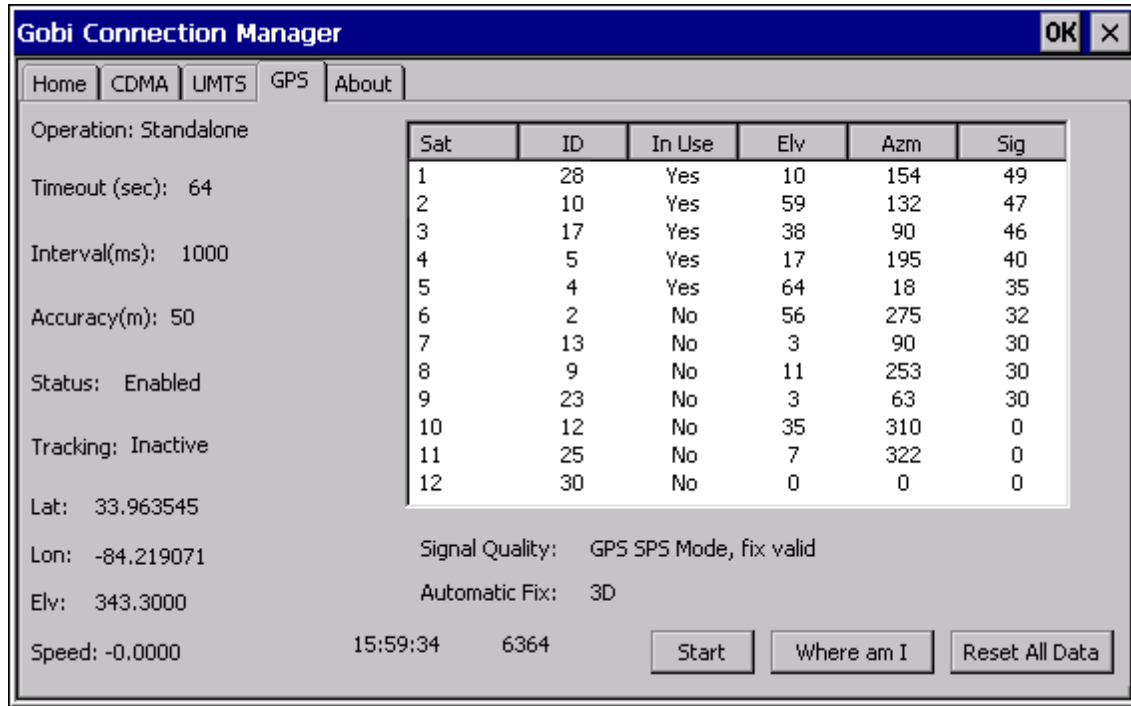
Tap the **Connect** button to make a temporary test connection to validate the carrier account.

Entries identified with an asterisk (*) are used to configure the test connection.

Tap the **Save Connection Data** button to save the connection parameters.

GPS

This tab displays the information available from the GPS built into the Gobi radio.



Tap the **Start** button to initiate a scan for GPS data. The information on this tab is updated every 3 seconds.

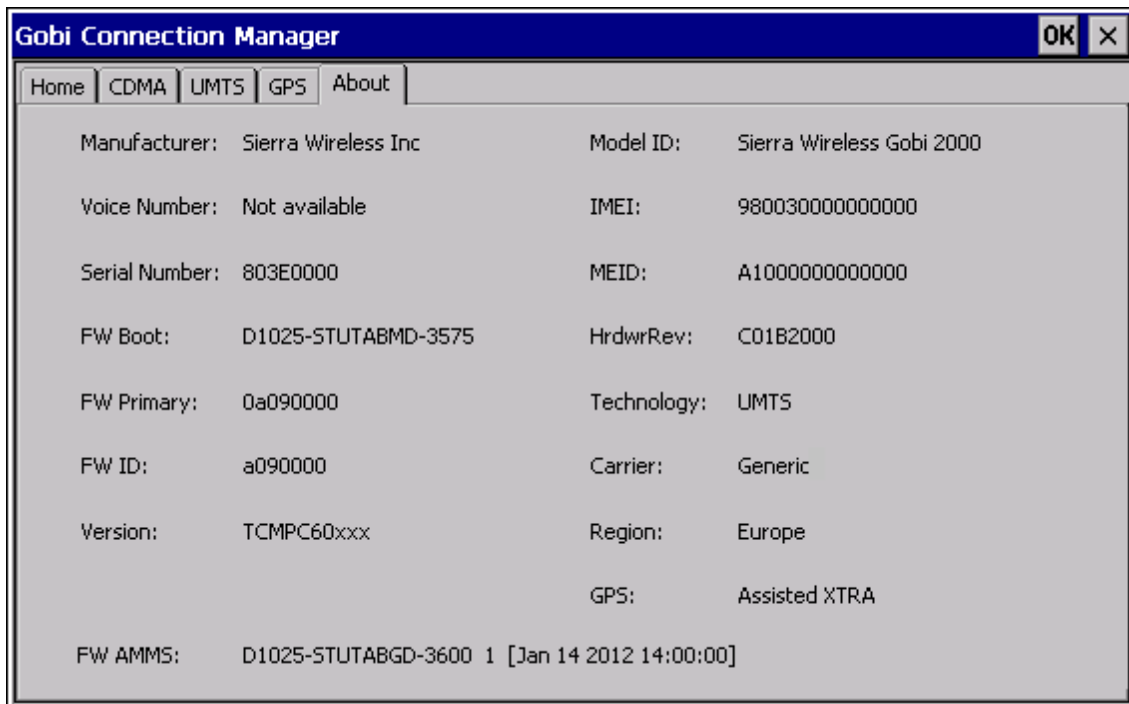
Tap the **Reset All Data** button to clear all GPS data from the Gobi radio. You must confirm that you want to reset the data. Use this button with caution as it takes a longer time for the GPS to establish a valid fix after the data is cleared.

After the GPS establishes a coordinate fix, the **Where am I** button is active. Tapping this button activates Internet Explorer to display a Google map of the current location.

The GPS time and NMEA (National Maritime Electronics Association) string count are displayed at the bottom of this tab.

About

This tab displays information on the Gobi 2000 radio installed in the Thor VM1.



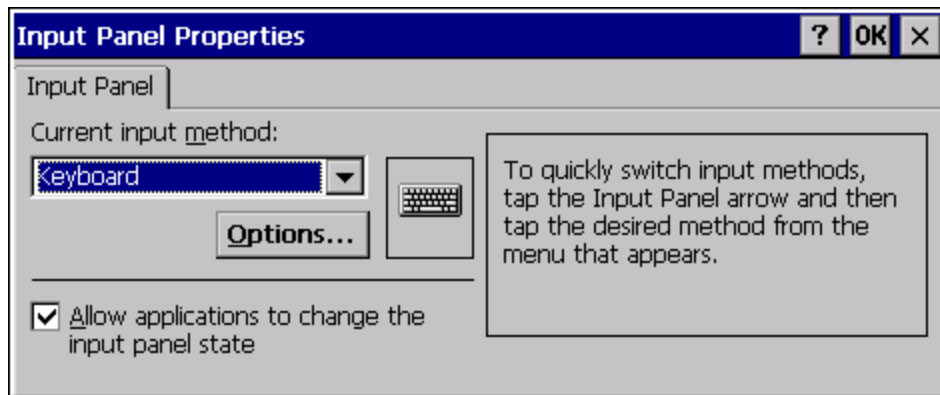
Input Panel

Start > Settings > Control Panel > Input Panel

Set the current Thor VM1 keys and data input method.

Factory Default Settings

Input Panel tab	
Input Method	Keyboard
Allow applications to change input panel state	Enabled
Options button	
Keys	Small keys
Use gestures	Disabled



Use this panel to make the Input Panel (on-screen keyboard) or the physical keypad primarily available when entering data on any screen. Selecting Keyboard enables both.

Tap the Options button to set the size of the keys displayed on-screen and whether Transcriber gestures are enabled or disabled.

Transcriber

When choosing Transcriber as the Current Input Method, first tap the Keyboard icon in the status bar. Select Transcriber from the pop-up menu. Then open the Input control panel and tap the Options button. Transcriber Options (**Start > Settings > Control Panel > Input Panel**) are available only when Transcriber is selected as the active input method. Tap the “?” button or the Help button to access Transcriber Help.

Note: Contact [Technical Assistance](#) for language packs as they become available.

Internet Options

Start > Settings > Control Panel > Internet Options

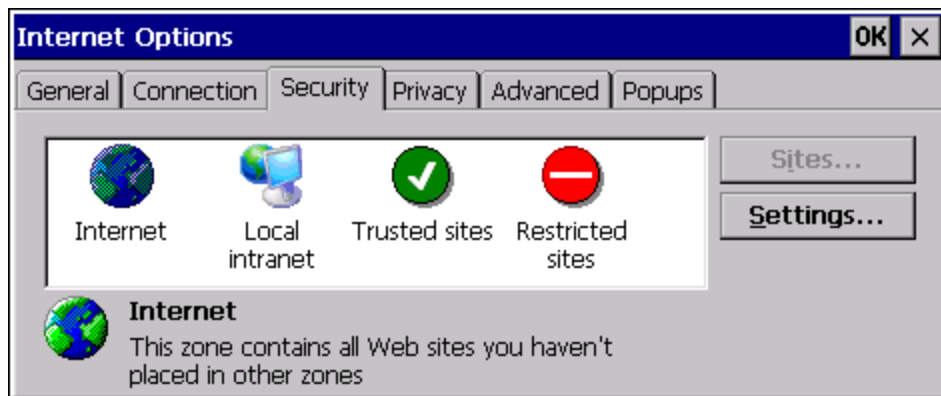
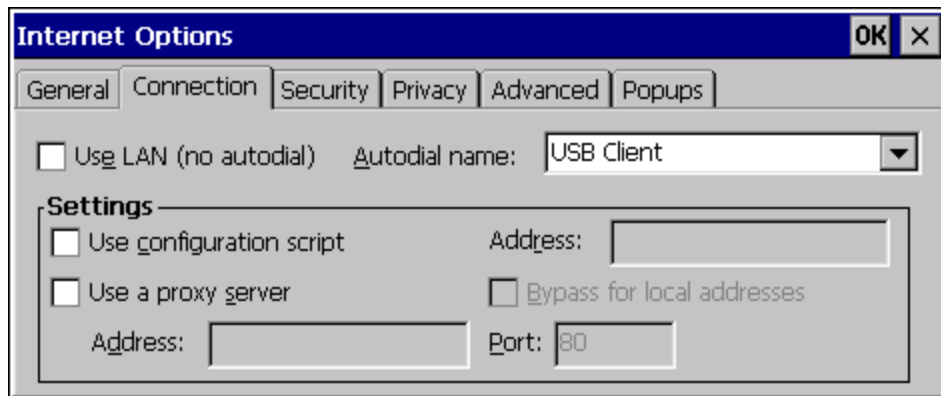
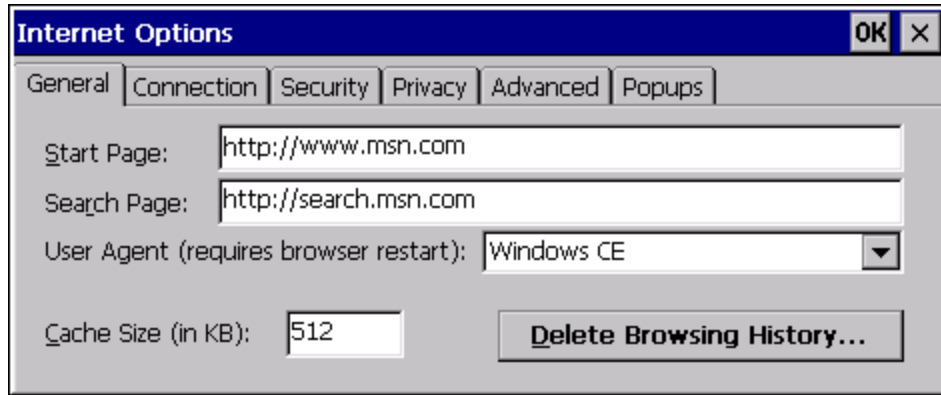
Set options for Thor VM1 Internet connectivity.

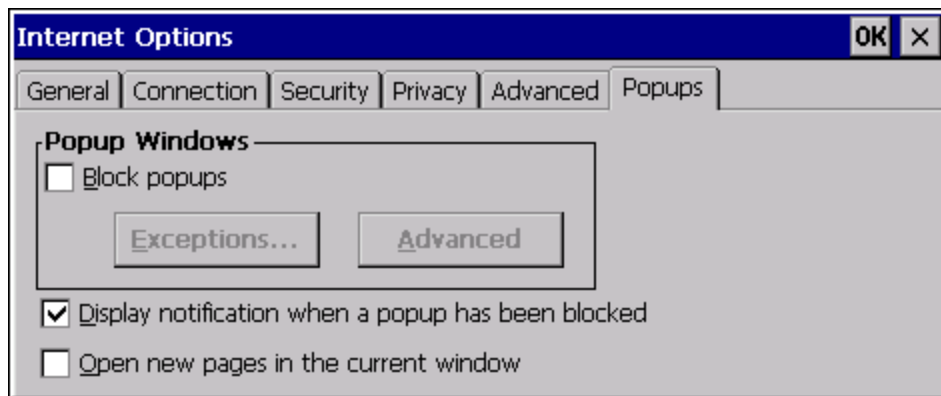
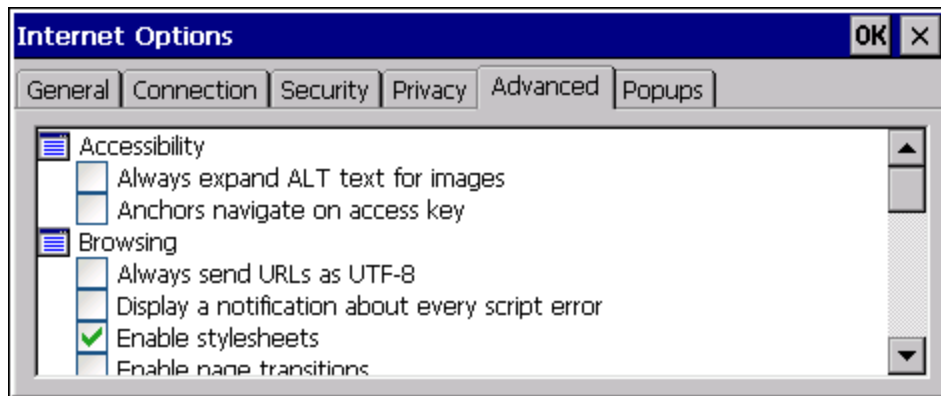
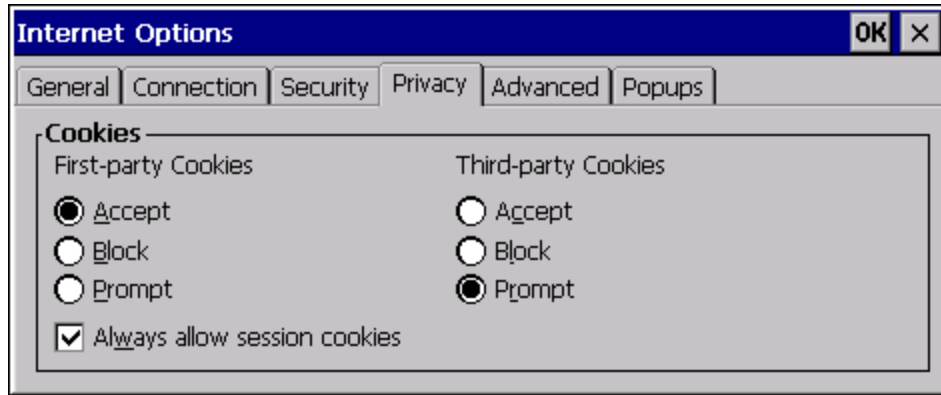
Select a tab. Tap the ? button for help using Windows CE Help installed in your mobile device. Adjust the settings and tap the OK button. The changes take effect immediately.

Factory Default Settings

General tab	
Start Page	http://www.msn.com
Search Page	http://search.msn.com
User Agent	Windows CE
Cache Size	512 KB
Delete History	Button enabled
Connection tab	
Use LAN	Disabled
Autodial Name	USB Client
Proxy Server	Disabled
Bypass Proxy	Disabled
Security tab	
Internet	Default site (See Note)
Privacy tab	
First party cookies	Accept
Third party cookies	Prompt
Session cookies	Always allow
Advanced tab	
Stylesheets	Enabled
Theming Support	Enable
Multimedia	All options enabled
Security	All options enabled
Popups tab	
Block popups	Disabled
Display notification	Enabled
Use same window	Disabled

Note: **Security Tab:** Use the **Settings** button to set ActiveX control, scripting and plug-in behavior for each zone (Internet, Local intranet, Trusted Sites, Restricted Sites). Use the Site button to add sites to each zone.





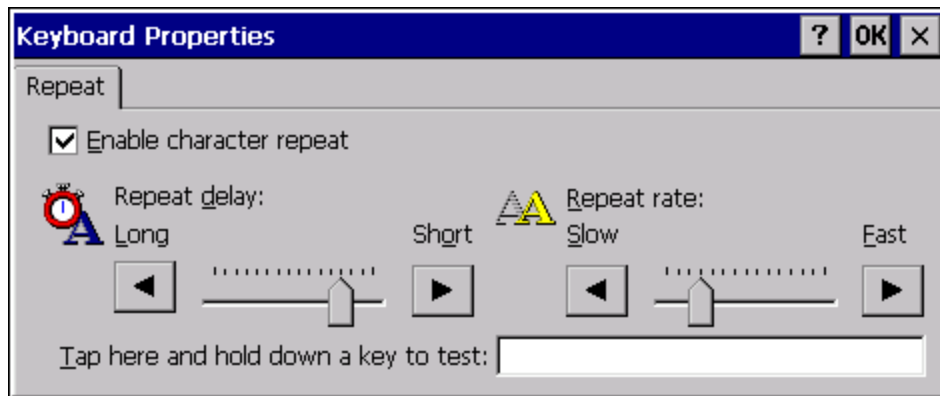
Keyboard

Start > Settings > Control Panel > Keyboard

Set keypad key map, keypad key repeat delay, and key repeat rate.

Factory Default Settings

Repeat character	Enable
Repeat Delay	Short
Repeat Rate	Slow



KeyPad

Start > Settings > Control Panel > KeyPad

Use this control panel option to assign key functions to mappable keys available on your Thor VM1, determine application launch sequences and program command Run sequences.

Factory Default Settings

KeyMap	
Modifier Mode	None
LaunchApp	
App1	Empty
App2	Empty
App3	Empty
App4	Empty
App/Opt	EXE
RunCmd	
Cmd1	Empty
Cmd2	Empty
Cmd3	Empty
Cmd4	Empty
File/Parm	FILE

The KeyPad 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](#)

Note: KeyPad Control Panel options LaunchApp and RunCmd do not inter-relate with similarly-named options contained in other Control Panel applets. For example, the AppLock Administrator Control panel file Launch option.

KeyMap Tab



If **2nd + F5** is remapped to another key, pressing **2nd + F5** generates the remapped key. However, if the next keypress is **Shift**, the Thor VM1 reboots. The remapped keypress DOES NOT affect the **2nd + F5 + Shift** reboot key sequence.

The screenshot shows the 'Keypad Control' dialog box with the following elements:

- Title bar: Keypad Control [?] [OK] [X]
- Tab: KeyMap (with sub-tabs LaunchApp and RunCmd)
- Modifier Mode: None, Shift, Function
- Key: [Dropdown menu]
- Remapped Key: [Dropdown menu]
- Key Sequence: [Text input field]
- Escape: [Dropdown menu]
- Add: [Button]
- U+ [] = []
- Clear: [Button]

Assign settings by clicking radio buttons and selecting keys from the drop down boxes. Tap the OK button when finished. The changes take effect immediately.

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 7 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 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.

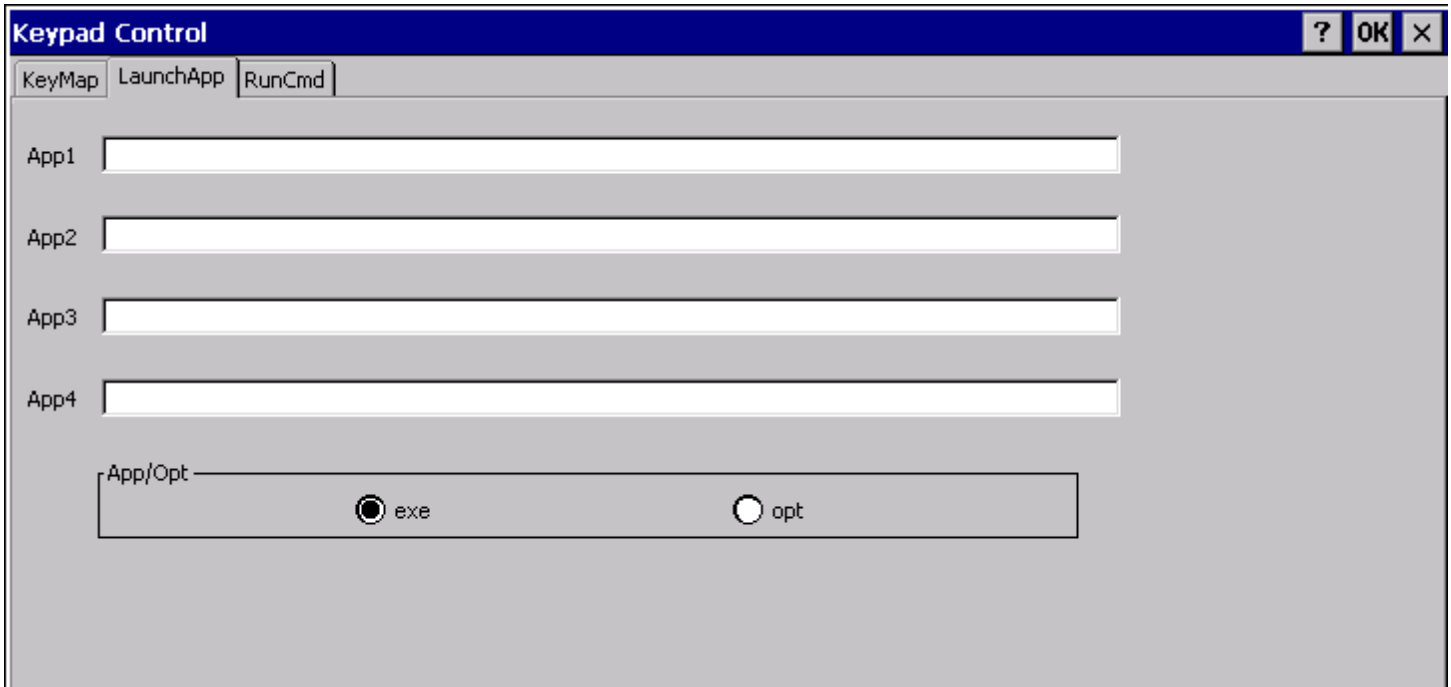
Remap a Command

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.

Note that executables and parameters are not checked for accuracy by the keyboard driver. If the launch fails, the Thor VM1 emits a single beep, if the launch is successful, it is silent.



The screenshot shows the 'Keypad Control' application window. The title bar is blue and contains the text 'Keypad Control' and three buttons: a question mark, 'OK', and a close button. Below the title bar are three tabs: 'KeyMap', 'LaunchApp', and 'RunCmd'. The 'LaunchApp' tab is selected. The main area of the window is light gray and contains four text input fields labeled 'App1', 'App2', 'App3', and 'App4'. Below these is a larger text box labeled 'App/Options' which contains two radio buttons: 'exe' (which is selected) and '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 EXE 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 EXE to OPT clears the text box (but the information previously entered is stored), allowing parameter entry.

Tap the OK button when finished. The changes take effect immediately.

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

RunCmd Tab

The default for all text boxes is Empty, Null or "". The text boxes accept string values only.

Note that executables and parameters are not checked for accuracy by the keyboard driver. If the launch fails, the Thor VM1 emits a single beep, if the launch is successful, the mobile device is silent.

The screenshot shows the 'Keypad Control' application window. The title bar is dark blue with a question mark icon, 'OK', and 'X' buttons. Below the title bar are three tabs: 'KeyMap', 'LaunchApp', and 'RunCmd'. The 'RunCmd' tab is active and contains four text input fields labeled 'Cmd1', 'Cmd2', 'Cmd3', and 'Cmd4'. At the bottom of the tab is a 'File/Parm' section with two radio buttons: 'file' (selected) and '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 when finished. The changes take effect immediately.

License Viewer

Start > Settings > Control Panel > License Viewer

Use this option to view software license registration details, and service contract length for a Thor VM1. Information on the License Viewer tabs is unique for each Thor VM1.

Note: Following image is a sample screen.

Your License Viewer control panel may show more tabs, e.g., RFTerm, depending on the number of software applications running on the Thor VM1 that require a license. Contact [Technical Assistance](#) for software updates and releases as they become available.



Software and driver version information is located in the [About](#) control panel. Copyright information is located in the [System](#) control panel.

Mixer

Start > Settings > Control Panel > Mixer

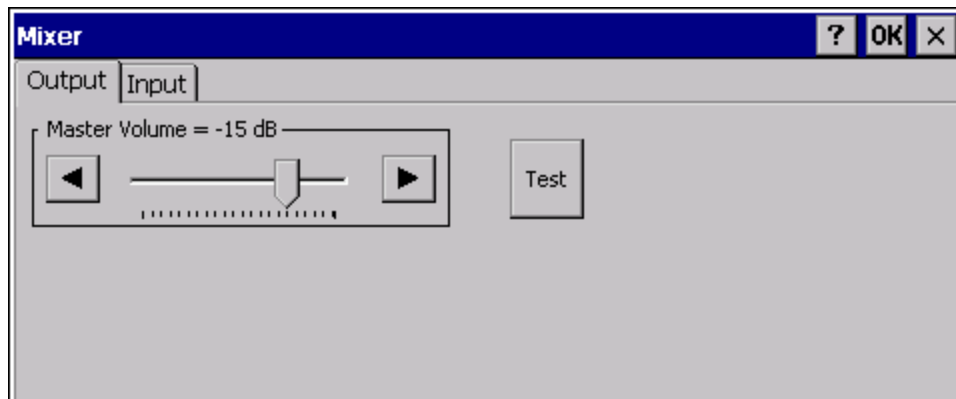
The Thor VM1 has two speakers (located at the bottom front of the unit) and one microphone (located at the top front of the unit).

Use the settings on these panels to adjust the master volume, record gain and sidetone.

Factory Default Settings

Output	
Master Volume	-15 dB
Input	
Record Gain	0.0 dB
Sidetone	0.0 dB Disabled

Output Panel



Tap and hold the Master Volume slider and move either left or right, or tap the left and right arrows, to adjust Speaker volume decibel level.

Tap the **Test** button to play a sample sound at the selected volume.

Input Panel



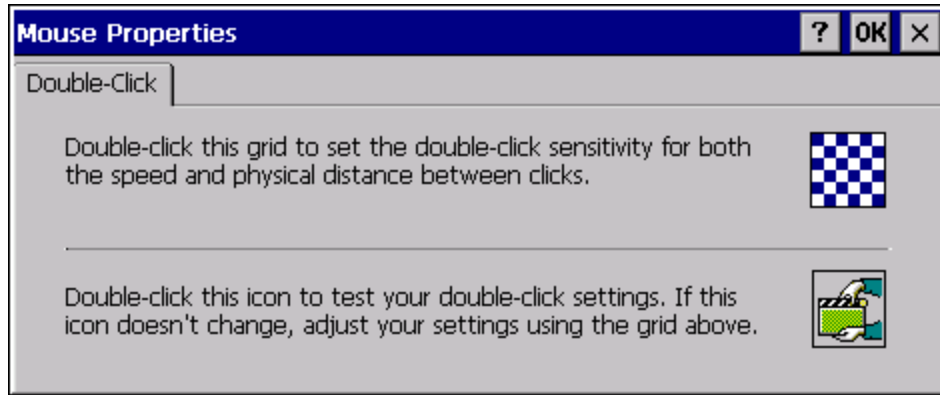
Use the radio buttons to enable or disable the sidetone.

Tap and hold the Record Gain or Sidetone sliders and move either left or right, or tap the left and right arrows, to adjust the levels.

Mouse

Start > Settings > Control Panel > Mouse

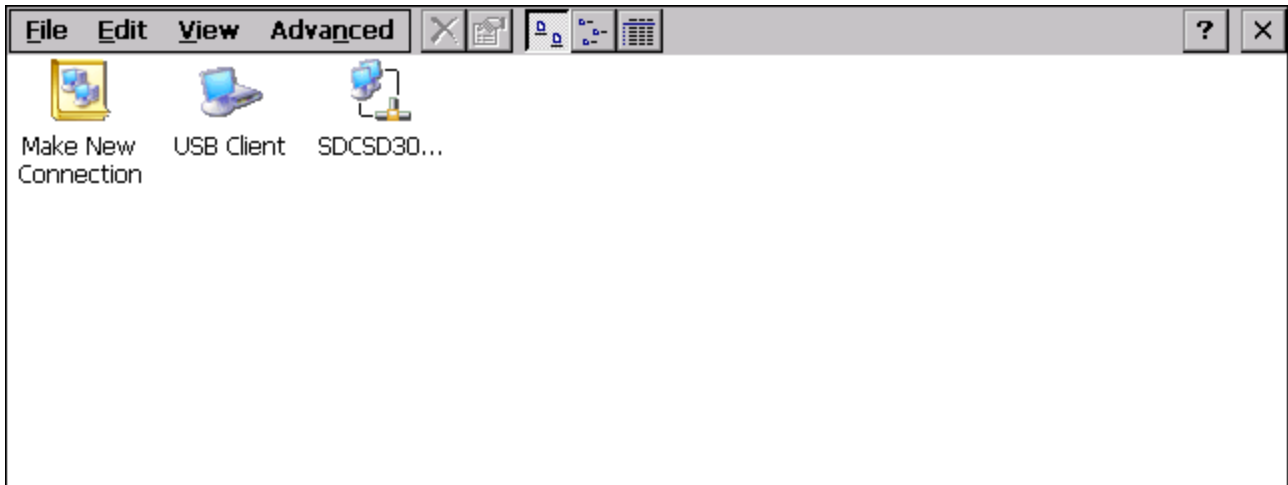
Use this option to set the double-tap sensitivity for stylus taps on the Thor VM1 touch screen.



Network and Dialup Options

Start > Settings > Control Panel > Network and Dialup Connections

Set Thor VM1 network driver properties and network access properties. Select a connection to use, or create a new connection.



Create a New Connection

1. On the mobile device, select **Start > Settings > Control Panel > Network and Dialup Connections**. A window is displayed showing the existing connections.
2. Assuming the connection you want does not exist, double-tap **Make New Connection**.
3. Give the new connection an appropriate name (My Connection @ 9600, etc.). Tap the **Direct Connection** radio button. Tap the **Next** button.
4. From the popup menu, choose the port you want to connect to. Only the available ports are shown.
5. Tap the **Configure...** button.
6. Under the **Port Settings** tab, choose the appropriate baud rate. Data bits, parity, and stop bits remain at 8, none, and 1, respectively.
7. Under the **Call Options** tab, be sure to turn off Wait for dial tone, since a direct connection will not have a dial tone. Set the timeout parameter (default is 5 seconds). Tap **OK**.
8. **TCP/IP Settings** should not need to change from defaults. Tap the **Finish** button to create the new connection.
9. Close the **Remote Networking** window.
10. To activate the new connection select **Start > Settings > Control Panel > PC Connection** and tap the **Change Connection...** button.
11. Select the new connection. Tap **OK** twice.
12. Close the Control Panel window.
13. Connect the desktop PC to the mobile device with the appropriate cable.
14. Click the desktop **Connect icon** to test the new connection.

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

Network Capture

Start > Settings > Control Panel > Network Capture

Note: Verify the [date and time](#) before using the logging utilities to ensure meaningful data.

The Network Capture panels provide configuration options for logging utilities.

Two types of logging are configurable:

Netlog is a Windows CE utility that monitors network traffic. Netlog creates a .CAP file that can be read using Microsoft Windows Network Monitor or any compatible tool that supports .CAP files.

NDISLog monitors the NDIS interface between the Summit radio and the NDIS driver. This utility creates a .TXT log file.

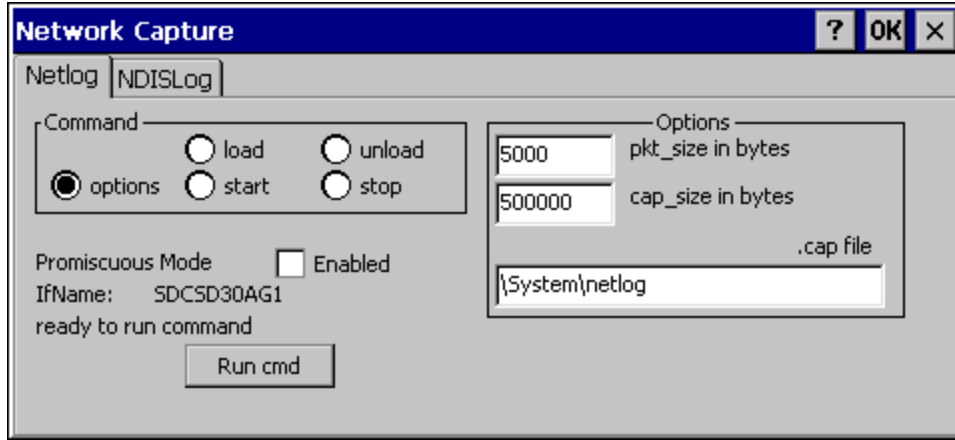
Factory Default Settings

Netlog tab	
Command	options
pkt_size in bytes	5000
cap_size in bytes	500000
.cap file	\netlog
Promiscuous Mode	Disabled
NDISLog tab	
Command	stop
file	\ndislog.txt

Netlog

Use this control panel to configure the Netlog utility. By configuring Netlog using the control panel, Netlog remains running across a warmboot. However, please note that:

- Netlog first stores data to a file named netlog0.cap, then netlog1.cap. Any time the current file reaches maximum size, Netlog switches to the other file.
- If the log file is stored in the root directory, any previous data is lost and a new log file started after the warmboot
- If the log file is stored in \System, all previous data is saved across the warmboot.
- If Netlog is enabled across the warmboot, a series of brief popups may be displayed during the boot cycle. No user interaction is required.



Command

Command	Function
options	Specifies the option to perform. See the table below for the option parameters and values.
load	Loads and starts Netlog.
start	Starts the Netlog process of logging the network traffic.
stop	Stops Netlog from logging network traffic.
unload	Unloads Netlog.

Options

Options	Function
pkt_size in bytes	Specifies the maximum packet size captured in bytes. This option should only be run after you have called load and stop . Default is 5000.
cap_size in bytes	Specifies the maximum size of Netlog0.cap or Netlog1.cap in bytes. This option should only be run after you have called load and stop . Default is 500,000.
.cap file	Specifies the name of the file to which network traffic information is saved. This option should only be run after you have called load and stop . Default is \netlog.

Run cmd

Performs the command selected. For example, to run Netlog and modify the packet size do the following:

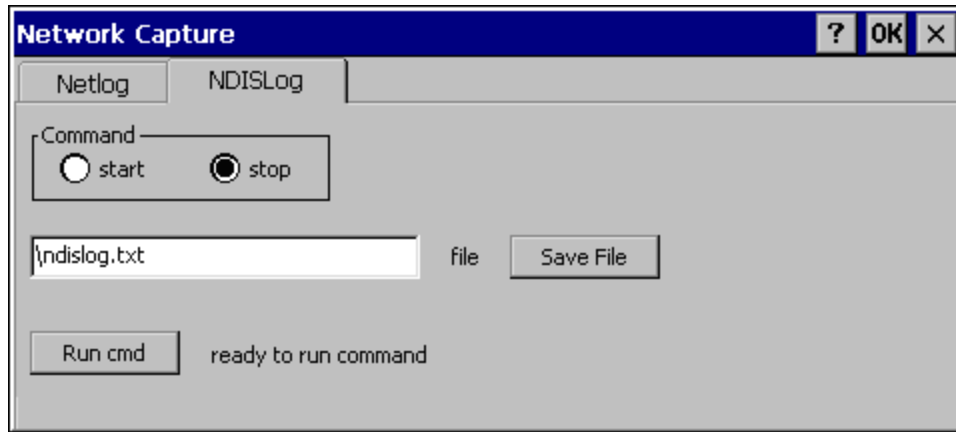
Select **load** from the Commands list and click the **Run cmd** button.

Select **stop** from the Commands list and click the **Run cmd** button.

Select **options** from the Commands list, enter the new packet size in the Options list and click the **Run cmd** button.

NDISLog

NDISLog creates a .TXT file that can be viewed with any text editor program that supports .TXT files.



Command

Command	Function
start	Starts logging the network traffic.
stop	Stops logging network traffic.

file

Specifies the name of the file to which NDISLog information is stored.

Save File

Stores the file name.

Run cmd

Performs the selected start or stop command.

Options

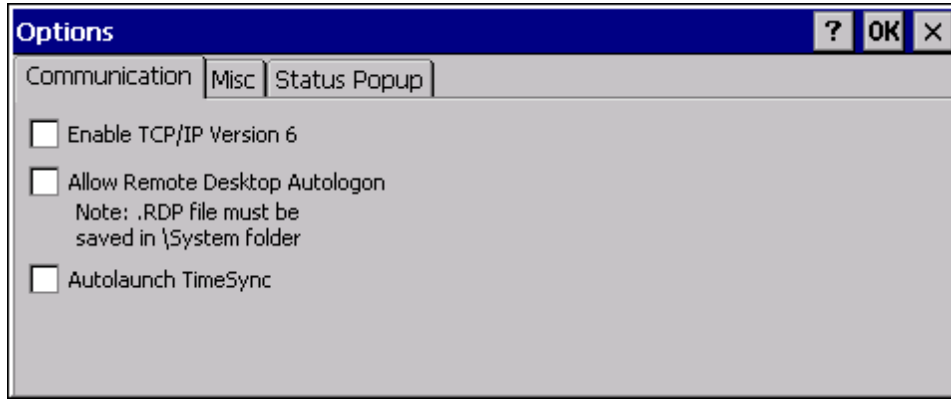
Start > Settings > Control Panel > Options

It may be necessary to warmboot the Thor VM1 after making desired changes. A pop up window indicates if a warmboot is required.

Note: If there is no icon corresponding to this item in the Control Panel, contact your Contact [Technical Assistance](#) for upgrade details.

Communication

Options on this tab configure communication options for the Thor VM1.



Enable TCP/IP Version 6

By default, IPv6 is disabled on the Thor VM1. Check this checkbox to enable IPv6.

Allow Remote Desktop Autologon

By default, Remote Desktop Autologon is disabled. Check this checkbox to enable Remote Desktop Autologon.

Note: The .RDP file must be saved in the \System folder. When prompted, use the Save As button to save the .RDP file in the \System directory. If the .RDP file is saved in the default root folder location, the .RDP file will not persist across a warmboot.

Autolaunch TimeSync

By default, TimeSync does not automatically run on the Thor VM1. To enable TimeSync to run automatically on the Thor VM1, check this checkbox.

Synchronize with a Local Time Server

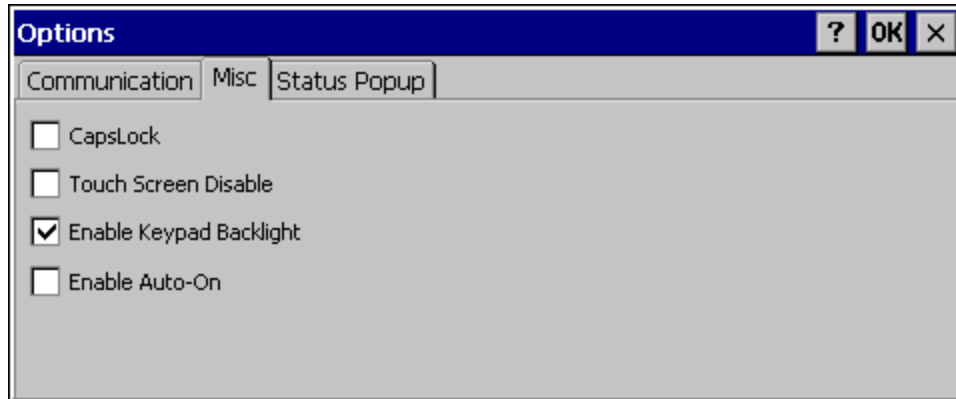
By default, GrabTime synchronizes via an Internet connection. To synchronize with a local time server:

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

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

Misc

Options on this tab configure device specific options. Note that options not available on the Thor VM1 are dimmed or grayed out.



CapsLock

By default, CapsLock is disabled after a warmboot. To enable CapsLock after a warmboot, click this checkbox.

Touch Screen Disable

By default, the Thor VM1 touch screen is enabled. To disable the touch screen after a warmboot, click this checkbox.

Note: If the touch screen is disabled on a Thor VM1 with the 12 key keypad, you must use a USB mouse or keyboard attached to the Thor VM1 to access this tab to re-enable the touch screen.

Enable Keypad Backlight

By default, the keypad backlight default setting is to follow the display backlight setting until it is changed by the user. Click the checkbox to disable the keypad backlight.

Enable Auto-On

When Auto-On is enabled, the Thor VM1 boots when external power is applied.

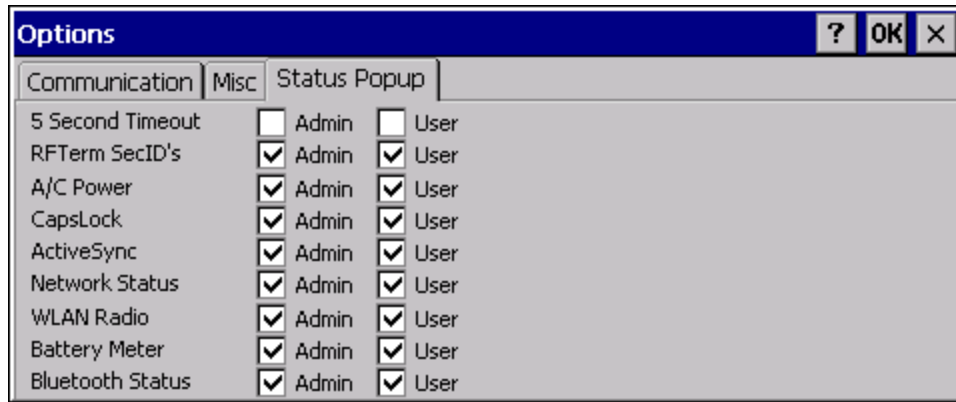
When Auto-On is disabled:

- if the ignition input signal is connected, when ignition changes from Inactive to Active the Thor VM1 boots.
- if the ignition input is not connected, the Thor VM1 only boots when the power button is pressed.

The default is disabled.

Status Popup

Options on this tab configure the Status Popup window. When the Status popup window is displayed, it is placed on top of the window in focus and hides any data beneath it. It is closed by pressing the assigned Status User or Status Admin key sequence.



Using the [key mapping control panel](#), the System Administrator must first assign a **Status User** key sequence for the end-user when they want to toggle the Status Popup Window on or off.

The System Administrator must also assign a **Status Admin** key sequence to perform the same function. Status popup window display options (taskbar icons) are assigned on the Status Popup tab. E.g. AC Power, ActiveSync, WLAN radio, CapsLock, Network status, Bluetooth status, etc.

The default for the User and Admin status popup windows is to show all status information. The 5 second timeout to remove the status popup from the display is disabled by default for the User and Admin status popup windows.

Owner

Start > Settings > Control Panel > Owner

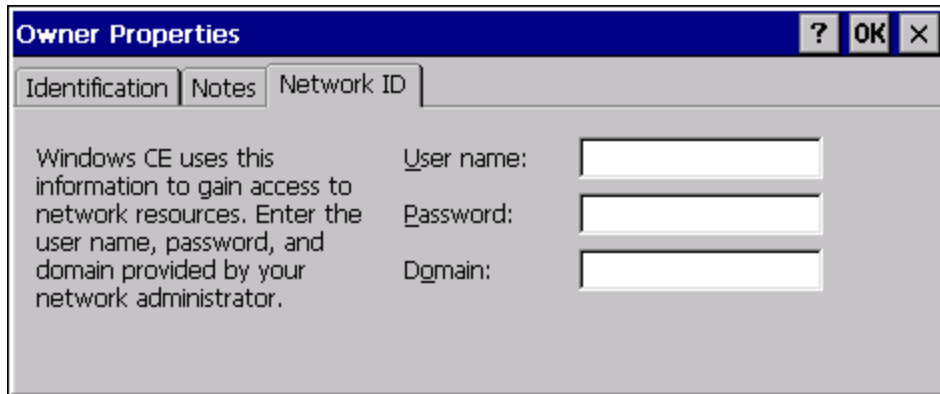
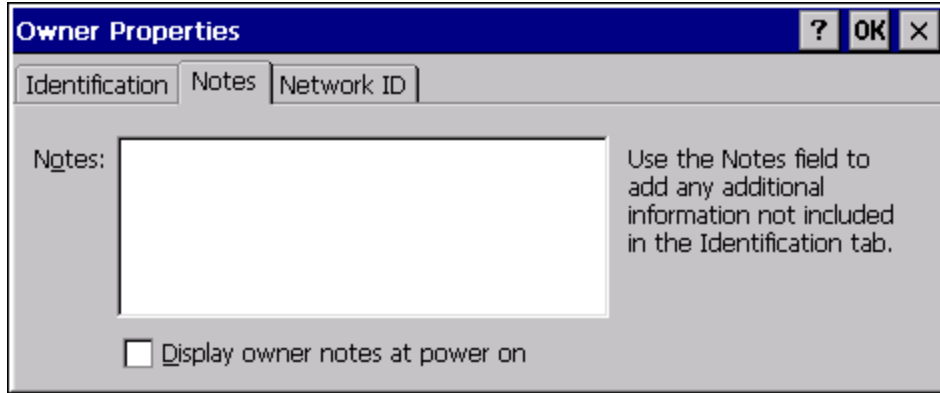
Set the Thor VM1 owner details. The Network ID is used when logging into a remote network.

Factory Default Settings

Identification tab	
Name	Blank
Company	Blank
Address	Blank
Telephones	Blank
Display owner ID at power-on	Disabled
Notes tab	
Notes	Blank
Display notes at power-on	Disabled
Network ID tab	
User Name	Blank
Password	Blank
Domain	Blank

The screenshot shows the 'Owner Properties' dialog box with the 'Identification' tab selected. The dialog has three tabs: 'Identification', 'Notes', and 'Network ID'. The 'Identification' tab contains the following fields:

- Name: [Text Input]
- Company: [Text Input]
- Address: [Text Input]
- At Power On: Display owner identification
- Area code: [Text Input]
- Phone: [Text Input]
- Work: [Text Input]
- Home: [Text Input]



Enter user name, password and domain to be used when logging into network resources.

Password

Start > Settings > Control Panel > Password

Use this panel to set Thor VM1 user access to control panels and power up password properties.

Important: This password must be entered before performing a Load Factory Defaults.

If entering a power-on or screen saver password does not allow you to disable this password protection or perform a Load Factory Defaults, contact Customer Support.

Factory Default Settings

Password	Blank
Enter password at Power On	Disabled
Enter password at Remote Desktop Screen Saver	Disabled



- The password and password settings are saved during a warm boot and a restart.
- The screensaver password affects the Remote Desktop screensaver only.
- After a password is assigned and saved, each time a **Settings > Control Panel** option is selected, the user will be required to enter the password before the Control Panel will open.
- The screensaver password is the same as the power-on password. They are not set independently.
- A screensaver password cannot be created without first enabling the “Enable password protection at power-on” checkbox.
- The screensaver password is not automatically enabled when the “power-on” checkbox is enabled.

Enter the password in the Password text box, then press Tab and type the password again to confirm it.

Enable the power-on checkbox and, if desired, the screensaver checkbox.

A changed/saved password is in effect immediately.

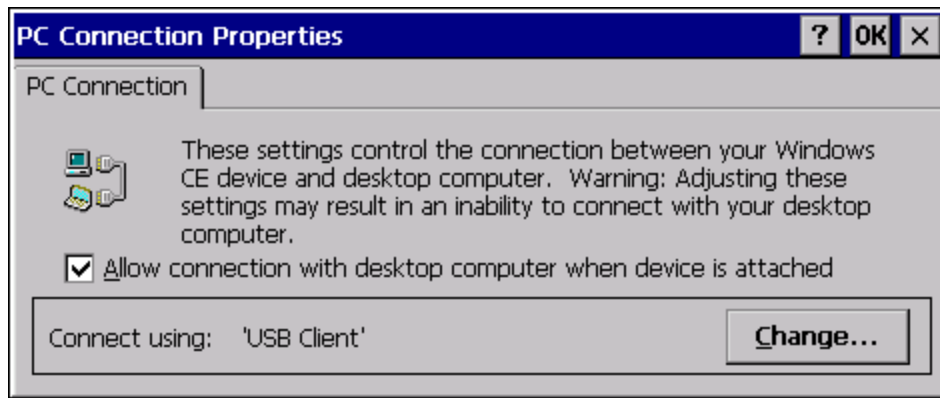
PC Connection

Start > Settings > Control Panel > PC Connection

Use these options to control a cabled connection (USB, serial) between the Thor VM1 and a nearby desktop/laptop computer.

Factory Default Settings

Enable direct connection	Enabled
Connect using	USB Client



Tap the **Change** button to change the direct connect setting.

Tap the drop-down box to view a list of pre-configured connection settings.

Peripherals

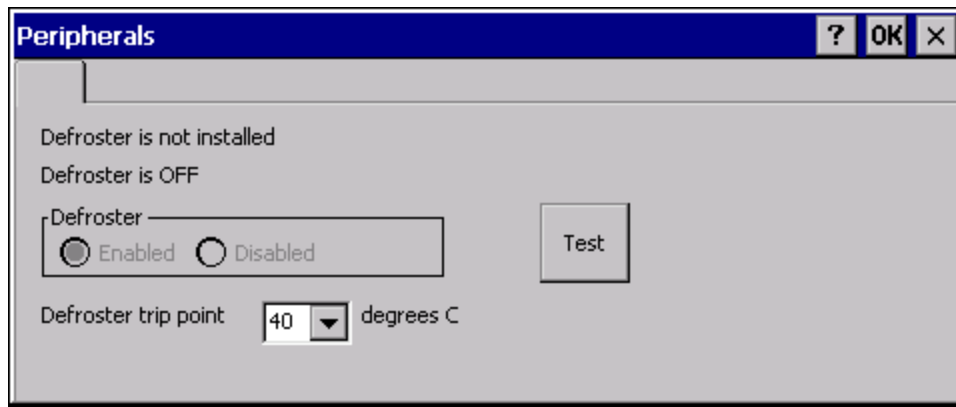
Start > Settings > Control Panel > Peripherals

This panel is used to enable and disable the touch screen defroster.

Factory Default Settings

Defroster	Enabled (if installed)
Defroster Trip Point	40° C / 104° F

Note: Settings have no effect if the defroster is not installed.



The screen displays the information about the defroster:

- If the defroster is installed
- The current state of the defroster, ON or OFF
- If the defroster is Enabled or Disabled
- The defroster trip point.

Tap the **Test** button to determine the presence of the defroster. Use this button when the front panel of the Thor VM1 has been swapped. For example, if the Thor VM1 did not contain a defroster but a new front panel with a defroster is installed, tap the **Test** button to update the defroster presence status on this tab.

If a defroster is installed, the defroster can be switched between the **Enabled** and **Disabled** states using the radio buttons on this tab. The default is **Enabled**.

Specify the **Defroster trip point**. The default trip point is 40° C / 104° F.

Power

Start > Settings > Control Panel > Power

The Thor VM1 power mode timers are cumulative.

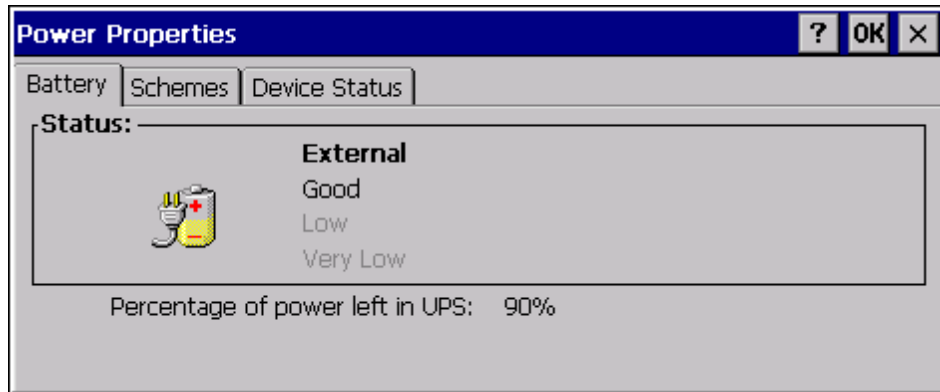
The System Idle timer begins the countdown after the User Idle timer has expired and the Suspend timer begins the countdown after the System Idle timer has expired.

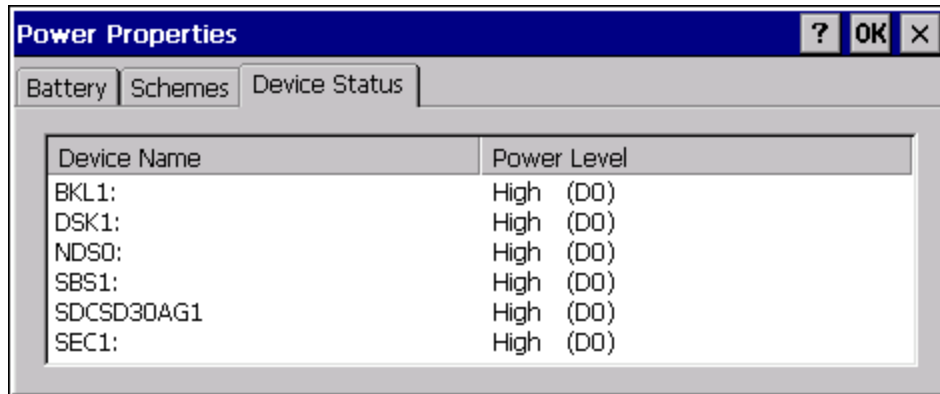
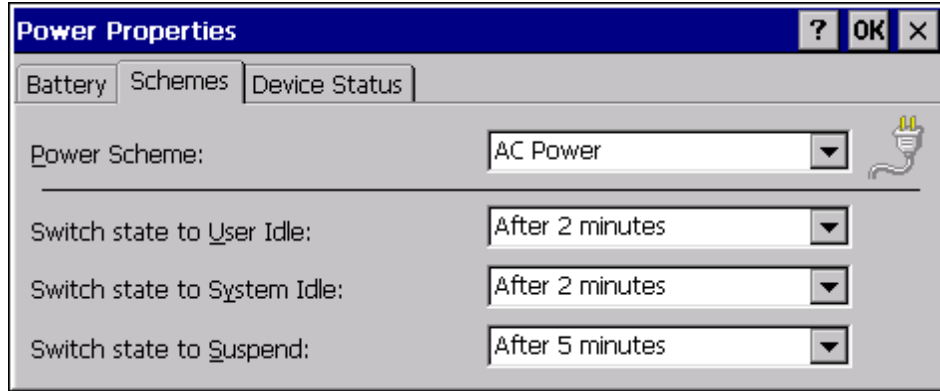
When the User Idle timer is set to “Never”, the power scheme timers never place the device in User Idle, System Idle or Suspend modes (even when the device is idle).

The Display > Backlight setting is synchronized with the User Idle setting in the Schemes tab in the Power control panel.

Factory Default Settings

Battery tab	No user interaction	
Schemes tab		
Power Scheme	Battery Power	AC Power
User Idle Timeout	3 seconds	2 minutes
System Idle Timeout	15 seconds	2 minutes
Suspend Timeout	5 minutes	8 hours
Device Status tab	No user interaction	





Because of the cumulative effect, if the Battery Power Scheme timers are set to 3 seconds, 15 seconds and 5 minutes:

- The backlight turns off after 3 seconds of no activity,
- The display turns off after 18 seconds of no activity (15 sec + 3 sec),
- And the Thor VM1 enters Suspend after 5 minutes and 18 seconds of no activity.
- If the User Idle timer is set to Never, the power scheme timers never place the Thor VM1 in User Idle, System Idle or Suspend modes.

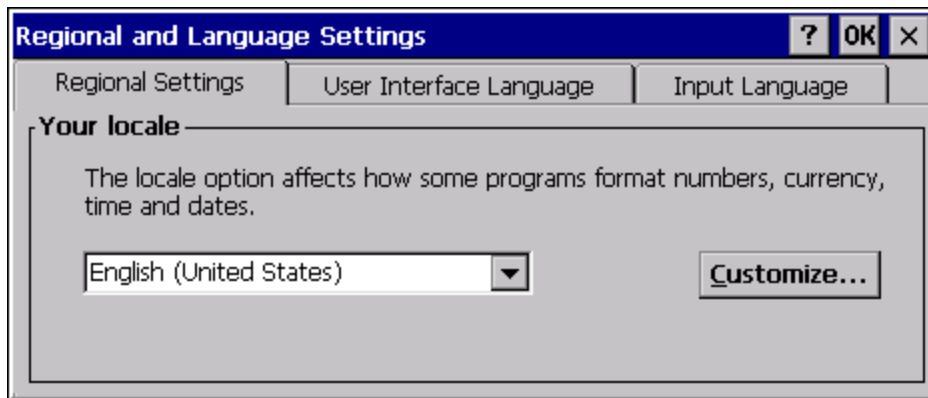
Regional and Language Settings

Start > Settings > Control Panel > Regional Settings

Set the appearance of numbers, currency, time and date based on regional and language settings. Set the Thor VM1 user interface language and the default input language.

Factory Default Settings

Region	
Locale	English (United States)
Number	123,456,789.00 / -123,456,789.00 neg
Currency	\$123,456,789.00 pos / (\$123,456,789.00) neg
Time	h:mm:ss tt (tt=AM or PM)
Date	M/d/yy short / dddd,MMMM,dd,yyyy long
Language	
User Interface	English (United States)
Input	
Language	English (United States)-US
Installed	English (United States)-US

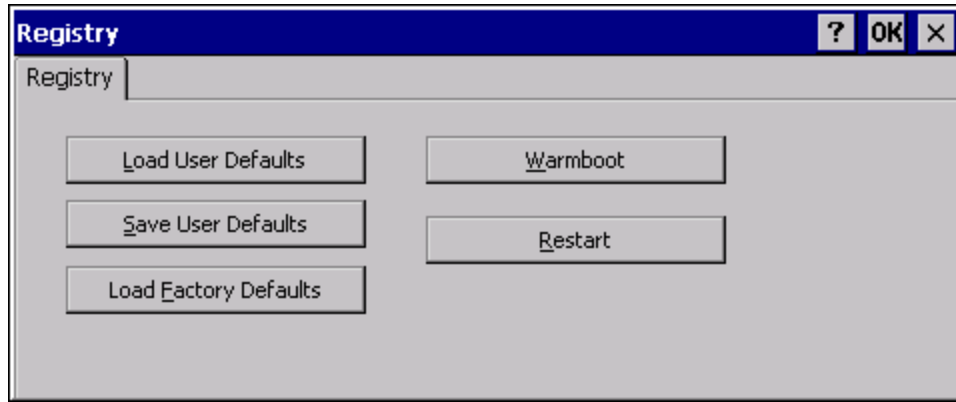




Registry

Start > Settings > Control Panel > Registry

Choose options for managing the registry and rebooting the Thor VM1.



Button	Action
Load User Defaults	When clicked, a standard load file dialog is opened, to allow the user to pick a Registry Save (.RSG) file. The applet then copies the specified User registry file to the Active registry. The user is asked to verify a reboot, and then the applet does a warmboot to activate the new registry.
Save User Defaults	When clicked, a standard Save File dialog is opened, to allow the user to name the Registry Save (.RSG) file. The applet then copies the Active registry to the specified User registry file and reboots the device.
Load Factory Defaults	The applet copies the Factory Default registry from the OS to the Active registry (by deleting the current registry). The user is asked to verify a reboot, and then the applet performs a restart to activate the factory default registry. If a user password has been set, the applet warns the user that the password will be erased, and asks them to enter it before the reboot is allowed.
Warmboot	When clicked, the OS performs a registry save (Active registry saved to Flash registry hive), and then a warmboot. The contents of RAM are preserved. CAB files already loaded into RAM remain loaded.
Restart	When clicked, the OS performs a registry save, and then a restart. OS and CAB files are reloaded.

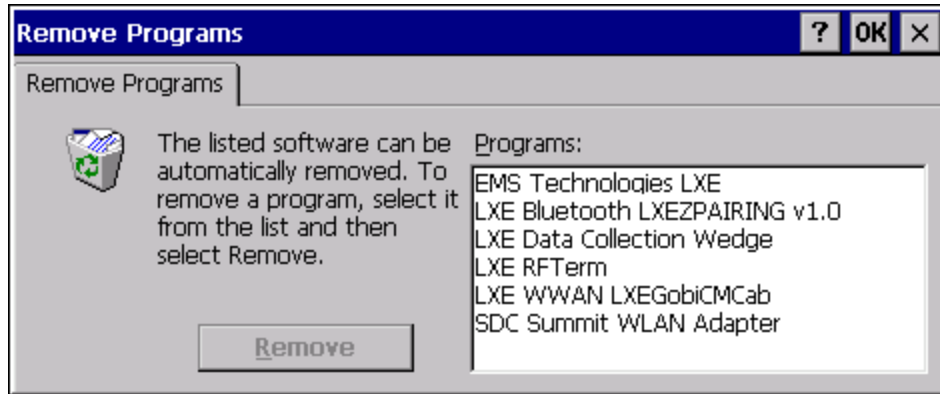
Remove Programs

Start > Settings > Control Panel > Remove Programs

Note: Lists programs installed in RAM that have been marked for removal.

Select a program and tap Remove. Follow the prompts on the screen to uninstall Thor VM1 user-installed only programs. The change takes effect immediately.

Files stored in the **My Documents** folder are not removed using this option.



Note: Do not remove factory installed programs using this option. Contact [Technical Assistance](#) if factory installed programs must be deleted.

Screen Control

Start > Settings > Control Panel > Screen Control

Set screen properties for the Thor VM1.

Factory Default Settings

Screen Blanking (Blackout)	
Enable screen blanking	Disabled
Screen on delay (ms)	1000
COM Port	none selected
Current Level	
LCD Brightness (%)	100 (see note)
Ambient Light (%)	(see note)
Automatic Brightness Control	
<i>Automatic brightness control is only available on a Thor VM1 with an outdoor display.</i>	
Enable automatic brightness control	Disabled
Low to medium light level (%)	25
Medium to high light level (%)	75

Note: If Automatic Brightness Control is enabled for an outdoor display, the value for LCD Brightness depends on the Ambient Light %. Otherwise, the display defaults to 100% brightness.

Note: There is no default value for Ambient Light % as it varies depending on the level of light where the Thor VM1 is located. If the Thor VM1 has an indoor display it does not have an ambient light sensor and the Ambient Light % is always 0.

Screen Control v0.2

Screen Blanking (Blackout)

Enable screen blanking

Screen on delay (ms)

COM Port

Current Level

LCD Brightness (%) Ambient Light (%)

Automatic Brightness Control (for outdoor display only)

Enable automatic brightness control

Low to medium light level (%)

Medium to high light level (%)

Cancel OK

Note: Touch screen defroster controls are located on the [Peripherals](#) tab.

Screen Blanking

Screen blanking requires the following hardware:

- A [Screen Blanking Box](#) or [user-supplied switch](#)
- A [cable](#) from the serial port to the box or switch.



Do not enable Screen Blanking until the [cable](#) is properly connected to the specified COM port.

Screen blanking allows the Thor VM1 display to automatically be turned off whenever the vehicle is in motion. When the Thor VM1 display is off due to vehicle motion, the integrated keypad backlight remains on.

Screen blanking requires a user supplied cable properly connected as shown below. To enable blanking, check the **Enable screen blanking** checkbox. The default is disabled.

Use the **Screen on delay** to specify the period of time in ms (milliseconds) between when the vehicle stops and the Thor VM1 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, either COM1 or COM2. If a COM port is in use by another application (such as DC Wedge), that COM port is grayed out and cannot be selected for screen blanking.

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

Current Level

LCD brightness displays the current LCD brightness level. The default brightness is 100%.

- LCD brightness can be manually adjusted using the **2nd plus F7** or **2nd plus F8** keypress sequences. Any changes to brightness level using the keypresses are reflected in this section.
- If Automatic Brightness Control is enabled (outdoor display only), the value for LCD brightness depends on the current Ambient Light value and the values for the Automatic Brightness Control thresholds.

Automatic Brightness Control

When the Thor VM1 is equipped with the outdoor display, automatic brightness control can be enabled. When enabled, display brightness is based on ambient light detected by the ambient light sensor, located near the top right of the display. The default is disabled. To enable, check the **Enable automatic brightness control** checkbox and specify the thresholds for display backlight transition.

When enabled, the thresholds can be entered for display brightness transitions.

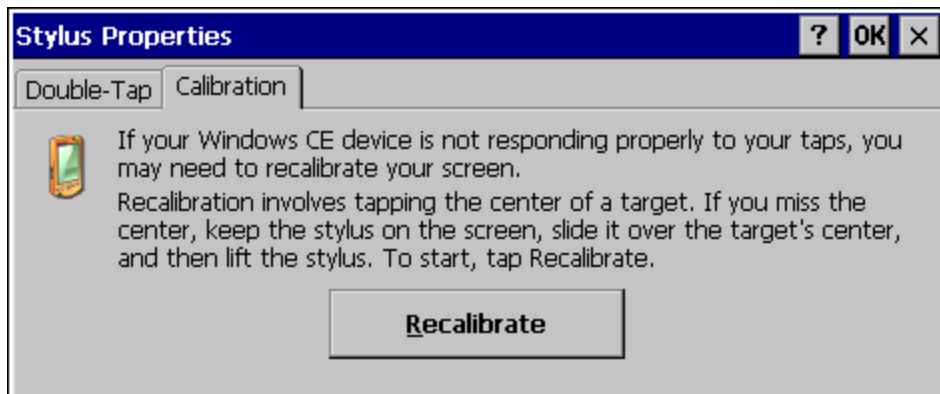
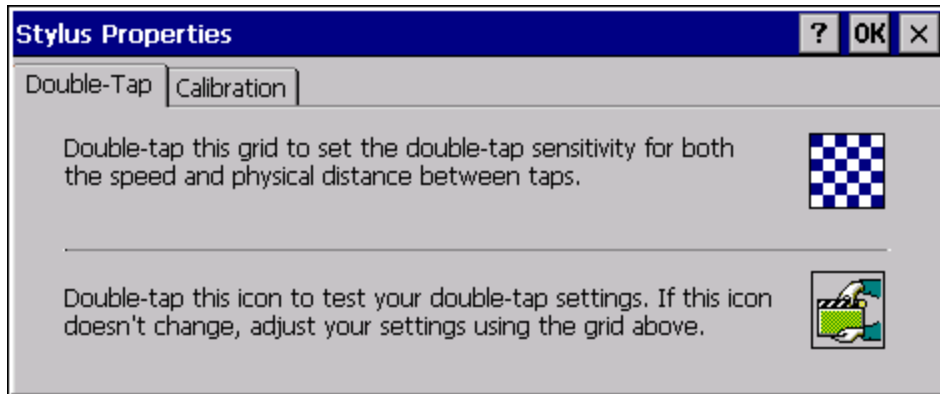
- When a low level of ambient light is detected, the display backlight is set to low level.
- When the ambient light exceeds the threshold specified in **Low to medium light level (%)**, the display backlight is automatically increased to a medium level.
- When the ambient light exceeds the threshold specified in **Medium to high light level (%)**, the display backlight is automatically increased to a high level.
- Likewise if the Thor VM1 is returned to a lower ambient light area, the display backlight automatically transitions to the appropriate lower display backlight level.

By default, the **keypad backlight** follows the display backlight. If the display backlight is on, the keypad backlight is on.

Stylus

Start > Settings > Control Panel > Stylus

Use this control panel option to set stylus double-tap sensitivity properties and calibrate the Thor VM1 touch panel when needed.



Double-Tap

Follow the instructions on the screen and tap the OK button to save any double-tap changes.

Calibration

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

To begin, tap the **Recalibrate** button on the screen with the stylus. Press and hold the stylus on the center of the target as it moves around the screen. Press the Enter key to keep the new calibration setting or press the Esc key to revert to the previous calibration settings.

Note: If the touch screen loses calibration on a Thor VM1 with the 12 key keypad, you must use a USB mouse or keyboard attached to the Thor VM1 to access this tab to recalibrate the touch screen.

System

Start > Settings > Control Panel > System

Use these Thor VM1 panels to:

- Review System and mobile device data and revision levels.
- Adjust Storage and Program memory settings.
- Assign a device name and device descriptor.

Factory Default Settings

General	No user interaction
Memory	1/4 storage, 3/4 program memory
Device Name	Unique to equipment type
Device Description	Unique to equipment type
Copyrights	No user interaction

General Tab

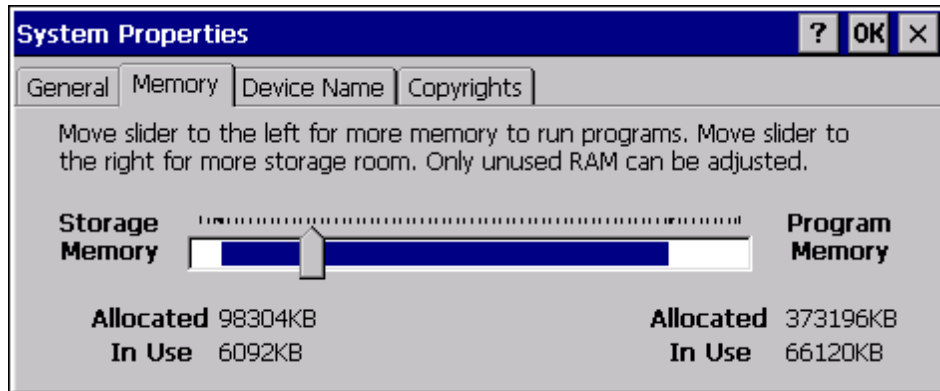


System: This screen is presented for information only. The System parameters cannot be changed by the user.

Computer: The processor type is listed. The type cannot be changed by the user. Total computer memory and the identification of the registered user is listed and cannot be changed by the user.

Memory sizes given do not include memory used up by the operating system. For example, a system with 128 MB may only report 99 MB memory, since 29 MB is used by the operating system. This is actual DRAM memory, and does not include internal flash used for storage.

Memory Tab



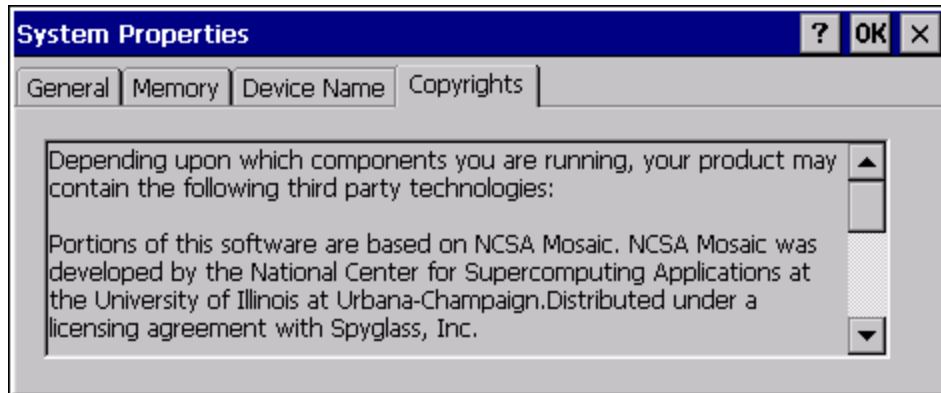
Move the slider to allocate more memory for programs or storage. If there isn't enough space for a file, increase the amount of storage memory. If the mobile device is running slowly, try increasing the amount of program memory.

Device Name Tab



The device name and description can be changed by the user. Enter the name and description using either the keypad or the Input Panel and tap OK to save the changes. This information is used to identify the Thor VM1 to other computers and devices.

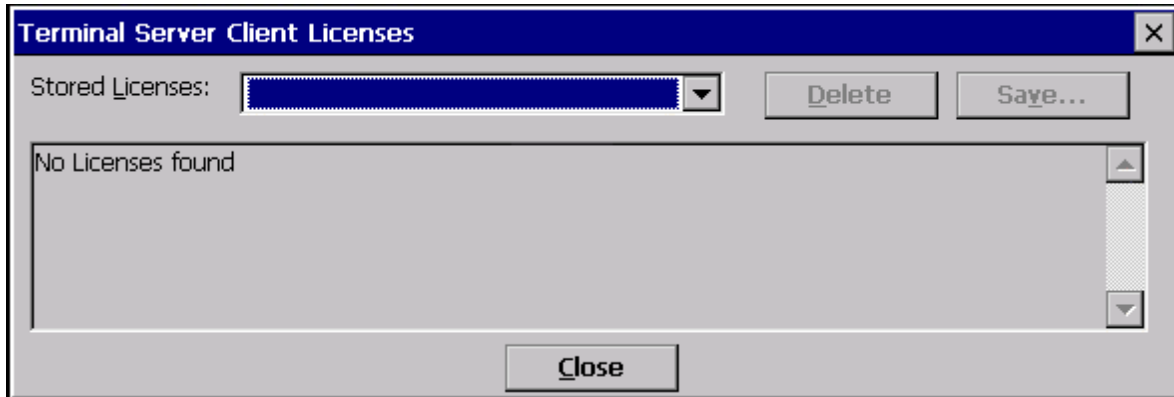
Copyrights Tab



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

Terminal Server Client Licenses

Start > Settings > Control Panel > Terminal Server Client Licenses



Any licenses stored on the Thor VM1 appear in the drop-down list. Select a license and tap the Close button. The license is available for use immediately.

Volume and Sounds

Start > Settings > Control Panel > Volume & Sounds

Note: An application may override the control of the speaker volume. Turning off sounds saves power and prolongs battery life.

Set volume parameters and assign sound WAV files to CE events using these options.

You can also select / deselect sounds for key clicks and screen taps and whether each is loud or soft.

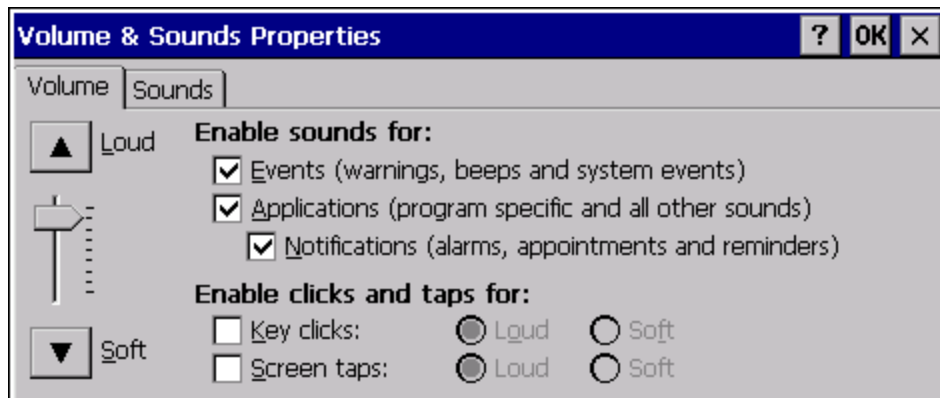
As the volume scrollbar is moved between Loud and Soft, the Thor VM1 emits a tone each time the volume increases or decreases.

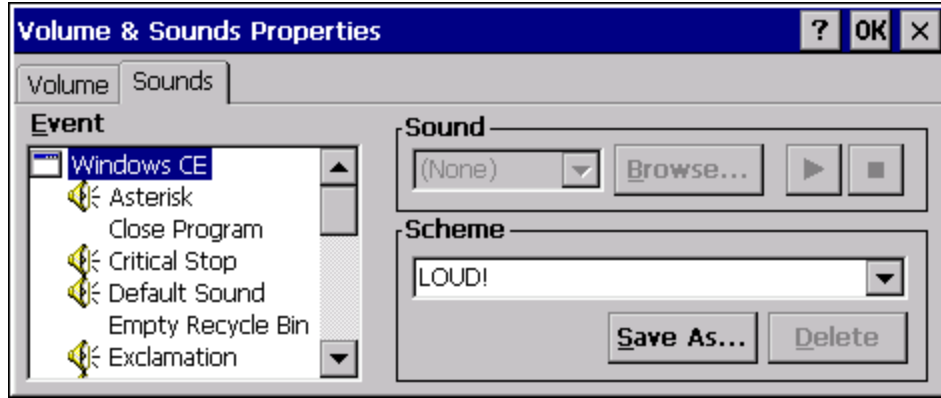
Volume must be enabled when you want to adjust volume settings using keypad keys.

Factory Default Settings

Volume	
Events	Enabled
Application	Enabled
Notifications	Enabled
Volume	One level below Loud
Key click	Disabled
Screen tap	Disabled
Sounds	
Scheme	LOUD!

Good Scan and Bad Scan Sounds





The volume setting is stored in the registry and is recalled at power on.

Note: Rejected bar codes generate a bad scan beep. In some cases, the receipt of data from the scanner triggers a good scan beep from a tethered scanner, and then the rejection of scanned bar code data by the bar code processing causes a bad scan beep from the mobile device on the same data.

Good Scan and Bad Scan Sounds

Good scan and bad scan sounds are stored in the Windows directory, as SCANGOOD.WAV and SCANBAD.WAV. These are unprotected WAV files and can be replaced by a WAV file of the user's choice.

By default a good scan sound on the Thor VM1 is a single beep, and a bad scan sound is a double beep.

WiFi Control Panel

Start > Settings > Control Panel > WiFi

or click the **Summit Client Utility icon**

Use this option to set parameters and manage profiles for the wireless client pre-loaded on your Thor VM1.

See the *Summit Client Utility* for information and instruction.



Chapter 4: ActiveSync

Introduction

Requirement : ActiveSync (version 4.5 or higher for **Windows XP** desktop/laptop computers) must be resident on the host (desktop/laptop) computer. **Windows Mobile Device Center** (version 6.1 or higher) is required for a **Windows Vista/Windows 7** desktop/laptop computer. ActiveSync and Windows Mobile Device Center for the PC is available from the Microsoft website. Follow their instructions to locate, download and install ActiveSync or Windows Mobile Device Center on your desktop computer.

Note: For readability in this section, ActiveSync will be used in instructions and explanations. If you have a Windows Vista or Windows 7 operating system on your desktop/laptop, replace ActiveSync with Windows Mobile Device Center.

Using Microsoft ActiveSync, you can synchronize information on your desktop computer with the Thor VM1 and vice versa. Synchronization compares the data on your mobile device with your desktop computer and updates both with the most recent data.

For example, you can:

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

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

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

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

Because ActiveSync is already installed on your device, your first synchronization process begins automatically when you finish setting up your desktop computer in the ActiveSync wizard. For more information about using ActiveSync on your desktop computer, open ActiveSync, then open ActiveSync Help.

Initial Setup

The initial setup of ActiveSync must be made via a USB connection. When there is a Connect icon on the desktop, this section can be bypassed. Partnerships can only be created using USB cable connection.

Connect via USB

The default connection type is **USB Client**

This is the only connection option supported on the Thor VM1.

To verify it is set to USB, select

[Start > Settings > Control Panel > PC Connection](#)

Tap the Change button. From the popup list, choose

USB Client

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

Tap OK to return to the Control Panel. If desired, any control panel windows may be closed.

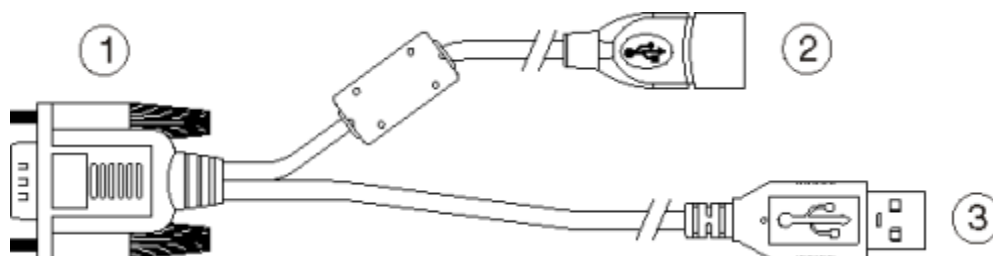
Connect the USB cable to the PC (the host) and the mobile device (the client) as detailed below. USB will start automatically when the USB cable is connected, not requiring you to select “Connect” from the start menu.

When the Thor VM1 loses connection, e.g. enters Suspend Mode, etc., the connection to ActiveSync will be lost. When the Thor VM1 resumes, the ActiveSync session will automatically re-connect.

Cable for USB ActiveSync Connection:

VM1052CABLE - Thor VM1 Dongle cable provides USB type A connector.

- D9 connector (labeled as #1 below) connects to the USB port on the Thor VM1 dock.
- The USB type A connector (labeled as #3 below) on cable connects to a USB port on a PC or laptop.
- The USB host (port #2) connector on the dongle cable does not need to be connected.



Explore

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

Backup Data Files using ActiveSync

Use the following information to backup data files from the mobile device to a desktop or laptop PC using the appropriate cable and Microsoft's ActiveSync.

Prerequisites

A partnership between the mobile device and ActiveSync has been established.

- A desktop or laptop PC with an available USB port and a mobile device with a USB port. The desktop or laptop PC must be running Windows XP or greater.
- Use the specific USB cable as listed in [Connect Via USB](#).

Connect

Connect the USB cable to the PC (the host) and the mobile device (the client).

The "Get Connected" wizard on the host PC checks COM ports to establish a connection for the first time.

Note: USB synchronization will start automatically when the cable is connected.

Disconnect

- Disconnect the cable from the Thor VM1.
- Open the status bar icon in the lower right hand corner of the status bar. Then tap the Disconnect button.

When the Thor VM1 loses connection, e.g. enters Suspend Mode, etc., the connection to ActiveSync will be lost. When the Thor VM1 resumes, the ActiveSync session will automatically re-connect.

Thor VM1 with a Disabled Touch Screen

An Thor VM1 touch screen can be disabled (using the Options control panel Misc tab). In these cases, it may be easier to configure the Thor VM1 using ActiveSync and LXEConnect rather than using the Thor VM1 keypad only.

Reset and Loss of Host Re-connection

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

When the mobile device is reset (return to default settings), the random number is deleted – and the partnership with the last one of the two hosts is also deleted. The host retains the random numbers and unique names of all devices having a partnership with it. Two clients cannot have a partnership with the same host if they have the same name. (**Control Panel > System > Device Name**)

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

Troubleshooting ActiveSync

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

Verify the dongle cable is attached to the Thor VM1. Disconnect and reconnect the cable from the PC.

Check that the correct connection is selected (USB "Client").

See Also: "Cold Boot and Loss of Host Reconnection".

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

One or more control lines are tied together incorrectly. This is usually a cable problem.

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

Check that the correct connection is selected (USB "Client")

-or-

Incorrect or broken data lines in cable.

ActiveSync indicator on the host remains gray

Solution 1: ActiveSync icon on the PC does not turn green after connecting USB cable from Thor VM1.

1. Disconnect Thor VM1 USB cable from PC.
2. Suspend/Resume or Restart the Thor VM1.
3. In **ActiveSync > File > Connection Settings** on PC disable Allow USB Connections and click OK.
4. Re-enable Allow USB Connections on the PC and click OK.
5. Reconnect USB cable from Thor VM1 to PC.

Solution 2: The host doesn't know you are trying to connect. May mean a bad cable, with no control lines connected, or an incompatible baud rate. Try the connection again, with a known good cable.

Configuring the Thor VM1 with LXEConnect

LXEConnect allows a user to view the Thor VM1 screen remotely from a PC using an ActiveSync connection:

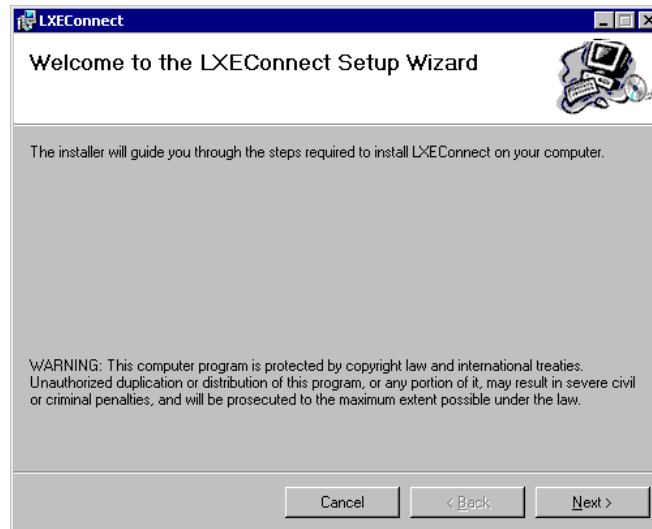
Requirements: ActiveSync version 4.5 (or higher) must be resident on a Windows XP (desktop/laptop) host computer.

Windows Mobile Device Center (version 6.1 or higher) is required for a Windows Vista/Windows 7 desktop/laptop computer.

ActiveSync is already installed on the Thor VM1. The Thor VM1 is preconfigured to establish a USB ActiveSync connection to a host PC when the USB cable is attached to the Thor VM1 and the host PC.

Install LXEConnect

1. Contact [Technical Assistance](#) for the LXEConnect files.
2. Download the files to a location on your host PC hard drive.
3. Execute the setup.exe file that was copied to the host PC. This setup program installs the LXEConnect utility.



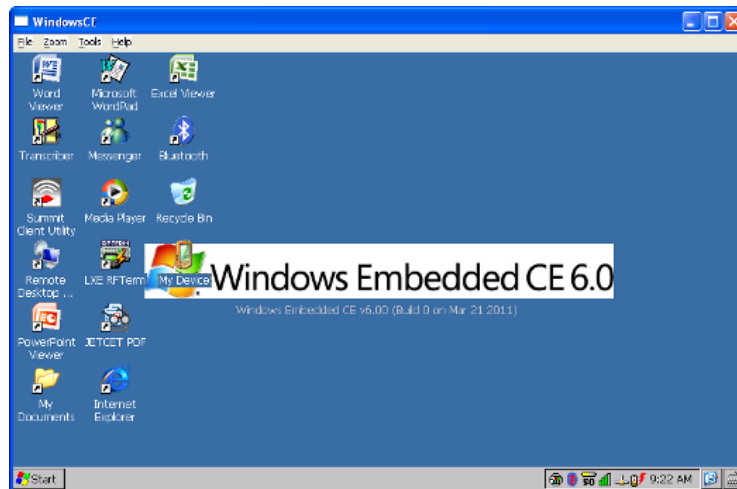
4. Follow the on screen installation prompts. The default installation directory is C:\Program Files\LXE\LXEConnect.
5. When the installation is complete, create a desktop shortcut to the LXEConnect.exe file located in the directory above. If a different directory was selected during installation, please substitute the appropriate directory.
6. LXEConnect is now installed on the host PC and ready to use.

Using LXEConnect

1. Power up the Thor VM1.
2. Connect the Thor VM1 to the host PC using the USB connection cable. Once connected, the ActiveSync dialog box appears and the ActiveSync connection is automatically established.
3. Select “No” for partnership when prompted. Dismiss any ActiveSync dialog boxes warning a partnership is not set up. It is not necessary to establish a partnership to use LXEConnect. However, if a partnership is desired for other reasons, one may be established now.
4. Double-click the LXEConnect icon that was created on the PC desktop.
5. LXEConnect launches.



6. Click the OK button to dismiss the About CERDisp dialog box (see *Example LXEConnect Notice* image above) on the Thor VM1 desktop by clicking the OK button in the LXEConnect window on the PC desktop. The dialog box automatically times out and disappears after approximately 20 seconds.



7. The Thor VM1 can now be configured from the LXEConnect window. Input from the PC’s mouse and keyboard are recognized as if they were attached to the Thor VM1.
8. When the remote session is completed, terminate the LXEConnect program by selecting **File > Exit** or clicking on the **X** in the upper right hand corner to close the application, then disconnect the ActiveSync cable.



Chapter 5: Enabler Installation and Configuration

Introduction

This section discusses Honeywell supported features with Wavelink Avalanche Mobile Device Servers. This section is split into three basic areas:

- Installation
- User Interface
- Enabler Configuration

Installation

To use the Wavelink Avalanche MC System, the following items are required:

- A desktop or laptop PC on which to install the Avalanche MC Console.
- A desktop or laptop PC on which to install the Avalanche Mobile Device Server (this can be the same PC where the Avalanche MC Console is installed).
- Wavelink Avalanche MC Console 4.2 or later.
- A Wavelink Device License for each client device.

To use Avalanche Remote Control, the follow additional items are required:

- Wavelink Remote Control plug-in, 2.0 or later
- A Wavelink Remote Control License for each client device

Installing the Enabler on Mobile Devices

Supported devices have the Avalanche Enabler installation files loaded, but not installed, on the mobile device when it is shipped. The installation files are located in the \System folder on Windows devices.

Note: ***Important:** If the user is NOT using Wavelink Avalanche to manage their mobile device(s), the Enabler should not be installed on the mobile device(s). Doing so results in unnecessary delays when booting the device.*

The Avalanche Enabler installation file LXE_ENABLER.CAB is loaded on the Thor VM1 by Honeywell; however, the device is not configured to launch the Enabler installation file automatically. The installation application must be run manually the first time Avalanche is used.

After installation, the Enabler runs as a background application monitoring for updates. This behavior can be modified by accessing the Avalanche Update Settings panel through the Enabler interface.

This behavior can be modified by accessing the Avalanche Update Settings panel through the Enabler Interface.

The RMU.CE.CAB file is placed on the device during manufacturing in the \System\RMU folder.

During the Enabler installation process, the Enabler checks for the RMU.CE.CAB file in the \System folder.

- If present, it assumes the RMU.CE.CAB file is already installed and continues.
- If the file RMU.CE.CAB file is not present, it looks for the file in the \System\RMU folder.
- If present, the Enabler copies the file to the \System folder and installs it.

At this point, the OS will automatically install the Remote Management Utility (RMU) after the Thor VM1 reboots.

Enabler Uninstall Process

To remove the Avalanche Enabler from the Thor VM1:

- Delete the Avalanche folder located in the \System directory.
- Warm boot the Thor VM1.

The Avalanche folder cannot be deleted while the Enabler is running. See [Stop the Enabler Service](#).

If sharing errors occur while attempting to delete the Avalanche folder, warm boot the Thor VM1, immediately delete the Avalanche folder, and then perform another warm boot.

Stop the Enabler Service

To stop the Enabler from monitoring for updates from the Mobility Center Console:

1. Open the Enabler Settings Panels by tapping the Enabler icon on the Thor VM1 desktop.
2. Select **File > Settings**.
3. Select the **Preferences** tab.
4. Select **Do not monitor** to prevent automatic monitoring upon **Startup**.
5. Select **Exit Application** for an immediate shutdown of all Enabler update functionality upon exiting the user interface.
6. Click the **OK** button to save the changes.
7. **Reboot** the Thor VM1 if necessary.

Update Monitoring Overview

There are three methods by which the Enabler on the Thor VM1 can communicate with the Mobile Device Server running on the host machine.

- Wired via a serial cable between the Mobile Device Server PC and the Thor VM1.
- Wired via a USB connection, using ActiveSync, between the Mobile Device Server PC and the Thor VM1.
- Wirelessly via the Thor VM1 2.4GHz radio and an access point

After installing the Enabler on the Thor VM1 the Enabler searches for a Mobile Device Server, first by polling all available serial ports and then over the wireless network.

The Enabler running on the Thor VM1 will attempt to access COM1, COM2, and COM3. "Agent not found" will be reported if the Mobile Device Server is not located or a serial port is not present or available (COM port settings can be verified using the bar code wedge panels on the Thor VM1).

The wireless connection is made using the default wireless [radio] interface on the mobile device therefore the Thor VM1 must be actively communicating with the network for this method to succeed.

If a Mobile Device Server is found, the Enabler automatically attempts to apply all wireless and network settings from the active profile. The Enabler also automatically downloads and processes all available packages.

If the Enabler does not automatically detect the Mobile Device Server, the IP address of the Mobile Device Server can be entered on the Connect tab of the Enabler setup. Please see [Enabler Configuration](#) for details.

Mobile Device Wireless and Network Settings

Once the connection to the Mobile Device Server is established, the Thor VM1 Enabler attempts to apply all network and wireless settings contained in the active profile.

The success of the application of settings is dependent upon the local configuration of control parameters for the Enabler.

These local parameters cannot be overridden from the Avalanche MC Console.

The default Enabler adapter control settings are:

- Manage network settings – enabled
- Use Avalanche network profile – enabled
- Manage wireless settings – disabled

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

1. Open the Enabler Settings Panels by tapping the **Enabler icon** on the desktop.
2. Select **File > Settings**.
3. Select the **Adapters** tab.
4. Choose settings for the **Use Manual Settings** parameter.
5. Choose settings for **Manage Network Settings**, **Manage Wireless Settings** and **Use Avalanche Network Profile**.
6. Click the **OK button** to save the changes.
7. **Reboot** the device.

Preparing a Device for Remote Management

Two additional utilities are necessary for remote management.

- The **Remote Management Utility (RMU)** must be installed on all mobile devices first – then you can control mobile device reboot, storage RAM adjustment, real-time updates and Avalanche Enabler properties. If the RMU is not already installed on the Thor VM1, see [Using Wavelink Avalanche to Upgrade System Baseline](#). If in doubt, verify RMU.CE.CAB exists in the \System folder. If the RMU.CE.CAB file is present when the Enabler is installed, the RMU is also installed.

Important: If the OS package includes double-byte Asian fonts, the storage RAM property of the RMU must be higher than the default value (40MB).

If the amount of storage RAM is too low, the Enabler returns a “Mobile unit out of resources” error.

- Use the **Wireless Configuration Application (WCA)** when you want to remotely manage the Summit client device. This utility is downloaded and installed in addition to the Remote Management Utility. The WCA is included when the Summit radio driver software is updated. The WCA is automatically installed when the radio driver is updated.

If the Remote Management Utility (RMU) is not present on the Thor VM1, see [Using Wavelink Avalanche to Upgrade System Baseline](#).

Using Wavelink Avalanche to Upgrade System Baseline

This procedure assumes the Avalanche Enabler is already installed on the Thor VM1 and is already in communication with the Avalanche MC Console.

Part 1 – Bootstrapping the RMU

1. Install the RMUCEbt package into the Avalanche MC Console. Do NOT include the Reboot option as part of the configuration (i.e. the **Reboot button** in the “Reboot Options” branch must be unbolded).
2. Enable ONLY the RMUCEbt package in the Avalanche MC Console and update the devices. The RMU is downloaded and automatically installed.
3. **Disable** the RMUCEbt package in the Avalanche MC Console.
4. For each device, **double-click** on the device to open the Client Controls dialog box.
5. Check the **Delete Orphaned Packages** checkbox and click the **Update Now** button.
6. After the sync completes, uncheck **Delete Orphaned Packages** and close the dialog box.

Part 2 – Installing Packages

1. **Enable** the RMUCE package in the Avalanche MC Console.
2. **Enable** all remaining packages and send them down. It is important that you include the new OS package in this group (be sure to include the Enabler). If the radio is to be managed remotely, it is important to include the radio package in this group so that after the reboot the radio can automatically associate. If the radio package is not sent, the device loses connection to the network and manual configuration of the radio parameters is required.
3. Set the Reboot setting for the OS package to **Auto**.
4. After all packages are downloaded (this may take several minutes) the Remote Management Utility (RMU) is launched. The RMU processes all the downloaded packages. If the radio package was downloaded, the Wireless Configuration Application (WCA) is launched to process the new radio settings.
5. After the RMU finishes installing all the packages, the device is automatically coldbooted (assuming the Reboot setting was set to Auto in Step 3).
6. After the Device completes the coldboot, the RMU is autoinstalled by the OS and the previously downloaded packages are restored. Assuming at least one package has registry settings that were restored, and that package was set to reboot (either auto or prompt), the RMU then performs an automatic warmboot.
7. After the warmboot, the device is configured.
8. If the device will no longer be monitored by Wavelink Avalanche, you may remove the Enabler to eliminate boot up delays, if desired. Even if the Enabler is removed, the installed packages and their configurations continue to be restored with every reboot by the RMU.

Version Information on Mobile Devices

The VersionInfo.EXE file is included in the Remote Management Utility package downloaded to the Thor VM1. It is stored in the \Program Files\RMU folder. When VersionInfo.EXE is opened, a dialog box is presented to the Thor VM1 user displaying:

- Remote Management Utility (RMU) version
- Wireless Configuration Application (WCA) version

VersionInfo displays the version for each utility only after that utility has been executed at least once.

User Interface

The Enabler can be configured and controlled manually through the user interface on the Thor VM1. This section details the functionality that can be controlled by the user or system administrator.

Parameters and Screen Displays

Screen displays shown in this section are designed to present the end-user with information graphically.

Placement of information on the screen displays may be split between one or many tabbed panels.

Standard Avalanche Enabler parameters that are not supported by Honeywell may be missing or dimmed (visible but unable to be edited) on the tabbed panels or screen displays.

Enabler Configuration

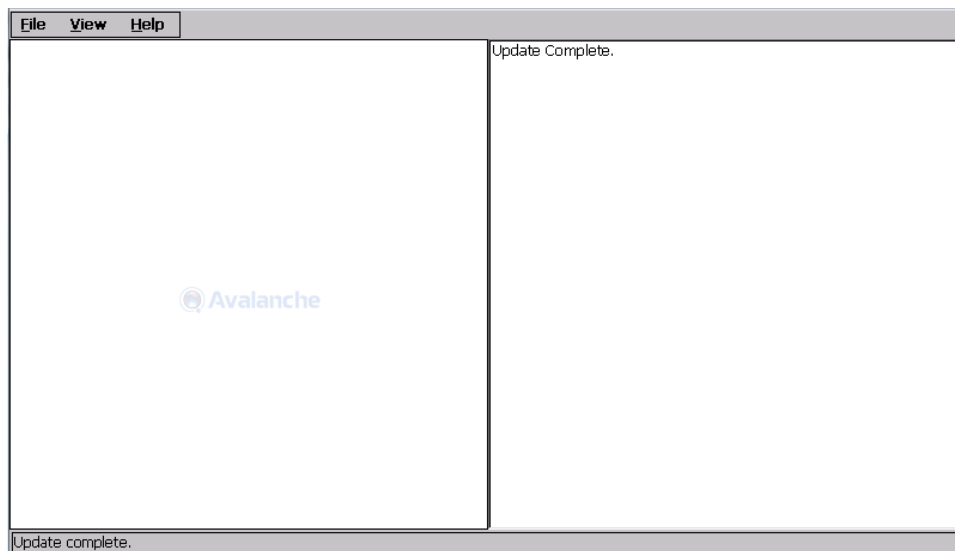
Depending on the version of the Enabler running on the Thor VM1, the desktop Enabler icon may look like one of the following:



The available configuration options and tabs may vary by Enabler version. The examples shown in this section assume the latest version of the Enabler is installed on the Thor VM1.


The Enabler user interface application is launched by clicking either the **Enabler icon** on the desktop or Taskbar or by selecting **Avalanche Enabler** from the Programs menu.

The opening screen presents the Thor VM1 user with the connection status and a navigation menu.



Note: Some parameters and features described in this section may not be available if you are not running the latest version of the Enabler. Contact [Technical Assistance](#) for upgrades.

File Menu Options

Connect	The Connect option under the File menu allows the user to initiate a manual connection to the Mobile Device Server. The connection methods, by default, are wireless and COM connections. Any updates available will be applied to the Thor VM1 immediately upon a successful connection.
Scan Config	<i>The Scan Configuration feature is not supported.</i> The Scan Config option under the File menu allows the user to configure Enabler settings using a special bar code that can be created using the Avalanche MC Console utilities. Refer to the Wavelink Avalanche Mobility Center User Guide for details.
Settings	<p>The Settings option under the File menu allows the Thor VM1 user to access the control panel to locally configure the Enabler settings. The Enabler control panel is, by default, password protected.</p>  <p>The default Settings password is system. The password is not case-sensitive.</p>

Avalanche Update using File > Settings

Use these menu options to setup the Avalanche Enabler on the Thor VM1. Change the settings and save them by rebooting before connecting to the network.

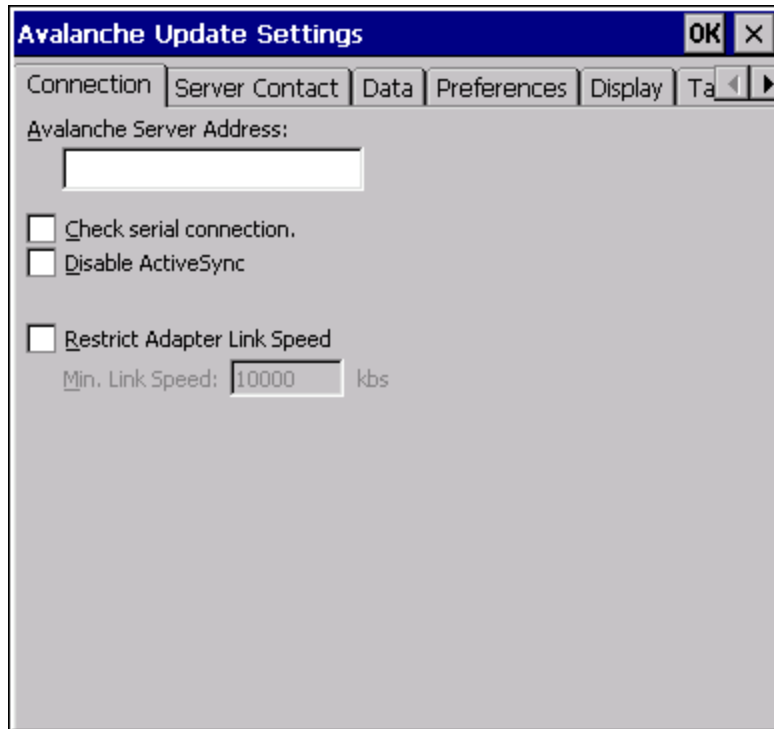
Alternatively, the Mobile Device Server can be disabled until needed (refer to the **Wavelink Avalanche Mobility Center User's Guide** for details).

Menu Options

Note: Your Thor VM1 screen display may not be exactly as shown in the following menu options. Contact [Technical Assistance](#) for version information and upgrade availability.

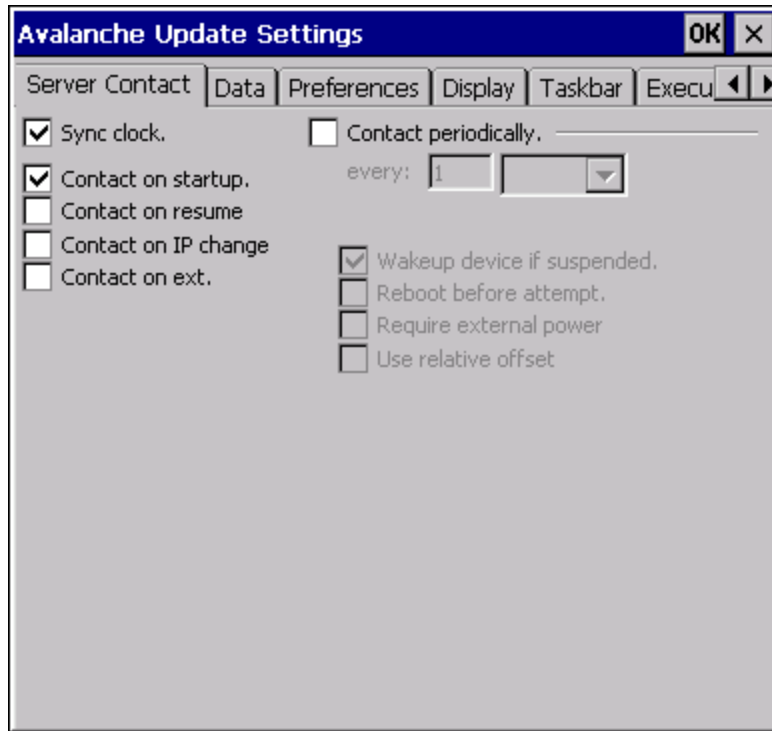
Connection	Enter the IP Address or host name of the Mobile Device Server. Set the order in which serial ports or RF connections are used to check for the presence of the Mobile Device Server.
Server Contact	Setup synchronization, scheduled Mobile Device Server contact, suspend and reboot settings.
Data	Control when data is transferred between the device and the Mobile Device Server.
Preferences	Set options for Enabler startup or shutdown and logging.
Display	Set up the Windows display at startup, on connect and during normal mode. The settings can be adjusted by the user.
Taskbar	Set options for Taskbar.
Execution	<i>Not available in this release.</i> Use AppLock instead, which is resident on each device.
Scan Config	This option allows the user to configure Enabler settings using a special bar code that is created by the Avalanche MC Console. <i>Scan Config not currently supported.</i>
Shortcuts	Add, delete and update shortcuts to user-allowable applications.
SaaS	Configure the Enabler to connect with Avalanche on Demand.
Adapters	Enable or disable network and wireless settings. Select an adapter and switch between the Avalanche Network Profile and manual settings.
Status	View the current adapter signal strength and quality, IP address, MAC address, SSID, BSSID and Link speed. The user cannot edit this information.

Connection



Avalanche Server Address	Enter the IP Address or host name of the Mobile Device Server assigned to the Thor VM1.
Check Serial Connection	Indicates whether the Enabler should first check for serial port connection to the Mobile Device Server before checking for a wireless connection to the Mobile Device Server.
Disable Active-Sync	Disable ActiveSync connection with the Mobile Device Server.
Restrict Adapter Link Speed	Default is disabled. Minimum Link Speed dimmed. When enabled, the Enabler only allows a connection to the server if the detected link speed is greater than or equal to the specified value.

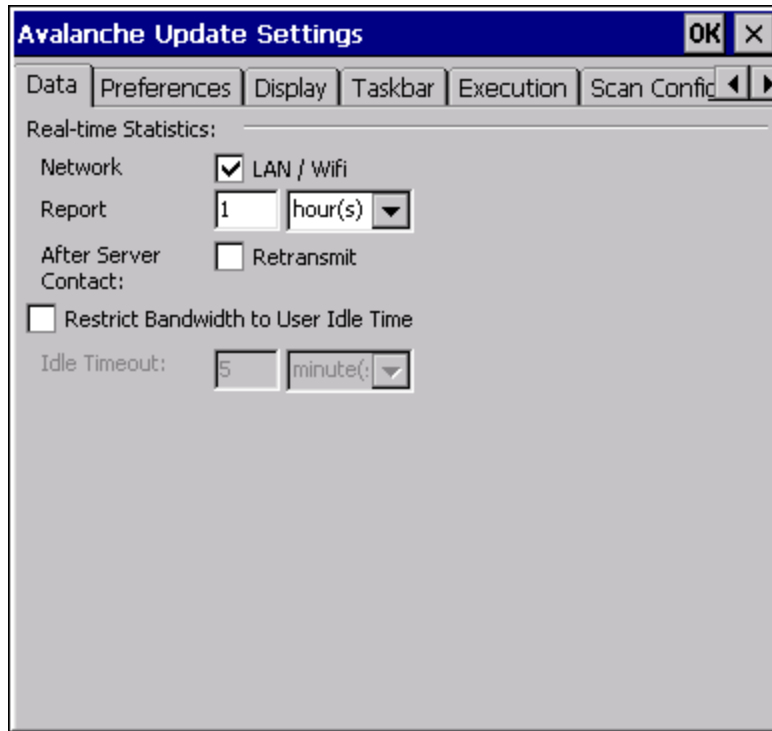
Server Contact



Note: Your Thor VM1 screen display may not be exactly as shown above. Contact [Technical Assistance](#) for upgrade availability and version information.

Sync Clock	Reset the time on the Thor VM1 based on the time on the Mobile Device Server host PC.
Contact	On Startup – Connect to the Mobile Device Server when the Enabler is accessed.
	On Resume – Connect to the Mobile Device Server when resuming from Suspend mode.
	On IP Change – Connect to the Mobile Device Server when the IP address of the Thor VM1 changes.
	On Ext. Power – Initiate connection to the Mobile Device Server when the device is connected to an external power source, such as based on a docking event.
Contact Periodically / Periodic Update	Allows the administrator to configure the Enabler to contact the Mobile Device Server and query for updates at a regular interval beginning at a specific time.
Wakeup device if suspended	If the time interval for periodic contact with the Mobile Device Server occurs, a mobile device that is in Suspend Mode can wakeup and process updates.
Reboot before attempt	Reboot mobile device before attempting to contact Mobile Device Server.
Require external power	Only connect when the mobile device has external power.
Use relative offset	Dimmed.

Data

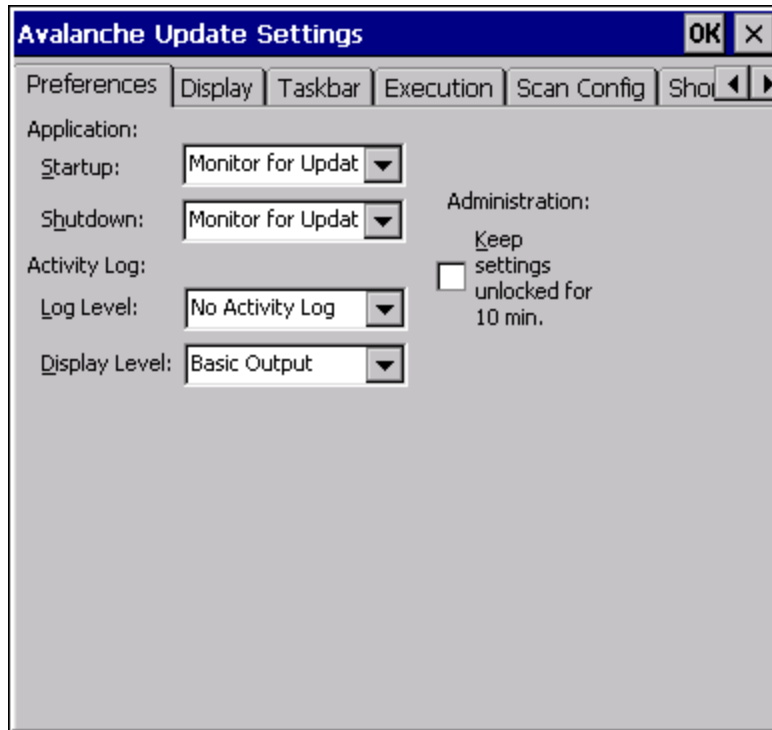


The Data tab controls when data is transferred between the Thor VM1 and the Mobile Device Server.

Network	When checked, the LAN/WiFi network is enabled to transfer statistics.
Report	Specifies the Report Interval, how frequently the Enabler reports statistics to the Mobile Device Server.
Retransmit After Server Contact	Specifies if the device sends statistics to the Mobile Device Server immediately following a connection to the server.
Restrict Bandwidth to User Idle Time	When enabled, periodic updates from the Mobile Device Server are postponed until the Thor VM1 has been idle for the specified period of time. The default is disabled.
Idle timeout	Specify the length of time the device must be idle before a periodic update can run, used when the parameter above is enabled.

Preferences

For best results, use *AppLock* to manage the taskbar. AppLock is resident on each mobile device.



Administration

By default, *Keep settings unlocked for 10 minutes* is disabled (checkbox is blank).

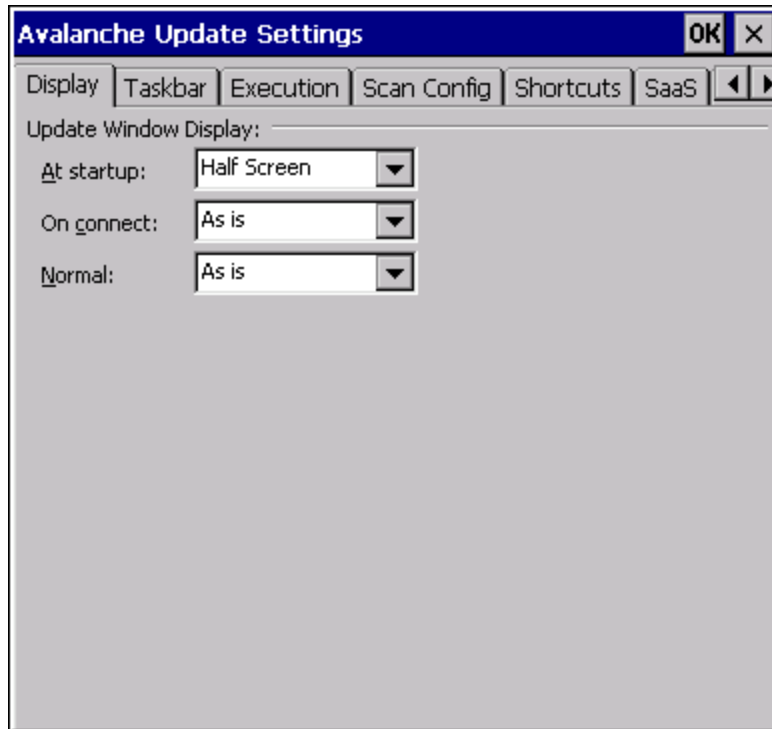
Application

Startup	<p>Behavior of the Enabler when the Thor VM1 boots up. The default is Monitor for Updates.</p> <ul style="list-style-type: none">• Do not Monitor - When the device boots, do not launch the Enabler application and do not attempt to connect to the Mobile Device Server.• Monitor for Updates - Attempt to connect to the Mobile Device Server and process any updates that are available. Do not launch the Enabler application.• Launch User Interface - Attempt to connect to the Mobile Device Server and process any updates that are available. Launch the Enabler application.
Shutdown	<p>Behavior of the monitor when the Enabler is exited. The default is Monitor for Updates.</p> <ul style="list-style-type: none">• Monitor for Updates - Attempt to connect to the Mobile Device Server and process any updates that are available. Do not launch the Enabler application.• Exit Application - Terminates the monitor (requires successful password entry if a password has been configured).

Activity Log

Log Level	<p>Use this option to control the level of detail recorded in the log file. The default is No Activity Log.</p> <ul style="list-style-type: none">• No Activity Log - No log file is written.• Critical - Only critical errors written to the log files.• Error - Communication or configuration problems are written to the log file along with critical messages.• Warning - Possible operation problems are written to the log file along with critical and error messages.• Info - Operational information is written to the log file.• Debug - The most detailed log file.
Display Level	<p>Use this option to control the level of detail shown on the main Enabler screen. The default is Basic Output.</p> <ul style="list-style-type: none">• Basic Output - General information is displayed.• Critical - Critical errors are displayed in addition to those above.• Error - Communication or configuration problems are displayed in addition to those above.• Warning - Possible operation problems are displayed in addition to those above.• Info - Operational information is displayed in addition to those above.• Debug - The most detailed list is displayed.

Display



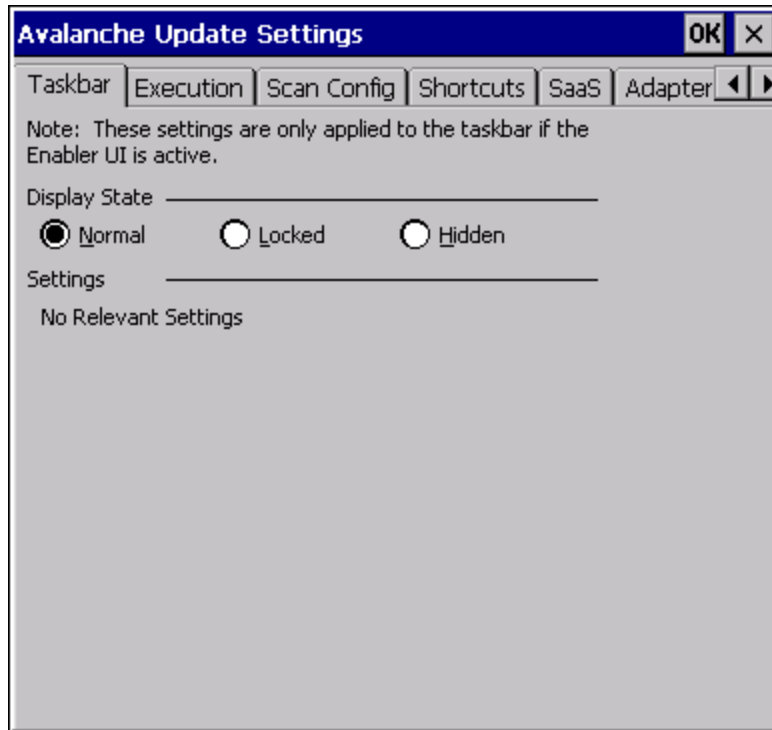
Update Window Display

The user interface for the Enabler can be configured to dynamically change based on the status of the Thor VM1 connection with the Mobile Device Server.

At startup	Default is Half Screen. Options are Half screen, Hidden or Full screen.
On connect	Default is As Is. Options are As is, Half screen, or Full screen.
Normal	Default is As Is. Options are Half screen, Hidden or As Is.

Taskbar

For best results, use *AppLock* to manage the taskbar. AppLock is resident on each mobile device.

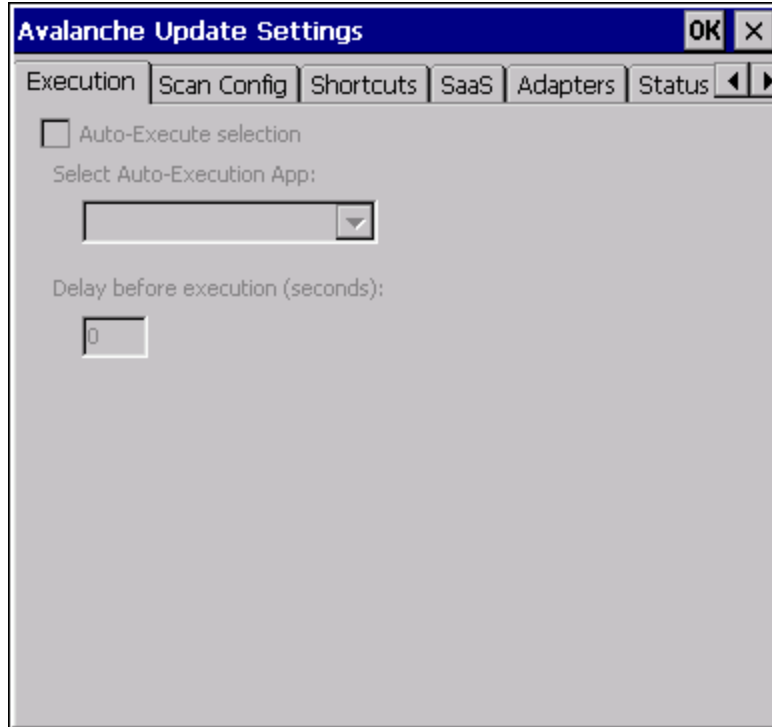


The Display State options control the appearance of the taskbar while using the Enabler interface.

- Normal - taskbar is visible, taskbar icons function normally.
- Hidden - taskbar is not displayed
- Locked - taskbar is visible, but most icons are hidden or for information only.

Execution

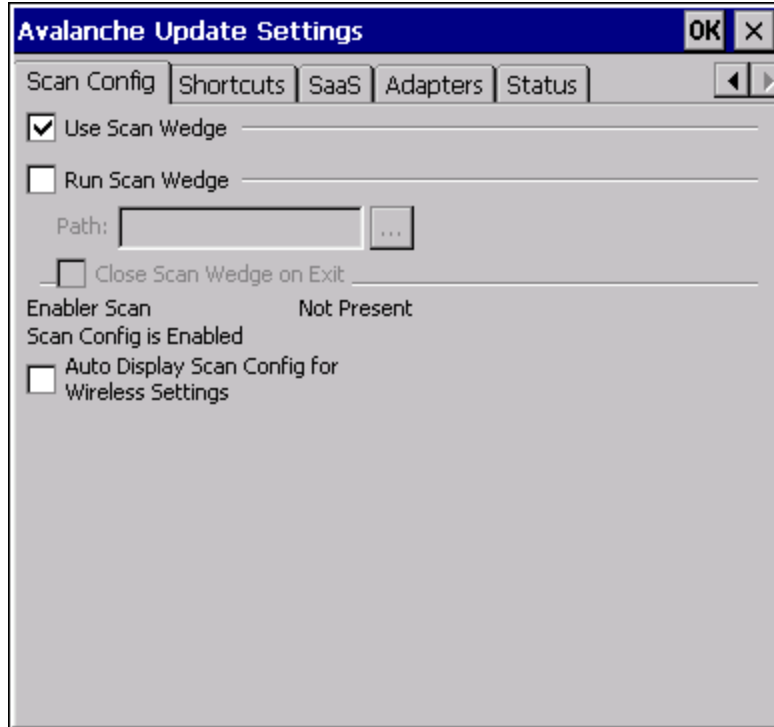
Note the dimmed options on this Thor VM1 panel. This menu option is designed to manage downloaded applications for automatic execution upon startup.



Auto-Execute Selection	An application that has been installed with the Avalanche Management system can be run automatically following each boot.
Select Auto-Execute App	The drop-down box provides a list of applications that have been installed with the Avalanche Management System.
Delay before execution	Time delay before launching Auto-Execute application.

Scan Config

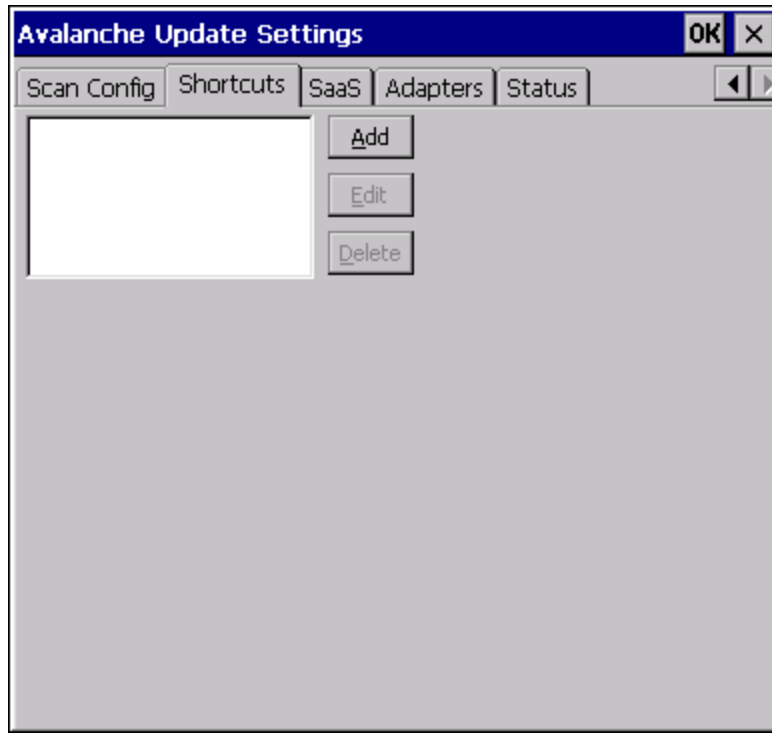
For best results, use *eXpress Config* and *eXpress Scan* for this function. *eXpress Scan* is included with the updated Thor VM1 enablers.



Scan Config functionality is a standard option of the Wavelink Avalanche MC system but is *not currently supported* on the Thor VM1.

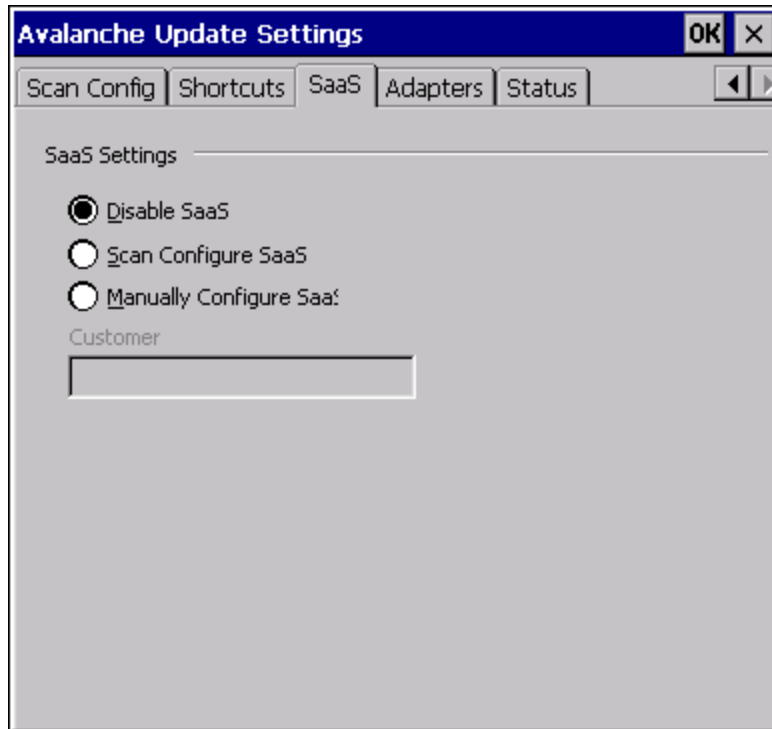
Shortcuts

For best results, use *AppLock* for this function. AppLock is resident on each mobile device.



Configure shortcuts to other applications on the Thor VM1. Shortcuts are viewed and activated in the Programs panel. This limits the user's access to certain applications when the Enabler is controlling the mobile device display.

SaaS

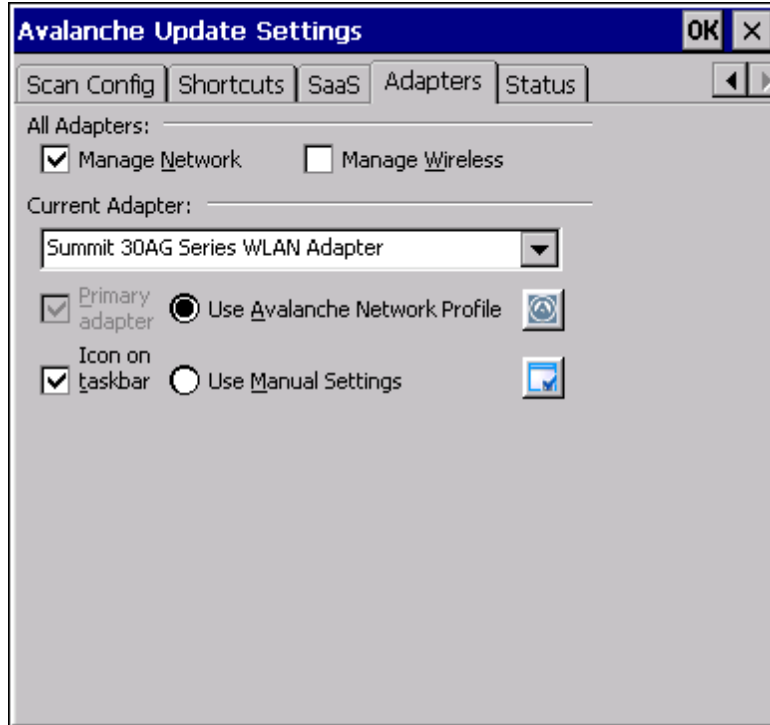


Use to configure the Enabler to connect with Avalanche on Demand. This is a Software-as-a-Service version of Avalanche. Using either of the SaaS configuration options below assumes the user has registered with Wavelink.



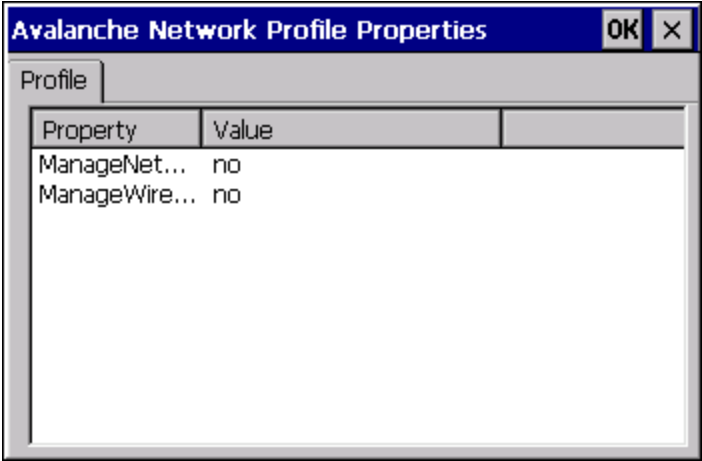
Disable SaaS	No SaaS connection is used.
Scan Configure SaaS	Scan bar codes printed from within the Avalanche Console to configure the Enabler for the SaaS connection.
Manually Configure SaaS	Manually enter the SaaS connection information. Enter the server address on the Connection tab and the customer ID in the Company textbox.

Adapters

Note: Review the network settings configuration utilities and the default values before setting All Adapters to Enable in the Adapters applet.




Manage Network Settings	When enabled, the Enabler will control the network settings. This parameter cannot be configured from the Avalanche Mobility Center Console and is enabled by default.
Manage Wireless Settings	When enabled, the Enabler will control the wireless settings. This parameter cannot be configured from the Avalanche Mobility Center Console and is disabled by default. For Summit clients, Manage Wireless Settings should not be checked as configuration packages provide more radio configuration options.
Current Adapter	Lists all network adapters currently installed on the Thor VM1.
Primary Adapter	Indicates if the Enabler is to attempt to configure the primary adapter (active only if there are multiple network adapters).
Icon on taskbar	Places the Avalanche icon in the Avalanche taskbar that may, optionally, override the standard Windows taskbar.
Use Avalanche Network Profile	The Enabler will apply all network settings sent to it by the Mobile Device Server.

<p>Avalanche Icon (varies by Enabler version)</p>  	<p>Selecting the Avalanche Icon will access the Avalanche Network Profile tab which will display current network settings.</p> 
<p>Use Manual Settings</p>	<p>When enabled, the Enabler will ignore any network or wireless settings coming from the Avalanche MC Console and use only the network settings on the Thor VM1.</p>
<p>Properties Icon</p>	<p>Selecting the Properties icon displays the Manual Settings Properties dialog applet. From here, the user can configure Network, DNS and Wireless parameters using the displays shown below:</p>

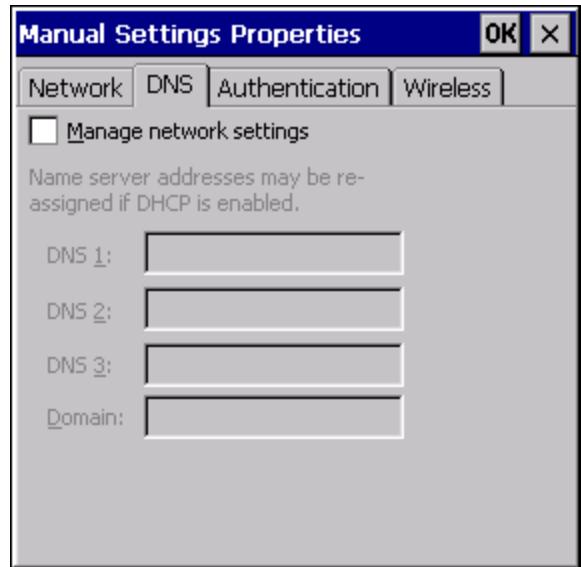
Note: A reboot may be required after enabling or disabling these options.

Network

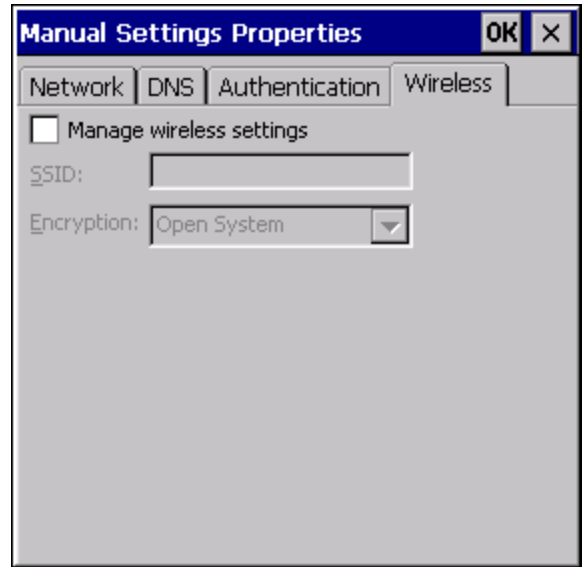


Authentication

DNS



Wireless



Note: The Authentication tab may not be present in all versions of the Enabler.

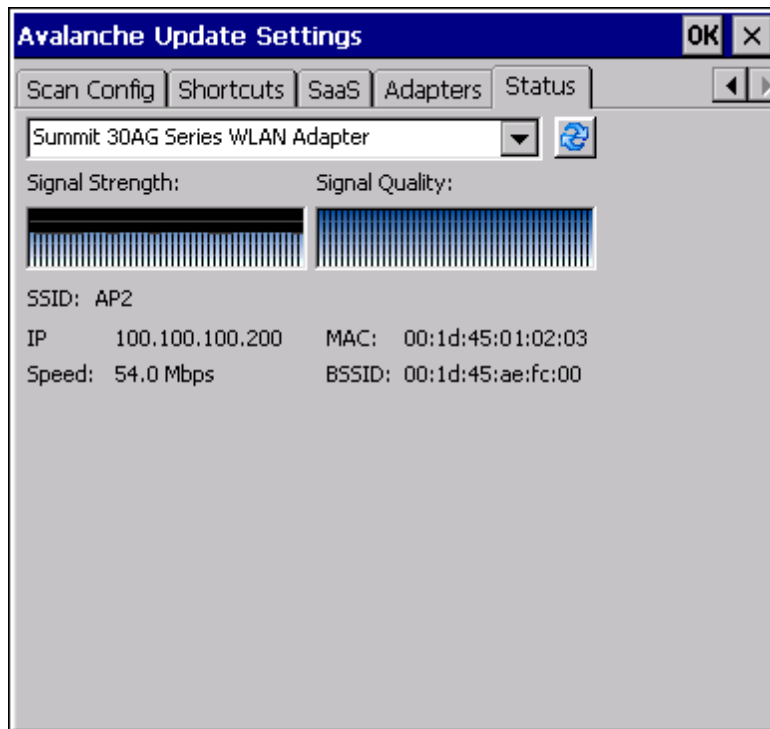
It is not recommend to enable "Manage Wireless Settings" for Summit Client devices.

Troubleshooting: When you download a profile that is configured to manage network and wireless settings, the Enabler will not apply the manage network and wireless settings to the adapter unless the global Manage wireless settings and Manage network settings options are enabled on the Adapters panel (see Figure titled [Adapters Options – Network](#), earlier in this section). Until these options are enabled, the network and wireless settings are controlled by the third-party software associated with these settings.

Status

The Status panel displays the current status of the Thor VM1 network adapter selected in the drop down box. Note the availability of the Windows standard Refresh button.

When the Windows Refresh button is tapped, the signal strength, signal quality and link speed are refreshed for the currently selected adapter. It also searches for new adapters and may cause a slight delay to refresh the contents of the drop-down menu.



Link speed indicates the speed at which the signal is being sent from the adapter to the Thor VM1. Speed is dependent on signal strength.

Exit

The Exit option is password protected. The default password is **leave**. The password is not case-sensitive.



Depending on the behavior chosen for the Shutdown parameter, the following screen may be displayed:



Note: The icon on the screen above may differ based on the version of the Enabler installed on the Thor VM1.

Change the option if desired. Tap the X button to cancel Exit. Tap the OK button to exit the Avalanche applet.

Using Remote Management

1. Configure the radio to connect to the network running the Mobile Device Server. After the Thor VM1 is connected, proceed to step 2.
2. If it is desired to configure the radio using the Summit package, add the configured package to the Wavelink Avalanche MC Console and enable it.
3. Verify RMU.CE.CAB exists in the \System\RMU folder.
4. Double-click the Thor VM1 enabler CAB file in the \System folder.
5. The enabler automatically launches after installation and contacts the Mobile Device Server. The Avalanche MC Console connected to that Mobile Device Server identifies the remote device and performs a sync. This downloads any available packages available for the Thor VM1.

Using eXpress Scan



eXpress Scan Desktop Icon

If the Thor VM1 has an eXpress Scan icon on the desktop, eXpress Scan may be used for the initial configuration of the device. If the eXpress Scan icon is not present on the desktop, [install the Enabler](#). If the icon is still not present, [the Enabler must be updated](#).

If the eXpress Scan icon is present, follow these steps to configure the Thor VM1 to connect with the wireless network and the Mobile Device Server.

Step 1: Create Bar Codes

Bar codes are created with the eXpress Config utility on the desktop/laptop computer, not the mobile device. Depending on the bar code length and the number of parameters selected, eXpress Config generates one or more bar codes for device configuration. The bar codes contain configuration parameters for the wireless client in the mobile device and may also specify the address of the Mobile Device Server.

Bar codes should be printed at a minimum of 600 dpi.

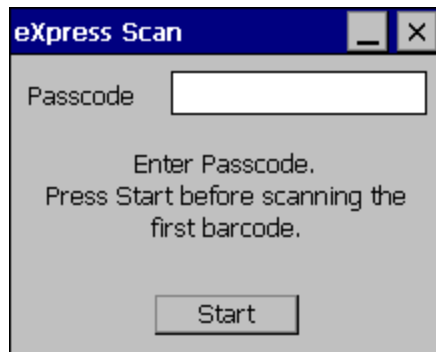
Please see *Using Wavelink Avalanche* for details on creating barcodes.

Step 2: Scan Bar Codes

For each mobile device to be configured, please follow these instructions.

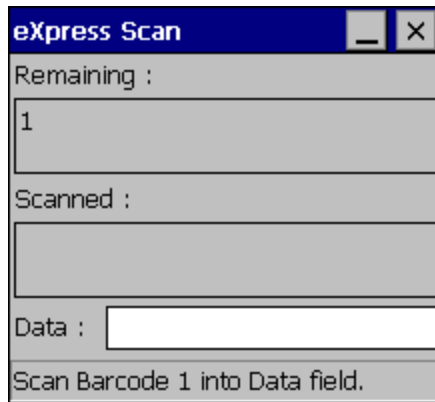
Start eXpress Scan on the Thor VM1 by double-clicking the eXpress Scan icon.

Enter the bar code password, if any.



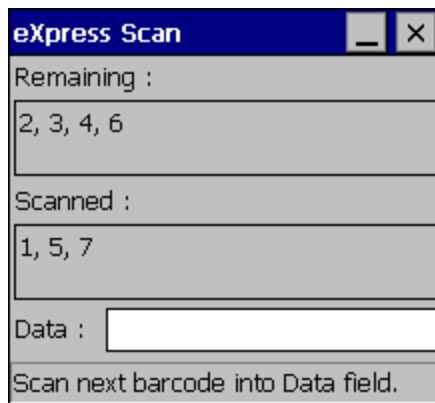
Click Start.

Bar code 1 must be scanned first. The scanned data is displayed in the "Data" text box. The password, if any, entered above is compared to the password entered when the bar codes were created.



If the passwords match, the bar code data is processed and the screen is updated to reflect the number of bar codes included in the set.

If the passwords do not match, an error message is displayed. The current screen can be closed using the X box in the upper right corner. The password can be re-entered and Bar Code 1 scanned again.



The remaining bar codes may be scanned in any order. After a bar code is scanned, that bar code is removed from the "Remaining:" list and placed in the "Scanned:" list.

Step 3: Process Completion

After the last bar code is scanned, the settings are automatically applied.



Once configured, the Thor VM1 is warmbooted. Once connected to the wireless network and the Mobile Device Server, any software updates and additional configuration data are downloaded.

Chapter 6: Wireless Network Connections




Summit Wireless Network Configuration

The Summit client device is a Summit 802.11a/b/g radio, capable of 802.11a, 802.11b and 802.11g 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 VM1 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, warmboot the Thor VM1.

Summit Client Utility

Note: When making changes to profile or global parameters, the device should be warmbooted afterwards.

Start > Programs > Summit > SCU 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

 The Summit tray icon provides access to the SCU and is a visual indicator of radio status.

The Summit tray icon is displayed when:

- The Summit radio is installed and active
- The Windows Zero Config utility is not active
- The Tray Icon setting is On

Click the icon to launch the SCU. Use the tray icon to view the radio status:

	The radio is not currently associated or authenticated to an Access Point
	The signal strength for the currently associated/authenticated Access Point is less than -90 dBm
	The signal strength for the currently associated/authenticated Access Point is -71 dBm to -90 dBm
	The signal strength for the currently associated/authenticated Access Point is -51 dBm to -70 dBm
	The signal strength for the currently associated/authenticated Access Point is greater than -50 dBm

Wireless Zero Config Utility and the Summit Radio



- The WZC utility has an icon in the toolbar that looks like a networked computer with a red X beside it, indicating that 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 list as the active profile (see [Main Tab](#)).
2. Warmboot the device.

The Summit Client Utility passes control to Wireless Zero Config and the WZC Wireless Information control panel. Using the options in the Wireless Zero Config panels, setup radio and security settings. 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 in the SCU Active Config drop down list, except **ThirdPartyConfig**.
2. Warmboot the device.

Radio control is passed to the SCU.

Main Tab

Start > Programs > Summit > Main tab

Factory Default Settings

Admin Login	SUMMIT
Radio	Enabled
Active Config/Profile	Default
Regulatory Domain	Worldwide



The Main tab displays information about the wireless client device including:

- SCU (Summit Client Utility) version
- Driver version
- Radio Type (ABG is an 802.11 a/b/g 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 Windows Zero Config 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.

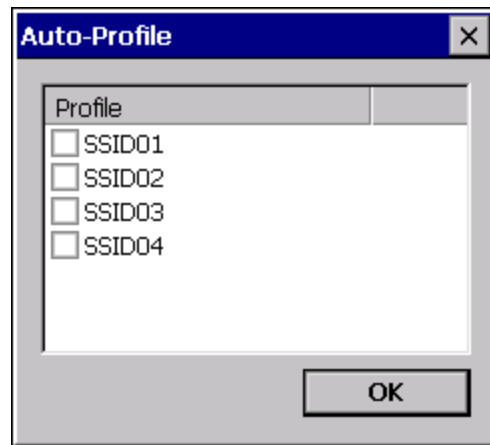
The **Admin Login** button provides access to editing wireless parameters. Profile and Global may only be edited after entering the Admin Login password.

The password is case-sensitive.

Auto Profile

If the Auto Profile selection is not present on the Main tab, an SCU upgrade is necessary to support this feature on the Thor VM1.

Auto Profile allows the user to configure a list of profiles that the SCU can search when a radio connection is lost. After using the Profile tab to create any desired profiles, return to the Main tab. To specify which profiles are to be included in Auto Profile, click the **List** button.



The Auto Profile selection screen displays all currently configured profiles. Click on the checkbox for any profiles that are to be included in Auto Profile selection then click ok to save.

To enable Auto Profile, click the **On** button on the **Main** tab.

When Auto Profile is On, if the radio goes out of range from the currently selected profile, the radio then begins to attempt to connect to the profiles listed under Auto Profile.

The search continues until:

- the SCU connects to and, if necessary, authenticates with, one of the specified profiles or
- the Off button is clicked to turn off Auto Profile.

Note: Do not include any profiles with an [Ad Hoc Radio Mode](#) in this listing.

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.

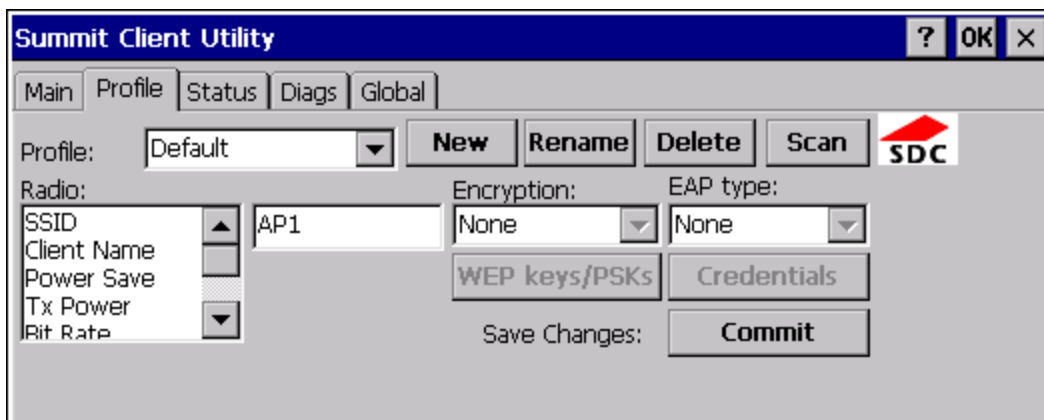
Profile Tab

Start > Programs > Summit > 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



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

Button	Function															
Commit	Saves the profile settings made on this screen. Settings are saved in the profile.															
Credentials	Allows entry of a username and password, certificate names, and other information required to authenticate with the access point. The information required depends on the EAP type.															
Delete	Deletes the profile. The current active profile cannot be deleted and an error message is displayed if a delete is attempted.															
New	Creates a new profile with the default settings (see Profile Parameters) and prompts for a unique name. If the name is not unique, an error message is displayed and the new profile is not created.															
Rename	Assigns a new, unique name. If the new name is not unique, an error message is displayed and the profile is not renamed.															
Scan	<p>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.</p> <p>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.</p> <div data-bbox="634 932 1117 1371" data-label="Image"> <table border="1"> <thead> <tr> <th>SSID</th> <th>RSSI</th> <th>Secure</th> </tr> </thead> <tbody> <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> </tbody> </table> </div> <p>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).</p>	SSID	RSSI	Secure	Net4	-47	true	Net2	-48	true	Net1	-51	true	Net3	-51	false
SSID	RSSI	Secure														
Net4	-47	true														
Net2	-48	true														
Net1	-51	true														
Net3	-51	false														
WEP Keys / PSK Keys	Allows entry of WEP keys or pass phrase as required by the type of encryption.															

Note: Unsaved Changes – The SCU will display a reminder if the Commit button is not clicked before an attempt is made to close or browse away from this tab.

Important – The settings for Auth Type, EAP Type and Encryption depend on the security type chosen.

Profile Parameters

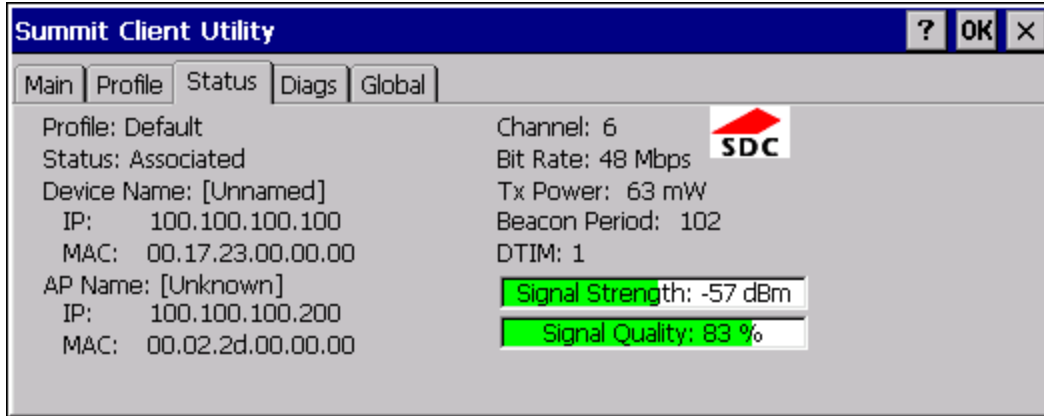
Parameter	Default	Explanation
Edit Profile	Default	A string of 1 to 32 alphanumeric characters, establishes the name of the Profile. Options are Default or ThirdPartyConfig.
SSID	Blank	A string of up to 32 alphanumeric characters. Establishes the Service Set Identifier (SSID) of the WLAN to which the client connects.
Client Name	Blank	A string of up to 16 characters. The client name is assigned to the network card and the device using the network card. The client name may be passed to networking wireless devices, e.g. Access Points.
Power Save	CAM	Power save mode. Options are: Constantly Awake Mode (CAM) power save off, Maximum (power saving mode) and Fast (power saving mode). When using power management, use FAST for best throughput results.
Tx Power	Maximum	Maximum setting regulates Tx power to the Max power setting for the current regulatory domain. Options are: Maximum, 50mW, 30mW, 20mW, 10mW, 5mW, or 1mW.
Bit Rate	Auto	Setting the rate to Auto will allow the Access Point to automatically negotiate the bit rate with the client device. This parameter cannot be changed.
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. <i>Note: EAP Type chosen determines whether the Credentials button is active and also determines the available entries in the Credentials pop-up window.</i>
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 VM1. <i>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.</i>
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 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 VM1 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 VM1.

Status Tab

Start > Programs > Summit > Status tab



This screen provides information on the radio:

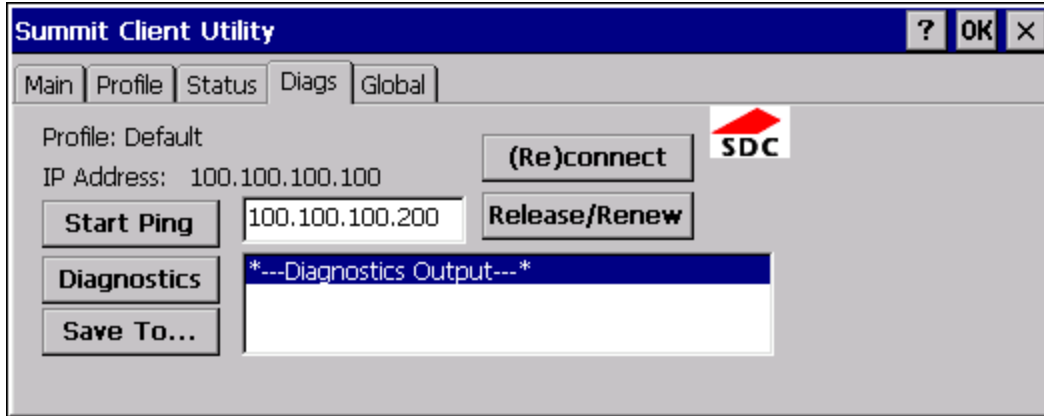
- The profile being used.
- The status of the radio card (down, associated, authenticated, etc.).
- Client information including device name, IP address and MAC address.
- Information about the Access Point (AP) maintaining the connection to the network including AP name, IP address and MAC address.
- Channel currently being used for wireless traffic.
- Bit rate in Mbit.
- Current transmit power in mW.
- Beacon period – the time between AP beacons in kilomicroseconds. (one kilomicrosecond = 1,024 microseconds).
- DTIM interval – A multiple of the beacon period that specifies how often the beacon contains a delivery traffic indication message (DTIM). The DTIM tells power saving devices a packet is waiting for them. For example, if DTIM = 3, then every third beacon contains a DTIM.
- Signal strength (RSSI) displayed in dBm and graphically.
- Signal quality, a measure of the clarity of the signal displayed in percentage and graphically.

There are no user entries on this screen.

Note: After completing radio configuration, it is a good idea to review this screen to verify the radio has associated (no encryption, WEP) or authenticated (LEAP, any WPA), as indicated above.

Diags Tab

Start > Programs > Summit > Diags tab



The Diags screen can be used for troubleshooting network traffic and radio connectivity issues.

- **(Re)connect** – Use this button to apply (or reapply) the current profile and attempt to associate or authenticate to the wireless LAN. All activity is logged in the Diagnostic Output box on the lower part of the screen.
- **Release/Renew** – Obtain a new IP address through release and renew. All activity is logged in the Diagnostic Output box. If a fixed IP address has been assigned to the radio, this is also noted in the Diagnostic Output box. Note that the current IP address is displayed above this button.
- **Start Ping** – Start a continuous ping to the IP address specified in the text box to the right of this button. Once the button is clicked, the ping begins and the button label changes to **Stop Ping**. Clicking the button ends the ping. The ping also ends when any other button on this screen is clicked or the user browses away from the Diags tab. The results of the ping are displayed in the Diagnostic Output box.
- **Diagnostics** – Also attempts to (re)connect to the wireless LAN. However, this option provides more data in the Diagnostic Output box than the (Re)connect option. This data dump includes radio state, profile settings, global settings, and a list of broadcast SSID APs.
- **Save To...** – Use this to save the results of the diagnostics to a text file. Use the explorer window to specify the name and location for the diagnostic file. The text file can viewed using an application such as WordPad.

Global Tab

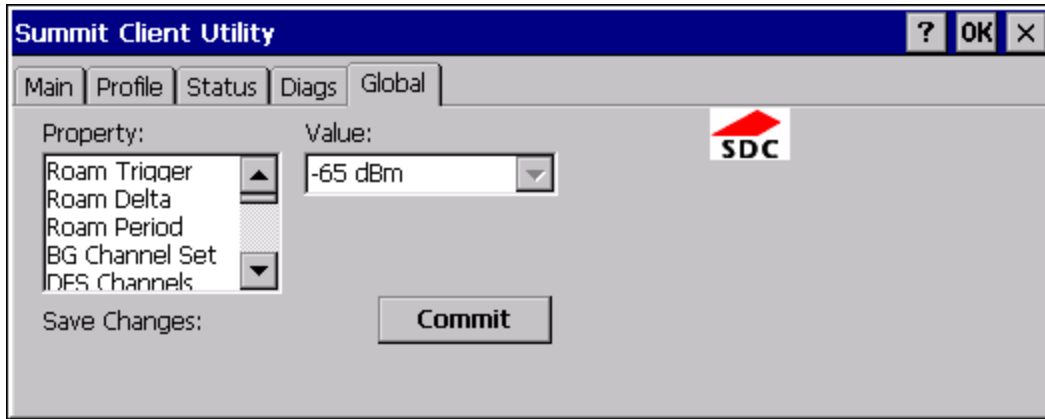
Start > Programs > Summit > Global tab

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	ABG: 10 sec.
BG Channel Set	Full
DFS Channels	Off
DFS Scan Time	120 ms.
Ad Hoc Channel	1
Aggressive Scan	On
CCX Features	ABG: Optimized
WMM	Off
Auth Server	Type 1
TTLS Inner Method	Auto-EAP
PMK Caching	Standard
WAPI	Off (dimmed)
TX Diversity	ABG: On
RX Diversity	ABG: 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	System
Ping Payload	32 bytes
Ping Timeout	5000 ms
Ping Delay ms	1000 ms



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	ABG: 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. <i>Note: Not supported (always off) in some releases.</i>
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	ABG: Optimized	Use of Cisco Compatible Extensions (CCX) radio management and AP specified maximum transmit power features. This parameter cannot be changed.
WMM	Off	Use of Wi-Fi Multimedia extensions. Options are: On, Off Devices running Windows XP can change the default value. Devices running all other OS cannot change the default value.
Auth Server	Type 1	Specifies the type of authentication server. Options are: Type 1 (ACS server) and Type 2 (non-ACS server)
TTLS Inner Method	Auto-EAP	Authentication method used within the secure tunnel created by EAP-TTLS. Options are: AUTO-EAP (Any available EAP method) MSCHAPV2 MSCHAP PAP CHAP EAP-MSCHAPV2
PMK Caching	Standard	Type of Pairwise Master Key (PMK) caching to use when WPA2 is in use. PMK caching is designed to speed up roaming between APs by allowing the client and the AP to cache the results of 802.1X authentications, eliminating the need to communicate with the ACS server. Standard PMK is used when there are no controllers. The reauthentication information is cached on the original AP. The client and the AP use the cached information to perform the four-way handshake to exchange keys. Opportunistic PMK (OPMK) is used when there are controllers. The reauthentication information cached on the controllers. The client and the controller behind the AP use the cached information to perform the four-way handshake to exchange keys. If the selected PMK caching method is not supported by the network infrastructure, every roam requires full 802.11X authentication, including interaction with the ACS server. If the active profile is using WPA2 CCKM, the global PMK Caching setting is ignored and the client attempts to use CCKM. Options are: Standard, OPMK
WAPI	Off	Default is Off and dimmed (cannot be changed).
TX Diversity	ABG: On	How to handle antenna diversity when transmitting packets to the Access Point. Options are: Main only (use the main antenna only), Aux only (use the auxiliary antenna only), or On (use diversity or both antennas).

Parameter	Default	Function
RX Diversity	ABG: On Start on Main	How to handle antenna diversity when receiving packets from the Access Point. Options are: Main Only (use the main antenna only), Aux Only (use the auxiliary antenna only), On-start on Main (on startup, use the main antenna), or On-start on Aux (on startup, use the auxiliary antenna).
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. This parameter cannot be changed.
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. This parameter cannot be changed.
Tray Icon	On	Determines if the Summit icon is displayed in the System tray. Options are: On, Off
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	System	<p>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.</p> <p>Options are: none.</p> <p>For example, when the valid certificate is stored as My Computer/System/MYCERTIFICATE.CER, enter System in the Certs Path text box as the Windows folder path.</p>
Ping Payload	32 bytes	<p>Maximum amount of data to be transmitted on a ping.</p> <p>Options are: 32 bytes, 64, 128, 256, 512, or 1024 bytes.</p>
Ping Timeout ms	5000	<p>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.</p> <p>Options are: Any number between 0 and 30000 ms.</p>
Ping Delay ms	1000	<p>The amount of time, in milliseconds, between each ping after a Start Ping button tap.</p> <p>Options are: Any number between 0 and 30000 ms.</p>

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

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.

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.

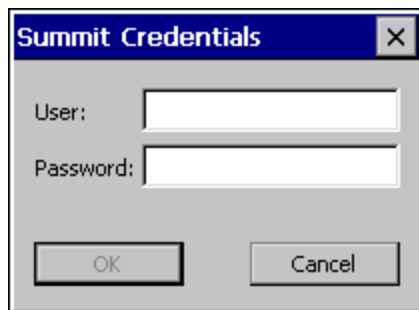
Note: See [Configuring the Profile](#) for more details.

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.

A screenshot of a dialog box titled "Summit Credentials". The dialog box has a blue header bar with the title and a close button (X). Below the header, there are two text input fields. The first is labeled "User:" and the second is labeled "Password:". At the bottom of the dialog box, there are two buttons: "OK" and "Cancel".

10. Verify the device is authenticated by reviewing the Status tab. When the device is properly 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.

Windows Certificate Store vs. Certs Path

Note: It is important that all dates are correct on the Thor VM1 and host computers when using any type of certificate. Certificates are date sensitive and if the date is not correct authentication will fail.

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 \System. A different location may be specified by using the Certs Path global variable. Please note the location chosen for certificate storage should persist after a reboot.
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.



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.

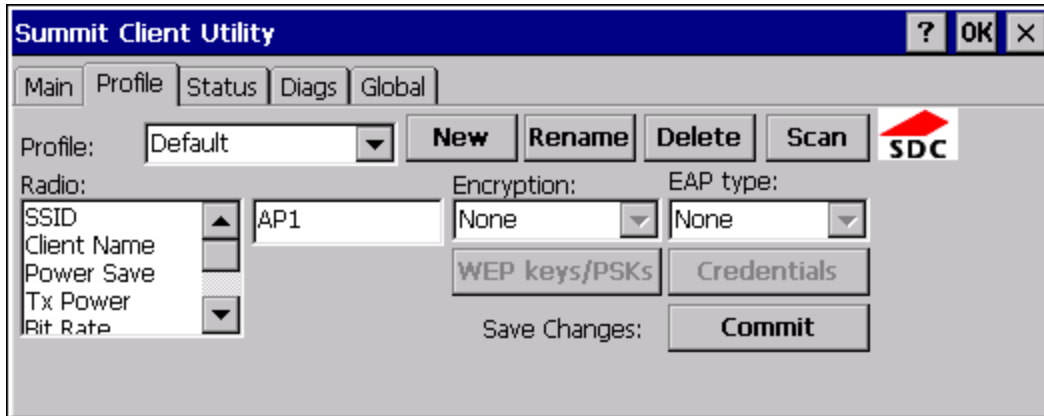
IMPORTANT – Remember to click the Commit button after making changes to ensure the changes are saved. Many versions of the SCU display a reminder if the Commit button is not clicked before an attempt is made to close or browse away from the tab in focus if there are unsaved changes.

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**



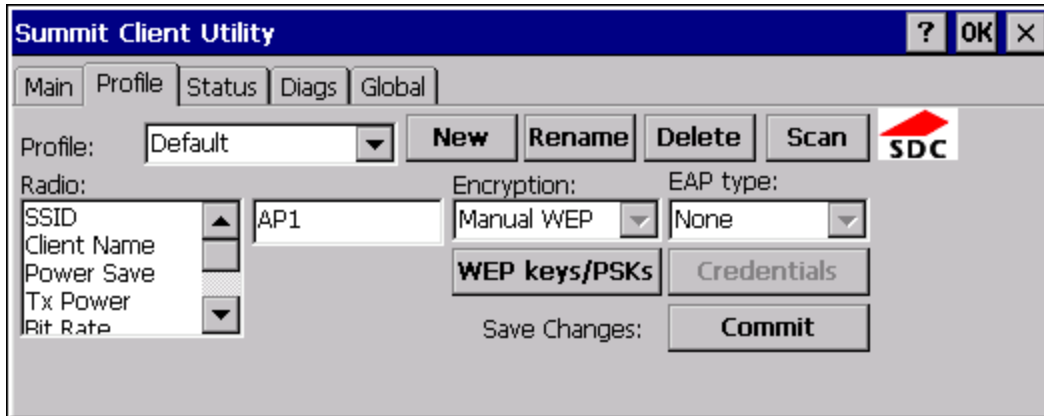
Once configured, click the **Commit** button.

Ensure the correct Active Profile is selected on the [Main tab](#) and warmboot. The SCU Main tab shows the device is associated after the radio connects to the network.

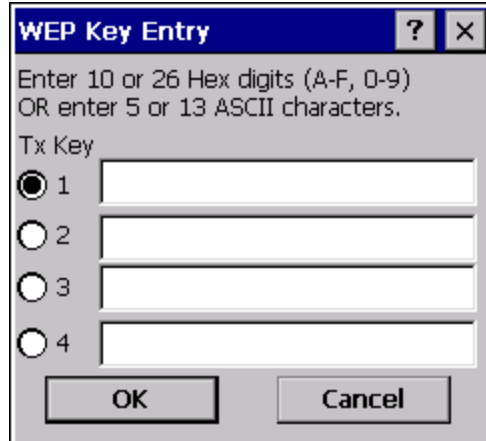
WEP

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

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



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



Valid keys are 10 hexadecimal or 5 ASCII characters (for 40-bit encryption) or 26 hexadecimal or 13 ASCII characters (for 128-bit encryption). Enter the key(s) and click **OK**.

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

Ensure the correct Active Profile is selected on the [Main tab](#) and warmboot. The SCU Main tab shows the device is associated after the radio connects to the network.

LEAP

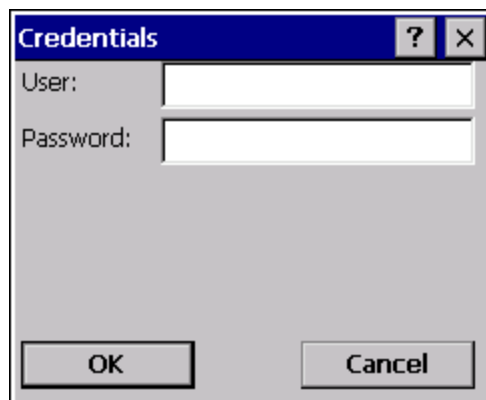
To use LEAP (without WPA), make sure the following profile options are used.

- 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**.



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**.

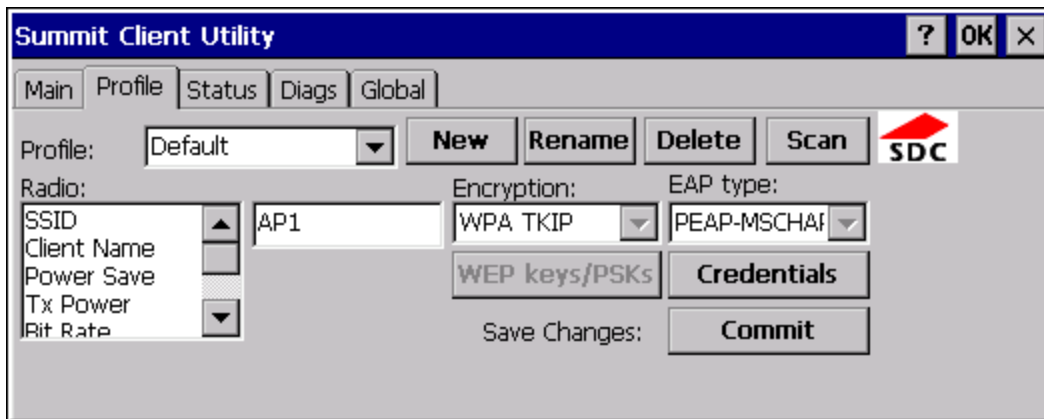
Ensure the correct Active Profile is selected on the [Main tab](#) and warmboot. The SCU Main tab shows the device is associated after the radio connects to the network.

PEAP/MSCHAP

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

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

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

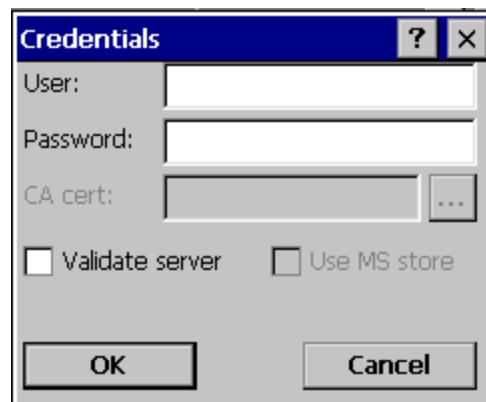


See [Sign-On vs. Stored Credentials](#) for information on entering credentials.

Click the **Credentials** button.

- No entries except the CA Certificate Filename are necessary for Sign-On Credentials as the user will be prompted for the User Name and Password when connecting to the network.
- For Stored Credentials, User, Password and the CA Certificate Filename must be entered.

Enter these items as directed below.



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

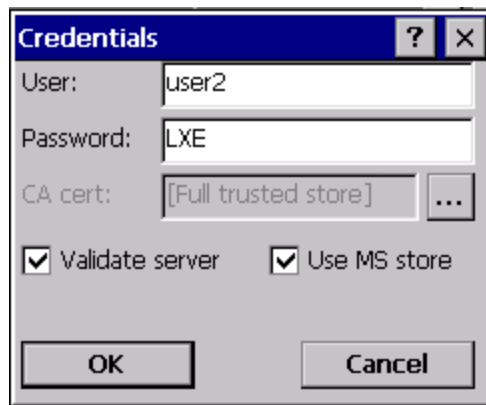
Enter the password.

Leave the CA Certificate File Name blank for now.

Click **OK** then click **Commit**. Ensure the correct Active profile is selected on the [Main Tab](#).

See [Windows Certificate Store vs. Certs Path](#) for more information on certificate storage.

Once successfully authenticated, import the CA certificate into the Windows certificate store. Return to the Credentials screen and check the **Validate server** checkbox.



If using the Windows certificate store:

- 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 warmboot. The SCU Main tab shows the device is associated after the radio connects to the network.

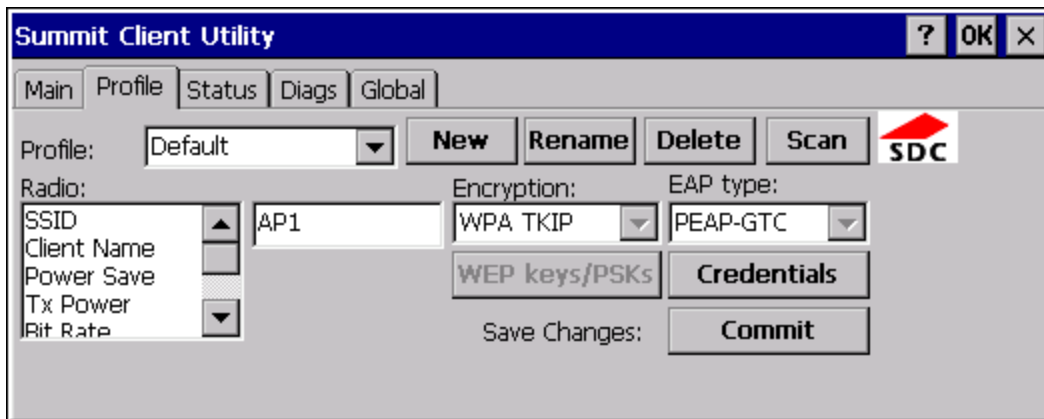
Note: The date must be properly set on the device to authenticate a certificate.

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.

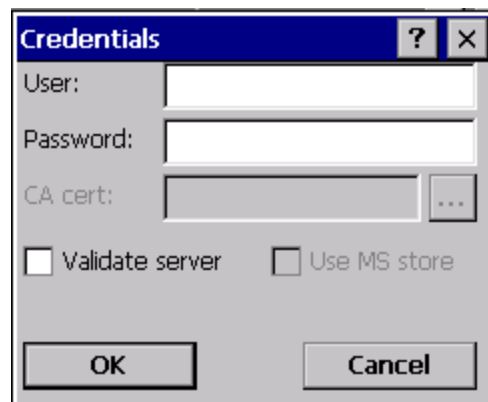


See [Sign-On vs. Stored Credentials](#) for information on entering credentials.

Click the **Credentials** button.

- No entries except the CA Certificate Filename are necessary for Sign-On Credentials as the user will be prompted for the User Name and Password when connecting to the network.

Enter these items as directed below.



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

Enter the password.

Leave the CA Certificate File Name blank for now.

Click **OK** then click **Commit**. Ensure the correct Active Profile is selected on the [Main Tab](#).

See [Windows Certificate Store vs. Certs Path](#) for more information on certificate storage.

Once successfully authenticated, import the CA certificate into the Windows certificate store. Return to the Credentials screen and check the **Validate server** checkbox.

Note: Some servers may be configured to allow only a single use of the password for PEAP/GTC. In this case, wait for the token to update with a new password before attempting to validate the server. Then enter the new password, check the Validate Server checkbox and proceed with the certificate process below.



If using the Windows certificate store:

- 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 warmboot. The SCU Main tab shows the device is associated after the radio connects to the network.

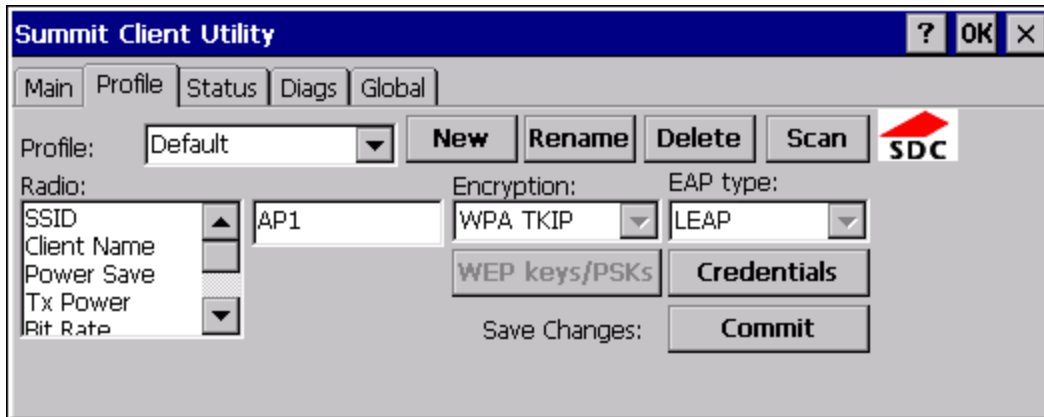
Note: The date must be properly set on the device to authenticate a certificate.

WPA/LEAP

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

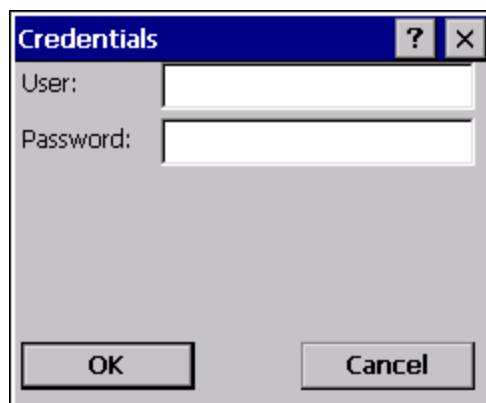
- Enter the **SSID** of the Access Point assigned to this profile
- Set **EAP Type** to **LEAP**
- Set **Encryption** to **WPA TKIP**
- Set **Auth Type** as follows:
 - If the Cisco/CCX certified AP is configured for open authentication, set the **Auth Type** radio parameter to **Open**.
 - If the AP 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.



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 warmboot. The SCU Main tab shows the device is associated after the radio connects to the network.

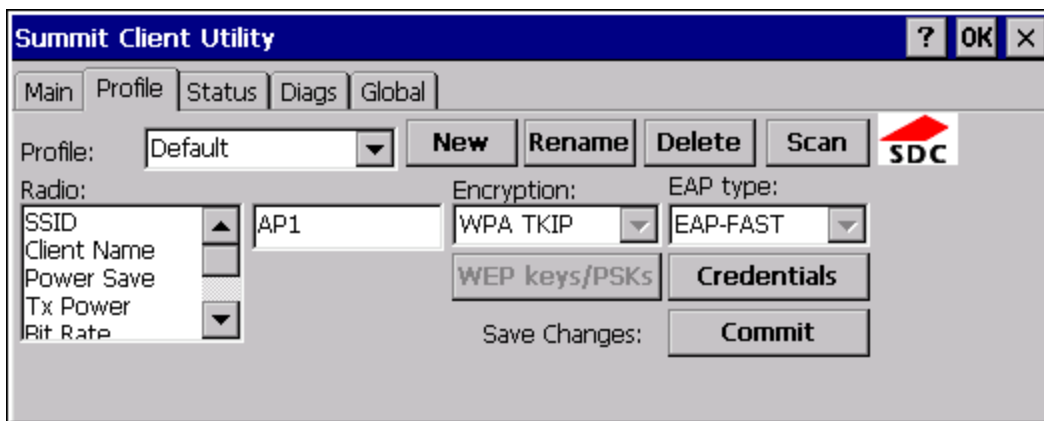
EAP-FAST

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

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

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 VM1.



For automatic PAC provisioning, once a username/password is authenticated, the PAC information is stored on the Thor VM1. The same username/password must be used to authenticate each time. See the note below for more details.

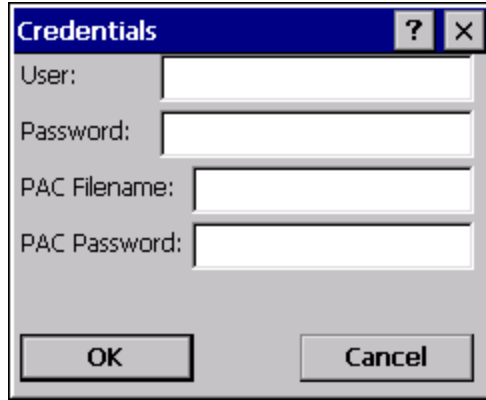
For manual PAC provisioning, the PAC filename and Password must be entered.

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 warmboot. The SCU Main tab shows the device is associated after the radio connects to the network.

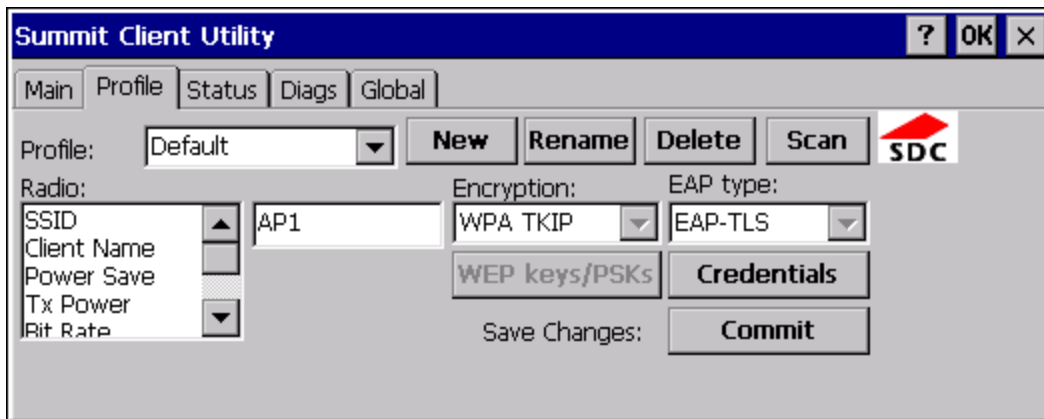
Note: When using Automatic PAC Provisioning, once authenticated, there is a file stored in the \System directory with the PAC credentials. If the username is changed, that file must be deleted. The filename is autoP.00.pac.

EAP-TLS

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

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

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

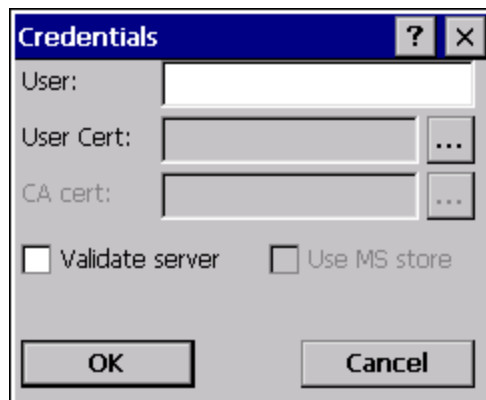


See [Sign-On vs. Stored Credentials](#) for information on entering credentials.

Click the **Credentials** button.

- No entries except the User Certificate Filename and the CA Certificate Filename are necessary for Sign-On Credentials as the user will be prompted for the User Name when connecting to the network.
- For Stored Credentials, User Certificate Filename and the CA Certificate Filename must be entered.

Enter these items as directed below.



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

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

Some versions of the SCU require a User Cert password. If this entry field is present, enter the password for the user certificate in the User Cert pwd box.

If there are no user certificates in the Windows certificate store, follow these instructions 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.



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 VM1 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 warmboot. The SCU Main tab shows the device is associated after the radio connects to the network.

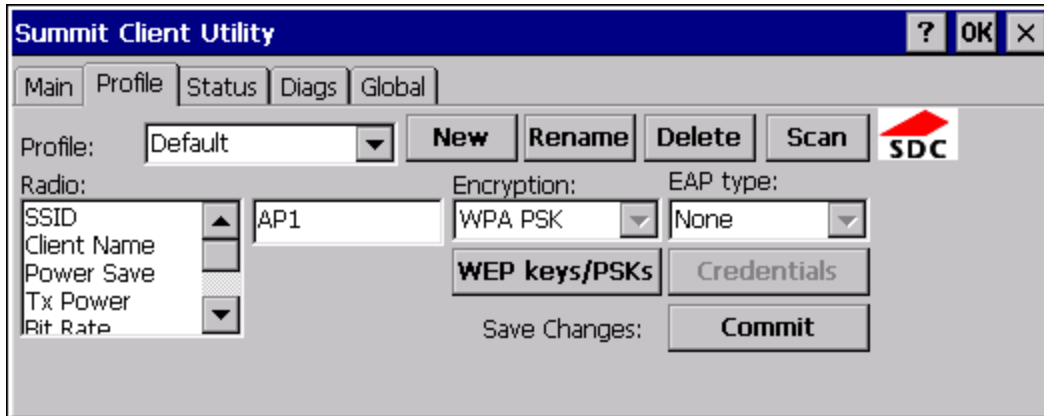
See [Certificates](#) for information on generating a Root CA certificate or a User certificate.

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

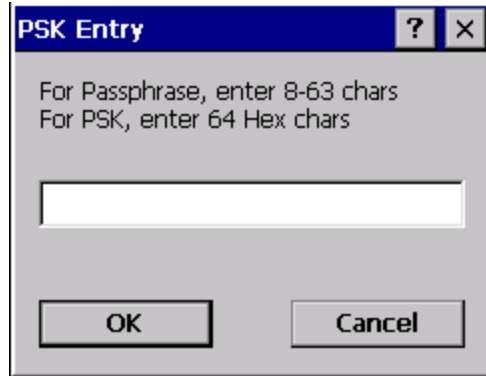
WPA PSK

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**



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



This value can be 64 hex characters or an 8 to 63 byte ASCII value. Enter the key and click **OK**.

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

Ensure the correct Active Profile is selected on the [Main tab](#) and warmboot. 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 VM1 and host computers when using any type of certificate. Certificates are date sensitive and if the date is not correct authentication will fail.

Quick Start

Root Certificates are necessary for EAP-TLS, PEAP/GTC and PEAP/MSCHAP.

1. [Generate a Root CA Certificate](#) and download it to a PC.
2. Connect the Thor VM1 to the desktop PC using ActiveSync and copy the certificate to the Thor VM1 \System folder.
3. [Install the Root CA Certificate](#).

User Certificates are necessary for EAP-TLS

1. [Generate a User Certificate and Private Key file](#) and download it to a PC.
2. Connect the Thor VM1 to the desktop PC using ActiveSync and copy the certificate and private key file to the Thor VM1 \System folder.
3. [Install the User Certificate and Private Key file](#).
4. After installation, perform a Suspend/Resume.
5. [Verify installation](#).

Generating a Root CA Certificate

Note: It is important that all dates are correct on the Thor VM1 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 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.



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.

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:

A dropdown menu with a blue header containing the text "Current". The menu is currently open, showing the selected item.

Encoding method:

- DER
- Base 64

[Download CA certificate](#)

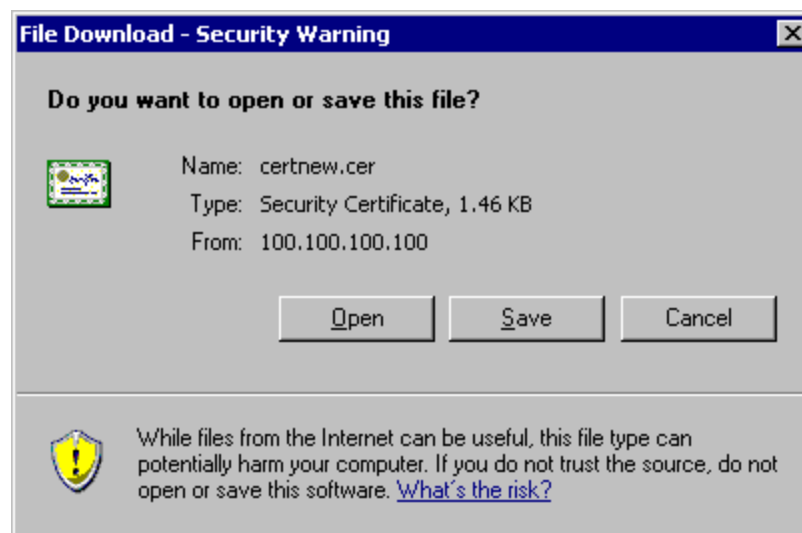
[Download CA certificate chain](#)

[Download latest base CRL](#)

[Download latest delta CRL](#)

Click the **DER** button.

To download the CA certificate, click on the **Download CA certificate** link.



Click the **Save** button and save the certificate. Make sure to keep track of the name and location of the certificate. [Install](#) the certificate on the Thor VM1.

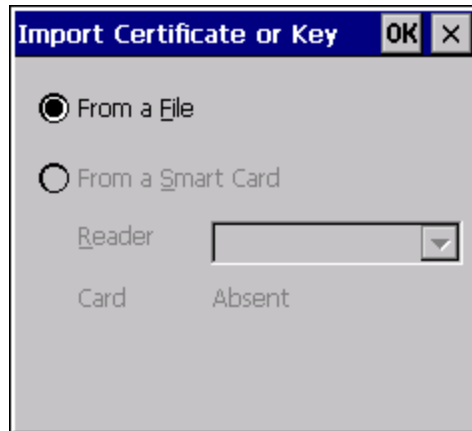
Installing a Root CA Certificate

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

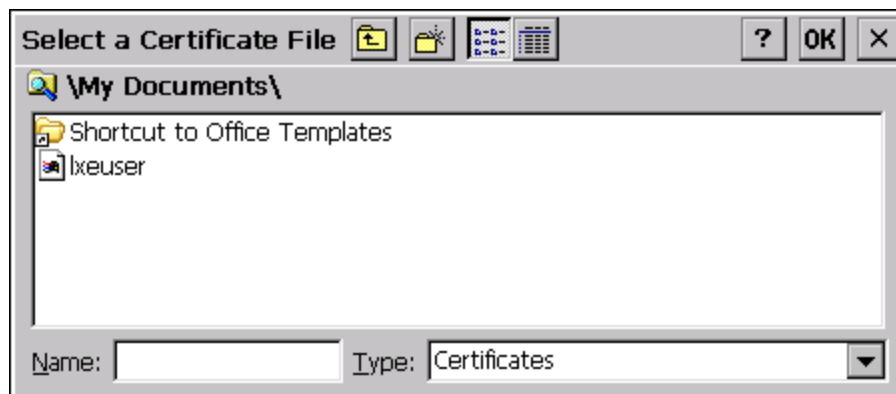
Copy the certificate file to the Thor VM1. Import the certificate by navigating to **Start > Control Panel > Certificates**.



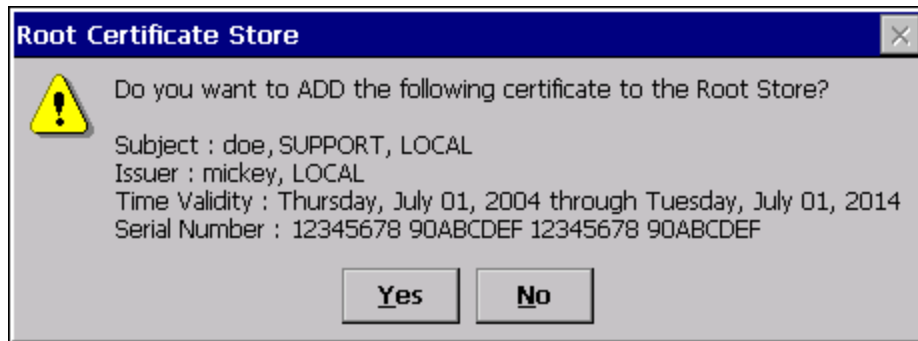
Tap the **Import** button.



Make sure **From a File** is selected and tap **OK**.



Using the explorer buttons, browse to the location where you copied the certificate, select the certificate desired and tap **OK**.



Tap **Yes** to import the certificate.

Once the certificate is installed, return to the proper authentication section, earlier in this manual.

Generating a User Certificate

The easiest way to get the user certificate is to use a browser on 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.



This process saves a user certificate and a separate private key file. Windows CE equipped devices such as the Thor VM1 require the private key to be saved as a separate file rather than including the private key in the user certificate.

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 **advanced certificate request** link.

Advanced Certificate Request

The policy of the CA determines the types of certificates you can request. Click one of the following options to:

[Create and submit a request to this CA.](#)

[Submit a certificate request by using a base-64-encoded CMC or : PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.](#)

[Request a certificate for a smart card on behalf of another user by using the smart card certificate enrollment station.](#)

Note: You must have an enrollment agent certificate to submit a request on of another user.

Click on the **Create and submit a request to this CA** link.

Advanced Certificate Request

Certificate Template:

User

Key Options:

Create new key set Use existing key set

CSP: Microsoft Enhanced Cryptographic Provider v1.0

Key Usage: Exchange

Key Size: 1024 Min: 384 Max: 16384 (common key sizes: [512](#) [1024](#) [2048](#) [4096](#) [8192](#) [16384](#))

Automatic key container name User specified key container name

Mark keys as exportable

Export keys to file

Full path name: user1key.pvk

Enable strong private key protection

Store certificate in the local computer certificate store
Stores the certificate in the local computer store instead of in the user's certificate store. Does not install the root CA's certificate. You must be an administrator to generate or use a key in the local machine store.

Additional Options:

Request Format: CMC PKCS10

Hash Algorithm: SHA-1

Only used to sign request.

Save request to a file

Attributes:

Empty list box for attributes with scroll arrows.

Friendly Name:

Empty text box for friendly name.

Submit >

For the **Certificate Template**, select **User**.

Check the **Mark keys as exportable** and the **Export keys to file** checkboxes.

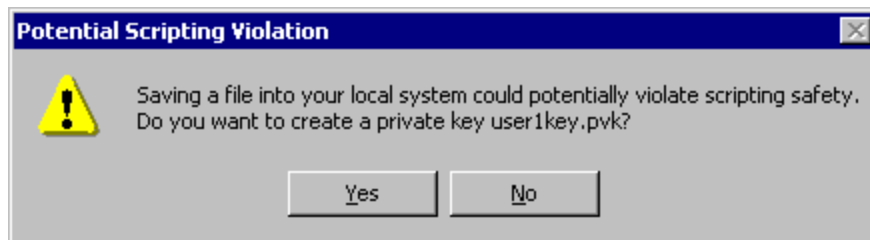
Type the full path on the local PC where the private key is to be copied. Also specify the private key filename.



Be sure to note the name used for the private key file, for example AAAUSER.PVK. The certificate file created later in this process must be given the same name, for example, AAAUSER.CER.

DO NOT check to use strong private key protection.

Make any other desired changes and click the **Submit** button.



If any script notifications occur, click the “**Yes**” button to continue the certificate request.



When prompted for the private key password:

- Click **None** if you do not wish to use a password, or
- Enter and confirm your desired password then click **OK**.

Certificate Issued

The certificate you requested was issued to you.

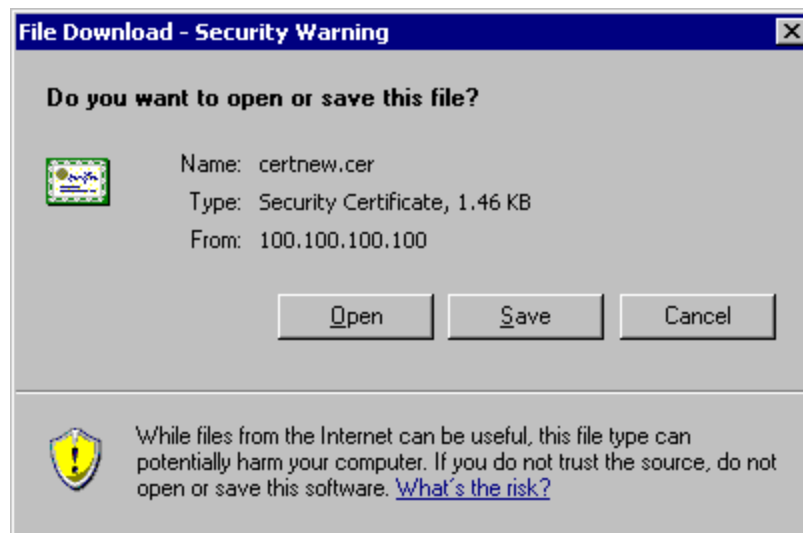
DER encoded or Base 64 encoded



[Download certificate](#)

[Download certificate chain](#)

Click the **Download certificate** link.



Click **Save** to download and store the user certificate to the PC. Make sure to keep track of the name and location of the certificate. The private key file is also downloaded and saved during this process.

Be sure use the same name for the certificate file as was used for the private key file. For example, if the private key was saved as AAAUSER.PVK then the certificate file created must be given the same name, for example, AAAUSER.CER.

[Install](#) the user certificate.

Installing a User Certificate

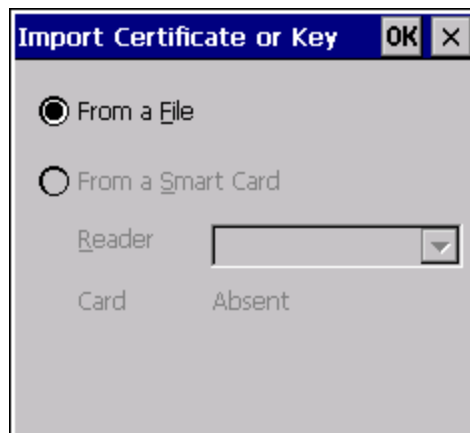
Copy the certificate and private key files to the Thor VM1. Import the certificate by navigating to **Start > Control Panel > Certificates**.



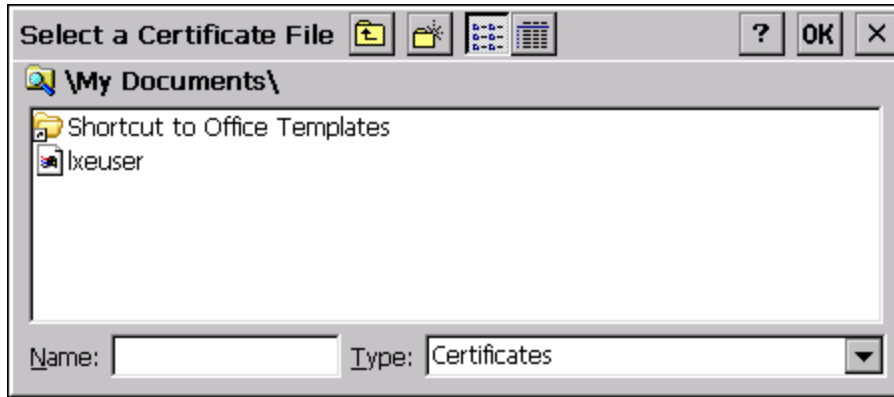
Select **My Certificates** from the pull down list.



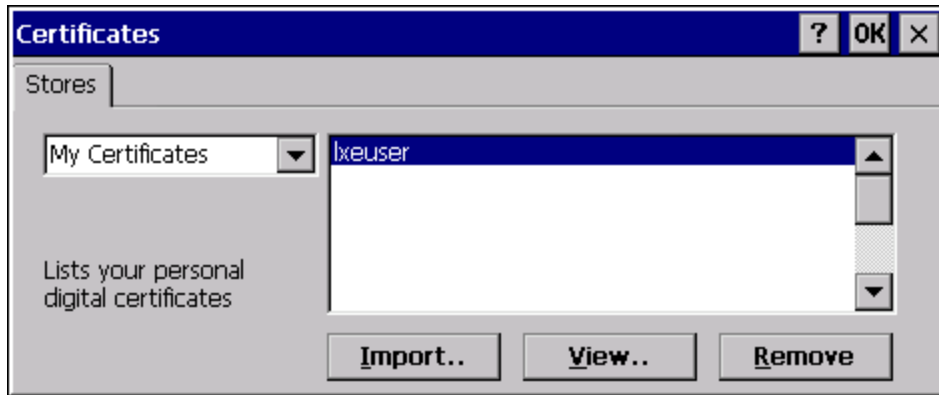
Tap the **Import** button.



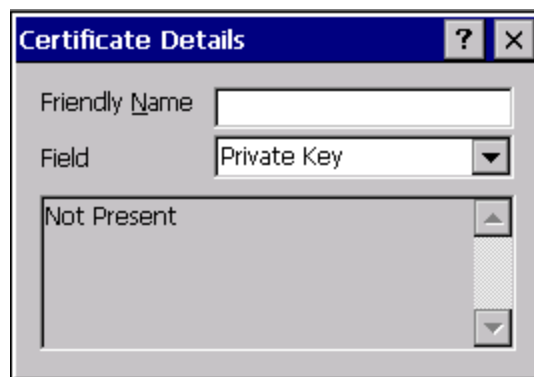
Make sure **From a File** is selected and tap **OK**.



Using the explorer buttons, browse to the location where you copied the certificate, select the certificate desired and tap **OK**. The certificate is now shown in the list.

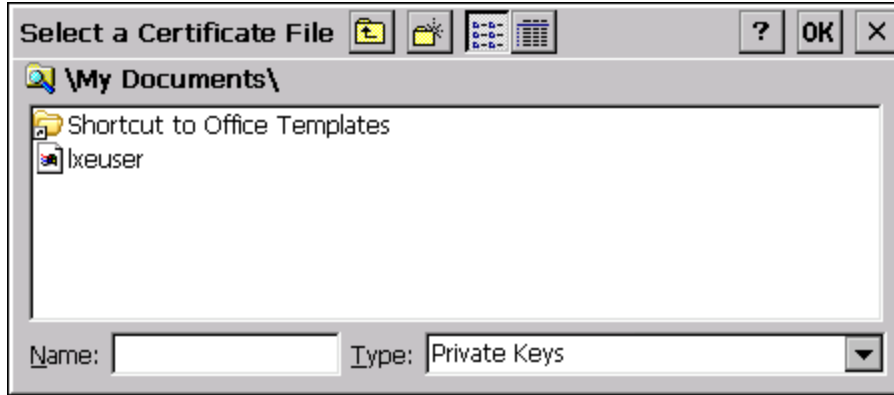


With the certificate you just imported highlighted, tap **View**. From the Field pull down menu, select **Private Key**.



- If the private key is present, the process is complete.
- If the private key is not present, import the private key.

To import the private key, tap **OK** to return to the Certificates screen. Tap import.



Using the explorer buttons, browse to the location where you copied the private key file, change the Type pull down list to **Private Keys**, select the certificate desired and tap **OK**. Enter the password for the certificate if appropriate.

Verify Installation

Tap on **View** to see the certificate details again.



The private key should now say present. If it does not, there is a problem. Possible items to check:

- Make sure the certificate was generated with a separate private key file, as shown earlier in this section. If the certificate was not generated with a separate private key file, generate a new certificate and follow the import process again.
- Make sure the certificate and private key file have the same name, for example AAAuser.cer for the certificate and AAAuser.pvk for the private key file. If the file names are not the same, rename the private key file and import it again.

Chapter 7: Technical Specifications

Thor VM1

Processor	Atom CPU operating at 1.6 GHz.
Memory	1GB SDRAM
Mass Storage	1GB CompactFlash
Storage Expansion	User installable , supports 1 to 4GB SD card
Operating System	Microsoft CE 6.0
Radio Modules	802.11 a/b/g radio / Bluetooth Optional GPS / WWAN
Scanner Options	No integrated scanner Optional serial, USB or Bluetooth scanners.
Display Technology	Controller: WVGA compatible controller Active matrix TFT Resolution: 800 x 480 pixels 400 NIT (indoor) or 900 NIT (outdoor) brightness 8" (measured horizontally) display Transmissive with LED backlight Automatic brightness control on outdoor display Vehicle motion screen blanking available
Touch Screen	Impact resistive Signature capture capability Optional defroster Field replaceable front panel including touch screen and optional defroster
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, field replaceable
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 Client Port and USB Host Port via adapter cable
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 VM1

Width	10.6" (26.8 cm)
Height	8.4" (21.4 cm)
Depth	1.7" (4.3 cm) to 2.6" (6.6 cm) (at latch)
Weight	5.6 lb. (2.1 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. (1.2 kg)

Environmental Specifications

Thor VM1 and Quick Mount Smart Dock

Operating Temperature	Standard: -4°F to 122°F (-20°C to 50°C) [non-condensing] Extended temperature: -22° to 122° F (-30°C to 50°C) [condensing]
Storage Temperature	Standard and Extended 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 802.11a/b/g

Bus Interface	32-bit SDIO (Secure Digital I/O)
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	1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps
RF Power Level	64 mW (18dBm)
Channels	FCC: 1-11, 36, 40, 44, 48, 149, 153, 157, 161 ETSI: 1-13, 36, 40, 44, 48
Operating Temperature	Same as Thor VM1 Operating Temperature
Storage Temperature	Same as Thor VM1 Storage Temperature
Connectivity	TCP/IP, Ethernet, ODI
Diversity	Yes

Bluetooth

Bus Interface	CompactFlash
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 8: Key Maps

64-Key QWERTY Keypad Key Map



- Because the keyboard only has 64 keys, all functions are not visible (or printed on the keyboard). Therefore the Thor VM1 keyboard supports what is called hidden keys – keys that are accessible but not visible on the keyboard.
- A key or combination of 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 KeyPad option in the Control Panel ([Start > Settings > Control Panel > KeyPad](#)).
- Remapped keys persist across a warmboot or power cycle.
- The keyboard does not have a NumLock indicator or key. NumLock is always On.
- The warmboot behavior of CapsLock can be set via the Misc tab in [Start > Settings > Control Panel > Options](#).

The Thor VM1 keyboard keys are backlit.

- By default, the keyboard backlight follows the display backlight. When the display backlight is on, the keyboard backlight is on.
- If the display backlight brightness is increased (or decreased) the keyboard backlight brightness is increased (or decreased).
- The keyboard backlight and the display share the same timer, which is configured in [Start > Settings > Control Panel > Power](#).
- The keyboard backlight can be disabled. See [Start > Settings > Control Panel > Options > Misc](#) tab.

Note: When automatic brightness control is enabled for a Thor VM1 with an Outdoor display, the manual display brightness controls in the table below have no effect.

To get this Key / Function	Press These Keys in this Order	
Power On/Suspend	Power	
2nd mode	2nd	
Volume Up	2nd	F9
Volume Down	2nd	F10
Display Backlight Brightness Up	2nd	F7 (see note above)
Display Backlight Brightness Down	2nd	F8 (see note above)
Shift	Shift	
Alt	Alt	
Ctrl	Ctrl	
Esc	Esc	
Space	Space	
CapsLock	2nd	Shift
Enter	Enter	
Delete	Del	
. (VK_DECIMAL)	.	
Back Space	BkSp	
Insert	2nd	BkSp
Tab	Tab	
Back Tab	2nd Tab	
Ctrl-Break		
Pause		
Up Arrow	Up Arrow	
Down Arrow	Down Arrow	
Right Arrow	Right Arrow	
Left Arrow	Left Arrow	
Page Up	2nd	Up Arrow
Page Down	2nd	Down Arrow
End	2nd	Right Arrow
Home	2nd	Left Arrow
F1 - F10	F1 - F10	
F11 - F20	Shift	F1 - F10
F21 - F30	Alt	F1 - F10
F31 - F40	Ctrl	F1 - F10

a	A	
b	B	
c	C	
d	D	
e	E	
f	F	
g	G	
h	H	
i	I	
j	J	
k	K	
l	L	
m	M	
n	N	
o	O	
p	P	
q	Q	
r	R	
s	S	
t	T	
u	U	
v	V	
w	W	
x	X	
y	Y	
z	Z	
A	Shift	A
B	Shift	B
C	Shift	C
D	Shift	D
E	Shift	E
F	Shift	F
G	Shift	G
H	Shift	H
I	Shift	I

J	Shift	J
K	Shift	K
L	Shift	L
M	Shift	M
N	Shift	N
O	Shift	O
P	Shift	P
Q	Shift	Q
R	Shift	R
S	Shift	S
T	Shift	T
U	Shift	U
V	Shift	V
W	Shift	W
X	Shift	X
Y	Shift	Y
Z	Shift	Z
	2nd	A
~	2nd	B
:	2nd	D
#	2nd	E
;	2nd	F
"	2nd	G
'	2nd	H
*	2nd	I
,	2nd	J
.(VK_PERIOD)	2nd	K
?	2nd	L
_	2nd	M
`	2nd	N
(2nd	O
)	2nd	P
!	2nd	Q
\$	2nd	R
\	2nd	S

%	2nd	T
&	2nd	U
@	2nd	W
^	2nd	Y
1	1	
2	2	
3	3	
4	4	
5	5	
6	6	
7	7	
8	8	
9	9	
0	0	
>	2nd	1
[2nd	2
]	2nd	3
=	2nd	4
{	2nd	5
}	2nd	6
/	2nd	7
-	2nd	8
+	2nd	9
<	2nd	0
!	Shift	1
@	Shift	2
#	Shift	3
\$	Shift	4
%	Shift	5
^	Shift	6
&	Shift	7
*	Shift	8
(Shift	9
)	Shift	0

12-Key Keypad Key Map

The 12-key keyboard is available on the Thor VM1 running Windows CE 6.0.



- Because the keyboard only has 12 keys, all functions are not visible (or printed on the keyboard). Therefore the Thor VM1 keyboard supports what is called hidden keys -- keys that are accessible but not visible on the keyboard.
- A key or combination of 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 keyboard option in the Control Panel ([Start > Settings > Control Panel > KeyPad](#)).
- Remapped keys persist across a warmboot or power cycle.
- The keyboard does not have a NumLock indicator or key. NumLock is always On.
- The warmboot behavior of CapsLock can be set via the Misc tab in [Start > Settings > Control Panel > Options](#).

The Thor VM1 keyboard keys are backlit.

- By default, the keyboard backlight follows the display backlight. When the display backlight is on, the keyboard backlight is on.
- If the display backlight brightness is increased (or decreased) the keyboard backlight brightness is increased (or decreased).
- The keyboard backlight and the display share the same timer, which is configured in [Start > Settings > Control Panel > Power](#).
- The keyboard backlight can be disabled. See [Start > Settings > Control Panel > Options > Misc](#) tab.

Note: When automatic brightness control is enabled for a Thor VM1 with an Outdoor display, the manual display brightness controls in the table below have no effect.

To get this Key / Function	Press These Keys in this Order	
Power On/Suspend	Power	
F1 - F10	F1 - F10	
F11 - F20	Shift	F1 - F10
Brightness Up	2nd	F7 (see note above)
Brightness Down	2nd	F8 (see note above)
Volume Up	2nd	F9
Volume Down	2nd	F10

IBM Terminal Emulation

The Thor VM1/IBM 3270 and IBM 5250 Terminal Emulator keypads are designed to allow the user to enter terminal emulator commands when running the RFTerm program. When running RFTerm on the Thor VM1, please refer to the *RFTerm Reference Guide* for equivalent keys and keypress sequences.

IBM 3270



Legend on Keypad	Explanation	Key Sequence
Attn	Attention	Ctrl + A
Clr	Clear	Ctrl + C
Del	Delete	Ctrl + D
E-Inp	Erase Input	Ctrl + BkSp
Ins	Insert	Ctrl + I
NL	New Line	Ctrl + N
PA1		Ctrl + F1
PA2		Ctrl + F2
PA3		Ctrl + F3
Rst	Reset	Ctrl + R
SysReq	System	Ctrl + S

IBM 5250



Legend on Keypad	Explanation	Key Sequence
Attn	Attention	Ctrl + A
Clr	Clear	Ctrl + C
Del	Delete	Ctrl + D
Dup	Duplicate	Ctrl + U
E-Inp	Erase Input	Ctrl + Bksp
Field Exit	Enter	Enter
Fld -	Field Minus	Ctrl + M
Fld +	Field Plus	Ctrl + L
Ins	Insert	Ctrl + I
NL	New Line	Ctrl + N
SysReq	System	Ctrl + S



Chapter 9: 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 VM1 is 1 year.

The duration of the limited warranty for the Thor VM1 Quick Mount Smart Dock is 1 year.

The duration of the limited warranty for the Thor VM1 Vehicle Mount Assembly is 1 year.

The duration of the limited warranty for the Thor VM1 internal UPS battery is 1 year.

The duration of the limited warranty for the Thor VM1 AC power supply and cables is 1 year.

The duration of the limited warranty for the Thor VM1 DC-DC Converter is 1 year.

The duration of the limited warranty for the Thor VM1 cables (USB, Serial, Communication, Power) is 1 year.



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

E-EQ-VM1CERG
Rev D
10/12