Your Trusted Partner for Time and
Attendance Terminals and Integrated Solutions

Reference Manual

Maximus Reference Manual

Part Number: MANU-MAXIMUS-02
Revision-02

Revision History

Revision	Date	Description
00	02/10/2015	Extensive revision to previous documents requiring new Part Number.
01	04/20/2015	Added WiFi security protocol note on page page 3-34 and added "Configuring WiFi" to Chapter 4, "Color Terminals."
02	08/27/2015	Graphic changes to the cover.

Trademarks

Copyright

The information in this document is subject to change without notice. Accu-Time Systems assumes no responsibility for any damages arising from the use of this document, including but not limited to, lost revenue, lost data, claims by third parties, or other damages

Table of Contents

Preface

P

Preface

Purpose

This manual describes the Maximus® terminal. It tells you how to install, set up, and test a Maximus terminal, and how to get firmware version information from the terminal to help diagnose a problem if one occurs.

Intended Audience

You should read this manual if you are responsible for the installation or operation of a Maximus terminal.

- Chapter 1, "Terminal Description.", gives a general overview of the characteristics and specifications of Accu-Engine Serial terminals.
- Chapter 2, "Installation.", interests those responsible for the installation of the terminal or its wiring.
- Chapter 3, "Monochrome Terminals.", tells how to use the setup, test, and information menus in your monochrome Maximus terminal.
- Chapter 4, "Color Terminals.", tells how to use the setup, test, and information menus in your color Maximus terminal.
- Chapter 5, "Maintenance.", provides an overview of power, maintenance, and troubleshooting for your Maximus terminal.
- Appendix Title A, "Biometrics." describes using a biometric reader.
- Appendix Title B, "Badge Specifications." provides the specifications for employee badges.
- Appendix Title C, "Using the USB." describes using a USB drive with the terminal.
- Appendix Title D, "GSM/GPRS Setup." provides details for configuring a GSM/GPRS modem.

This page intentionally left blank.

Document Conventions

The sections below explain the conventions used to present information in this manual.

Text Conventions

Table P-1 lists the text conventions used in this document (manual).

Table P-1 Document Text Conventions

Convention	Description
Subscripts	Subscripts indicate the base of a number. For example, 28_{10} is 28 base 10, and $3F_{16}$ is 3F base 16.
####	#### represents a string of digits (unless the digits have a specific reference).
aaaa	*aaaa* represents a string of alphabetic characters (unless the characters have a specific reference).
Blue Underlined Text	Hyperlinks to sources external to this document appear in blue underlined text (e.g., http://www.accu-time.com).
Blue Text	Hyperlinks to internal sources (within this document) appear in non-underlined blue text (e.g., Chapter 2, "Installation.").
Bold Body Text	Bold text in the document body text represents names and symbols that appear on the user interface screens. For example: Select **Administration** from the **Main Menu**. The **System Administration** screen appears. In this example "**Administration**" is a parameter on a screen that you select and "**Main Menu**" and "**System Administration**" are titles/labels that appear on the screens. This rule applies only to paragraph body text and does not apply to chapter titles, headers, footers, or figure and table numbers.
Bold Typewriter Font	Courier font, also referred to as "typewriter font" appears in this document as something you type (enter) into the User Interface. For example: Type **`connect1`** in the **Name** text box then press the Enter key. In this example **`connect1`** is what you actually type and **Name** is the text box label as it appears on the screen.
Grey Text	**Text in grey indicates that the commands/descriptions are not yet implemented/active.**
Table P-1	

Control Character Representation

The syntax of UCS commands includes some non-printing control characters (character codes 000 to 031_{10}, 000 to $1F_{16}$) plus the space character. These non-printing characters and the space character are represented in this manual in various ways as shown in Table P-2. In many text editors, you can generate a control character by holding down the CTRL key and pressing the appropriate printing key. For example, you can generate a record separator (30_{10}, $1E_{16}$) by holding down the CTRL key and pressing the up caret (^) key (SHIFT-6). This key sequence is represented as CTRL/^ and shown in this document as the symbol: **»**. Other text editors let you enter control characters by pressing the ALT key, then entering the three-digit decimal value. Or, you can write a custom application, which inserts control characters as required, to generate download files.

Table P-2 Control Character Symbols Used in this Document

Value	Use	Symbol	CTRL
28_{10}, $1C_{16}$	Field separator	◆	CTRL/\
29_{10}, $1D_{16}$	Group separator	⊃	CTRL/]
30_{10}, $1E_{16}$	Record separator	»	CTRL/^
31_{10}, $1F_{16}$	Unit separator	¤	CTRL/_
32_{10}, 20_{16}	Space character	■	
09_{10}, 09_{16}	Tab	➤	
Table P-2			

Command Format

The command strings shown in this manual are color coded to more clearly separate the parameters of the command. Some fields can be left empty when not required, although most must be space- or zero-filled to size. The parameters in each command string are explained below it, color coded to match their position in the command.

Example:

L04B00**»***VFN***»***NVE***»***VEL***»***VBPN***»***VT***»**

Note & Warning Formats

This section describes the note and warning formats used in this document (manual) and the circumstances to which they apply.

Notes

Important information and tips appear as notes. Notes have a special format and appearance. The following is an example of the note format:

NOTE: This is how a note appears in this document.

Warning Formats

This document may use warnings for various potential conditions. The following are the warning formats with descriptions of their use:

DANGER SHOCK

This format is used for an electrical danger that may injure or kill the user

DANGER

This format is used for a non-electrical condition that is potentially fatal to the user.

Warning

This format is used for a hazardous condition that may cause personal injury to the user.

CAUTION

This format is used for a condition that may damage equipment but with little or no risk of personal injury.

This page intentionally left blank.

Terminal Description

1

Chapter

About this Chapter

This chapter provides an overview of the Maximus terminal and lists its Part Numbers and specifications.

Chapter Contents

This chapter contains the following topics:

This page intentionally left blank.

Maximus Overview

The Maximus® time and attendance terminal for workforce management features rugged aluminum construction and flexible configuration options. Due to its compact design, Maximus is selected by well-respected companies throughout the world. Founded on a Linux operating system, Maximus has the flexibility to meet a wide array of needs, including Java programmability, Web services, open standards, XML, and a keypad with user defined function keys.

The Maximus terminal supports a variety of features, such as GSM/GPRS, Ethernet, and serial connectivity, as well as barcode, magnetic, and proximity readers.

To eliminate buddy punching, Maximus terminals can be equipped with fingerscan biometric readers.

Programming the Terminal

Maximus terminals recognize the Accu-Time universal command set (UCS). Those programming commands are described in the *Universal Command Set Reference Manual*, the *Advanced Development Manual for Accu-Time Terminals*, or the documentation from your reseller.

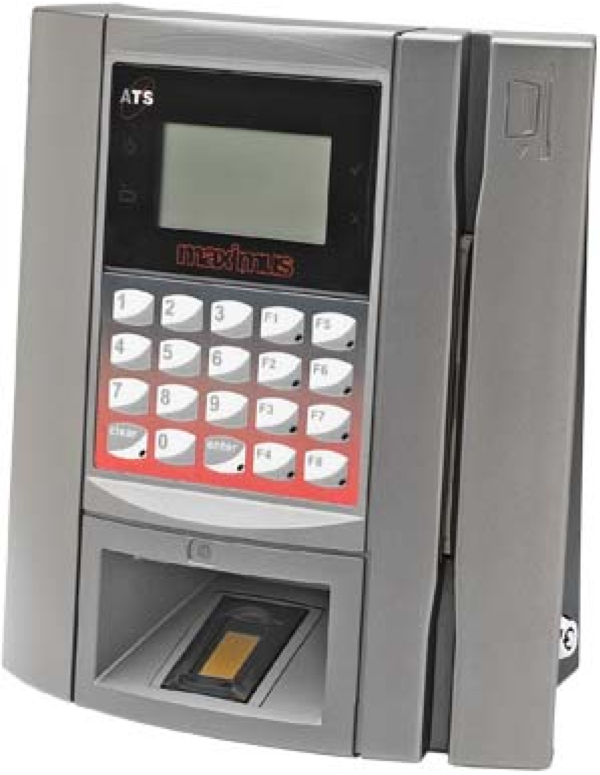
In addition, the Maximus reliably supports third-party software and the needs of our partners for human capital management, payroll data collection, and workforce tracking.

Maximus Features

The Accu-Time Maximus terminal, shown in Figure 1-1, is available in both standard (monochrome) and color display versions. Highly versatile for incorporation into many time or data collection environments, the Maximus offers a large user memory base of up to 128 MB. The Maximus supports a standard TCP/IP Ethernet 10/100BASE-T interface and serial EIA RS232. The many options of the Maximus include:

- **Multi-Media**: Can support most standard bar code formats.
- **Flexibility**: An Maximus can act as a stand-alone time station or as part of a local or wide area network. The terminal can also interface with virtually any host hardware or software platform.
- **Custom Applications**: Custom programs and programmable function keys provide you with the flexibility to create a variety of options.
- **Reliability**: A Real Time Clock (RTC) provides 12 or 24 hour time formats with quartz precision. An optional non-interruptible power supply (UPS) provides terminal operation for up to 1.5 hours during power outages. Data storage is preserved with a flash memory backup system.
- **Durability**: A rugged metal enclosure protects circuitry from environmental conditions such as extreme temperatures and airborne dust.

Figure 1-1 Standard Maximus Terminal (with biometric and "swipe" card readers)



Specifications

Table 1-1 lists the specifications for Maximus terminals.

Table 1-1 Maximus Specifications

Display	128 x 64 pixel monochrome LCD (standard) or 320x240 transmissive color LCD.
RTC	Battery-backed Real-time Clock, 12- or 24-hour format (quartz precision)
Keypad	20 key push-button 4x5 matrix 0–9 numeric keypad 8 software-defined function keys 10 LED illuminated keys (function keys plus “clear” and “enter”).
Memory	Linux: 32 MB RAM and 32 MB flash XML: 32 MB RAM and 32 MB flash Java: 128 MB RAM and 128 MB flash
Programming	Java® ATS Universal Command Set (over Linux) or third-party custom application packages Web services enabled
Diagnostics	On-board diagnostics and remote diagnostic capability
Interfaces	IEEE 802.3 10/100BASE-T Ethernet with DHCP HTTP, FTP, XML USB port for mass storage device Optional EIA RS232 Optional GSM/GPRS modem Optional internal modem (FCC Part 68 certified)
Host Connectivity	Ethernet (standard), serial RS232 (option) or dial-up modem (option)
Power	12 VDC ±5%, 1.25 A, 15 W maximum Optional non-interruptible power source with charger Optional IEEE 802.3af-compliant power over Ethernet
Ethernet	Ethernet IEEE 802.3, with a default host port of 2500 and Microsoft or UNIX Berkeley sockets. DHCP (Dynamic Host Configuration Protocol) support standard. Optional IEEE 802.3af power over Ethernet (PoE). DHCP

Table 1-1 (page 1 of 2)

Table 1-1 Maximus Specifications

WiFi	Available in two versions: • WPA2/802.11i (enterprise-grade security and authentication protocols) • IEEE 802.11b; 802.11g (Non-Enterprise Version)
Optional UPS Battery	Discharge life: 1.5 hours at 23°C (73°F) Charging (normal): 0° to 45°C (32° to 113°F) Storage: -20° to 35°C (-4° to 95°F) Discharging (battery operation): -20° to 60°C (-4° to 140°F)
Enclosure	Die-cast aluminum housing hinged to key-lockable base
Environmental	Operating temperature: 0° to 50°C (32° to 122°F) Storage temperature: -20° to 80°C (-4° to 176°F)
Dimensions	21.33 cm x 22.22 cm x 9.91 cm (8.4” x 8.75” x 3.9”)
Certifications	CE Mark, FCC Part 15 Class A
Accessories	• Biometric readers – 1:1 and 1:n – fingerscan • Integrated visible or infrared barcode readers • Integrated magnetic stripe readers • Smartcard readers – contactless (Mifare™, iClass®) • Integrated proximity readers • Solid-state or dry-contact relay modules • Serial interface for printer
Table 1-1 (page 2 of 2)	

Part Numbers and Options

Table 1-2 lists the Maximus terminal main configuration Part Numbers and descriptions.

Table 1-2 Maximus Part Numbers

Part Number	Description
Maximus Base Unit	
MXS2000/XX	Base Maximus: • UCS running on Linux OS • 32MB RAM, 32MB Flash • Ethernet Host connection • 128x64 monochrome LCD • 0-9 numeric keypad w/ Clear, Enter and 8 Custom Function Keys
MCS2000/XX	Base Color Maximus: • UCS running on Linux OS • 32MB RAM, 32MB Flash • Ethernet Host connection • 320x240 transmissive LCD full color display • 0-9 numeric keypad w/ Clear, Enter and 8 Custom Function Keys
MXJ2000/XX	Base Java Maximus: • UCS running on Linux OS • 128MB RAM, 128MB Flash • Java license • Ethernet Host connection • 128x64 monochrome LCD • 0-9 numeric keypad w/ Clear, Enter and 8 Custom Function Keys
MCJ2000/XX	Base Java Color Maximus: • UCS running on Linux OS • 128MB RAM, 128MB Flash • Java license • Ethernet Host connection • 320x240 transmissive LCD full color display • 0-9 numeric keypad w/ Clear, Enter and 8 Custom Function Keys
Table 1-2 (page 1 of 9)	

Table 1-2 Maximus Part Numbers

Part Number	Description
MXS2100/XX	Biometric Verification Maximus: • 1:1 E-Field Fingerscan Reader (4K templates - requires PIN) • UCS running on Linux OS • 32MB RAM, 32MB Flash • Ethernet Host connection • 128x64 monochrome LCD • 0-9 numeric keypad w/ Clear, Enter and 8 Custom Function Keys
MCS2100/XX	Biometric Verification Color Maximus: • 1:1 E-Field Fingerscan Reader (4K templates - requires PIN) • UCS running on Linux OS • 32MB RAM, 32MB Flash • Ethernet Host connection • 320x240 transmissive LCD full color display • 0-9 numeric keypad w/ Clear, Enter and 8 Custom Function Keys • With pin
MXJ2100/XX	Biometric Verification Java Maximus: • 1:1 E-Field Fingerscan Reader (4K templates - requires PIN) • Java running on Linux OS • 128MB RAM, 128MB Flash • Java license • Ethernet Host connection • 128x64 monochrome LCD • 0-9 numeric keypad w/ Clear, Enter and 8 Custom Function Keys
MCJ2100/XX	Biometric Verification Java Color Maximus: • 1:1 E-Field Fingerscan Reader (4K templates - requires PIN) • Java running on Linux OS • 128MB RAM, 128MB Flash • Java license • Ethernet Host connection • 320x240 transmissive LCD full color display • 0-9 numeric keypad w/ Clear, Enter and 8 Custom Function Keys

Table 1-2 (page 2 of 9)

Table 1-2 Maximus Part Numbers

Part Number	Description
MXS2101/XX	Biometric Identification Maximus: • 1:N E-Field Fingerscan Reader (500 templates - no PIN required) • UCS running on Linux OS • 32MB RAM, 32MB Flash • Ethernet Host connection • 128x64 monochrome LCD • 0-9 numeric keypad w/ Clear, Enter and 8 Custom Function Keys
MCS2101/XX	Biometric Identification Color Maximus: • 1:N E-Field Fingerscan Reader (500 templates - no PIN required) • UCS running on Linux OS • 32MB RAM, 32MB Flash • Ethernet Host connection • 320x240 transmissive LCD full color display • 0-9 numeric keypad w/ Clear, Enter and 8 Custom Function Keys
MXJ2101/XX	Biometric Identification Java Maximus: • 1:N E-Field Fingerscan Reader (500 templates - no PIN required) • Java running on Linux OS • 128MB RAM, 128MB Flash • Java license • Ethernet Host connection • 128x64 monochrome LCD • 0-9 numeric keypad w/ Clear, Enter and 8 Custom Function Keys
MCJ2101/XX	Biometric Identification Java Color Maximus: • 1:N E-Field Fingerscan Reader (500 templates - no PIN required) • Java running on Linux OS • 128MB RAM, 128MB Flash • Java license • Ethernet Host connection • 320x240 transmissive LCD full color display • 0-9 numeric keypad w/ Clear, Enter and 8 Custom Function Keys
Table 1-2 (page 3 of 9)	

Table 1-2 Maximus Part Numbers

Part Number	Description
MXS2105/XX	Cogent Biometric Verification Maximus: • Cogent 1:1 Capacitive fingerscan Reader (9K templates - requires PIN) • UCS running on Linux OS • 32MB RAM, 32MB Flash • Ethernet Host connection • 128x64 monochrome LCD • 0-9 numeric keypad w/ Clear, Enter and 8 Custom Function Keys
MCS2105/XX	Cogent Biometric Verification Color Maximus: • Cogent 1:1 Capacitive Fingerscan Reader (9K templates - requires PIN) • UCS running on Linux OS • 32MB RAM, 32MB Flash • Ethernet Host connection • 320x240 transmissive LCD full color display • 0-9 numeric keypad w/ Clear, Enter and 8 Custom Function Keys
MXJ2105/XX	Cogent Biometric Verification Java Maximus: • Cogent 1:1 Capacitive Fingerscan Reader (9K templates - requires PIN) • Java running on Linux OS • 128MB RAM, 128MB Flash • Java license • Ethernet Host connection • 128x64 monochrome LCD • 0-9 numeric keypad w/ Clear, Enter and 8 Custom Function Keys
MCJ2105/XX	Cogent Biometric Verification Java Color Maximus: • Cogent 1:1 Capacitive Fingerscan Reader (9K templates - requires PIN) • Java running on Linux OS • 128MB RAM, 128MB Flash • Java license • Ethernet Host connection • 320x240 transmissive LCD full color display • 0-9 numeric keypad w/ Clear, Enter and 8 Custom Function Keys
Table 1-2 (page 4 of 9)	

Table 1-2 Maximus Part Numbers

Part Number	Description
MXS2106/XX	Cogent Biometric Identification Maximus: • Cogent 1:N Capacitive Fingerscan Reader (1200 templates - no PIN required) • UCS running on Linux OS • 32MB RAM, 32MB Flash • Ethernet Host connection • 128x64 monochrome LCD • 0-9 numeric keypad w/ Clear, Enter and 8 Custom Function Keys
MCS2106/XX	Cogent Biometric Identification Color Maximus: • Cogent 1:N Capacitive Fingerscan Reader (1200 templates - no PIN required) • UCS running on Linux OS • 32MB RAM, 32MB Flash • Ethernet Host connection • 320x240 transmissive LCD full color display • 0-9 numeric keypad w/ Clear, Enter and 8 Custom Function Keys
MXJ2106/XX	Cogent Biometric Identification Java Maximus: • Cogent 1:N Capacitive Fingerscan Reader (1200 templates - no PIN required) • Java running on Linux OS • 128MB RAM, 128MB Flash • Java license • Ethernet Host connection • 128x64 monochrome LCD • 0-9 numeric keypad w/ Clear, Enter and 8 Custom Function Keys
MCJ2106/XX	Cogent Biometric Identification Java Color Maximus: • Cogent 1:N Capacitive Fingerscan Reader (1200 templates - no PIN required) • Java running on Linux OS • 128MB RAM, 128MB Flash • Java license • Ethernet Host connection • 320x240 transmissive LCD full color display • 0-9 numeric keypad w/ Clear, Enter and 8 Custom Function Keys
Table 1-2 (page 5 of 9)	

Table 1-2 Maximus Part Numbers

Part Number	Description
MXS2107/XX	Suprema Biometric Verification Maximus: • Suprema 1:1 Capacitive Fingerscan Reader (9K templates - requires PIN) • UCS running on Linux OS • 32MB RAM, 32MB Flash • Ethernet Host connection • 128x64 monochrome LCD • 0-9 numeric keypad w/ Clear, Enter and 8 Custom Function Keys
MCS2107/XX	Suprema Biometric Verification Color Maximus: • Suprema 1:1 Capacitive Fingerscan Reader (9K templates - requires PIN) • UCS running on Linux OS • 32MB RAM, 32MB Flash • Ethernet Host connection • 320x240 transmissive LCD full color display • 0-9 numeric keypad w/ Clear, Enter and 8 Custom Function Keys
MXJ2107/XX	Suprema Biometric Verification Java Maximus: • Suprema 1:1 Capacitive Fingerscan Reader (9K templates - requires PIN) • Java running on Linux OS • 128MB RAM, 128MB Flash • Java license • Ethernet Host connection • 128x64 monochrome LCD • 0-9 numeric keypad w/ Clear, Enter and 8 Custom Function Keys.
MCJ2107/XX	Suprema Biometric Verification Java Color Maximus: • Suprema 1:1 Capacitive Fingerscan Reader (9K templates - requires PIN) • Java running on Linux OS • 128MB RAM, 128MB Flash • Java license • Ethernet Host connection • 320x240 transmissive LCD full color display • 0-9 numeric keypad w/ Clear, Enter and 8 Custom Function Keys.

Table 1-2 (page 6 of 9)

Table 1-2 Maximus Part Numbers

Part Number	Description
MXS2108/XX	Suprema Biometric Identification Maximus: • Suprema 1:N Capacitive Fingerscan Reader (1200 templates - no PIN required) • UCS running on Linux OS • 32MB RAM, 32MB Flash • Ethernet Host connection • 128x64 monochrome LCD • 0-9 numeric keypad w/ Clear, Enter and 8 Custom Function Keys
MCS2108/XX	Suprema Biometric Identification Color Maximus: • Suprema 1:N Capacitive Fingerscan Reader (1200 templates - no PIN required) • UCS running on Linux OS • 32MB RAM, 32MB Flash • Ethernet Host connection • 320x240 transmissive LCD full color display • 0-9 numeric keypad w/ Clear, Enter and 8 Custom Function Keys
MXJ2108/XX	Suprema Biometric Identification Java Maximus: • Suprema 1:N Capacitive Fingerscan Reader (1200 templates - no PIN required) • Java running on Linux OS • 128MB RAM, 128MB Flash • Java license • Ethernet Host connection • 128x64 monochrome LCD • 0-9 numeric keypad w/ Clear, Enter and 8 Custom Function Keys
MCJ2108/XX	Suprema Biometric Identification Java Color Maximus: • Suprema 1:N Capacitive Fingerscan Reader (1200 templates - no PIN required) • Java running on Linux OS • 128MB RAM, 128MB Flash • Java license • Ethernet Host connection • 320x240 transmissive LCD full color display • 0-9 numeric keypad w/ Clear, Enter and 8 Custom Function Keys
Table 1-2 (page 7 of 9)	

Table 1-2 Maximus Part Numbers

Part Number	Description
MXS2111/XX	Accu-Touch Biometric Verification Maximus: • Lumidigm 1:1 Multispectral Fingerscan Reader (requires PIN) • UCS running on Linux OS • 32MB RAM, 32MB Flash • Ethernet Host connection • 128x64 monochrome LCD • 0-9 numeric keypad w/ Clear, Enter and 8 Custom Function Keys
MCS2111/XX	Accu-Touch Biometric Verification Color Maximus: • Lumidigm 1:1 Multispectral Fingerscan Reader (requires PIN) • UCS running on Linux OS • 32MB RAM, 32MB Flash • Ethernet Host connection • 320x240 transmissive LCD full color display • 0-9 numeric keypad w/ Clear, Enter and 8 Custom Function Keys
MXJ2111/XX	Accu-Touch Biometric Verification Java Maximus: • Lumidigm 1:1 Multispectral Fingerscan Reader (requires PIN) • Java running on Linux OS • 128MB RAM, 128MB Flash • Java license • Ethernet Host connection • 128x64 monochrome LCD • 0-9 numeric keypad w/ Clear, Enter and 8 Custom Function Keys
MXJ2111/XX	Accu-Touch Biometric Verification Java Color Maximus: • Lumidigm 1:1 Multispectral Fingerscan Reader (requires PIN) • Java running on Linux OS • 128MB RAM, 128MB Flash • Java license • Ethernet Host connection • 320x240 transmissive LCD full color display • 0-9 numeric keypad w/ Clear, Enter and 8 Custom Function Keys

Table 1-2 (page 8 of 9)

Table 1-2 Maximus Part Numbers

Part Number	Description
MXS2112/XX	Accu-Touch Biometric Identification Maximus: • Lumidigm 1:N Multispectral Fingerscan Reader (no PIN required) • UCS running on Linux OS • 32MB RAM, 32MB Flash • Ethernet Host connection • 128x64 monochrome LCD • 0-9 numeric keypad w/ Clear, Enter and 8 Custom Function Keys
MXS2112/XX	Accu-Touch Biometric Identification Color Maximus: • Lumidigm 1:N Multispectral Fingerscan Reader (no PIN required) • UCS running on Linux OS • 32MB RAM, 32MB Flash • Ethernet Host connection • 320x240 transmissive LCD full color display • 0-9 numeric keypad w/ Clear, Enter and 8 Custom Function Keys
MXJ2112/XX	Accu-Touch Biometric Identification Java Maximus: • Lumidigm 1:N Multispectral Fingerscan Reader (no PIN required) • Java running on Linux OS • 128MB RAM, 128MB Flash • Java license • Ethernet Host connection • 128x64 monochrome LCD • 0-9 numeric keypad w/ Clear, Enter and 8 Custom Function Keys
MXJ2112/XX	Accu-Touch Biometric Identification Java Color Maximus: • Lumidigm 1:N Multispectral Fingerscan Reader (no PIN required) • Java running on Linux OS • 128MB RAM, 128MB Flash • Java license • Ethernet Host connection • 320x240 transmissive LCD full color display • 0-9 numeric keypad w/ Clear, Enter and 8 Custom Function Keys
Table 1-2 (page 9 of 9)	

Table 1-3 lists the Part Numbers for the Maximus modules.

Table 1-3 Maximus Modules

Part Number	Description
Internal Readers	
97-2111-04	HID Proxpoint
97-2111-03	HID Proxpoint with Biometric Capacitive Fingerscan 1:1 Reader
97-2111-05	HID Proxpoint with Biometric E-Field Fingerscan 1:1 Reader
97-2111-08	HID iClass (Reads card serial number only)
97-9016-02	Bar Code Visible Red
97-9016-03	Bar Code InfraRed
97-9016-04	Magnetic Stripe Track 2
97-9016-05	Magnetic Stripe Track 2 with Infrared
97-2111-01	Cogent Capacitive Fingerscan 1:1 (Not available for AccuTouch)
97-2111-10	Suprema Capacitive Fingerscan 1:1 (Not available for AccuTouch)
97-2111-02	E-Field Fingerscan1:1 (Not available for AccuTouch)
External Readers	
READER/K39	Kantec I/O Proximity
READER/K41	Keri Proximity
READER/K38	AWID Proximity
READERK37	HID-PP
READER/K58	Indala Proximity
DI/DO (Digital In/Digital Out Relay)	
RELAY/K29	120VAC @ 2A - solid state relay
RELAY/K30	240VAC @ 1A - solid state relay
RELAY/K31	60VDC @ 3A - solid state relay
RELAY/K27	Single Form-C Relay 120VAC @ 1A, 24VDC @ 2A
RELAY/K28	Dual Form-C Relay 120VAC @ 1A, 24VDC @ 2A
Power over Ethernet	
POE/K03	Power over Ethernet module (IEEE802.3AF Compliant)
Serial	
COMM/K58	RS232 Serial module
Table 1-3 (page 1 of 2)	

Table 1-3 Maximus Modules

Part Number	Description
Modem	
COMM/K56	56K Modem
COMM/K67	Airtime GSM/GPRS Cellular Field Upgrade Modem kit (Contact your salesperson for data plans)
WiFi	
	Enterprise Version (WPA2/802.11i enterprise-grade security and authentication protocols)
	Non-Enterprise Version (Wireless Standards: IEEE 802.11b; 802.11g)
Battery	
BATTERY/K14	UPS with battery charging kit for up to 1.5 hours of terminal operation
BASE EXT/K06	Base Extension and Power Cover
Table 1-3 (page 2 of 2)	

Table 1-4 lists the Part Numbers for the Maximus accessories.

Table 1-4 Maximus Accessories

Part Number	Description
BASE EXT/K06	Base extension & power cord
97-2111-00	Blank Plate (covers biometric area -not available for AccuTouch)
Memory	
90-1843-02	128/128 Memory Module
Power Supplies	
POWERPACK/K06	Recommended Domestic
POWERPACK/K03	Recommended International (comes with set of international adapter plugs)
BATTERY/K14	UPS with charging kit
39-1000-00	Replacement Back Up Battery
PoE Power Injector (connects to standard Ethernet & Power Pack)	
17-4800-04	Power Injector - Recommended
63-2005-05	Power Injector Cord - Recommended Domestic
Table 1-4 (page 1 of 2)	

Table 1-4 Maximus Accessories

Part Number	Description
63-2005-06	Power Injector Cord - Recommended UK
Remote Bar Code Readers	
9001/03	InfraRed - Weather Resistant - 20' cable
9001/01	Visible Red - Weather Resistant - 20' cable
9001/04	InfraRed - Weather Resistant - 4' cable
9001/02	Visible Red - Weather Resistant - 4' cable
9001/05	Visible Red - Weather Resistant - 30' cable
Scanners	
9000/39	CCD Scanner
Modular Network Cable (8 conductor w/8 pin modular plugs)	
63-2003-00	1 Foot Cable
63-2003-05	2 Foot Cable
63-2003-20	3 Foot Cable
63-2003-03	10 Foot Cable
63-2003-11	25 Foot Cable
63-2003-02	50 Foot Cable
63-2003-08	100 Foot Cable
Cat 5 Ethernet Cable (8 conductor w/8pin modular plugs)	
63-2016-00	Cat 5 Cable 15in 8cond 8-8plug
63-2016-03	Cat 5 Cable 10ft 8cond 8-8plug
63-2016-01	Cat 5 Cable 15ft 8cond 8-8plug
63-2002-11	Telco Cable
Miscellaneous Network Cable Items	
63-9001-02	8 Conductor flat cable, per foot
61-0000-44	Modular Plug 4 position
61-0000-64	Modular Plug 6 position (6 body /4 pins for Modem)
61-5547-10	Modular Plug 6 position (6 body /6 pins)
61-0000-88	Modular Plug 8 position

Table 1-4 (page 2 of 2)

Basic Communication

This sections discusses some basic communications functions of the Maximus.

Ethernet Communication Acknowledgement

Maximus terminals support two-way application acknowledgement for Ethernet communication.

Two-way application acknowledgement (TWAA) ensures both that transactions from the terminal are received by the host and also that transactions from the host are received by the terminal. The acknowledgement (ACK) that is sent by the terminal is also sent by the host.

The host application should send an ATS ACK to the terminal in response to all data messages received from the terminal except the following, which are not acknowledged:

- An ATS ACK received from the terminal
- A KeepAlive message received from the terminal

Should there be a connection failure, the terminal will continue from where it left off upon reconnection. Upon reconnection, the host also continues from where it left off, except when the terminal resets. In this case, a power-on message transmits, which indicates that the process needs to be restarted.

KeepAlives

KeepAlives are scheduled communications between network devices that indicate the network device is still online and active. By default, these communications are sent every 30 seconds. If KeepAlive communications stop, then the device that is no longer sending KeepAlive communications is offline or otherwise unavailable.

A KeepAlive uses the unique ID of the terminal (see *Terminal ID on page 1-5*). You can use the diagnostic window in ATS AccuEngine™ (see the *Accu-Engine Terminal Management Utilities User Guide*), or other communication software, to see KeepAlives.

- In static addressing mode, the KeepAlive is: *ATSnnnnnn***»***S* (the terminal's unique ID with a **»** (record separator) and an S for static mode)
- In dynamic addressing mode, the KeepAlive is: *ATSnnnnnn***»***D* (the terminal's unique ID with a **»** (record separator) and a D for dynamic mode)

DHCP

DHCP (Dynamic Host Configuration Protocol) allows a network DHCP server to set the IP addresses automatically for DHCP clients on the network. If a Maximus terminal is connected to a network that has a DHCP server, you can configure the terminal to its IP address from the DHCP server.

When a terminal configured to use DHCP comes online, it queries the network DHCP server to get assigned its own IP address.

NOTE: If the terminal's IP address lease (an amount of time an address is active) has timed out and addressing is not renewed, the terminal recycles the current settings until a DHCP server is online.

Installation

2

Chapter

About this Chapter

This chapter describes the Maximus installation and provides an overview of component and module locations.

Chapter Contents

This chapter contains the following topics:

This page intentionally left blank.

Installation Guidelines

The standard Maximus is designed to operate indoors. Exposure to outdoor elements, such as rain or snow, voids the manufacturer warranty and may cause damage to the device. Select a location with adequate lighting (away from direct sunlight) and accessibility so employees can operate the terminal safely. The terminal should be mounted on a vibration-free surface.

For more information about environmental requirements, see "Specifications" on page 1-5.

Installation Choices

You must choose:

- How the host computer communicates with the terminal.
- How to supply power to the terminal.

Wiring Distances

The Maximus can communicate with a host computer in these ways:

- 10/100 BASE-T Ethernet (standard)
- RS232 (option)
- Dial-up modem (option)

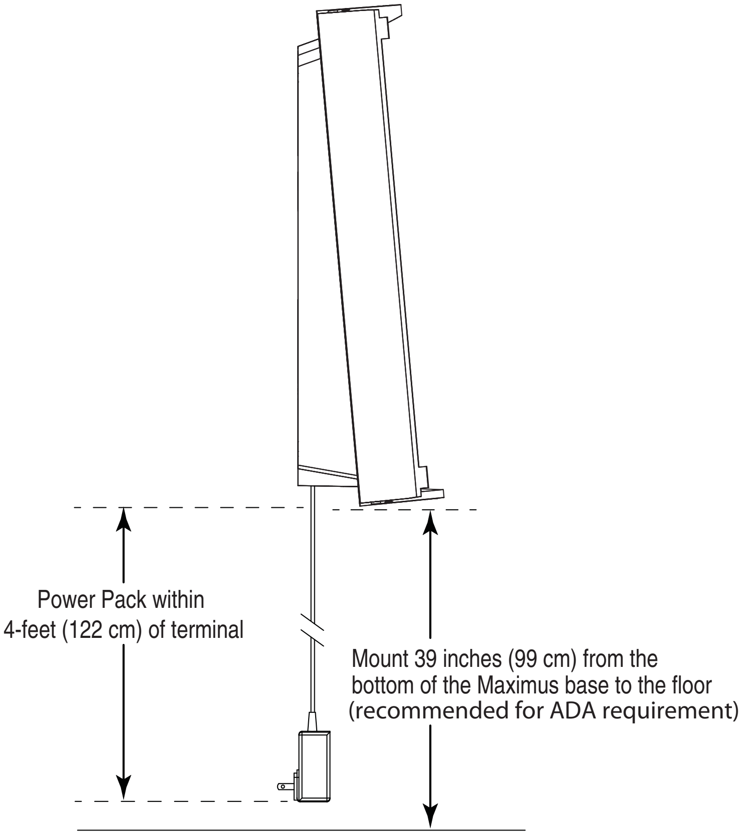
When you have chosen a communication method, run the required wiring from the host computer to the location selected for mounting the terminal. Sections below give more detail for each type of communication. Be sure the distance from the terminal's location to the host computer does not exceed the wire length limitation of the connection type you plan to use. These limits are shown in Table 2-1.

Table 2-1 Wire Length Limitations

Connection Type	Maximum Terminal-to-Host Distance
Ethernet 10/100BASE-T	328 wire-feet (100 meters) from terminal to Ethernet hub or switch
RS232	50 wire-feet
Table 2-1	

If you are using a modem connection, there must be an analog telephone jack available at the terminal's location.

Figure 2-1 Power Pack Location Requirements

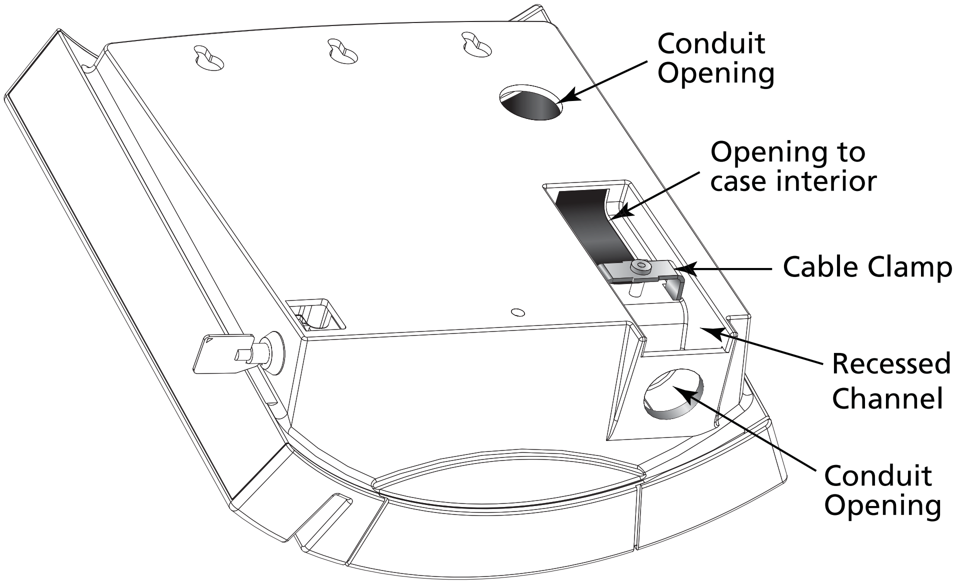

Power Pack within
4-feet (122 cm) of terminal
Mount 39 inches (99 cm) from the
bottom of the Maximus base to the floor
(recommended for ADA requirement)

Terminal Wiring Access

The Maximus provides three access points for routing wires into the terminal: two Conduit Openings (holes) and a recessed channel that leads to the “opening to case interior” and accepts surface wiring (see Figure 2-2). In addition, the Maximus is equipped with a cable clamp that secures surface wiring routed through the recessed channel or fed through the lower conduit opening.

Choose the wiring method best suited to your installation. Run required communication cabling (Ethernet, serial, or telephone line) to the location. If you have wiring for any optional devices such as DIDO, run those wires to the terminal location following all applicable electrical codes.

Figure 2-2 Wiring Access Locations (Rear View of Maximus)



Terminal Installation

This section describes how to wall mount the Maximus terminal and provides the locations of the main components inside.

Opening and Separating the Case

While not necessary, you may find it easier to install the mounting base on the wall if you separate the base from the terminal. Use the following procedure if you wish to separate the mounting base from the terminal:

1. Unlock the terminal with the supplied key (see Figure 2-3 for the chassis lock location).
2. Open the unit by pulling gently on the right-hand edge of the terminal, so it swings open on the hinges (the terminal is hinged to the base on the left edge as you face it).
3. If there are any short jumper cables between the terminal and the base, unplug each jumper from the terminal, making a note of where each one goes so you can reconnect them.
4. The terminal uses a fixed upper hinge-pin and a spring-loaded lower hinge-pin. Raise the spring-loaded lower pin until the terminal can pivot sideways enough to clear the lower pin support (see Figure 2-4).
5. Then, slide the terminal upward to free the upper pin. When the terminal and base are separated, lay the terminal aside in a safe place.

Figure 2-3 Chassis Key Location

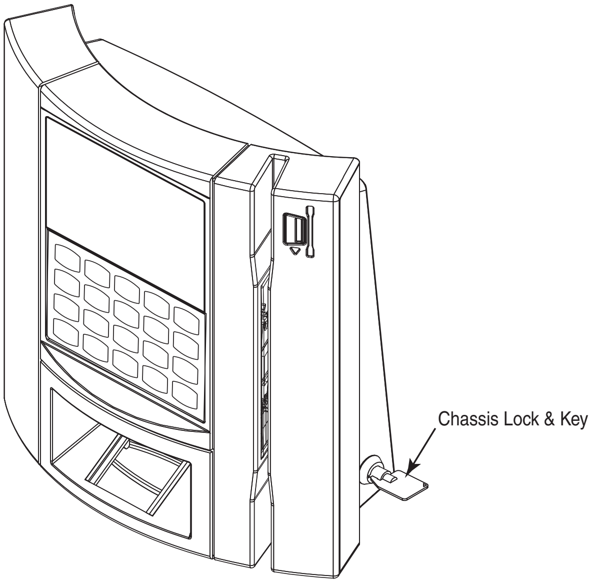
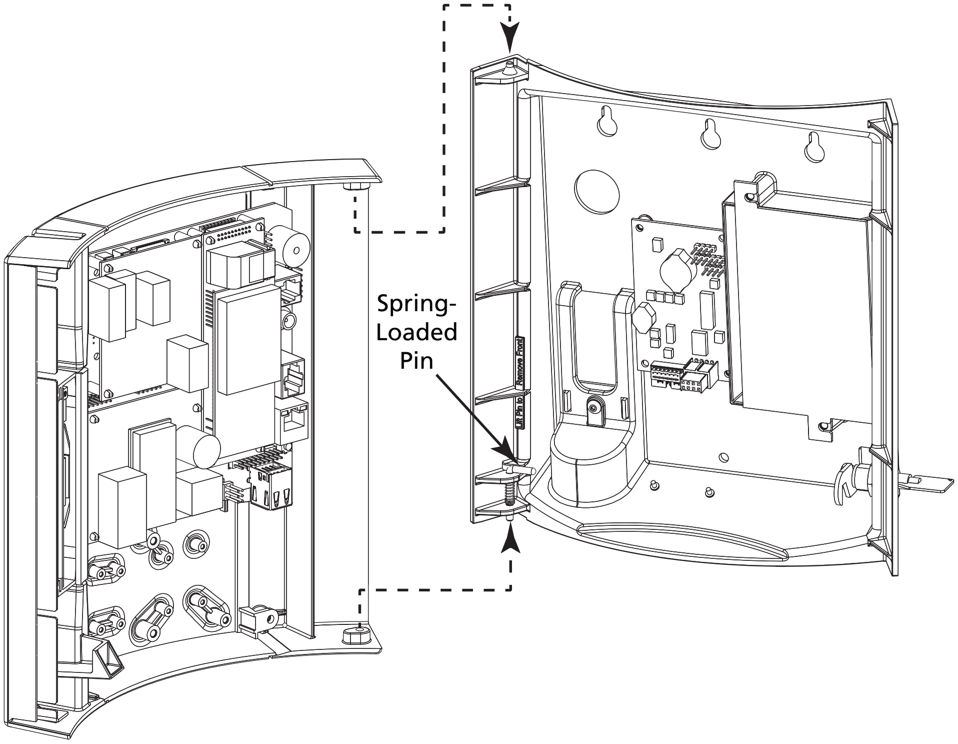


Figure 2-4 Separating the Terminal from the Base

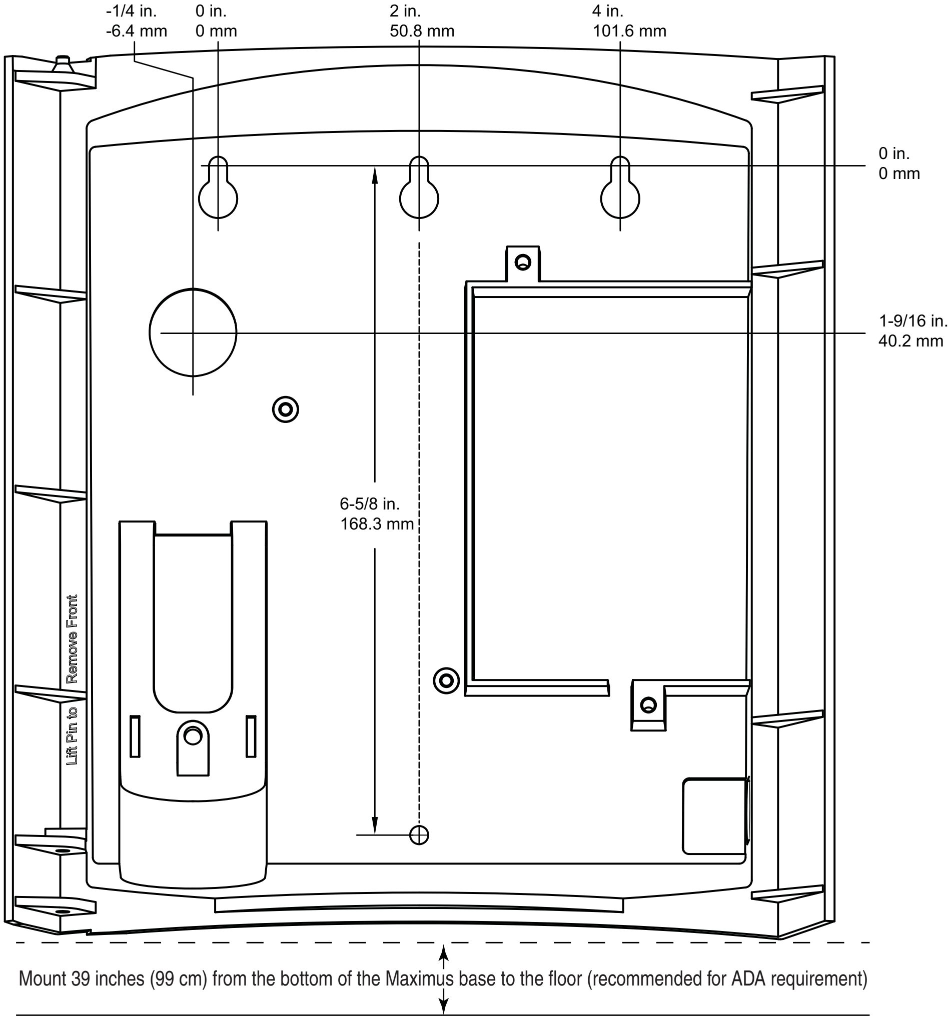


Mounting the Terminal

When you have run the necessary communication wiring to the terminal location and arranged for a power source, you can mount the terminal on the wall.

1. Choose a flat, smooth, interior wall for the terminal's location. You will mount the Maximus using 4mm / #8 pan head screws in four places. Refer to Figure 2-2 on page 2-5 or use the mounting template (Part Number 06-1100-02) to mark the wall prior to any drilling. To meet ADA recommendations for forward reach, position the screw locations / template so the bottom of the mounting base is 39 inches (99cm) above the floor.

Figure 2-5 Mounting Template Dimensions (Not to Scale)



2. Be sure all required wiring is present and any cable clamps properly installed. Follow any applicable wiring codes.
3. Partially install the three upper screws.
4. Lower the mounting base onto the three upper screws then tighten them (refer to Figure 2-6 on page 2-9 or Figure 2-7 on page 2-9 depending on if you separated the terminal or didn't separate the terminal, respectively).
5. Install the bottom screw and tighten until snug.

Figure 2-6 Installing the Mounting Base (with the terminal separated)

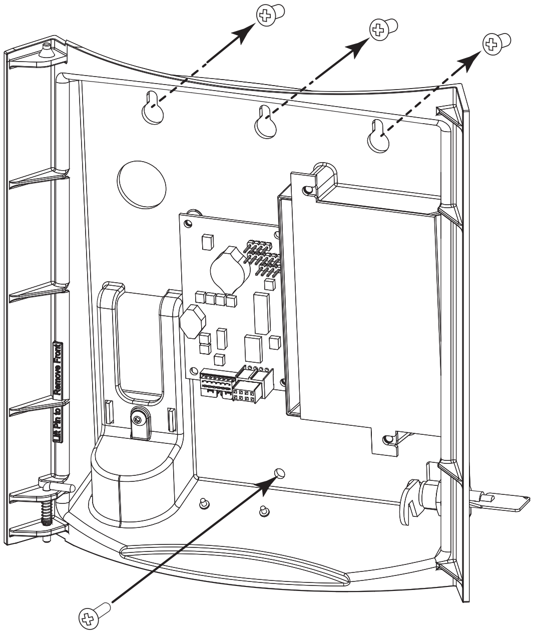
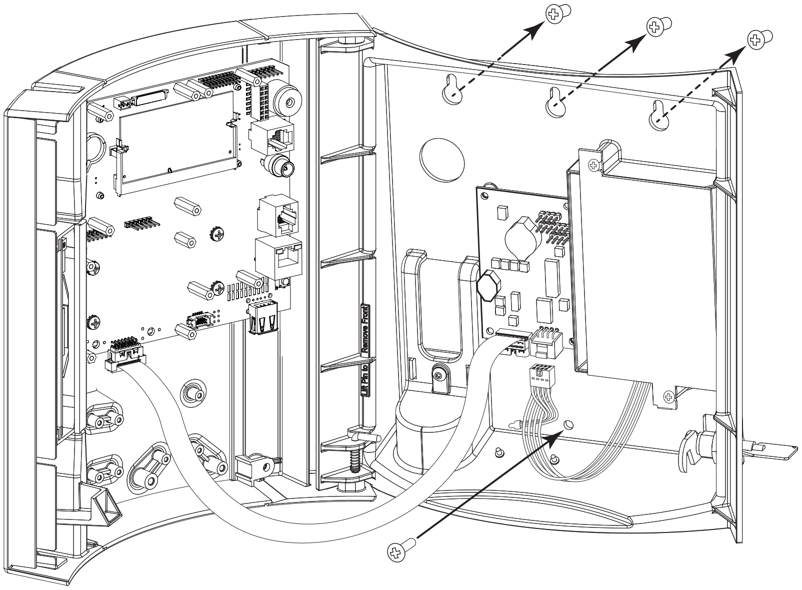

Mounting Screws “Started” on the Wall

Figure 2-7 Wall Mounting the Maximus (terminal not separated)


Mounting Screws “Started” on the Wall

6. If you separated the terminal from the mounting base, reinstall the terminal on the base by reinstalling the terminal's hinge screws or by sliding the fixed hinge pin into its mating top hole, lifting the lower spring-loaded pin, and pivoting the terminal until the pin drops into its mating hole. ("Terminal Wiring Access" on page 2-5).
7. If you unplugged any cables between the terminal and base, reconnect them as they were originally.

Main Components

This section provides the locations of the main components inside the Maximus terminal. Figure 2-8 shows the main components and modules locations with a Power over Ethernet module installed.

NOTE: Power over Ethernet modules are typically not installed with a GSM or Serial module installed. Figure 2-8 and Figure 2-9 illustrate locations only and does not represent functionality or available configurations.

Figure 2-8 Maximus Component Locations (1)

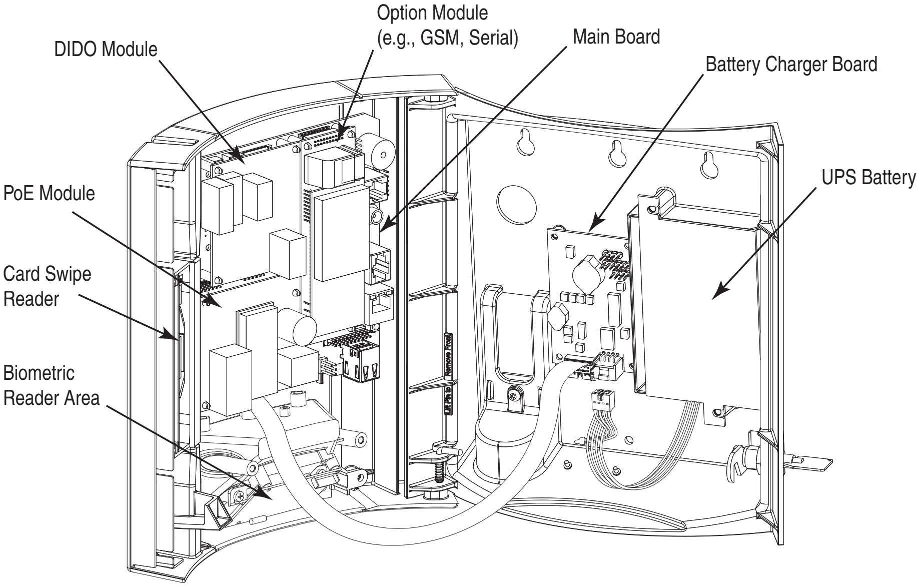
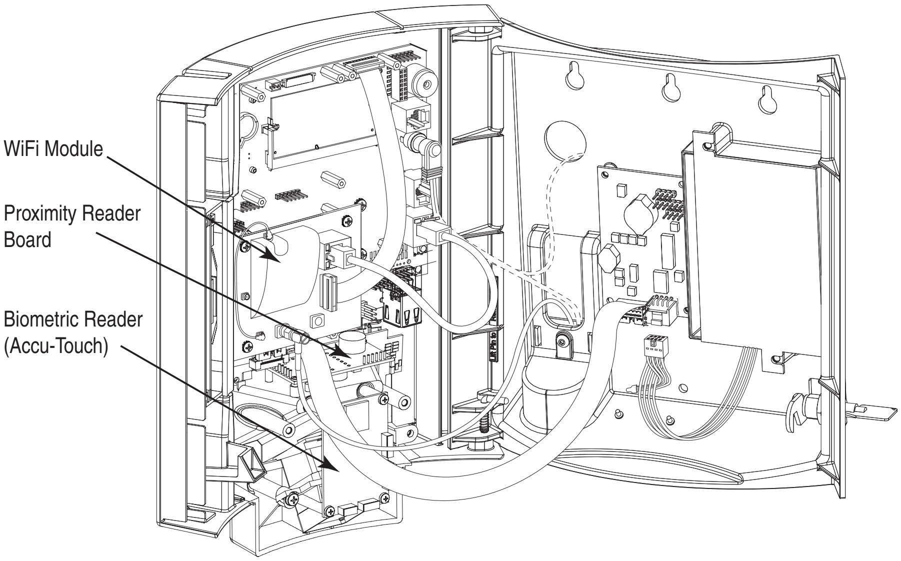


Figure 2-9 shows the main components and modules with a WiFi module and an Accu-Touch Biometric reader installed (the PoE and WiFi module use the same location in the terminal.

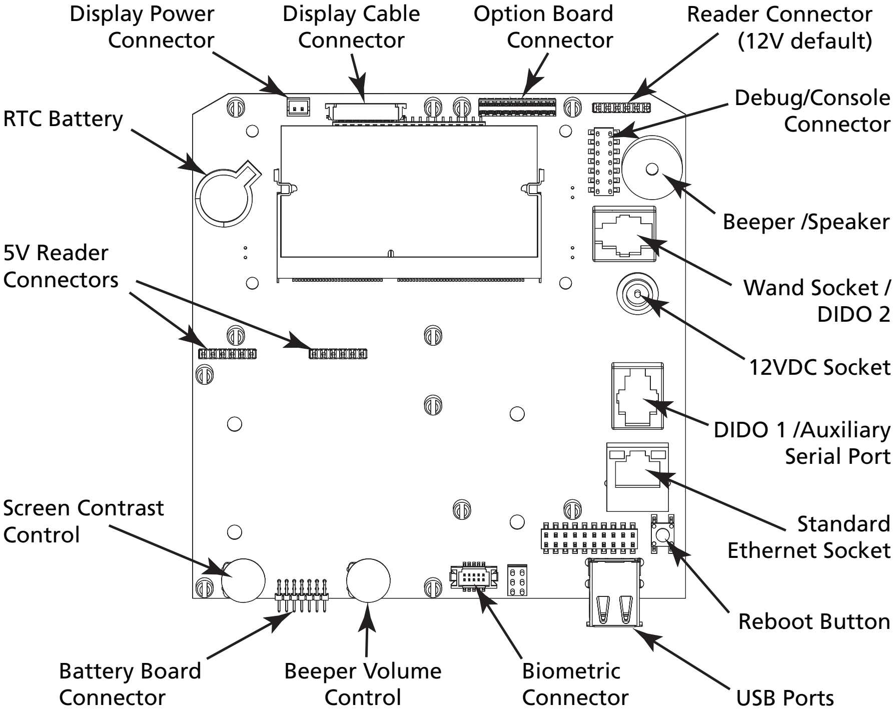
Figure 2-9 Maximus Component Locations (2)



Main Board Components

Figure 2-10 shows the locations of the main components and connectors on the main board.

Figure 2-10 Maximus Main Board Connectors



Connections

This section tells you how to connect the terminal communication and option wiring. The battery backup option, if present, is mounted in the terminal base. Your terminal may not have these options.

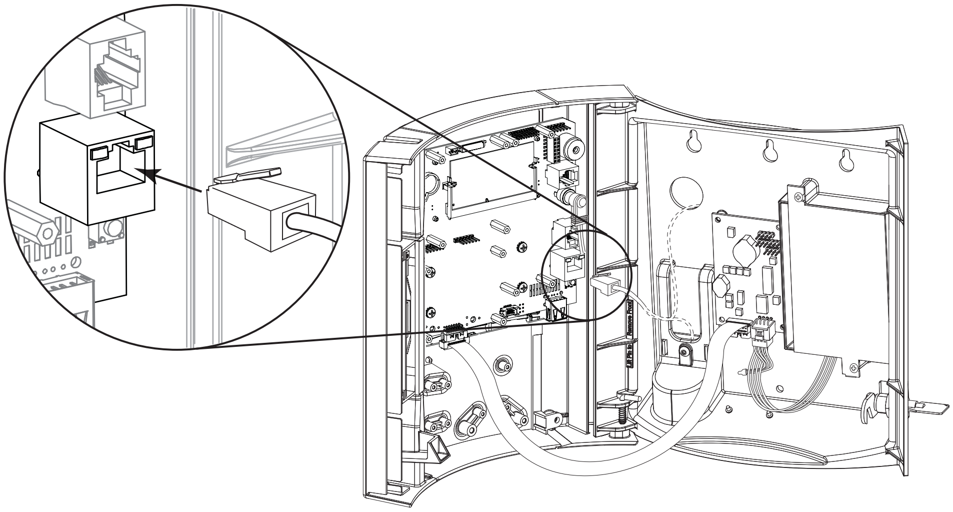
Standard Ethernet Connection

When using an Ethernet connection, the Maximus terminal can be located at any point in a TCP/IP Ethernet 10/100BASE-T network, providing the single segment length from the network hub or switch to the terminal does not exceed 328 wire-feet. A typical topology for the Maximus terminal in an Ethernet 10/100BASE-T network is a star configuration.

For Ethernet communication applications, we recommend using CAT-5 unshielded twisted-pair high-speed data transmission cable with RJ45 plugs wired according to the EIA/TIA 568B standard. One end of the RJ45-terminated cable plugs into the Maximus Ethernet communication port or PoE option card, while the other end plugs into the network hub.

Figure 2-11 shows connecting a standard Ethernet cable into the Ethernet Port on the Maximus.

Figure 2-11 Connecting Standard Ethernet to the Maximus Terminal

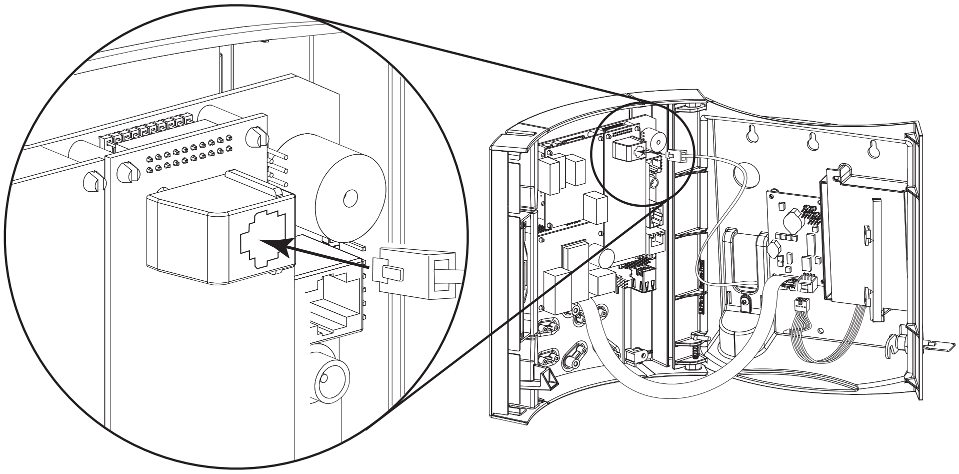


RS232 Connection

The Maximus options include an RS232 serial module with either an RJ11 or RJ45 socket.

ATS recommends using its modular telephone type data cable. This eight conductor shielded flat cable has RJ45 modular plugs on each end. Terminate one end of the cable at the Maximus terminal's serial option card and the other end at the host computer's serial port through an ATS RS232 communication adapter. Be sure to follow all applicable electrical codes when installing the cable.

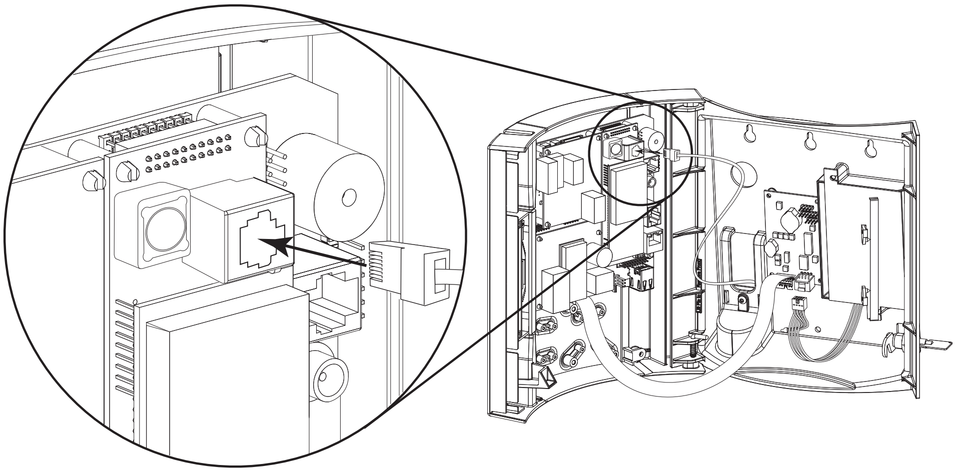
Figure 2-12 Connecting an RS232 Serial Module



56k Modem Connection

If your Maximus is equipped with a 56k Modem Module, plug one end of a standard RJ11 modular phone cable (customer-supplied) into the socket on the module (as shown in Figure 2-13) and the other end into an analog telephone socket. The modem does not support digital telephone lines.

Figure 2-13 Connecting a 56k Modem Module

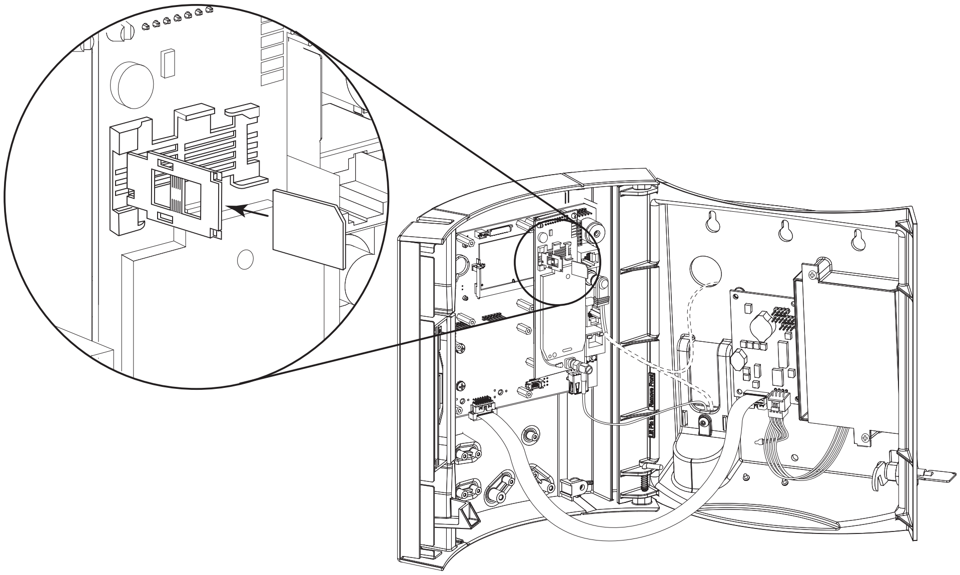


GSM Module

SIM Card Installation

If your Maximus is equipped with a GSM (Cellular) Module, install the SIM card (customer-supplied) into the module as shown in Figure 2-14.

Figure 2-14 Installing a SIM Card in a GSM Module



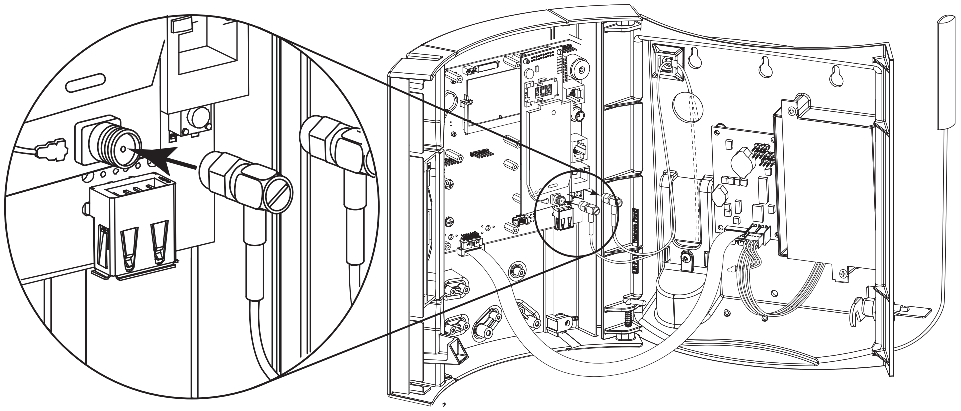
GSM Long Cable Antenna

The optional GSM/GPRS module comes with two antenna. One ships connected to the module and mounted to the outside of the Maximus outer case. A second antenna, equipped with a 5-meter cable (Part Number 17-7003-00), provides flexibility for locations with poor GSM signal reception.

Figure 2-15 shows how to connect/install the 5-meter antenna. Use the following procedure to install the 5-meter antenna:

1. Disconnect the factory installed antenna from the GSM/GPRS module.
2. Route the 5-meter antenna into the Maximus terminal and connect it to the GSM/GPRS module as shown in Figure 2-15.
3. Run the GSM Signal strength function in the Test Mode as described in "GSM Signal Strength" on page 3-57 (for a standard Maximus) or GSM Signal Strength on page 4-32 (for a Color Maximus).
4. Move the antenna to the strongest signal strength and secure it by removing the protective paper on adhesive back on the antenna then attaching the antenna to a wall or other stationary structure.
5. Exit the **GSM Signal Strength** function from **Test Mode**.

Figure 2-15 Installing the 5-Meter Cable Antenna



DIDO Relay Module Connection

The optional DIDO relay modules enable the terminal to control various external devices such as bells, horns, and doors. The modules provide a relay contact closure to activate electronic access entry, solenoids or buzzers. Two input connections provide contact monitoring.

The Maximus supports three types of optional DIDO modules (5 total):

- Solid State Relay DIDO Modules (120 VAC, 240VAC, 60VDC)
- Single Form-C Relay (Mechanical, Dry Contact) DIDO Module
- Dual Form-C Relay (Mechanical, Dry Contact) DIDO Module

DANGER SHOCK

We recommend that a qualified electrician perform relay wiring in accordance with local electrical regulations and best practices.
The minimum size wire that can be used to wire to the relay board is 17 AWG. A 5-amp fuse on the relay board protects it from over-current conditions.

Solid State DIDO Modules

The DO functionality of the modules utilize either a 120 VAC / 2 amp, a 240 VAC / 1 amp, or a 60 VDC, 3 amp solid state relay. A five-position screw down connector serves as the gateway between the Relay Module peripheral controller and the external mechanism. The DI portion of the module is an input-sensing device. Utilizing opto-isolation circuitry the module accepts make/break contacts used as monitoring devices or as input status messages. Figure 2-16 provides a wiring diagram for the 120 and 240 VAC versions of the module:

Figure 2-16 120/240 VAC Solid State DIDO Wiring Diagram

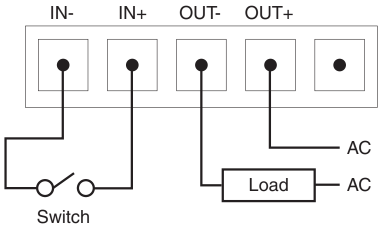
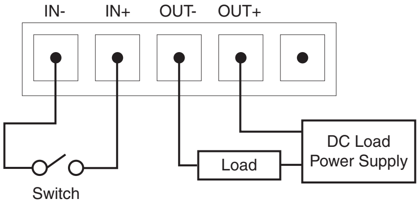


Figure 2-17 provides a wiring diagram for the 60 VDC version of the module:

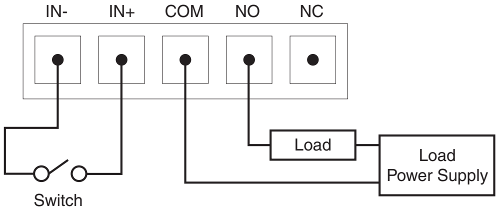
Figure 2-17 60 VDC Solid State DIDO Wiring Diagram



FORM-C DIDO Modules

The DO functionality of the Form "C" Relay Module utilizes an AC (Alternating Current) up to two hundred forty (240) volt, one ampere, Form "C" relay or up to a 24 VDC / 2 amp, Form "C" relay. The DI portion of the module is an input-sensing device. Utilizing opto-isolation circuitry, the module accepts externally generated signal levels such as make/break contacts used as monitoring devices or as input status messages. Figure 2-18 provides a wiring diagram for the Form-C modules (shown wired for Normally Open operation):

Figure 2-18 Form-C DIDO Wiring Diagram



Connecting the Module

The DIDO modules come equipped with Phoenix Contact PCB terminal block(s) to connect wiring to the DIDO module. You may disconnect the terminal block(s) from the module then connect the wiring for the appropriate module as described in the previous section.

Plug the terminal block back into the module as shown in Figure 2-19 (single module) or Figure 2-20 (dual module).

Figure 2-19 Connecting the PCB Block on a Single DIDO Module

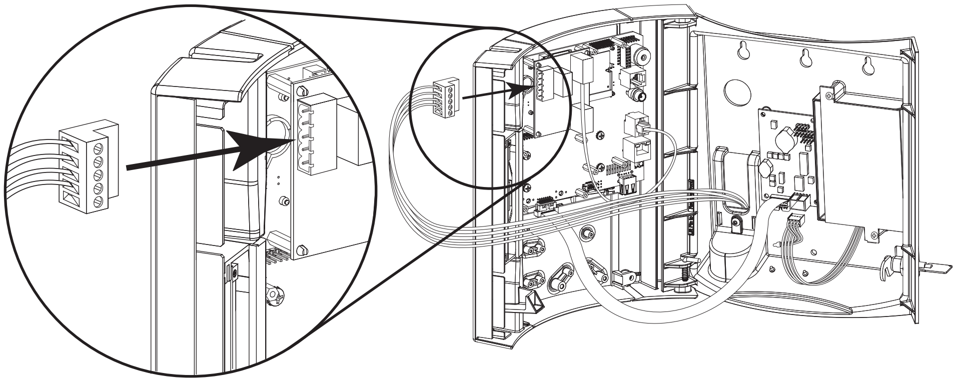
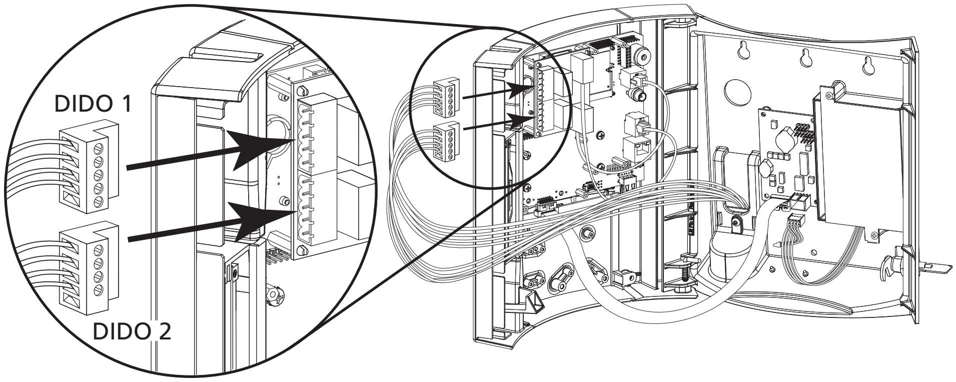


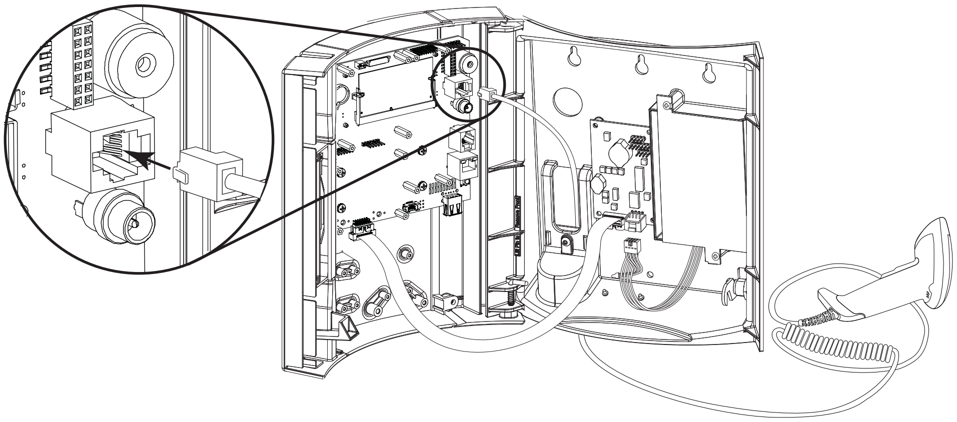
Figure 2-20 Connecting the PCB Blocks on a Dual DIDO Module



Hand-Held CCD Scanner

If you have an optional ATS hand-held CCD scanner (Part Number 9000/39), plug its cable into the Wand Socket on the Maximus Main Board as shown in Figure 2-21.

Figure 2-21 Connecting a Hand-Held CCD Scanner

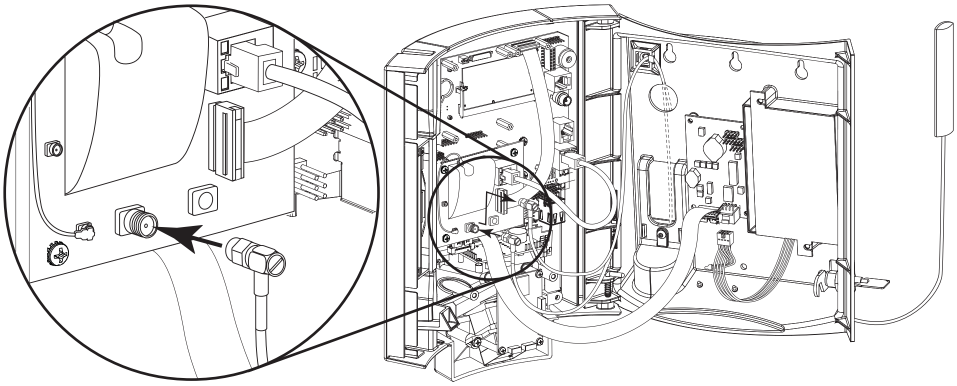


WiFi External Antenna

The optional WiFi module comes with two antenna. One ships connected to the module and mounted to the outside of the Maximus outer case. A second antenna, equipped with a 5-meter cable (Part Number 17-7005-00), provides flexibility for locations with poor WiFi reception. Use the following procedure to install the 5-meter antenna:

1. Disconnect the factory installed antenna from the WiFi module.
2. Route the 5-meter antenna into the Maximus terminal and connect it to the WiFi module as shown in Figure 2-22.
3. Move the antenna to the strongest signal strength and secure it by removing the protective paper on adhesive back on the antenna then attaching the antenna to a wall or other stationary structure.

Figure 2-22 Installing the 5-Meter Cable Antenna



Power Connection

A Maximus requires 12VDC power for operation. There are three ways to power the terminal:

- Power Pack - The ATS power pack plugs into an AC electrical wall outlet and delivers DC power to the 12VDC socket on the terminal main board.The outlet must be within 4 feet of the terminal to accommodate the length of the length of the ATS power pack cord.
- Through-the-network wiring using IEEE 802.3af-compliant power over Ethernet (requires installation of PoE option and PoE-enabled network). For more information, see "Power over Ethernet" on page 2-19.
- UPS Battery – The optional UPS battery backup system provides power if there is an interruption in power from the wall outlet/Power Pack or PoE.

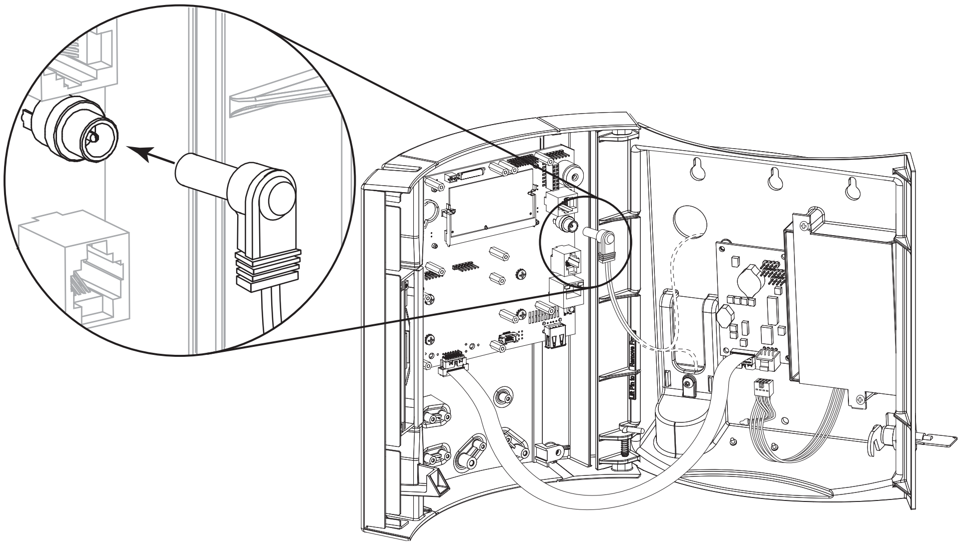
Choose the power source that is best suited to your installation.

Power Pack

When using a power pack, terminal power is supplied by plugging the output cable from an ATS 12VDC power pack directly into the DC Power connector on the back of the terminal. Ensure that a conventional 120VAC wall outlet (220VAC in Europe and other areas, check local electrical code requirements) is available to accept the power pack.

The power pack can be plugged into a wall outlet within four feet (1.2m) of the terminal's location and the cord from the power pack plugged into the back of the terminal.

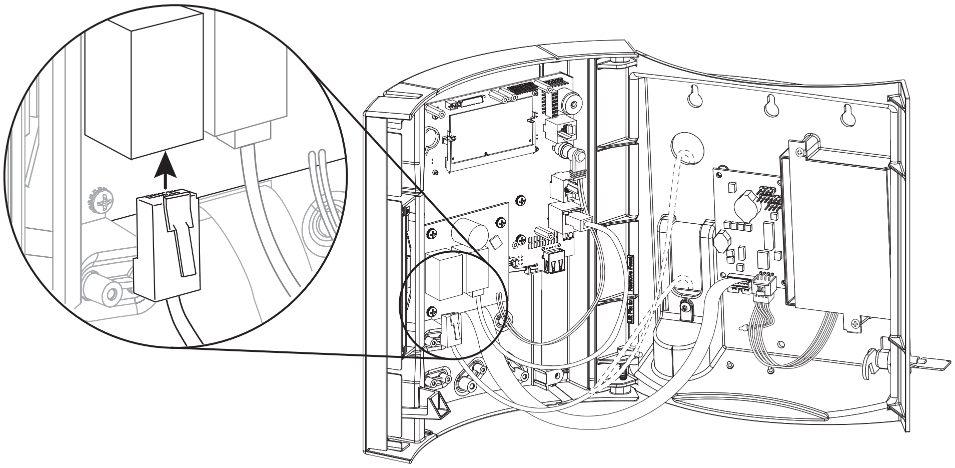
Figure 2-23 Connecting the Power Pack to the 12VDC Socket



Power over Ethernet

If you are planning to use Ethernet communication, the Maximus can receive its power through a network that supports IEEE 802.3af power over Ethernet (PoE). The Maximus must have the PoE option installed. PoE does away with the need for a separate power supply and power wiring. The Maximus supports both end-span and mid-span PoE configurations.

Figure 2-24 Connecting the PoE Module to Powered Ethernet



Connecting the UPS Battery

Maximus terminals can be equipped with an optional UPS battery system that supplies power to the terminal in the event of an electrical power outage.

ATS disconnects the UPS battery pack prior to shipping to prevent the battery pack from discharging in case of extended storage periods.

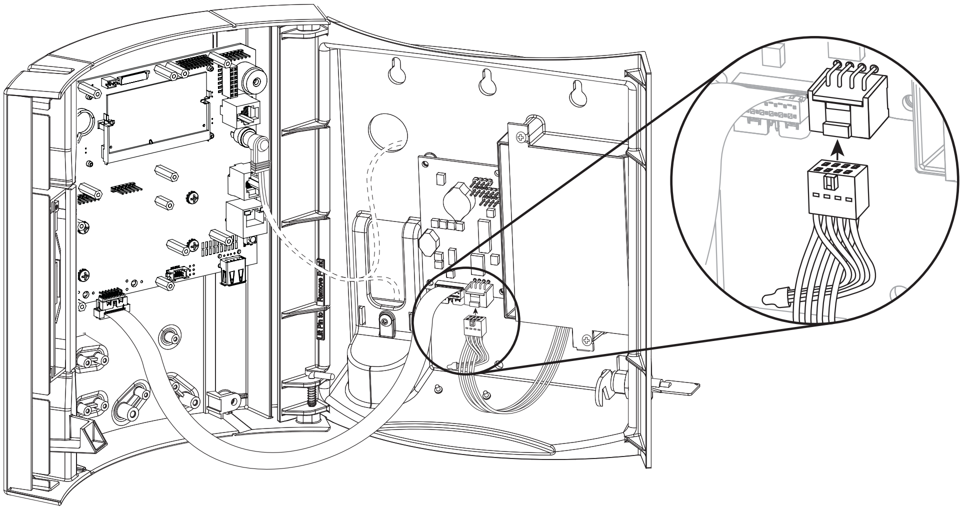
NOTE: If the battery backup option is installed, the terminal operates for approximately 1.5 hours after the primary voltage source is lost. After this, the terminal turns off. When the terminal is in battery backup mode, the yellow low-power indicator LED is lit by default.

The battery option includes a charger board, which is a circuit board that installs in the terminal case and electrically connects the battery with the terminal's main board. See the documentation included with the charger board for installation instructions.

- A ribbon cable attaches J2 on the charger board to J9 on the Global Series main board.
- A cable connects the battery to J3 on the charger board.

After providing power to the Maximus terminal you may connect the battery pack. Connect the UPS Battery plug to the battery charger board as shown in Figure 2-25 (If the power-over-Ethernet (PoE) option is present, the battery backup connector is under the PoE board).

Figure 2-25 Connecting the Battery Pack



The charger board has an LED, D3. The LED has three states: blinking, lit steadily on, and off.

- Blinking – Indicates the battery is being fast charged. It takes about seven hours to completely charge a fully drained battery.
- Steady – If the LED is lit steadily on:
    - The battery is fully charged
    - The battery is too discharged to use fast charge, and a trickle charge is being applied before charging can switch to fast charge
    - The temperature is too high or too low to permit charging
- Off – The LED is off when the terminal is using battery power. The LED only blinks or lights steadily when supplied with AC power.

This page intentionally left blank.

Monochrome Terminals

3

Chapter

About this Chapter

This section tells you how to use the monochrome Maximus menus to set up your monochrome terminal. (See Chapter 4, "Color Terminals" to set up a color Maximus).

NOTE: If you have a Accu-Engine Serial terminal configured for Java programming, see the *Advanced Development Manual for Accu-Time Terminals* for additional information.

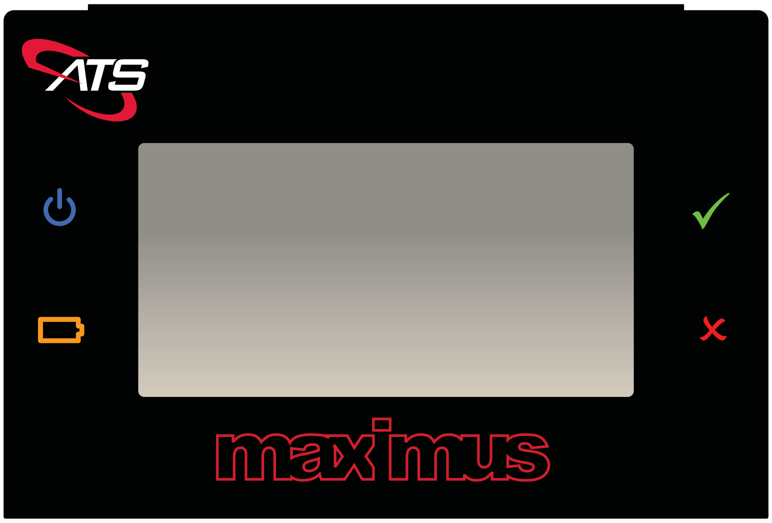
Chapter Contents

This chapter contains the following topics:

Monochrome Display

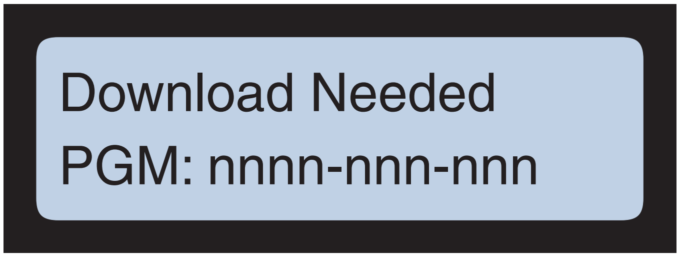
While the power and physical characteristics of a monochrome and color Maximus are the same, their setup menus are different. You can differentiate between the monochrome and color Maximus without turning on the terminal. The monochrome Maximus lens has a much smaller window/LCD display than the color lens. Figure 3-1 shows the color Maximus lens (see Figure 4-1 on page 4-3 for an illustration of the color lens).

Figure 3-1 Monochrome Maximus Lens



Power Up

If the terminal does not have an application saved the message **Download Needed** appears at power-up or after a re-boot showing that the terminal is ready to accept (needs) a program download from the host.



Download Needed
PGM: nnnn-nnn-nnn

The numeric value after the Program prompt (**PGM:**), *nnnn-nnn-nnn*, shows the terminal type, Universal Command Set (UCS) Version, and the no-longer applicable number of boards (N/A) in the terminal as follows:

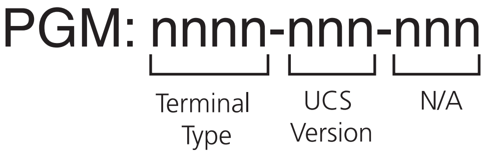


Table 3-1 lists the terminal type codes and the corresponding terminal descriptions.

Table 3-1 Terminal Type Codes

Code	Terminal Type Description
6100	Maximus, non-Java, UCS
6101	Maximus Java
6103	Maximus Python (Mono)
6150	Color Maximus, non-Java, UCS
6151	Color Maximus, Java, UCS
6155	Color Maximus, UCS with XML
6160	Maximus NEMA, mono, UCS
6161	Maximus NEMA, mono, Java
6163	Maximus NEMA, mono, Python

Table 3-1

Initial Setup

To enter configuration mode, press and hold both the **clear** and **enter** keys simultaneously for about five seconds. If the terminal prompts you to enter a password, type in the password using the numeric keys then press the **enter** key. The Initial Setup parameters appear starting with **Setup Host IP**.

NOTE: At any point in the configuration menus you can press and hold both the **clear** and **enter** keys simultaneously to return to the start of the "Initial Setup Parameters" on page 3-7.

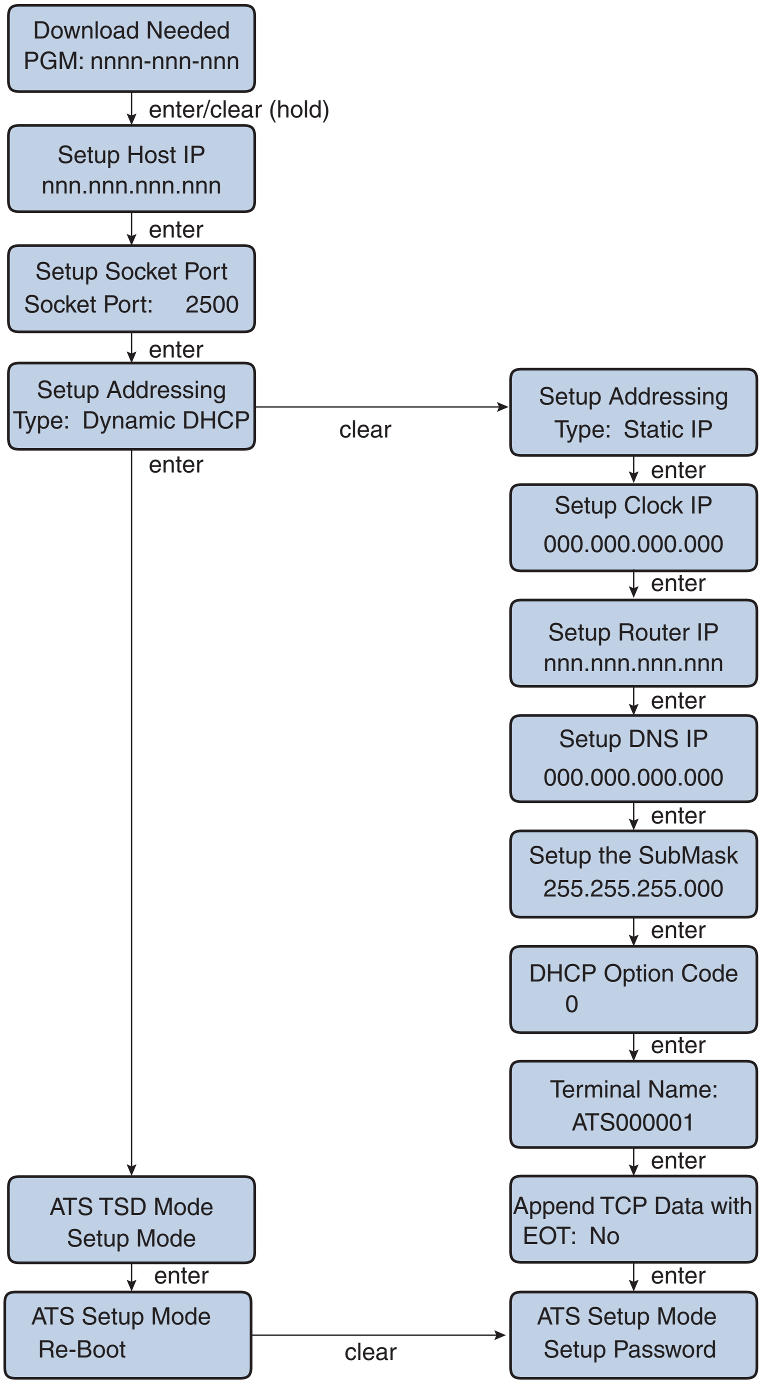
Initial Setup Menu Navigation

The terminal will display the saved or default values for the terminal IP connectivity options. In general, press the **enter** key to accept the displayed value and go to the next option or press the **clear** key to change the value.

NOTE: If you type an invalid IP, subnet mask, or other value, the terminal reports the error and returns to the previous value (the default value or the previously saved value).

Figure 3-2 provides a flow-chart of the Initial Setup Menu structure.

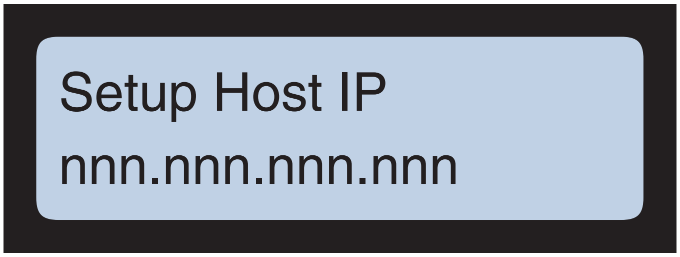
Figure 3-2 Initial Setup Menu Structure Flow Chart



Initial Setup Parameters

To enter the initial setup menu press the **clear** and **enter** keys simultaneously for 5-seconds (maximum). Enter a password if prompted.

1. The terminal displays the default (**192.168.001.100**) or saved value for the Host that provides communications to the terminal.



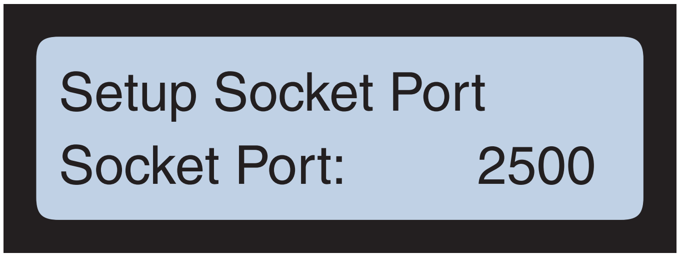
Setup Host IP
nnn.nnn.nnn.nnn

Press the **enter** key to accept the displayed IP address and continue to the next parameter or press the **clear** key to change the host IP address.

If you pressed the **clear** key use the numeric keys to type in the IP address of the host then press the **enter** key to save the new IP address.

If you type an invalid IP address, the terminal displays **Bad IP Address** and returns you to the saved/default value. Press the **clear** key again to correct the address then press the **enter** key to save it.

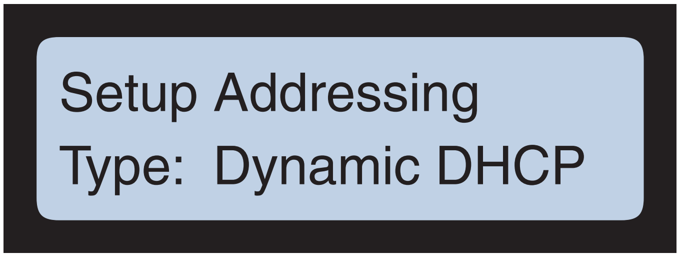
2. Next the terminal displays the default/saved socket port number used by the terminal. The default value is **2500**. Press the **enter** key to accept the displayed port number or press the **clear** key to change it using the numeric keys. When finished press the **enter** key to save the socket port number and continue to the next parameter.



Setup Socket Port
Socket Port: 2500

If you type an invalid socket port number the terminal displays **Invalid Socket Port**. and returns you to the saved/default value. Press the **clear** key again to correct the port number then press the **enter** key to save it.

3. Next the terminal displays the default/saved addressing mode for the terminal. The default value is **Dynamic DHCP**. In DHCP mode the terminal receives its IP address from the connected DHCP server (therefore the terminal IP address may periodically change).

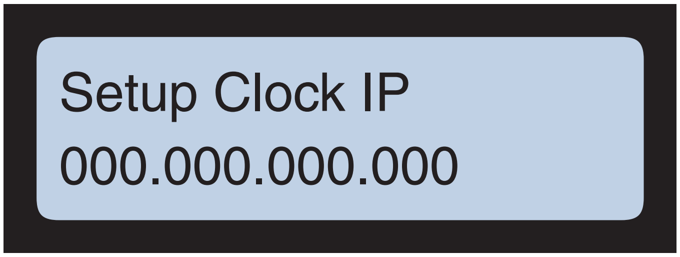


Setup Addressing
Type: Dynamic DHCP

Press the **enter** key to accept DHCP mode and continue or press the **clear** key to toggle the display between the **Static IP** and **Dynamic DHCP** selections.
If the terminal was already in the displayed mode (**Dynamic DHCP** or **Static IP**) and you pressed the **enter** key without changing it, the terminal enters the ATS TSD Mode. Proceed to "ATS TSD Mode" on page 3-13).

- The **Static IP** selection enables you to set the terminal to a permanent IP address.
- When the terminal displays the desired option (**Dynamic DHCP** or **Static IP**) press the **enter** key to save the selection and continue to the next parameter.
- If you changed to the **Static IP** option the terminal displays the static IP addressing parameters starting with **Setup Clock IP**.
- If the terminal is set to **Static IP** (and rebooted) the terminal displays **Static IP** for the **Type**.
  You can access the static IP parameters by pressing the **clear** key, toggling the **Static IP** and **Dynamic DHCP** options and re-saving the **Static IP** option.

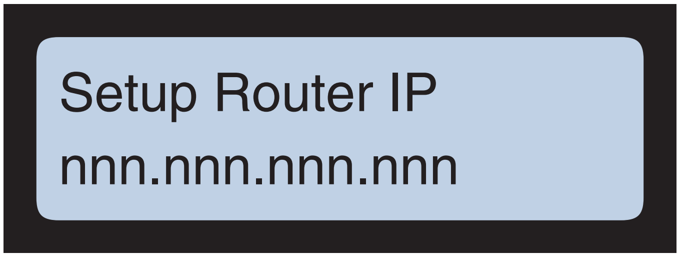
4. The **Setup Clock IP** parameter enables you to change the static IP address for the terminal. Press the **clear** key then use the numeric keys to change the terminal IP address. Press the **enter** key to save the new address and continue.



Setup Clock IP
000.000.000.000

If you type an invalid IP address, the terminal displays **Bad IP Address**.
Press the **clear** key again, correct the IP address then press the **enter** key to continue.

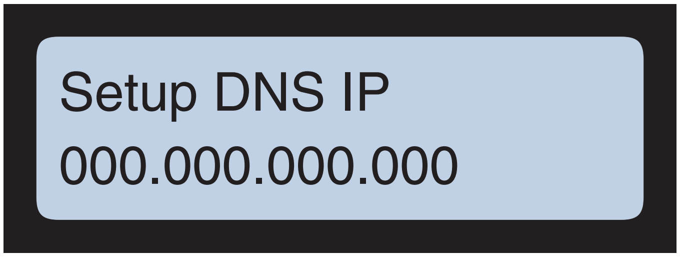
5. Next the terminal displays the **Setup Router IP** (Gateway IP address) parameter. Press the **enter** key to accept the displayed address or press the **clear** key then use the numeric keys to change the address. Press the **enter** key to save the new Gateway IP address when finished.



Setup Router IP
nnn.nnn.nnn.nnn

If you type an invalid IP address, the terminal displays **Bad IP Address**. Press the **clear** key again, correct the IP address then press the **enter** key to continue.

6. Next the terminal displays the **Setup DNS IP** parameter.

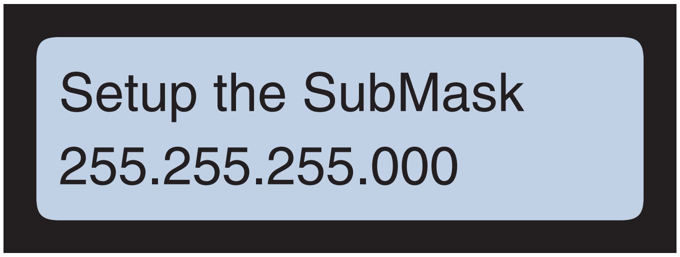


Setup DNS IP
000.000.000.000

Press the **enter** key to accept the displayed IP address for the DNS (Domain Name System) server or press the **clear** key then use the numeric keys to change the address. Press the **enter** key to save the new address and continue.

If you type an invalid IP address, the terminal displays **Bad IP Address**. Press the **clear** key again, correct the IP address then press the **enter** key to continue.

7. After saving the DNS server IP address the terminal displays the **Setup the Submask** parameter (the default subnet mask value is **255.255.255.000**).

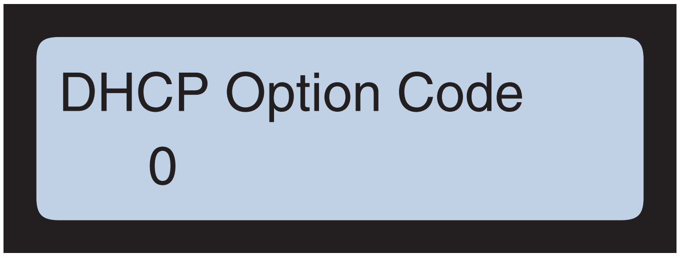


Setup the SubMask
255.255.255.000

Press the **enter** key to accept the displayed subnet mask value and continue or press the **clear** key then use the numeric keys to change the value. Press the **enter** key to save the new subnet mask to continue.

If you type an invalid subnet mask value, the terminal displays **Bad IP Address**. Press the **clear** key again, correct the value then press the **enter** key to continue.

8. Next the terminal displays **DHCP Option Code** setting. The default value is **0** (zero) which is “Pad, set by Protocol”.

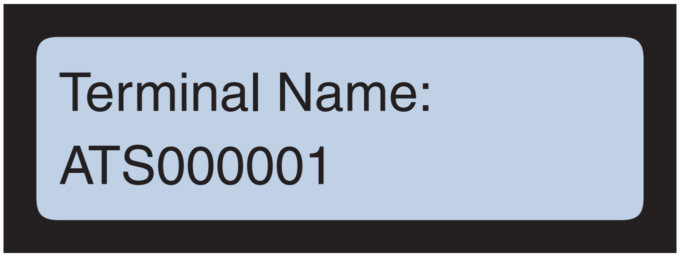


DHCP Option Code
0

Press the **enter** key to accept the displayed **DHCP Option Code** or press the **clear** key then use the numeric keys to change the code. Press the **enter** key to save the new code and continue.

If you type an invalid code, the terminal displays **Out of Range**.
Press the **clear** key again, correct the code, then press the **enter** key to continue.

9. Next the terminal displays the **Terminal Name** parameter that enables you to set a unique up-to-20 character administrative name for the terminal. The default name is "ATS" plus the last 6-digits of the terminal MAC address (e.g., **ATS000001**).



Terminal Name:
ATS000001

NOTE: Applications such as Accu-Engine require "ATS" as the first three characters of the Terminal Name. If not, Accu-Engine will only display the terminal IP address (that can change with DHCP enabled).

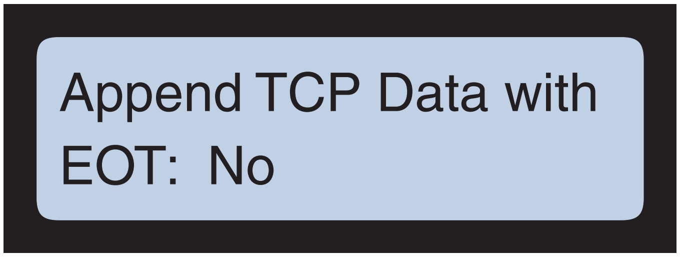
NOTE: Firmware Versions prior to 2.05.11(X) do not save any changes to the Terminal Name. If you make any changes the terminal reverts to the default Terminal Name after a re-boot.

Press the **enter** key to accept the displayed name or press the **clear** key then use the numeric keys and the **F2** to change the name. The F2 key toggles the active character (most recently typed) as listed in Table 3-2.
The **F1** key repeats the previous character and the **clear** key deletes the active (most recently typed) character.
When you are finished, press the **enter** key to save the new name and continue.

Table 3-2 Terminal Name Key to Character Mapping

Numeric Terminal Key	Toggling Characters (F2 Key)
0	0 (zero), Period (.), Space (_), Hyphen (-)
F1	A, B, C
F2	2, D, E, F
3	3, G, H, I
4	4, J, K, L
5	5, M, N, O
6	6, P, Q, R
7	7, S, T, U
8	8, V, W, X
9	9, Y, Z, Comma (,)
Table 3-2	

10. Next the terminal displays the **Append TCP Data with EOT** parameter (the default is **No**).



Append TCP Data with
EOT: No

Press the **enter** key to accept the displayed selection (**Yes** or **No**) or press the **clear** key to toggle between **Yes** and **No** for support of end-of-transmission (EOT) data. If you choose **Yes**, the terminal appends an ASCII EOT character (04_{16}) to each transaction record sent to the host. Press the **enter** key when the terminal displays the desired selection to save it and continue.

CAUTION

*Set **Append TCP Data with EOT** to **No** unless your communication software or networking software specifically support EOT (End Of Transmission).*
*If you set this to **Yes** and EOT is unsupported, the terminal could behave unpredictably, including not responding to input.*

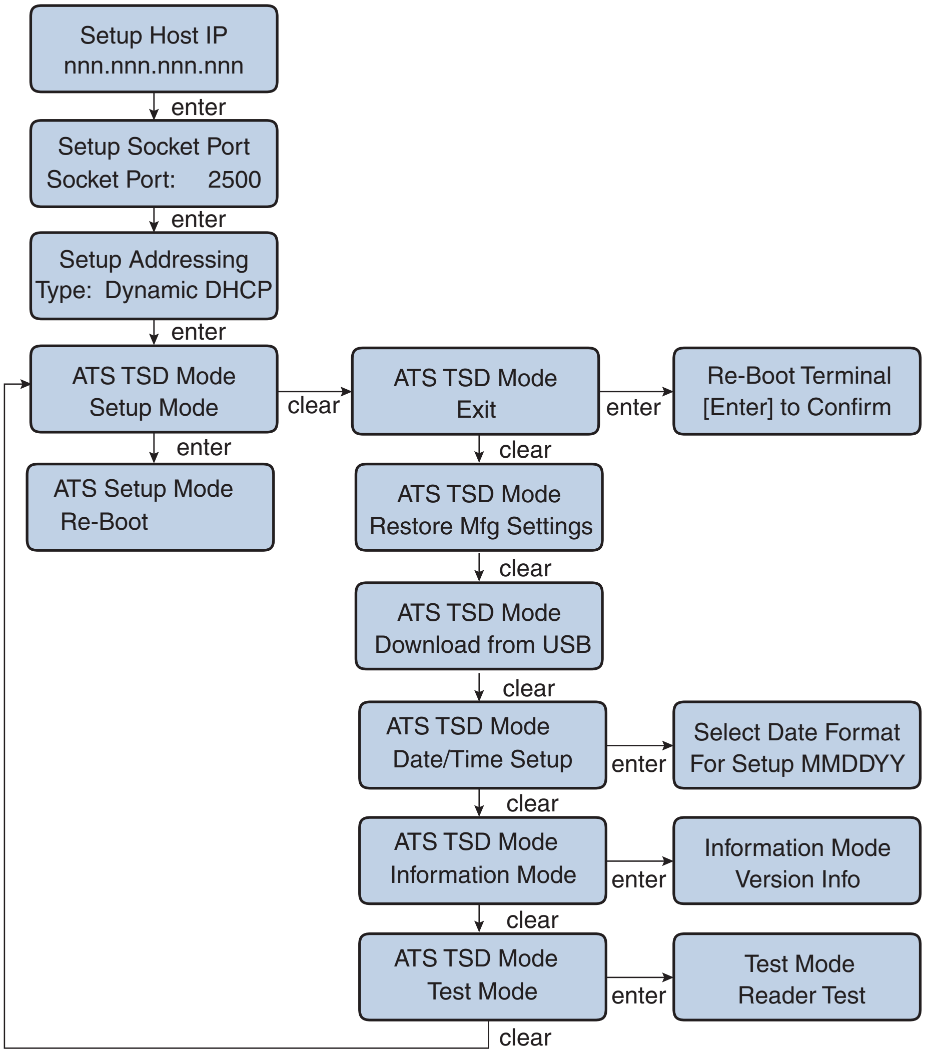
ATS TSD Mode

Maximus terminals have a built-in Test, Setup, and Diagnostics mode (TSD mode) that enables you to configure the terminal operating parameters, perform diagnostic self-tests, and access version information.

NOTE: You can enable password protection so only authorized persons can enter TSD mode. See "Setup Password" on page 3-17 for details.

Figure 3-3 provides a flow chart of the **ATS TSD Mode** menu navigation.

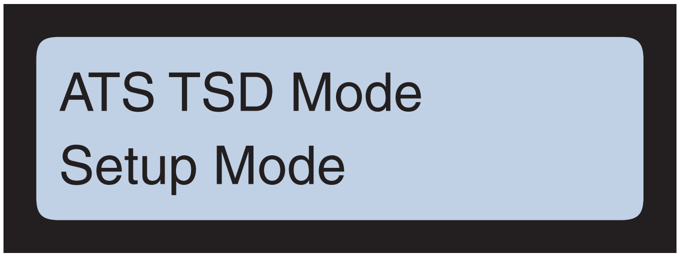
Figure 3-3 ATS TSD Mode Navigation Flow Chart



Using the TSD Mode

Once in the **ATS TSD Mode** menu you can navigate and make selections as follows:

- Press the **clear** key to cycle through the **ATS TSD Mode** menu items.
- Press the **enter** key to select the displayed item.



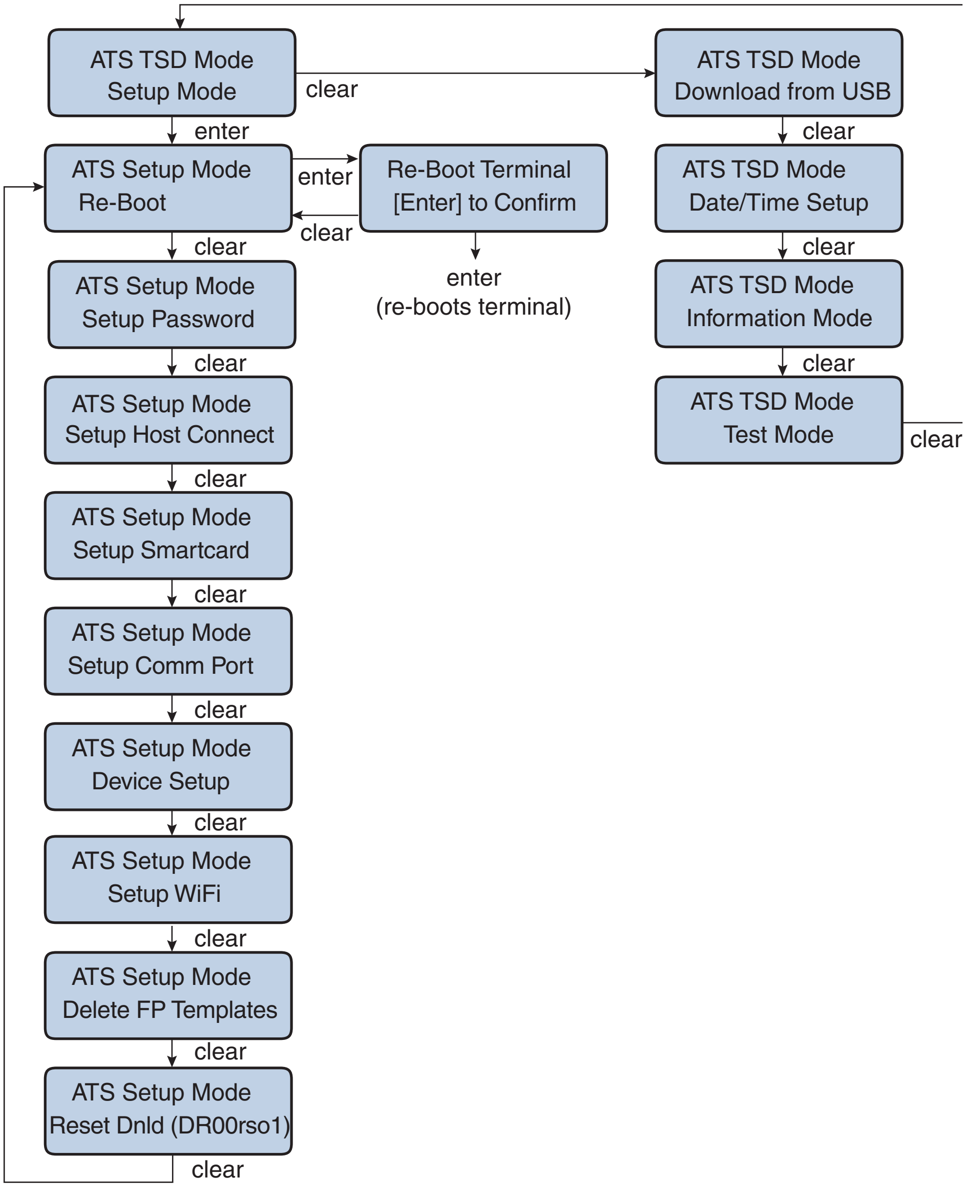
ATS TSD Mode
Setup Mode

1. Press the **clear** key in the **ATS TSD Mode** menu to navigate between the following items:
   - **Setup Mode** – See "Setup Mode Parameters" on page 3-16.
   - **Exit** – Select Exit at the TSD Mode screen to access Setup Mode (see "Setup Mode Parameters" on page 3-16).
   - **Restore Mfg Settings** - This function is reserved for specific applications. In typical Maximus configurations selecting the **Restore Factory Settings** command results in the “**Unable to Restore Settings”** response.
   - **Download from USB** – See "Download from USB" on page 3-38.
   - **Date/Time Setup** – See "Date/Time Setup" on page 3-39.
   - **Information Mode** – See "Information Mode" on page 3-41.
   - **Test Mode**– See "Test Mode" on page 3-46.
2. Press the **enter** key to select the currently displayed item.
   - If you select **Setup Mode** or **Exit** the **Re-Boot** prompt appears. See "ATS Setup Mode" on page 3-15 or "Re-Boot" on page 3-16.
   - If you select **Download from USB** the terminal begins the download operation. See Appendix B, "Using USB".
   - If you select **Date/Time Setup** the **Select Date Format** prompt appears. See "Date/Time Setup" on page 3-39.
   - If you select **Information Mode** the **Version Info** prompt appears. See "Information Mode" on page 3-41.
   - If you select **Test Mode** the **Reader Test** prompt appears. See "Test Mode" on page 3-46.

ATS Setup Mode

The **ATS Setup Mode** enables you to setup connected/installed devices, a password, and manage downloads. Figure 3-4 provides a flow chart of the **ATS Setup Mode** menu items.

Figure 3-4 ATS Setup Mode Flow Chart



Setup Mode Parameters

Setup Mode provides the following parameters:

- "Re-Boot" on page 3-16
- "Setup Password" on page 3-17
- "Setup Host Connect" on page 3-18
- "Setup Smartcard" on page 3-27
- "Setup Comm Port" on page 3-28
- "Device Setup" on page 3-29
- "Setup WiFi" on page 3-30
- "Reset Dnld" on page 3-37
- "Download from USB" on page 3-38
- "Date/Time Setup" on page 3-39

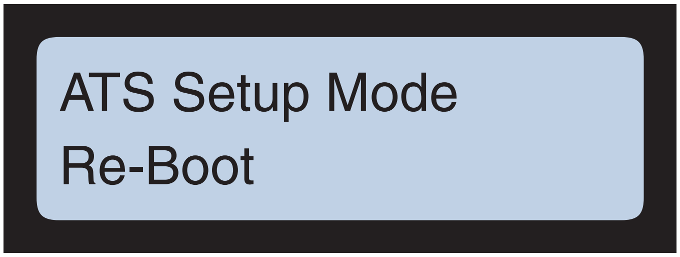
Re-Boot

Re-booting the terminal actives any changes made to the setup parameters. The terminal prompts you to re-boot each time you enter **Setup Mode**.

NOTE: Press the **clear** key at the **Re-Boot** prompt to enter **Setup Mode**. Rebooting is the only way to exit **Setup Mode** (though you can return to the start of the Initial setup menu by holding down the **clear** and **enter** keys).

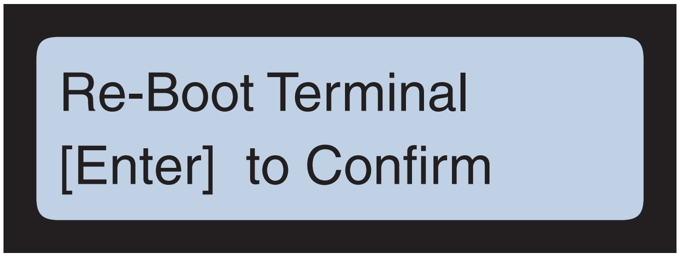
NOTE: Rebooting saves your changes and restarts the terminal. If you made no changes, then rebooting only restarts the terminal.

1. When you enter **Setup Mode** the terminal displays the **Re-Boot** prompt. Press the **enter** key to proceed with the re-boot or press the **clear** key to bypass **Re-Boot** and continue to the **Setup Password** parameter (described on page 3-17).



ATS Setup Mode
Re-Boot

2. If you pressed the **enter** key at the **Re-Boot** prompt the terminal prompts you to confirm the re-boot. Press the **enter** key to confirm and re-boot the terminal or press the clear key to return to the **Re-Boot** prompt.

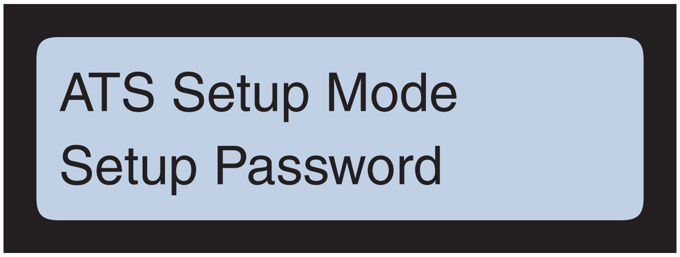


Re-Boot Terminal
[Enter] to Confirm

Setup Password

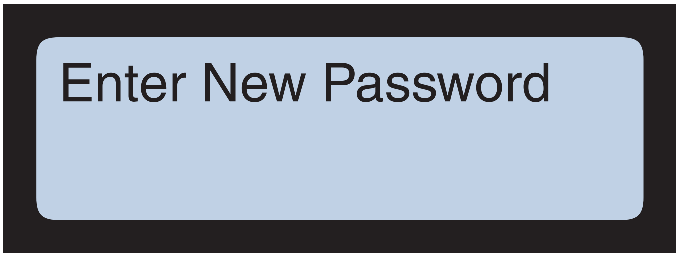
The **Setup Password** parameter enables you to create a password to restrict access to the terminal parameters (e.g., initial setup, TSD Mode, Setup Mode).

1. After you press the **clear** key at the **Re-Boot** prompt (page 3-16) the terminal displays the **Setup Password** parameter. Press the clear key to continue to the **Setup Host Connection** (page 3-18) or press the enter key to set a (new) password.



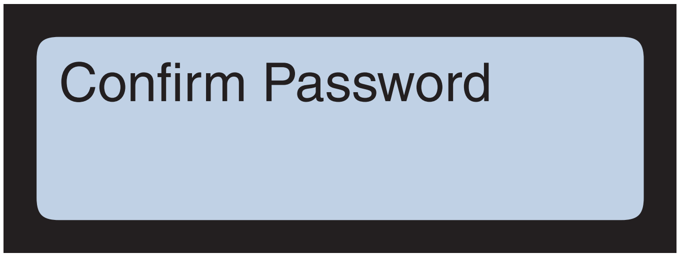
ATS Setup Mode
Setup Password

2. If you pressed the **enter** key the terminal displays the **Enter New Password** prompt. Use the numeric keys to enter a new, up to 7-digit, password for the terminal then press the **enter** key.



Enter New Password

3. The terminal now displays the **Confirm Password** prompt. Re-type the password from the previous step then press the **enter** key.



Confirm Password

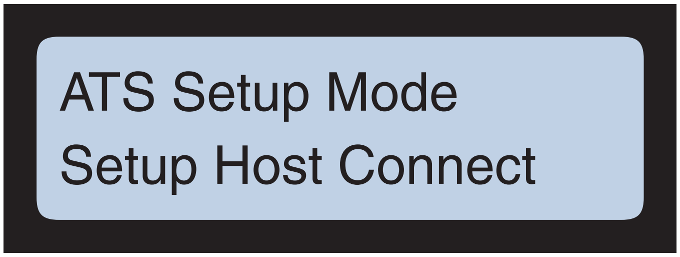
4. The terminal displays the **Re-Boot** prompt. Press the **enter** key to confirm and re-boot the terminal.

NOTE: You must re-boot the terminal immediately after changing/setting the password to "blank/no-password" (pressing the **enter** key at both the **Enter Password** and **Confirm Password** prompts without typing anything in). If you press the **clear** key to cycle through the setup menu parameters without rebooting the terminal may lock you out requiring you to contact technical support for a reset password specific to that terminal or completely removing power from the terminal for a few minutes to reset it.

Setup Host Connect

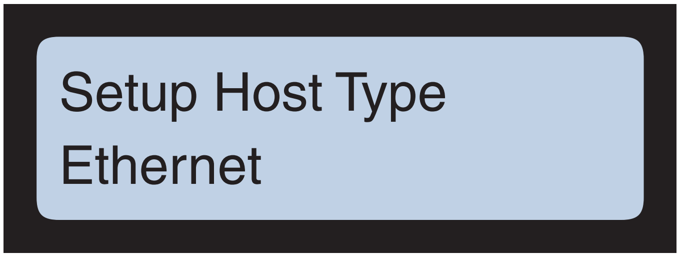
Set the network connection for terminals that use an Ethernet connection, so the terminal can communicate across the local computer network.

1. Press the **enter** key at the to **Setup Host Connect** prompt to access the host connection options or press the **clear** key to proceed to the next item (**Setup Smartcard**).



ATS Setup Mode
Setup Host Connect

2. If you pressed the **enter** key the terminal displays the current host type setting (either **Ethernet** and **Serial**). Press the **enter** key to accept (select) the displayed setting or press the **clear** key to change it (select the other option).



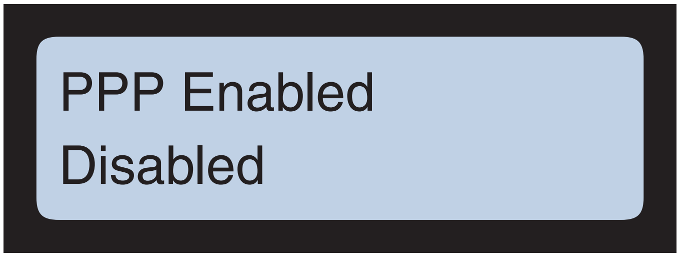
Setup Host Type
Ethernet

NOTE: Select **Ethernet** for the **Host Type** on terminals with GSM modems.

3. If you selected **Ethernet** proceed to "If you selected Ethernet for the Host Type" on page 3-19.
   If you selected **Serial** proceed to "If you selected Serial for the Host Type" on page 3-26.

If you selected Ethernet for the Host Type

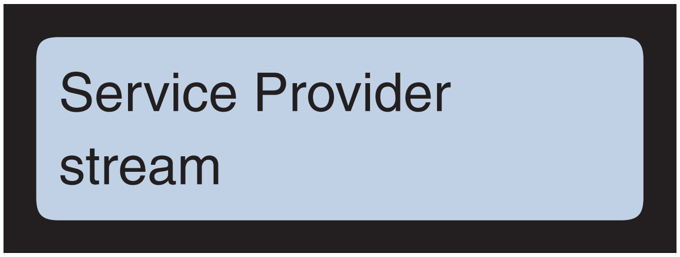
4. If you selected **Ethernet** for the **Setup Host Type** parameter the terminal displays the **PPP** parameter (Point-to-Point-Protocol). Press the **enter** key to accept the displayed setting (**Enabled** or **Disabled**) or press the **clear** key to toggle between the **Enabled** and **Disabled** options. Press the **enter** key when the terminal displays the desired setting.



PPP Enabled
Disabled

NOTE: PPP must be **Enabled** for terminals with GSM modems.

5. If you selected **Enabled** for the **PPP** parameter the terminal prompts you for the **Service Provider**. This parameter allows you to select your wireless network provider from the list of service providers.

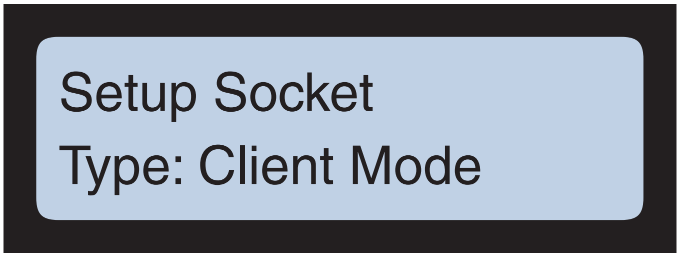


Service Provider
stream

Press the **enter** key to accept the displayed **Service Provider** or press the **clear** key to scroll through the list of providers. Press the **enter** key when the terminal displays the desired provider.

The available providers are; **stream**, **proximus**, **o2**, **etisalat**, **datalink**, **att-gold**, **att**, **ats-tm**, **O2UK**, **ATS-t-mobil**, **Wlogic-ATT**, **wlogic**, **AIS**, **vodafoneUK**, **vodafone**, **vodacom**, **vodaPAYG**, **telenor**, **t-mobil-uk**, **t-mobile**.

6. Next the terminal displays the current **Setup Socket Type** parameter setting (**Client Mode** or **Server Mode**).



Setup Socket
Type: Client Mode

In client mode, the terminal connects to the host server using the socket port as defined in the **Setup Socket Port** parameter. In client mode, the terminal makes the TCP/IP connection to the designated host computer. When in this mode, the terminal does not accept a connection request from any outside device.

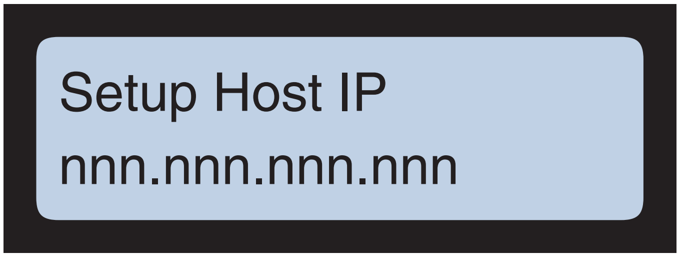
In server mode, the terminal awaits a connection initiated by the host using this socket port as follows:

- The terminal waits for a host server to initiate a connection. The terminal does not attempt to connect to any host server, so it is the host server's responsibility to make the connection request with a terminal. The terminal is set up to accept a single connection that can come from any host.
- A terminal connection needs to be maintained only when the host server needs to, which reduces network traffic, such as Keep Alives.
- You can change the host server without needing to set up your terminals.

- Since any host on the network can try to make a connection with the terminal, any host that knows how to communicate with the terminal can read data from the terminal.

The following parameters are the same as the terminal displays at initial setup ("Initial Setup Parameters" on page 3-7).

7. The terminal displays the default (**192.168.001.100**) or saved value for the Host that provides communications to the terminal. The host IP address is ignored if the terminal is in server mode.



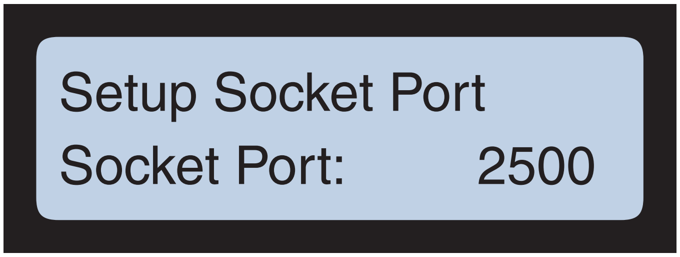
```
Setup Host IP
nnn.nnn.nnn.nnn
```

Press the **enter** key to accept the displayed IP address and continue to the next parameter or press the **clear** key to change the host IP address.

If you pressed the **clear** key use the numeric keys to type in the IP address of the host then press the **enter** key to save the new IP address.

If you type an invalid IP address, the terminal displays **Bad IP Address** and returns you to the saved/default value. Press the **clear** key again to correct the address then press the **enter** key to save it.

8. Next the terminal displays the default/saved socket port number used by the terminal. The default value is **2500**. Press the **enter** key to accept the displayed port number or press the **clear** key to change it using the numeric keys. When finished press the **enter** key to save the socket port number and continue to the next parameter.

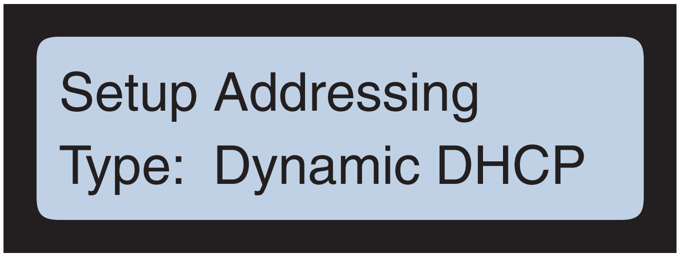


```
Setup Socket Port
Socket Port:       2500
```

If you type an invalid socket port number the terminal displays **Invalid Socket Port**. and returns you to the saved/default value. Press the **clear** key again to correct the port number then press the **enter** key to save it.

By default, ATS uses port 2500 for the network connection between the terminal and a connecting computer.

9. Next the terminal displays the default/saved addressing mode for the terminal. The default value is **Dynamic DHCP**. In DHCP mode the terminal receives its IP address from the connected DHCP server (therefore the terminal IP address may periodically change). The terminal uses standard DHCP conventions, does automatic lease renewal, and uses only standard option codes in the range 0 through 127.



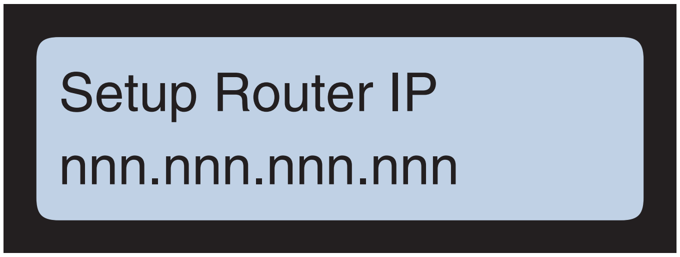
```
Setup Addressing
Type:  Dynamic DHCP
```

Press the **enter** key to accept DHCP mode and continue or press the **clear** key to toggle the display between the **Static IP** and **Dynamic DHCP** selections.
If the terminal was already in the displayed mode (**Dynamic DHCP** or **Static IP**) and you pressed the **enter** key without changing it, the terminal enters the ATS TSD Mode. Proceed to "ATS TSD Mode" on page 3-13).

- The **Static IP** selection enables you to set the terminal to a permanent IP address. The static IP address does not change until you type another one into the terminal.
- When the terminal displays the desired selection (**Dynamic DHCP** or **Static IP**) press the **enter** key to save the selection and continue to the next parameter.
- If you changed to the **Static IP** selection the terminal displays the next set of parameters that enable you to define the static IP addressing parameters starting with the **Setup Clock IP** parameter.
- If the terminal is set to **Static IP** (and rebooted) the terminal displays S**tatic IP** for the **Type**.
  You can access the following parameters by pressing the **clear** key, toggling the **Static IP** and **Dynamic DHCP** selections and re-saving **Static IP**.

NOTE: ATS supports Internet Protocol version 4 (IPv4) addressing. If you type an invalid IP, subnet mask, or other value, the terminal tells you the error and prompts you to retry using a valid entry.

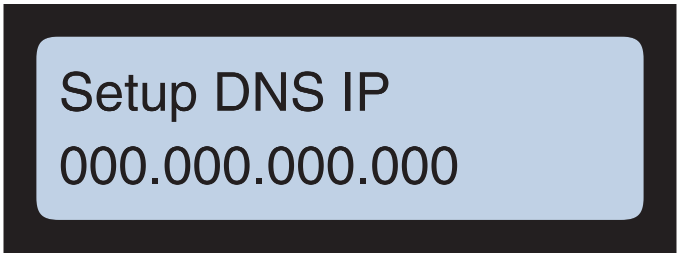
10. Next the terminal displays the **Setup Router IP** (Gateway IP address) parameter. Press the **enter** key to accept the displayed address or press the **clear** key then use the numeric keys to change the address. Press the **enter** key to save the new Gateway IP address when finished.



Setup Router IP
nnn.nnn.nnn.nnn

If you type an invalid IP address, the terminal displays **Bad IP Address**. Press the **clear** key again, correct the IP address then press the **enter** key to continue.

11. Next the terminal displays the **Setup DNS IP** parameter.

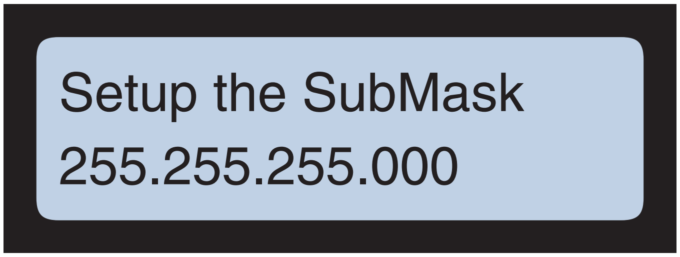


Setup DNS IP
000.000.000.000

Press the **enter** key to accept the displayed IP address for the DNS (Domain Name System) server or press the **clear** key then use the numeric keys to change the address. Press the **enter** key to save the new address and continue.

If you type an invalid IP address, the terminal displays **Bad IP Address**. Press the **clear** key again, correct the IP address then press the **enter** key to continue.

12. After saving the DNS server IP address the terminal displays the **Setup the Submask** parameter (the default subnet mask value is **255.255.255.000**).

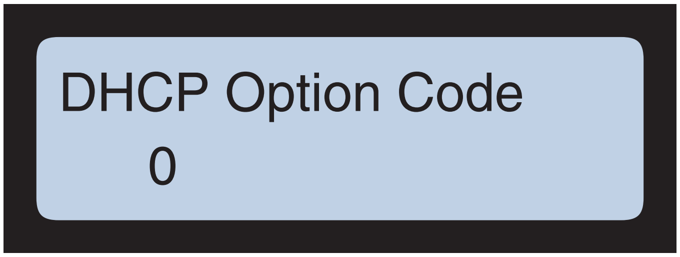


```
Setup the SubMask
255.255.255.000
```

Press the **enter** key to accept the displayed subnet mask value and continue or press the **clear** key then use the numeric keys to change the value. Press the **enter** key to save the new subnet mask to continue.

If you type an invalid subnet mask value, the terminal displays **Bad IP Address**. Press the **clear** key again, correct the value then press the **enter** key to continue.

13. Next the terminal displays **DHCP Option Code** setting. The default value is **0** (zero) which is “Pad, set by Protocol”.

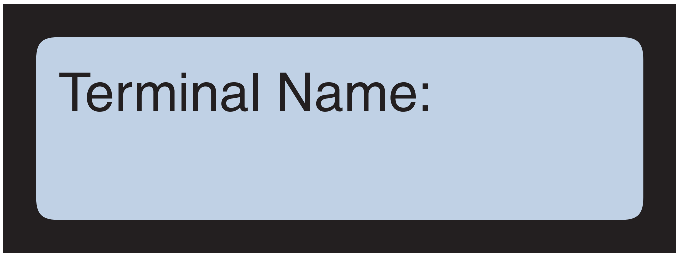


```
DHCP Option Code
    0
```

Press the **enter** key to accept the displayed **DHCP Option Code** selection or press the **clear** key then use the numeric keys to change the code. Press the **enter** key to save the new code and continue.

If you type an invalid code, the terminal displays **Out of Range**.
Press the **clear** key again, correct the code, then press the **enter** key to continue.

14. Next the terminal displays the **Terminal Name** parameter that enables you to set a unique up-to-20 character administrative name for the terminal. The default name is “ATS” plus the terminal serial number (e.g., **ATS000001**).

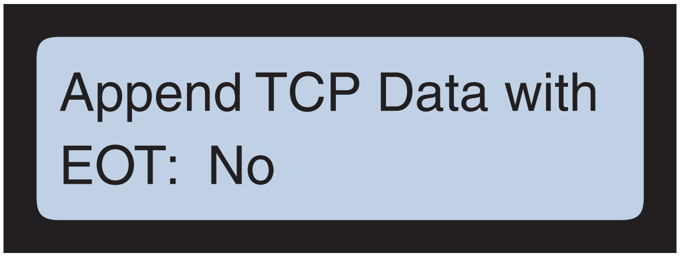


Terminal Name:

NOTE: At this time the terminal does not save any changes to the **Terminal Name**. If you make any changes the terminal reverts to the default **Terminal Name** after a re-boot. Use the following procedure and description for reference/future purposes only.

Press the **enter** key to accept the displayed name or press the **clear** key then use the numeric keys and the **F2** to change the name. The F2 key toggles the active character (most recently typed) as listed in Table 3-2, “Terminal Name Key to Character Mapping,” on page 3-11.

15. Next the terminal displays the **Append TCP Data with EOT** parameter (the default is **Yes**).



Append TCP Data with EOT: No

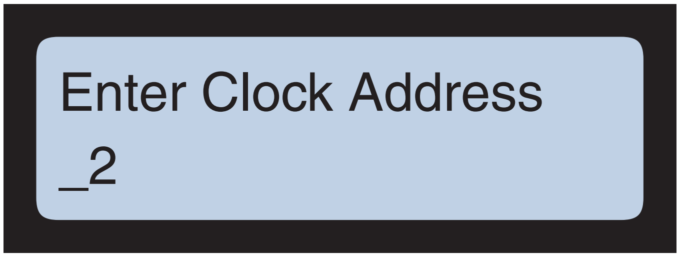
Press the **enter** key to accept the displayed selection (**Yes** or **No**) or press the **clear** key to toggle between **Yes** and **No** for support of end-of-transmission (EOT) data. If you choose **Yes**, the terminal appends an ASCII EOT character (04$_{16}$) to each transaction record sent to the host. Press the **enter** key when the terminal displays the desired selection to save it.
The terminal returns to the **Setup Password** prompt.

CAUTION

*Set **Append TCP Data with EOT** to **No** unless your communication software or networking software specifically support EOT (End Of Transmission).*
*If you set this to **Yes** and EOT is unsupported, the terminal could behave unpredictably, including not responding to input.*

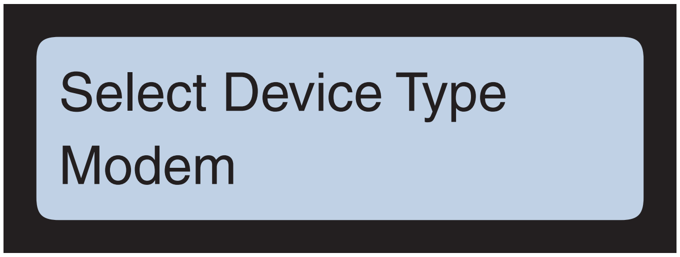
If you selected Serial for the Host Type

1. If you selected **Serial** for the **Host Type** the terminal prompts you to enter the terminal (clock) address (**Enter Clock Address**). Press the enter key to accept the displayed value or press the clear key then use the numeric keys to change it. The valid range is from **1** to **32**. Press the **enter** key to set the displayed value. This value needs to match what is set in the host computer.



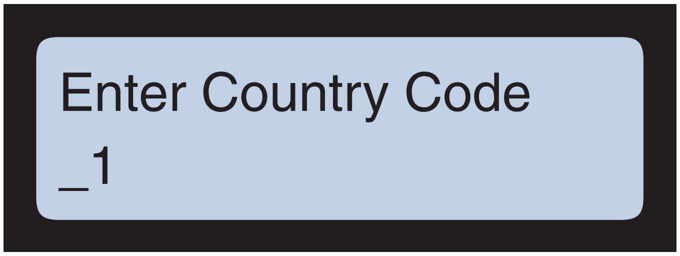
Enter Clock Address
_2

2. Next the terminal displays the **Select Device Type** parameter that enables you to select either **Modem** or **Direct**. Typically, you select **Direct** when the host connects directly to the terminal. In this case only one clock address applies (**1** set via the **Enter Clock Address** parameter).



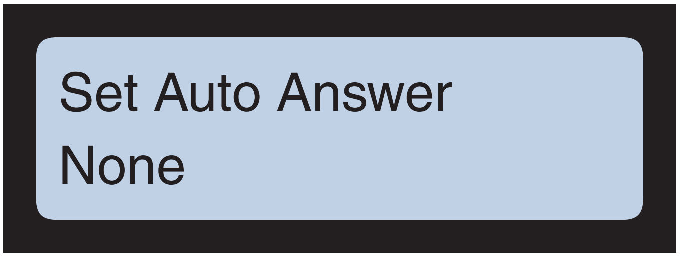
Select Device Type
Modem

3. Next the terminal displays the **Enter Country Code** parameter. Use the numeric keys to type the country code of the terminal. This can be a value from **01** to **FF**. Press the **enter** key to accept (set) the displayed value and continue or press the **clear** key then use the numeric keys and/or the function keys to enter the code (The function keys enable you to enter hexadecimal numbers A to F). Press the **enter** key when finished to save the code and proceed to the next menu item.



Enter Country Code
_1

4. Next the terminal displays the **Set Auto Answer** parameter. This parameter allows you to set the terminal to either None (immediate answer), or to answer after 1 Ring, 2 Rings, or 3 Rings. Press the **enter** key to accept (set) the displayed value and continue or press the **clear** key to change the setting. When you are finished press the enter key and the terminal returns to the **Setup Password** prompt (start of the **ATS Setup Menu**).

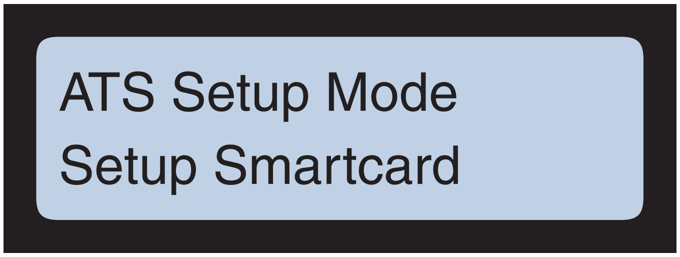


Set Auto Answer
None

Setup Smartcard

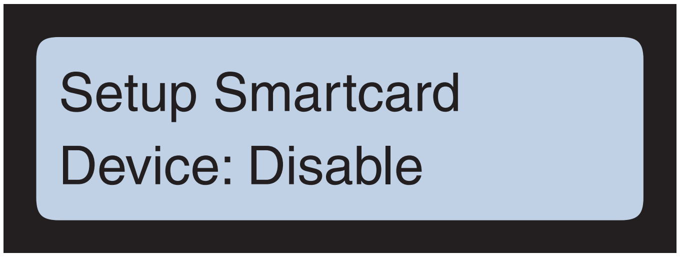
The **Setup Smartcard** parameter enables you to define the storage capacity of an optional Mifare^{TM} or iClass® contactless smartcard reader installed in the terminal (if applicable/ installed).

1. When the terminal displays the **Setup Smartcard** parameter (typically after the **Setup Host Connect** parameter) press the **enter** key to access the **Setup Smartcard** options (or press the **clear** key to proceed to the next parameter).



ATS Setup Mode
Setup Smartcard

2. Press the **clear** key to scroll between the **1k Card**, **4k Card**, and **Disabled** (default setting) options. Press the **enter** key when the terminal displays the desired setting to select the option and proceed to the next menu item.

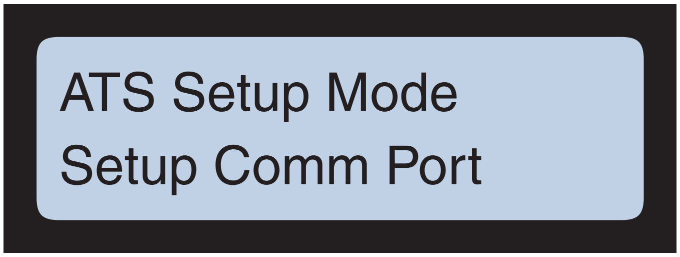


Setup Smartcard
Device: Disable

Setup Comm Port

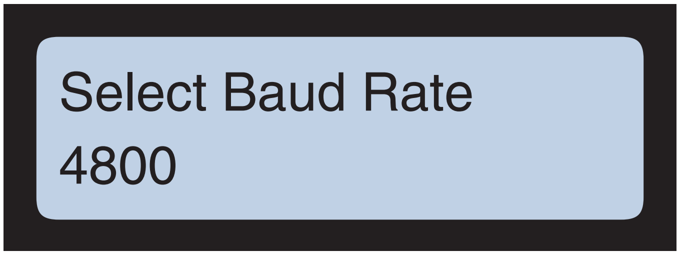
Set the communication port connection for terminals that use a serial connection. These settings must match the communication software and hardware you are using to connect to the terminal.

1. When the terminal displays the **Setup Comm Port** menu (typically after the **Setup Smartcard** parameter) press the **enter** key to access the comm port parameters (or press the **clear** key to proceed without configuring the comm port).



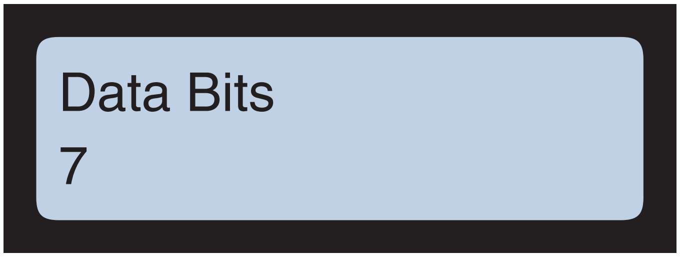
ATS Setup Mode
Setup Comm Port

2. If you pressed the enter key the first comm port parameter (**Select Baud Rate**) appears enabling you to set the baud rate for the port. Press the **enter** key to accept/set the displayed value or press the **clear** key to scroll between the **1200**, **4800**, **9600**, **19200**, **38400**, **57600**, **115200** baud (bps) options. Press the **enter** key when the terminal displays the desired option to set the option and proceed to the next menu item.



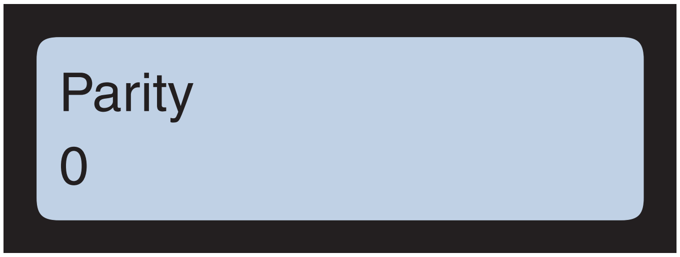
Select Baud Rate
4800

3. Next the terminal displays the **Data Bits** parameter. Press the **enter** key to accept/set the displayed setting or press the **clear** key to scroll between **7**, and **8**. Press the **enter** key when the terminal displays the desired option to set the option and proceed to the next menu item.



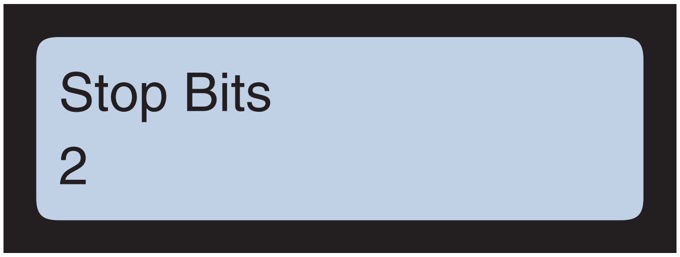
Data Bits
7

4. Next the terminal displays the **Parity** bit parameter. Press the **enter** key to accept/set the displayed value or press the **clear** key to scroll between the **O** (Odd), **E** (Even), and **N** (None) options. When finished press the **enter** key to save the setting and proceed to the next menu item.



Parity
0

5. Next the terminal displays the **Stop Bits** parameter. Press the **enter** key to accept/set the displayed value or press the **clear** key to scroll between the **1**, and **2**. When finished press the **enter** key to save the setting and proceed to the next menu item.

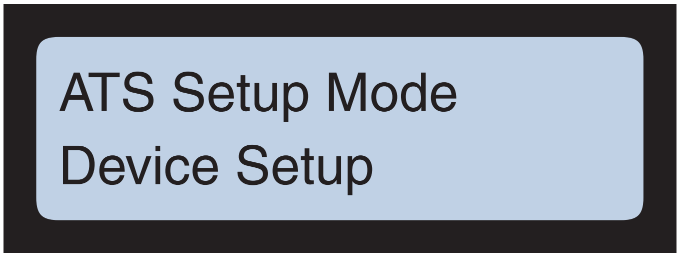


Stop Bits
2

Device Setup

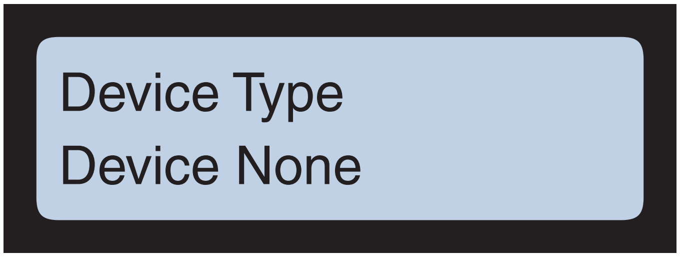
The **Device Setup** parameter enables you to setup the type of biometric fingerscan reader installed on the terminal.

1. When the terminal displays the **Device Setup** parameter (typically after the **Setup Comm Port**) press the **enter** key to access the device setup parameters (or press the **clear** key to proceed without configuring a device).



ATS Setup Mode
Device Setup

2. In the **Device Type** parameter menu, press the **clear** key to scroll between **Device None**, **Finger Geometry**, **FPR Lumidigm Verify**, **FPR Suprema Verify**, **FPR Bioscrypt**, **FPR Cogent Verify**, **FPR Lumidigm ID**, **FPR Suprema ID**, and **FPR Cogent ID** options.
   See "Verification and Identification Modes" on page A-5 of Appendix A, "Biometric Devices" for more information about Verification and Identification Modes and the various devices.



Device Type
Device None

NOTE: You must select the correct type of device installed in your terminal (or **Device None**). If you select an incorrect device type the terminal will continually reboot as it searches for the selected device type.

Do not let the system "time out" with an incorrect option highlighted unless it is **Device None**. Do not let the system "time out" with an incorrect option highlighted unless it is **Device None**. If you're unsure what device is installed in your Maximus scroll to **Device None** so that it is highlighted.

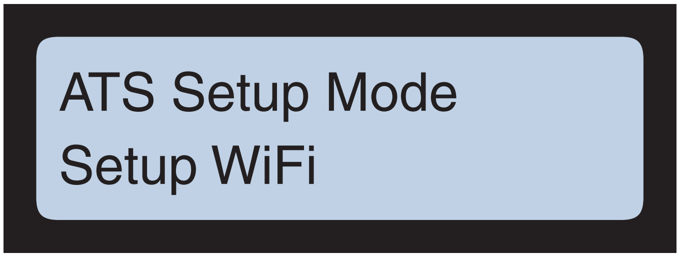
NOTE: Do not select the **Finger Geometry** option. The Maximus does not support finger geometry readers. The **Finger Geometry** option is removed from Firmware Version 2.05.17(X) and greater.

Setup WiFi

The **Setup WiFi** menu enables you to configure the optional WiFi device in your terminal (if installed). When WiFi is disabled the terminal displays the **Enable WiFi** prompt in place of the **Setup WiFi** menu prompt.

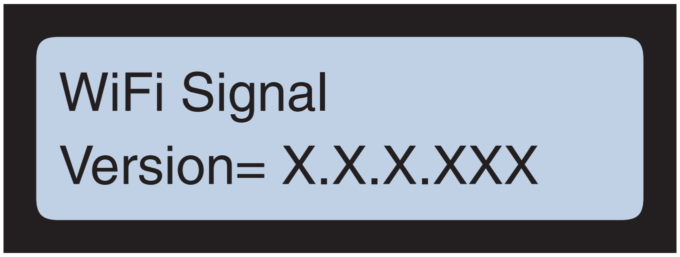
NOTE: You can use a USB keyboard plugged into the terminal USB port to help entering long text/ digit strings in the WiFi setup parameter (e.g., SSID, Security Key).

1. When the terminal displays the **Setup Wifi** menu (typically after **Device Setup**) press the **enter** key to access the **Setup WiFi** menu or press the **clear** key to proceed to the next item without configuring the WiFi device.



ATS Setup Mode
Setup WiFi

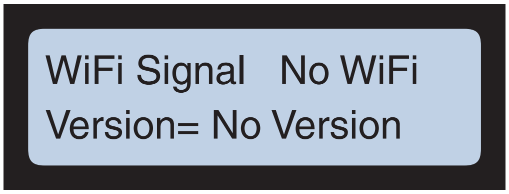
2. When you enter the **Setup WiFi** menu the terminal displays the WiFi version. When ready press the **clear** or **enter** key to proceed.



WiFi Signal
Version= X.X.X.XXX

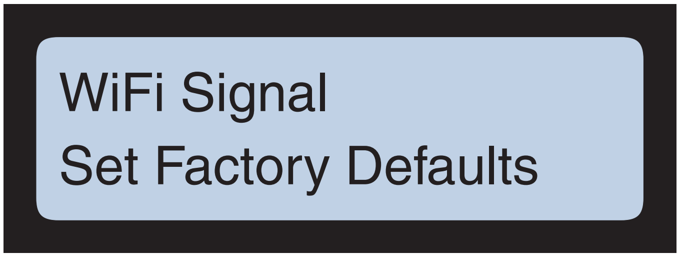
NOTE:

If the WiFi unit is not installed or functioning the terminal displays the **No WiFi** message:



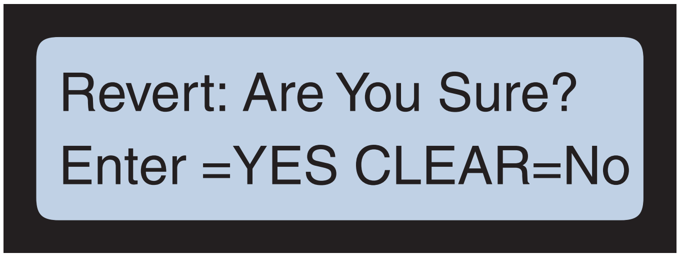
WiFi Signal No WiFi
Version= No Version

3. Next the terminal displays the **Set Factory Defaults** prompt. Press the **clear** key to proceed to the next menu item without resetting to the factory default WiFi configuration or press the **enter** key to proceed with the reset.



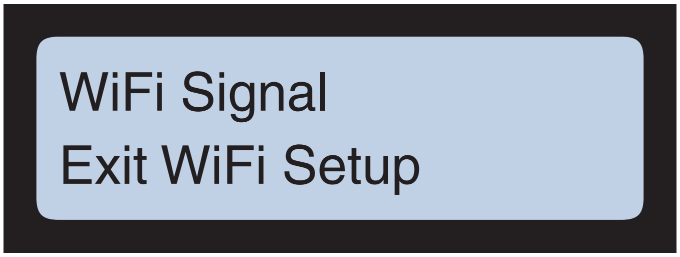
WiFi Signal
Set Factory Defaults

If you pressed the **enter** key the terminal prompts you to confirm the reset. Press the **enter** key to confirm the reset (**YES**) or press the **clear** key to cancel and return to the beginning of the WiFi menu.



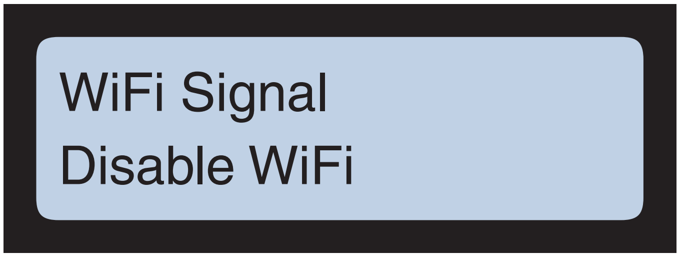
Revert: Are You Sure?
Enter =YES CLEAR=No

4. If you pressed clear at the **Set Factory Defaults** prompt the terminal displays the **Exit WiFi Setup** prompt. Press the **clear** key to proceed to the next item in the **Setup Wifi** menu or press the **enter** key to exit the WiFi.setup menu and return to the **ATS Setup Mode** menu.



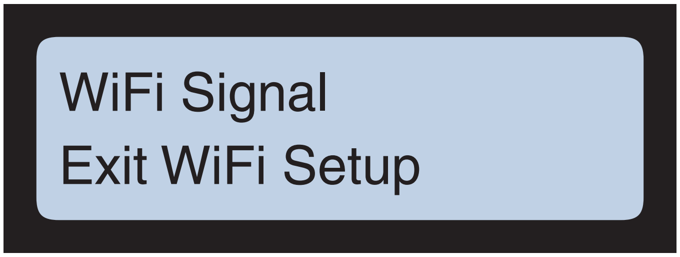
WiFi Signal
Exit WiFi Setup

5. If you pressed the clear key at the **Exit WiFi Setup** prompt the terminal displays the **Disable WiFi** prompt. Press the **enter** key to disable the WiFi device in the terminal or press the **clear** key to proceed without disabling the device.



WiFi Signal
Disable WiFi

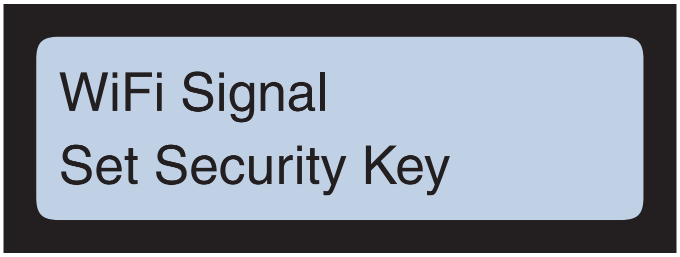
If you pressed the **enter** key the terminal prompts you to exit. Press the **enter** key to exit the WiFi.setup menu and return to the **ATS Setup Mode** menu or press the **clear** key to proceed to the next WiFi menu item.



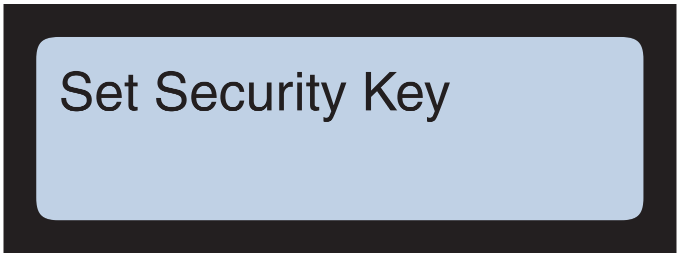
WiFi Signal
Exit WiFi Setup

If you disabled WiFi you can enable it in the **ATS Setup Mode** menu (the **Enable WiFi** prompt appears in the **ATS Setup Mode** menu when you disable WiFi).

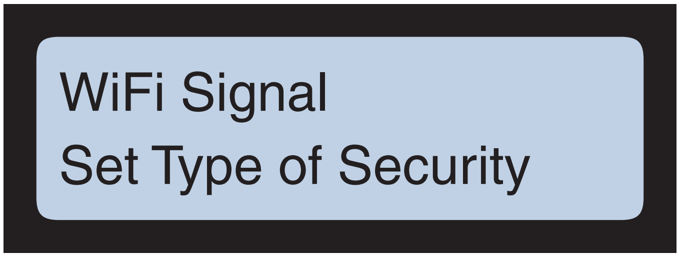
6. If you pressed the **clear** key at the **Exit WiFi Setup** prompt the terminal displays the **Set Security Key** prompt (WiFi network password).


WiFi Signal
Set Security Key

Press the **clear** key to proceed to the next menu item without setting a security key or press the **enter** key to set a key. If you pressed enter the **Set Security Key** prompt appears. Use the keypad to type in the WiFi network security key (password) then press the **enter** key to set the key and proceed to the next item.


Set Security Key

7. Next the terminal displays the **Set Type of Security** prompt. Press the **clear** key to proceed without setting the security encryption type or press the **enter** key to set the type.

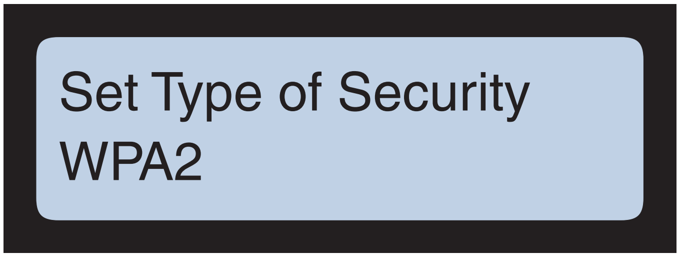

WiFi Signal
Set Type of Security

If you pressed the enter key you can use the clear key to scroll between the **WPA2**, **WPA**, **WEP**, and **None** options. When the terminal displays the desired option, press the **enter** key to set the encryption type and proceed.

NOTE:

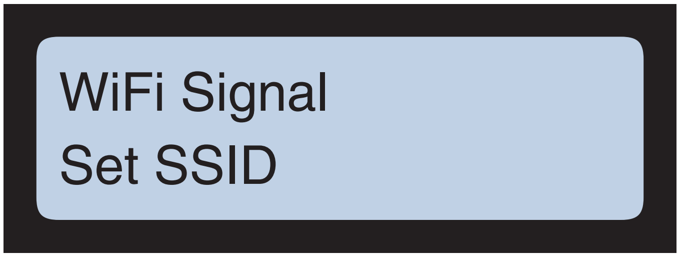
We recommend using the **WPA2** security protocol.
WEP has many security flaws and is easily broken.
WPA was introduced as an interim security enhancement over WEP and uses Temporal Key Integrity Protocol (TKIP) which is not secure and vulnerable to attack.

If the terminal is set to **WPA2** it may not connect to routers set to WPA/WPA2 (mixed mode). It will connect to a router set to "WPA2 Personal".



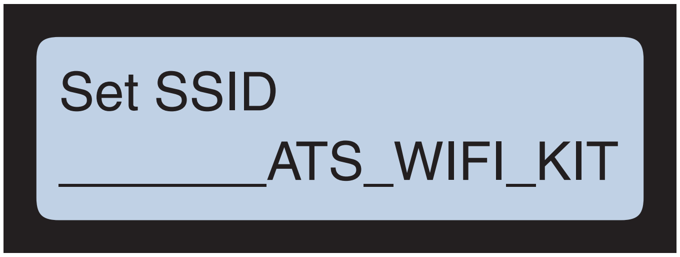
Set Type of Security
WPA2

8. Next the terminal displays the **Set SSID** prompt (Service Set Identifier, also known as the wireless network name). Press the **clear** key to proceed without setting the security encryption type or press the **enter** key to set the WiFi network SSID.



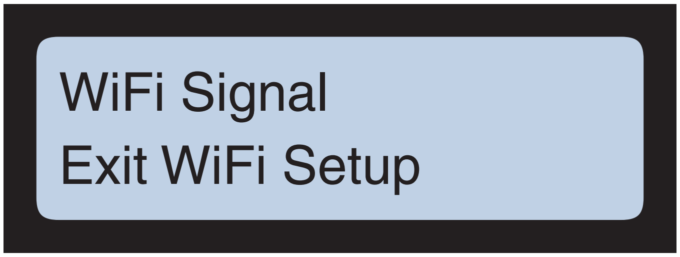
WiFi Signal
Set SSID

If you pressed enter the **Set SSID** prompt appears. Use the keypad to type in the SSID (WiFi network name) then press the **enter** key to set the SSID and proceed. The terminal returns to the start of the Setup WiFi menu.



Set SSID
________ATS_WIFI_KIT

9. Press the **clear** key repeatedly until the terminal displays the **Exit WiFi Setup** prompt. Press the **enter** key to exit and return to the **ATS Setup Mode**.



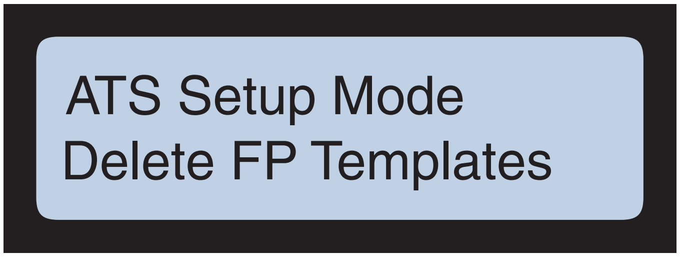
WiFi Signal
Exit WiFi Setup

Delete FP Templates

The **Delete FP Templates** command, added in Firmware 2.05.08(X), gives you the ability to erase all saved biometric templates via the terminal Setup Menu. This command only appears if your terminal is equipped with a FPR biometric device (“Finger Print Reader”).

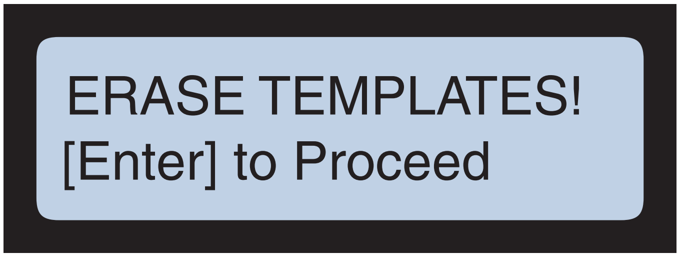
NOTE: Executing the **Delete FP Templates** command reboots the terminal.

1. When the terminal displays the **Delete FP Templates** parameter press the **enter** key to access the parameter or press the **clear** key to proceed without deleting the templates.



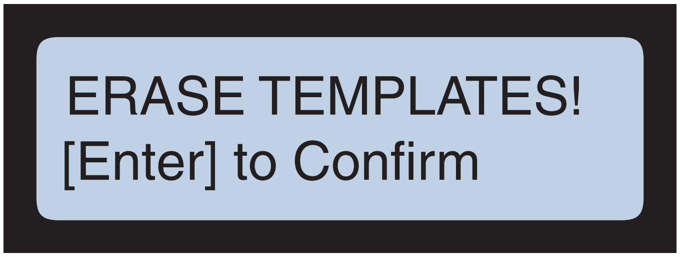
ATS Setup Mode
Delete FP Templates

2. The terminal prompts you if you want to proceed (**ERASE TEMPLATES!**). Press the **enter** key to proceed or press the **clear** key to return to the **Delete FP Templates** parameter.



ERASE TEMPLATES!
[Enter] to Proceed

3. If you pressed the **enter** key the terminal prompts you to confirm the **Erase Templates** command. Press the **enter** key to permanently delete all saved (enrolled) fingerscan templates from the biometric reader and reboot the terminal (or press the **clear** key to return to the **Delete FP Templates** parameter.)



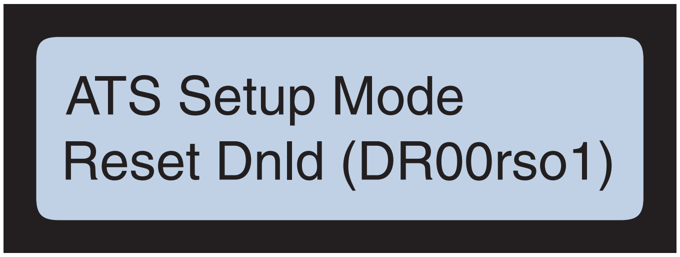
ERASE TEMPLATES!
[Enter] to Confirm

4. If you pressed **enter** at the **Confirm** prompt the terminal erases all saved biometric templates and reboots.

Reset Dnld

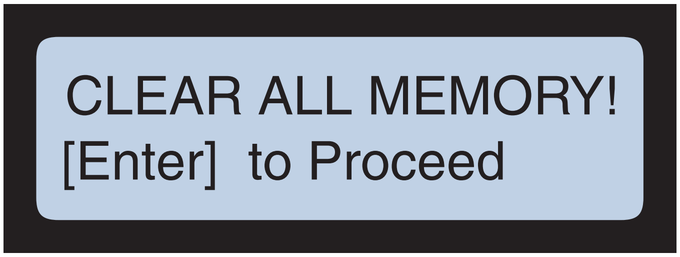
The **Reset Dnld** command clears the memory of the terminal, including all prompts and the data queue (e.g., employee badge numbers, schedules, punch history). After you perform this command the terminal displays the **Download Needed** prompt at startup (see "Power Up" on page 3-4). Use the following procedure to clear the terminal memory (reset the download):

1. Press the clear key repeatedly in the ATS Setup Mode menu until the terminal displays the **Reset Dnld (**XXXXXXXX**)** prompt.



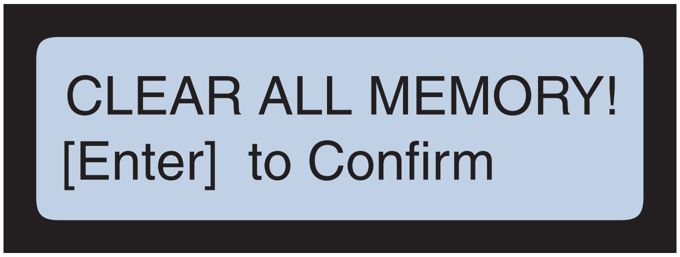
```
ATS Setup Mode
Reset Dnld (DR00rso1)
```

2. Press the clear key to exit the reset command or press the enter key to begin the reset. If you pressed enter the terminal displays the **CLEAR ALL MEMEORY! {Enter} to Proceed** confirmation prompt. You can press the **clear** key to exit leaving the terminal memory (download) intact or press the **enter** key to proceed.



```
CLEAR ALL MEMORY!
[Enter]  to Proceed
```

If you pressed the **enter** key the terminal displays the second confirmation prompt: **CLEAR ALL MEMEORY! {Enter} to Confirm**. Once again you can press the **clear** key to exit leaving the terminal memory (download) intact or press the **enter** key to proceed.



```
CLEAR ALL MEMORY!
[Enter]  to Confirm
```

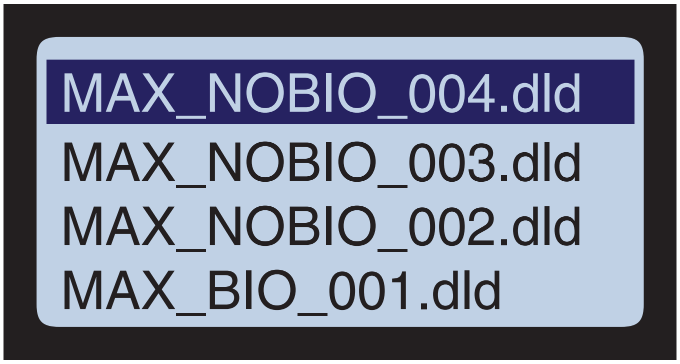
If you pressed the **enter** key the terminal purges the current download and memory then reboots and returns to the initial power-up prompt (see "Power Up" on page 3-4).

Download from USB

The **Download from USB** command enables you to install downloads (applications) to the Maximus terminal from a USB flash drive. With a USB flash drive that contains the (*.dld) download file(s) installed in the Maximus USB port, press the **enter** key to access the download selection screen as shown in Figure 3-5.

NOTE: Ensure the desired download file is present on the USB flash drive before entering the download selection screen. Once you enter the list the terminal will install a download if one is present. You won't be able to exit without installing a download if one is on the flash drive (both the clear and enter keys install the highlighted download file). If you are forced to install an undesired download file, you can remove it using the Reset Dnld command as described on page 3-37.

Figure 3-5 Selecting a Download File



```
MAX_NOBIO_004.dld
MAX_NOBIO_003.dld
MAX_NOBIO_002.dld
MAX_BIO_001.dld
```

Use the "F7" and "F8" keys to scroll between multiple download files (if applicable). With the desired download file highlighted, press the **enter** key to install the download file/application on the Maximus terminal.

For more information about the USB see Appendix C, "Using the USB"

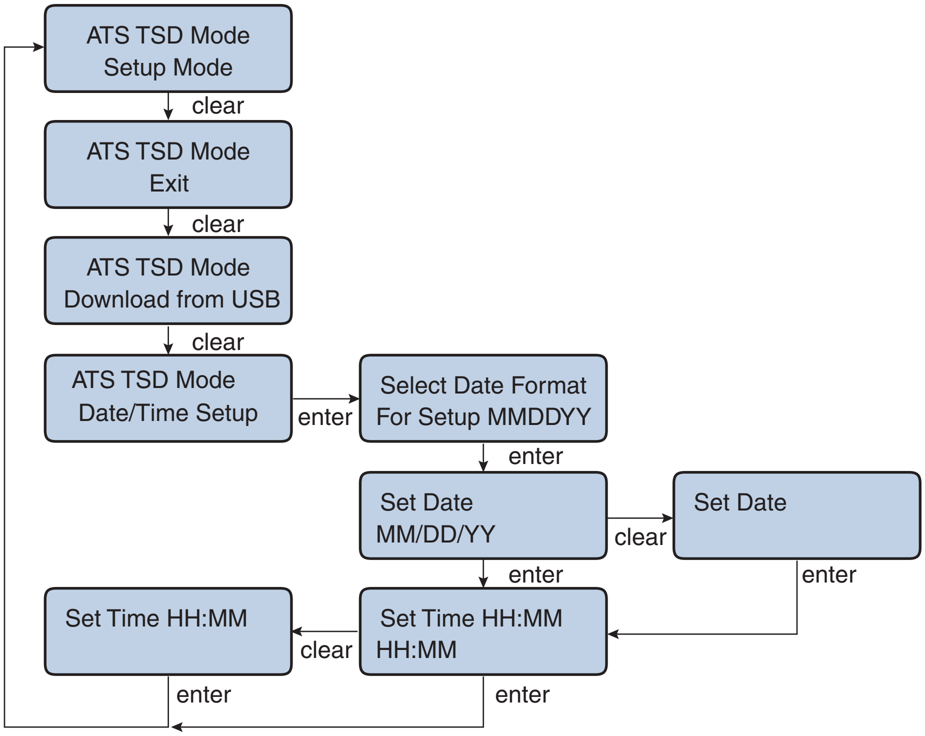
For more information about the UCS applications (downloads and *.dld files) see the Universal Command Set Manual, MANU-UCS-01.

Date/Time Setup

You can access the Date and Time Setup from the TSD Mode menu. For information on accessing TSD Mode, see "Initial Setup Menu Structure Flow Chart" on page 3-6.

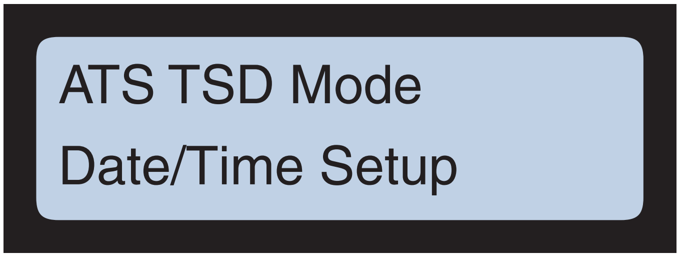
Figure 3-6 provides a flow chart of the **Date/Time Setup** menu from the **ATS TSD Mode** menu.

Figure 3-6 Date/Time Navigation Flow Chart



Use the following procedure to change the terminal Date and Time:

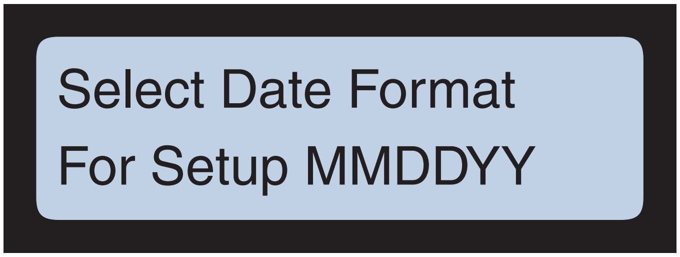
1. Go to the **ATS TSD Mode** and press the **clear** key until the **Date/Time Setup** prompt appears then press the **enter** key to access the Date/Time menu.



ATS TSD Mode

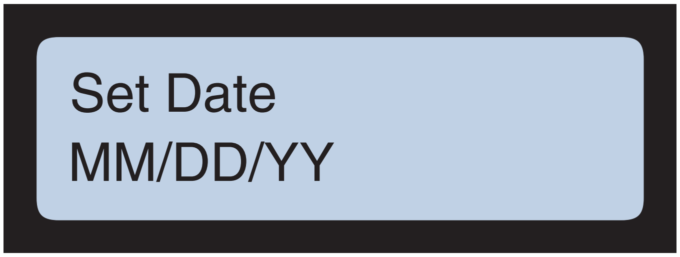
Date/Time Setup

2. The **Select Date Format For Setup MMDDYY** prompt appears. Use the “F8” function key to scroll between **MMDDYY** (month, day, year), **YYMMDD** (year, month, day), **DDMMYY** (day, month, year) formats. When the terminal displays the desired format press the **enter** key to save the format and proceed to the **Set Date** prompt.



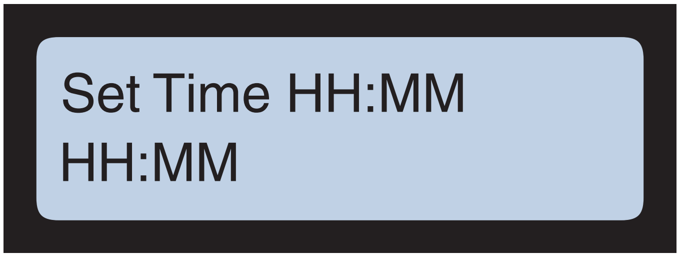
```
Select Date Format
For Setup MMDDYY
```

3. Press the **enter** key to accept the date displayed on the terminal or press the **clear** key to change it. If you pressed **clear**, press the **enter** key to exit without changing the date or use the numeric keys to set the desired date (you can use the **clear** key to delete the last number you entered). When you are finished press the **enter** key to save the date and proceed.



```
Set Date
MM/DD/YY
```

4. Next the terminal displays the **Set Time HH:MM** prompt. Press the **enter** key to accept the current time or press the **clear** key then use the numeric keys to enter a new time (you can use the **clear** key to delete the last number you entered). When you are finished press the **enter** key save the time and to return to the start of the **ATS TSD Mode** menu.



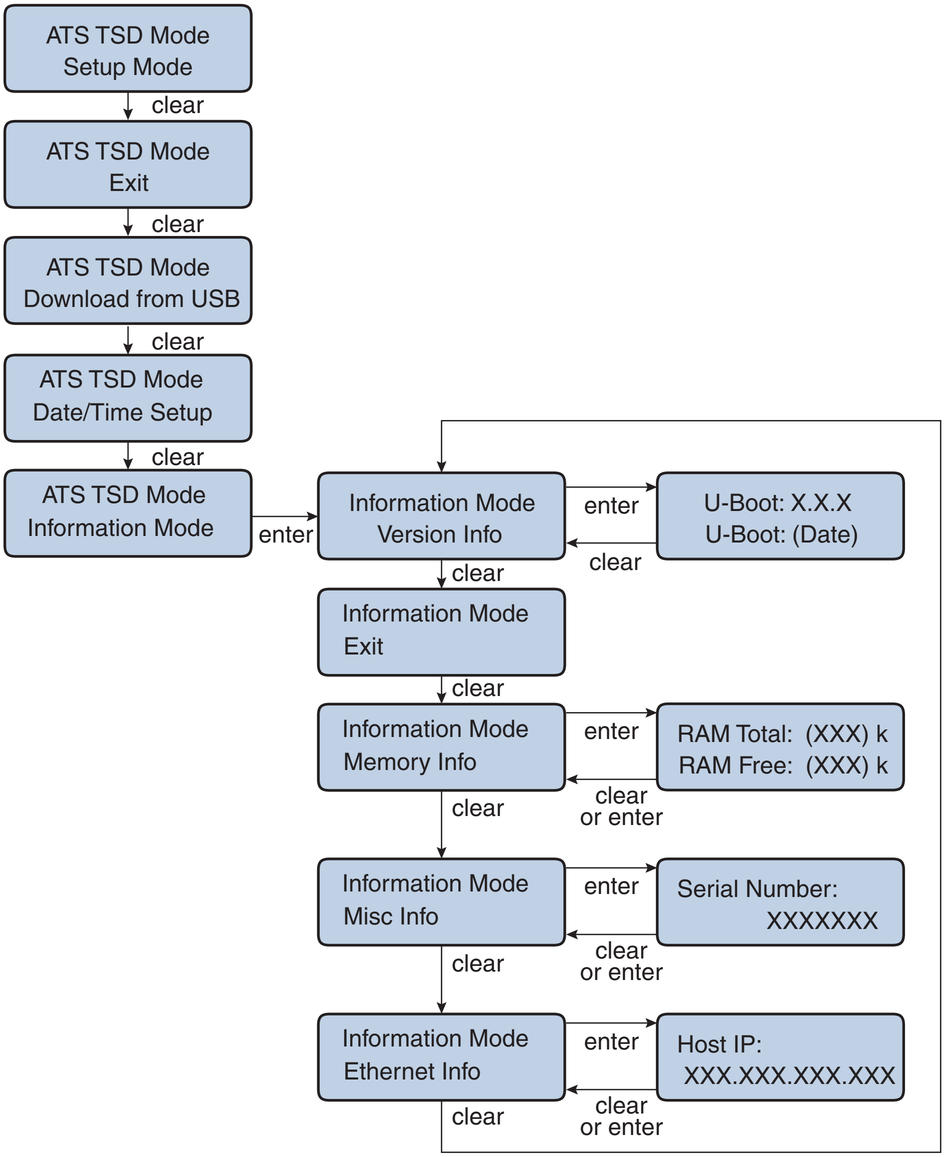
```
Set Time HH:MM
HH:MM
```

Information Mode

Information Mode enables you to view the terminal firmware version, memory size, hardware component versions, serial number, and Ethernet configuration settings.

You access the **Information Mode** from **ATS TSD Mode**. See "ATS TSD Mode" on page 3-13 for information on accessing the **ATS TSD Mode**. Figure 3-7 provides a flow chart of the **Information Mode** menu navigation.

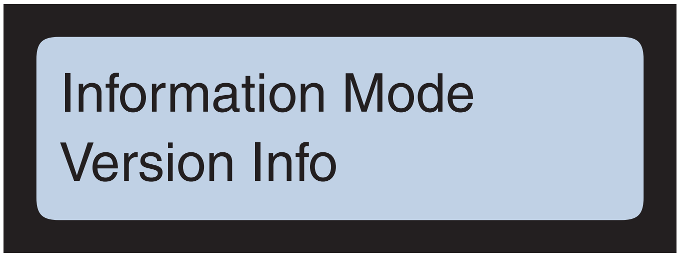
Figure 3-7 Information Mode Navigation Flow Chart



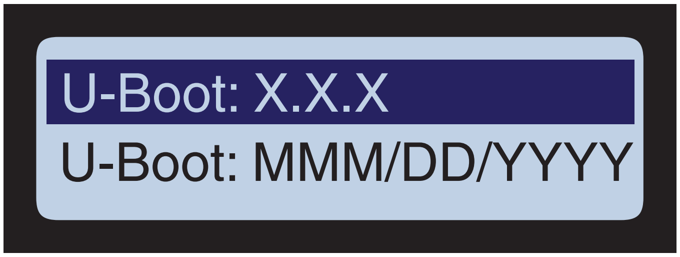
Version Info

Version Info enables you to view the version and date of firmware and hardware installed on the terminal. Use the following procedure to view the version information:

1. Enter the **Information Mode** menu then press the **enter** key when the **Version Info** menu prompt appears.



Information Mode
Version Info



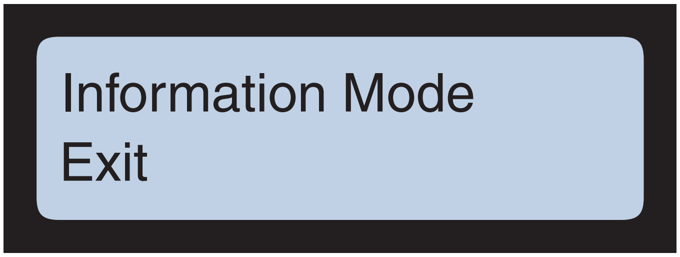
U-Boot: X.X.X
U-Boot: MMM/DD/YYYY

2. Use the “F7**”** and “F8” keys to scroll through the following information:

- **U-Boot** (boot-loader version information)
- **U-Boot** (date of the boot-loader version)
- **Kernel** (main operating system version)
- **Kernel** (main operating system version date)
- **Eeprom** (hardware driver version)
- **Eeprom** (hardware driver version date)
- **Speaker** (speaker driver version)
- **Speaker** (speaker driver version date)
- **AtsLeds** (LED driver version)
- **AtsLeds** (LED driver version date)
- **BarRdr** (barcode reader driver version)
- **BarRdr** (barcode reader driver version date)
- **Keypad** (keypad driver version)
- **Keypad** (keypad driver version date)
- **UCS** (Universal Command Set software version)
- **UCS** (Universal Command Set software version date)
- **glibc** (C library version for customization)

- **glibc** (C library branch information)
- **Java** (version found – on Java systems, reports the date of the latest component of the java library)
- **Biometric** (device found – provides information about any connected fingerprint reader
- **Smartcard** (provides information about any connected smartcard)

3. When finished, press the **enter** or **clear** key to return to the **Information Mode** menu then press the **clear** key to proceed to the **Exit** prompt.



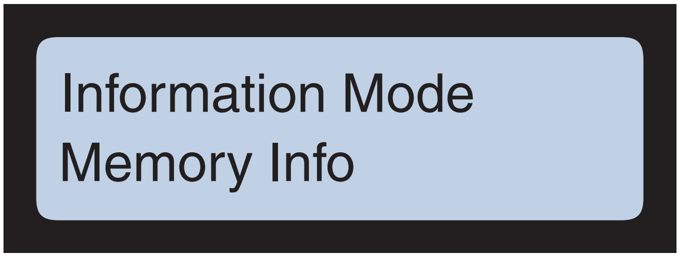
```
Information Mode
Exit
```

4. Press the **enter** key to exit from the **Information Mode** menu and return to the **ATS TSD Mode** menu or press the **clear** key to proceed to the **Memory Info** prompt.

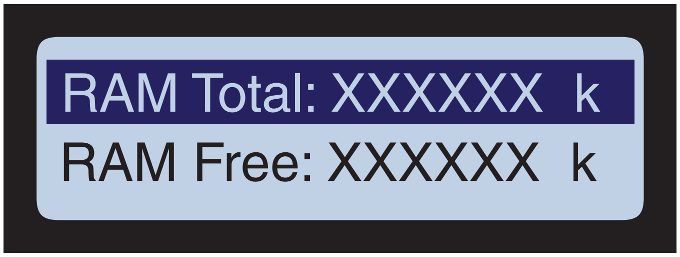
Memory Info

Memory Info enables you to view the amount of RAM and Flash memory installed on the terminal and the amount currently used. Use the following procedure to enter and view the memory status for the terminal:

1. Press the **clear** key when in the **Information Mode** menu until the **Memory Info** prompt appears then press the **enter** key.



```
Information Mode
Memory Info
```



```
RAM Total: XXXXXX  k
RAM Free: XXXXXX  k
```

2. Use the “F7**”** and “F8” keys to scroll through the following information:

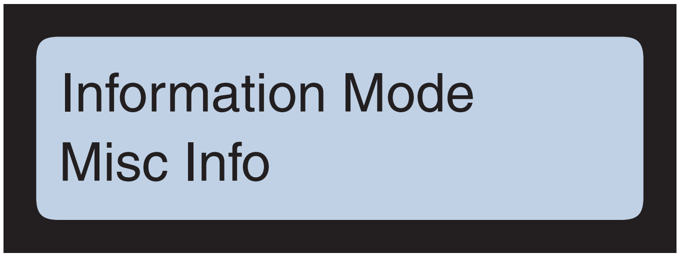
- **RAM Total** (the total Random Access Memory installed on the terminal)
- **RAM Free** (the amount of RAM available/unused on the terminal)
- **Flash Total** (the total flash memory installed on the terminal)
- **Flash Free** (the amount of flash memory available/unused on the terminal)

3. When finished, press the **enter** or **clear** key to return to the **Information Mode** menu then press the **clear** key to proceed to the **Misc Info** prompt.

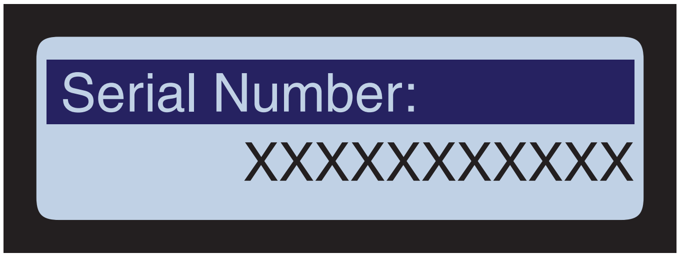
Misc Info

Misc Info enables you to view the serial number, customer number, CPU version, and PC board number (G-10) for the terminal. Use the following procedure to enter the **Misc Info** menu:

1. Press the **clear** key when in the **Information Mode** menu until the **Misc Info** prompt appears then press the **enter** key.



```
Information Mode
Misc Info
```



```
Serial Number:
      XXXXXXXXXXX
```

2. Use the “F7**”** and “F8” keys to scroll through the following information:

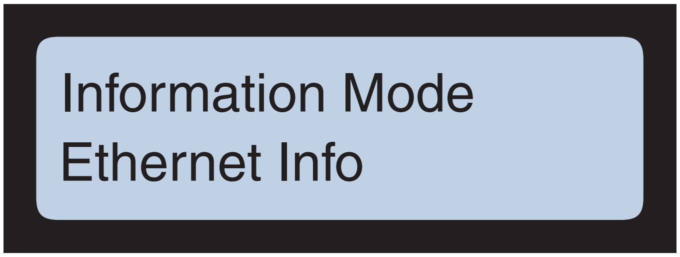
- **Serial Number** (the terminal serial number)
- **Customer Number** (customer number as noted at the ATS factory)
- **G-10 Number** (PC board assembly number)
- **CPU** (terminal CPU type and version)

3. When finished, press the **enter** or **clear** key to return to the **Information Mode** menu then press the **clear** key to proceed to the **Ethernet Info** prompt.

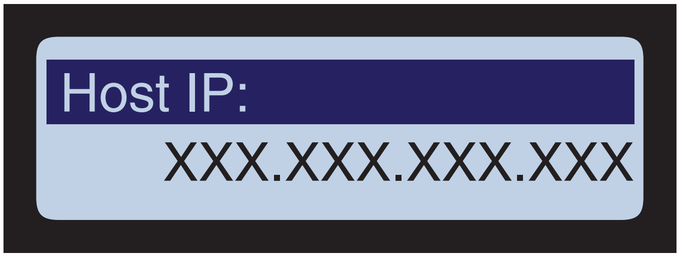
Ethernet Info

Ethernet Info enables you to view the network IP settings for the terminal. Use the following procedure to enter the **Ethernet Info** menu:

1. Press the **clear** key when in the **Information Mode** menu until the **Ethernet Info** prompt appears then press the **enter** key.



Information Mode
Ethernet Info



Host IP:
XXX.XXX.XXX.XXX

2. Use the “F7” and “F8” keys to scroll through the following information:

   - **Host IP** (IP address of the host computer that the terminal connects to)
   - **Local IP** (IP address of the terminal)
   - **Subnet Mask** (IP subnet mask used by the terminal)
   - **Gateway IP** (IP address of the gateway/router)
   - **DHCP OptionCode** (DHCP option code, e.g., **0** for pad, set by protocol)
   - **Mac Address** (Media Access Control address of the terminal)
   - **PHY** (Ethernet controller type, e.g., **Micrel KS8721 PHY**)

3. When finished, press the **enter** or **clear** key to return to the **Information Mode** menu (returns to beginning of the **Information Mode** menu - **Version Info** prompt). You can press **enter** to view the Version information or press **clear** to access the Information Mode **Exit** prompt.

Test Mode

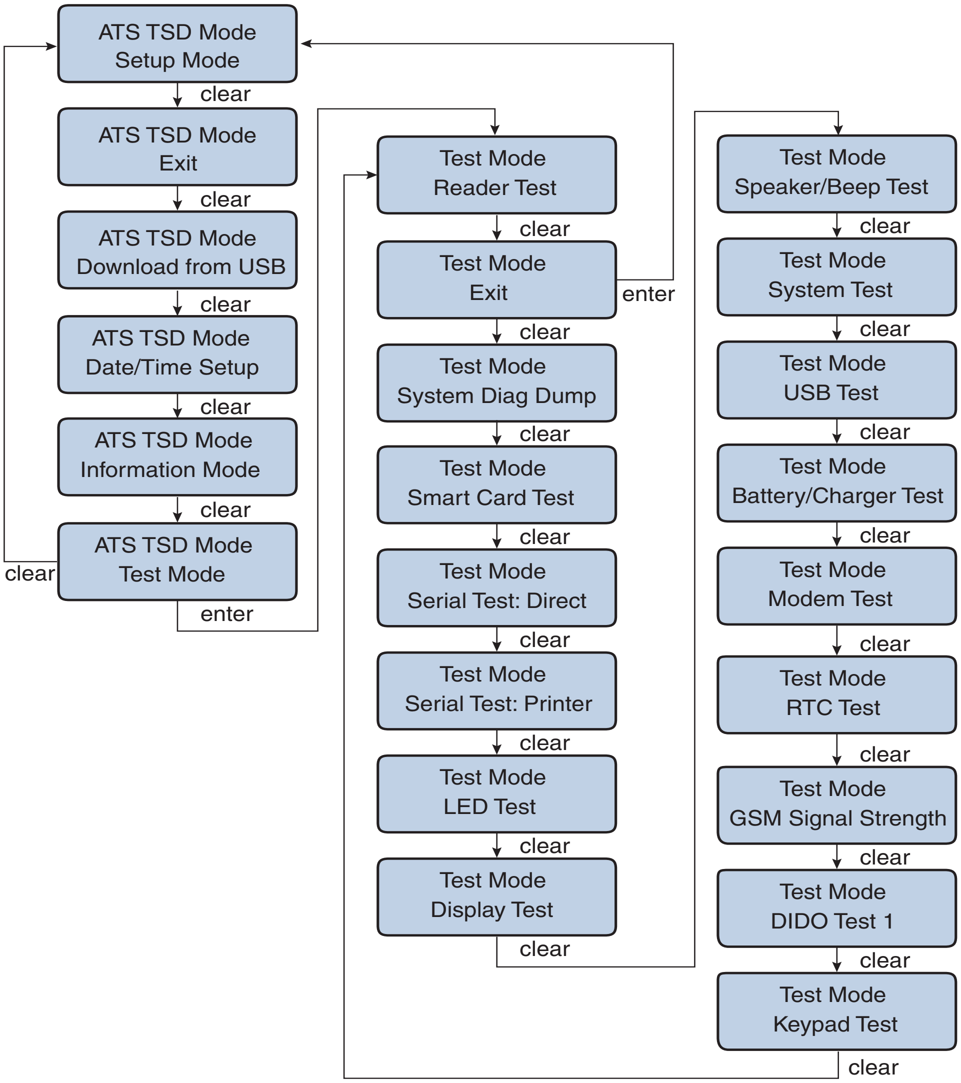
Test Mode enables you to run the built-in diagnostic tests on the terminal. These tests can identify malfunctioning components when troubleshooting the terminal.

Accessing Test Mode

You can access **Test Mode** from the **ATS TSD Mode** menu. See "ATS TSD Mode" on page 3-13 for how to access the **ATS TSD Mode** menu.

1. When in the **ATS TSD Mode**, press the **clear** key until the **Test Mode** menu option appears then press the **enter** key. Figure 3-8 provides a flow chart of the **Test Mode** menu navigation.

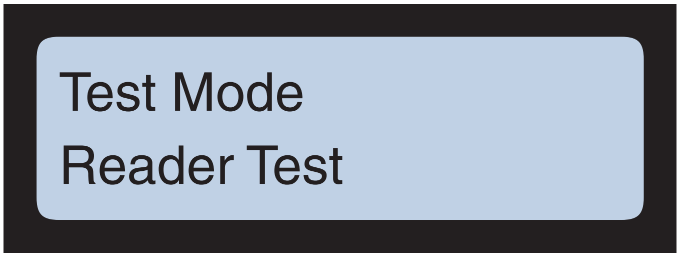
Figure 3-8 Test Mode Navigation Flow Chart



Reader Test

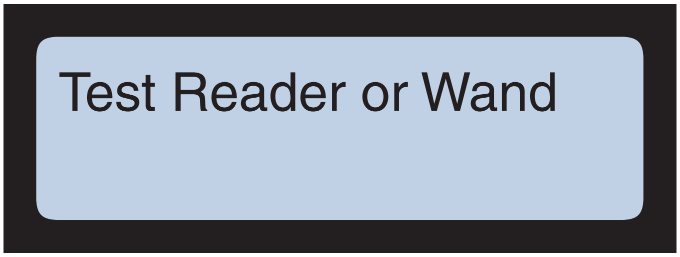
Reader Test enables you to test the functionality of a magnetic stripe, optical card, or proximity card reader installed in the Maximus terminal. Use the following procedure to select the **Reader Test** and test the installed reader:

1. In the **Test Mode** menu press the **enter** key when the terminal displays the **Reader Test** option.



Test Mode
Reader Test

2. The terminal displays the **Test Reader or Wand** prompt. When ready, press the **enter** key to start the test.



Test Reader or Wand

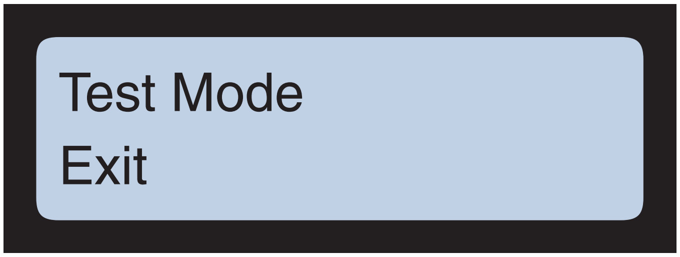
3. Use the appropriate "card" on the terminal. For example, if the terminal is equipped with a magnetic stripe reader, swipe the card.
   The terminal responds by flashing the appropriate LED (pass or fail) then displays the card badge number (if it successfully read the card).

4. When you are finished, press the clear key end the **Reader Test** and return to the **Test Mode** menu (at the **Test Mode**, **Exit** prompt).

Exit

Selecting **Exit** from the **Test Mode** menu returns you to the **ATS TSD Mode** menu. Use the following procedure to access the **Exit** command:

1. In the **Test Mode** menu, press the **clear** key until the **Exit** option appears.



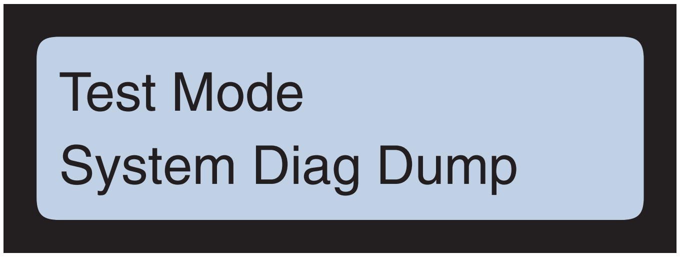
Test Mode
Exit

2. Press the **enter** key to exit test mode and return to start of the **ATS TSD Mode** menu (**Setup Mode** option), or press the **clear** key to proceed to the **System Diag Dump** option.

System Diag Dump

Typically an ATS technician requests/directs running this test to help troubleshoot the terminal. When complete, the **System Diag Dum**p test saves the results of the terminal tests in text file format to a USB flash drive plugged into the Maximus terminal. Use the following procedure to run a **System Diag Dump**:

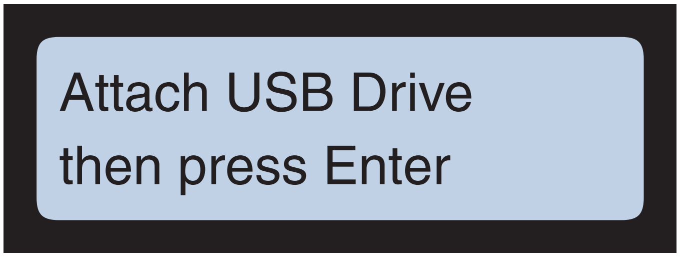
1. In the **Test Mode** menu, press the **clear** key until the **System Diag Dump** option appears.



Test Mode
System Diag Dump

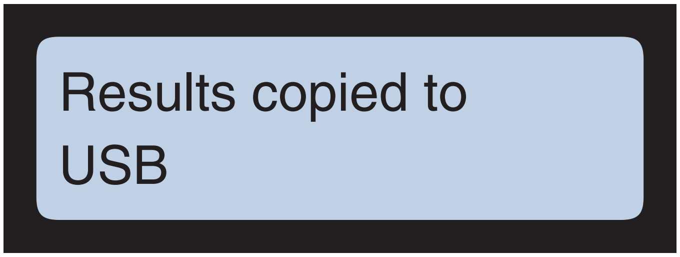
2. Press the **enter** key to start the **System Diag Dump** or press the **clear** key to return to the **Test Mode** menu.

3. If you selected the **System Diag Dump** option, the terminal prompts you to **Attach UDSB Drive then press Enter**. Insert a USB flash drive in the USB port on the Maximus terminal then press the **enter** key.



Attach USB Drive
then press Enter

4. The terminal displays the **Results copied to USB** message when the text file has been copied to the USB flash drive. You may now remove the USB flash drive then open the text file on a personal computer.



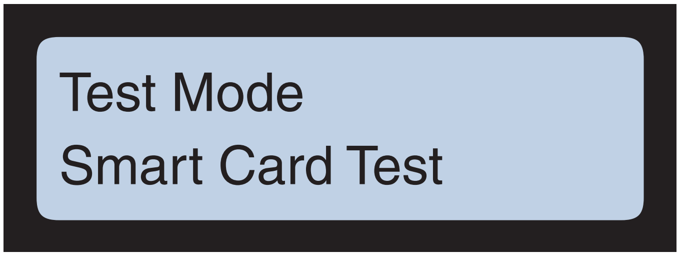
Results copied to
USB

5. When finished press the **clear** key to exit the **System Diag Dump** and return to the **Test Mode** menu (at the **Smart Card Test** option).

Smart Card Test

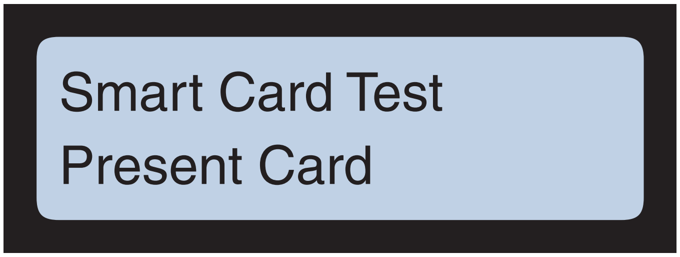
The **Smart Card Test** option tests an optional Mifare^{TM} or iClass® contactless smartcard reader (if installed in the terminal). Use the following procedure to test the smart card reader:

1. In the **Test Mode** menu, press the **clear** key until the **Smart Card Test** option appears.



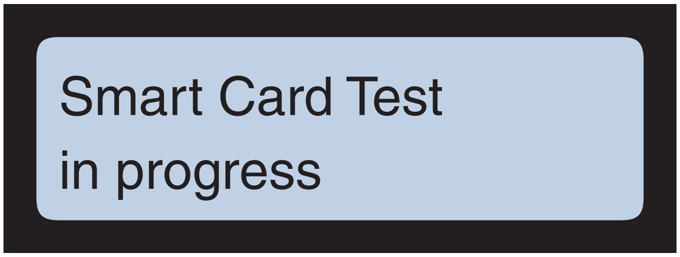
Test Mode
Smart Card Test

2. Press the **enter** key. The **Present Card** prompt appears.



Smart Card Test
Present Card

3. Press the **enter** key. The terminal displays the **in progress** message. Hold a smart card up to the terminal near the smart card reader (just under the keypad).



Smart Card Test
in progress

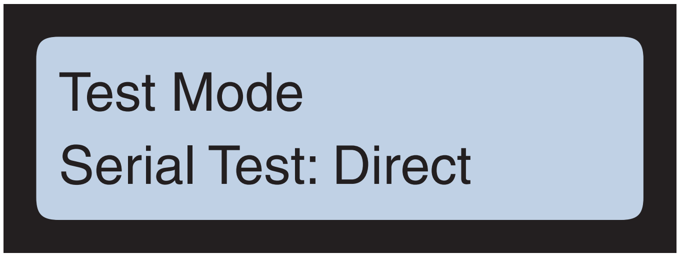
4. The terminal displays if the test passed or failed. When finished, press the clear key to return to the **Smart Card Test** option. You can now press the enter key to restart the test or press the clear key to exit the test and proceed to the next menu item (**Serial Test: Direct**).

Serial Test: Direct

This test requires specific loopback "jumper" and is typically only performed by an ATS service technician. It is noted here for reference purposes.

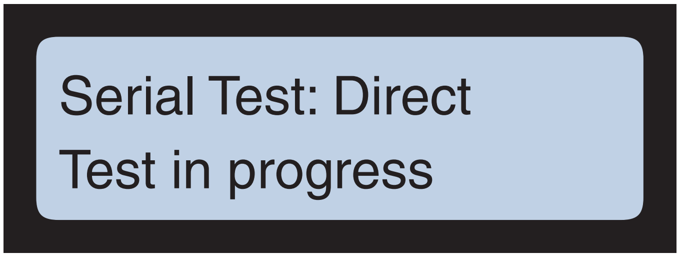
1. Install the "jumper" in the serial port on the terminal.

2. In the **Test Mode** menu, press the **clear** key until the **Serial Test: Direct** option appears.



Test Mode
Serial Test: Direct

3. Press the **enter** key to start the test. The terminal reports that the test is in progress. When the test is complete the terminal displays the result.



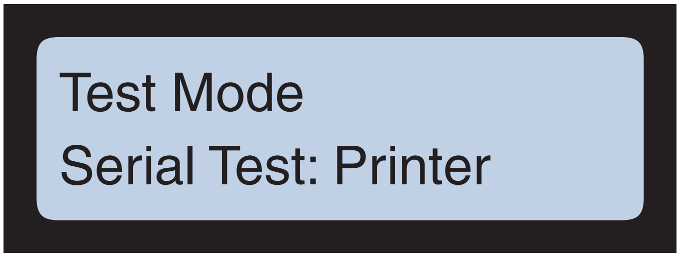
Serial Test: Direct
Test in progress

4. When you are finished, press the **clear** key to exit the direct serial test and display the **Serial Test: Printer** prompt. You may now remove the jumper from the terminal.

Serial Test: Printer

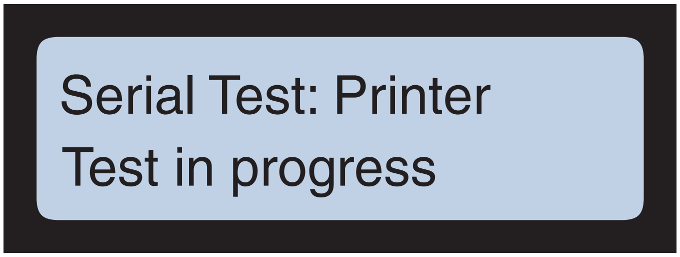
This test requires specific loopback "jumper" and is typically only performed by an ATS service technician. It is noted here for reference purposes.

1. Install the "jumper" in the serial /printer port on the terminal.
2. In the **Test Mode** menu, press the **clear** key until the **Serial Test: Printer** option appears.



Test Mode
Serial Test: Printer

3. Press the **enter** key to start the test. The terminal reports that the test is in progress If desired, you can interrupt and stop the test by pressing the **clear** key. When the test is complete the terminal displays the result.



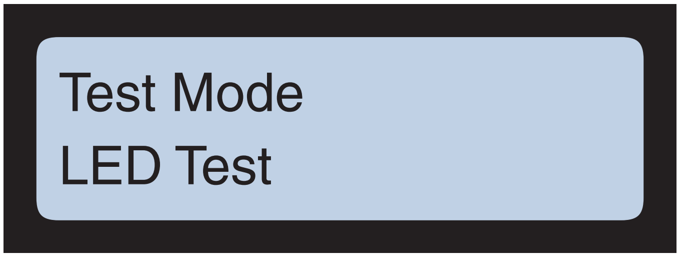
Serial Test: Printer
Test in progress

4. When you are finished, press the **clear** key to exit the serial printer test and display the **Serial Test: Printer** prompt. You may now remove the jumper from the terminal.

LED Test

The LED test cycles each LED on and off so you can confirm they are working. Use the following procedure to run the LED test:

1. In the **Test Mode** menu, press the **clear** key until the **LED Test** option appears.



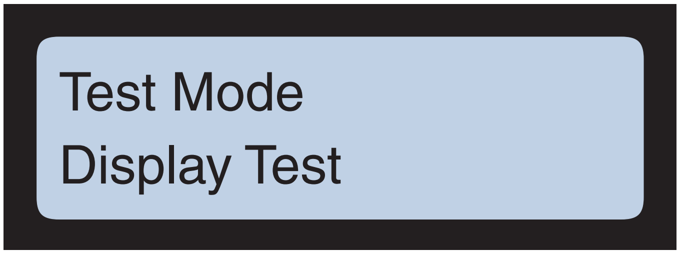
Test Mode
LED Test

2. Press the **enter** key to initiate the test. The terminal illuminates all the LEDs on the terminal then briefly shuts them all off. When the test is complete the "power LED" returns to the normal illuminated state (and any others if applicable). You can now press the **enter** key to run the test again or press the **clear** key to exit the LED test and return to the **Test Mode** menu.

Display Test

The display test cycles the all the pixels on the LCD display on and off so you can confirm they are working. Use the following procedure to run the display test:

1. In the **Test Mode** menu, press the **clear** key until the **Display Test** option appears.



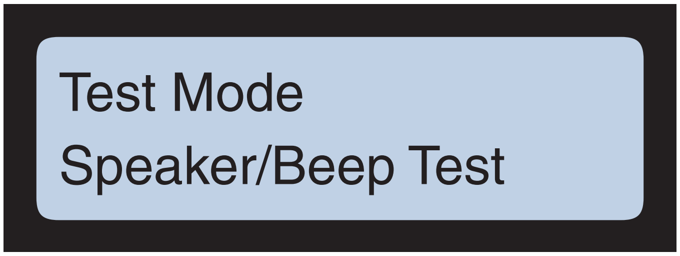
Test Mode
Display Test

2. Press the **enter** key to initiate the test. The terminal illuminates all the pixels on the LCD then briefly shuts them all off. When the test is complete the LCD returns to the **Test Mode**, **Display Test** option. You can now press the **enter** key to run the test again or press the **clear** key to exit the display test and return to the **Test Mode** menu.

Speaker/Beep Test

The speaker/beep test sends three increasing frequency tone signals to the speaker to ensure it is working properly. Use the following procedure to run the speaker/beep test:

1. In the **Test Mode** menu, press the **clear** key until the **Speaker/Beep Test** option appears.



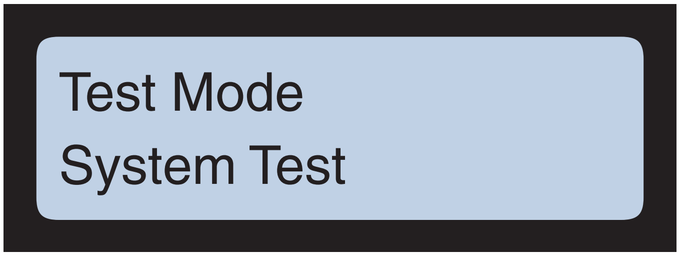
Test Mode
Speaker/Beep Test

2. Press the **enter** key to initiate the test. The terminal sends three increasing frequency tone signals to the speaker. You can now press the **enter** key to run the test again or press the **clear** key to exit the speaker/beep test and return to the **Test Mode** menu.

System Test

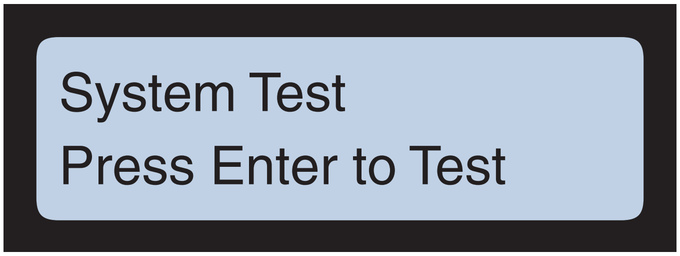
The system test performs a quick check on the integrity of the RAM, FLASH, and EEPROM installed on the terminal. Use the following procedure to initiate a system test:

1. In the **Test Mode** menu, press the **clear** key until the **System Test** option appears.



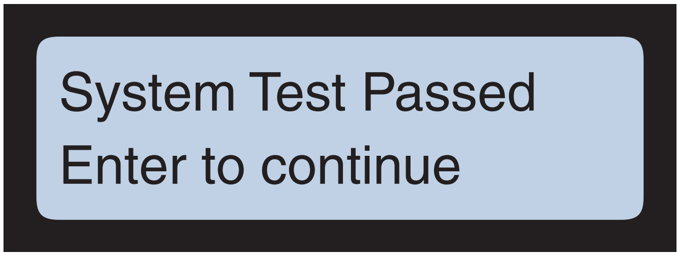
Test Mode
System Test

2. Press the **enter** key to select the **System Test** option. The terminal prompts you to press the enter key to start the test (**Press Enter to Test**)



System Test
Press Enter to Test

3. Press the **enter** key to start the test.
   When complete the terminal displays the results of the test.



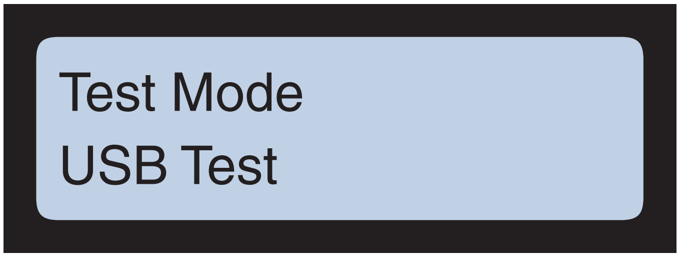
System Test Passed
Enter to continue

4. When finished press the **clear** key to exit the system test and return to the **Test Mode** menu (at the **USB Test** option).

USB Test

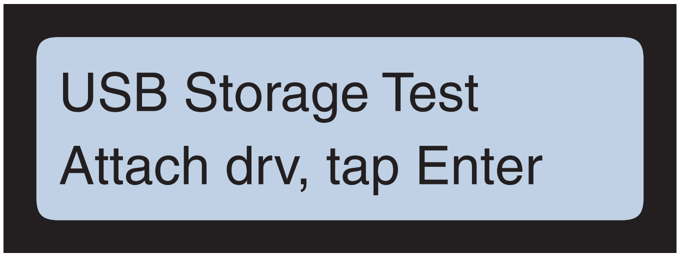
The USB test checks the functionality of the USB on the terminal. This test requires a USB flash drive. Use the following procedure to perform the USB test:

1. In the **Test Mode** menu, press the **clear** key until the **USB Test** option appears.



Test Mode
USB Test

2. Press the **enter** key to start the test. The terminal prompts you to install a USB flash drive into the USB post on the terminal (**Attach drv, tap Enter**).



USB Storage Test
Attach drv, tap Enter

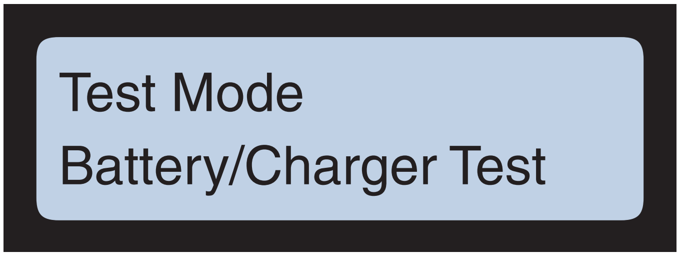
3. Install a USB flash drive into the USB port then press the **enter** key. The terminal displays the test result when the test is complete.

4. When you are finished press the **clear** key to exit the USB test and return to the **Test Mode** menu (at the **Battery/Charger Test** option) then remove the USB flash drive from the USB port.

Battery/Charger Test

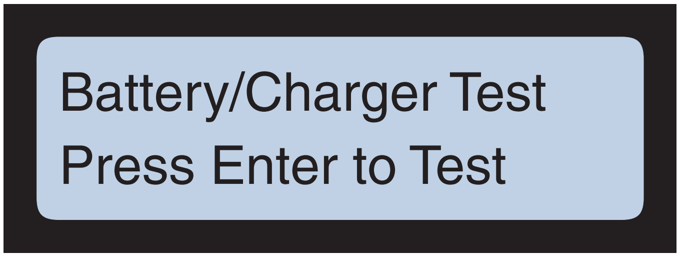
The battery/charger test checks the functionality of the optional UPS battery and charger (if installed). Use the following procedure to perform the battery/charger test:

1. In the **Test Mode** menu, press the **clear** key until the **Battery/Charger Test** option appears.



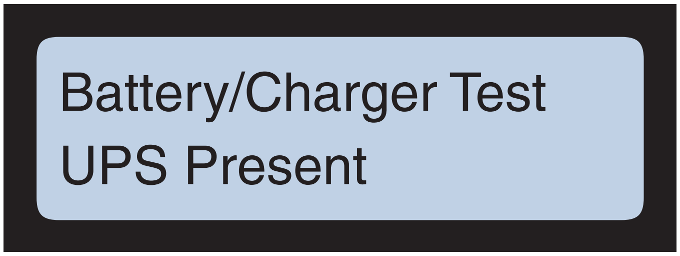
Test Mode
Battery/Charger Test

2. Press the **enter** key to select the **Battery/Charger Test** option.



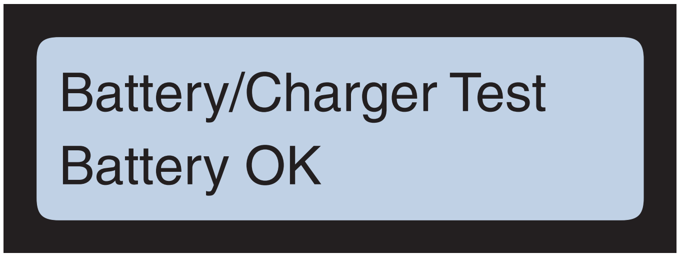
Battery/Charger Test
Press Enter to Test

3. Press the **enter** key to start the test. The system checks that the terminal is equipped with a UPS battery backup system and displays the result.



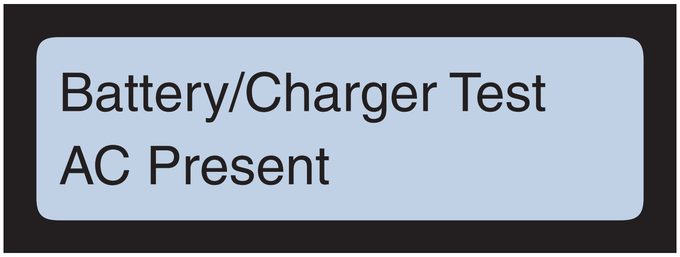
Battery/Charger Test
UPS Present

4. Press the **enter** key to test the condition of the battery. The system checks the battery and reports the result.



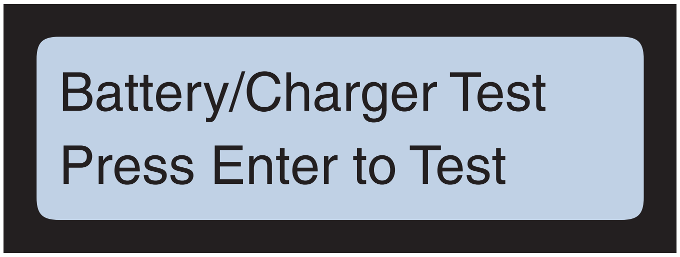
Battery/Charger Test
Battery OK

5. Press the **enter** key to test if AC power is present (charger). The system checks for AC power and reports the result.



Battery/Charger Test
AC Present

6. Press the **enter** key to return to beginning of the **Battery/Charger Test**.



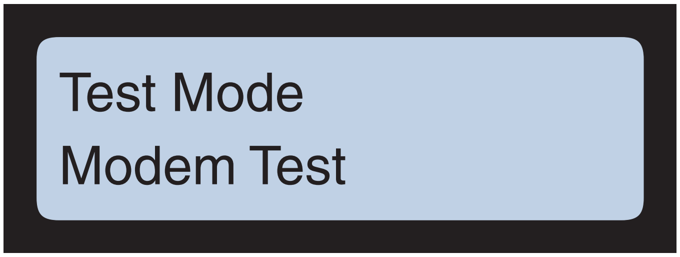
Battery/Charger Test
Press Enter to Test

7. When you are finished press the **clear** key to exit the battery/charger test and return to the **Test Mode** menu (at the **Modem Test** option).

Modem Test

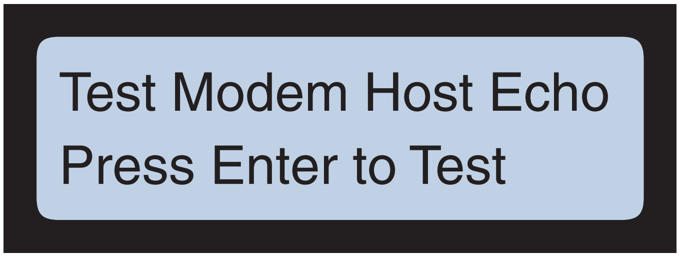
The modem test checks the functionality of an optional modem (if installed in the terminal). Use the following procedure to test the optional modem:

1. In the **Test Mode** menu, press the **clear** key until the **Modem Test** option appears.



Test Mode
Modem Test

2. Press the **enter** key to select the modem test. The terminal prompts you to start the test (**Press Enter to Test**).



Test Modem Host Echo
Press Enter to Test

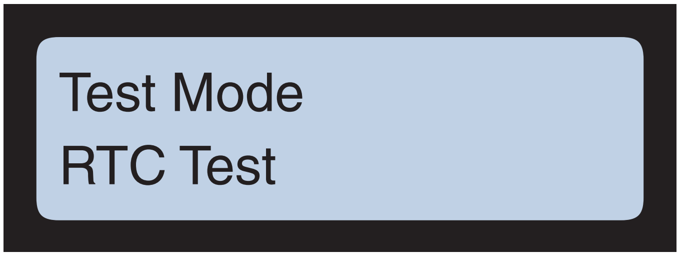
3. Press the **enter** key to start the test. The terminal displays the result when the test is complete.

4. When you are finished press the **clear** key to exit the modem test and return to the **Test Mode** menu (at the **RTC Test** option).

RTC Test

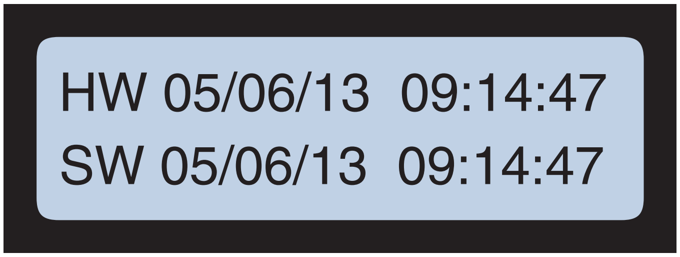
The RTC test checks the functionality of the Real Time Clock and beeps every second while flashing the “OK” LED during the test. Use the following procedure to run the RTC test:

1. In the **Test Mode** menu, press the **clear** key until the **RTC Test** option appears.



Test Mode
RTC Test

2. Press the **enter** key to start the RTC test. The terminal displays the RTC for the hardware and software and flashes the “OK” LED and beeps every second.



HW 05/06/13 09:14:47
SW 05/06/13 09:14:47

3. When you are finished press the **clear** key to stop the test and exit to the **Test Mode** menu (at the **DIDO Test 1** option).

GSM Signal Strength

This option only appears with a GSM / GPRS module installed and used primarily when installing a 5-meter antenna (see "GSM Long Cable Antenna" on page 2-14).

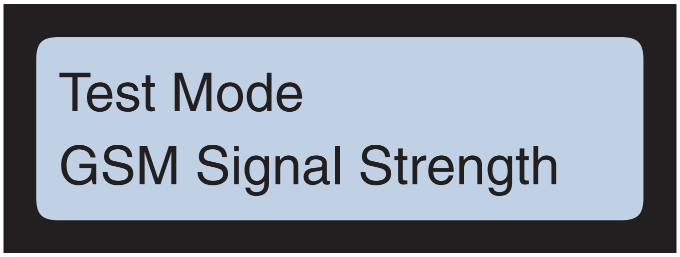
NOTE: This test will disconnect the terminal from the GSM/GPRS network for the duration of the test.

The test displays the signal strength of the cellular data network received by the GSM antenna. Move the terminal, antenna, or both to change the received signal strength. You need a signal strength of at least 15 for a GSM/GPRS terminal. Press the **clear** key to exit when finished.

NOTE: Signal strength measures from 0 to 32 with 15 or higher being best.

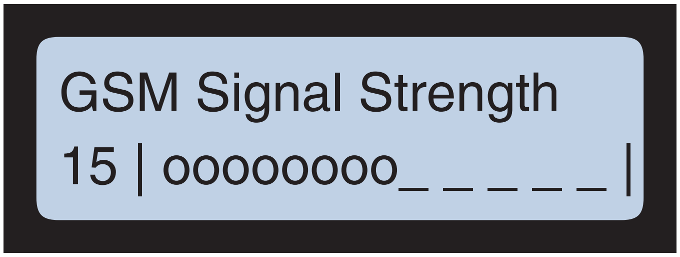
Use the following procedure to run the GSM Signal Strength test:

1. In the **Test Mode** menu, press the **clear** key until the **GSM Signal Strength** option appears.



```
Test Mode
GSM Signal Strength
```

2. Press the enter key to start the test. The display shows a numerical strength value on the left and a graphical representation of the strength to the right.



```
GSM Signal Strength
15 | oooooooo_ _ _ _ _ |
```

3. If desired, you can press the **enter** key to return to the GSM Signal Strength parameter (then press it again to restart the test).

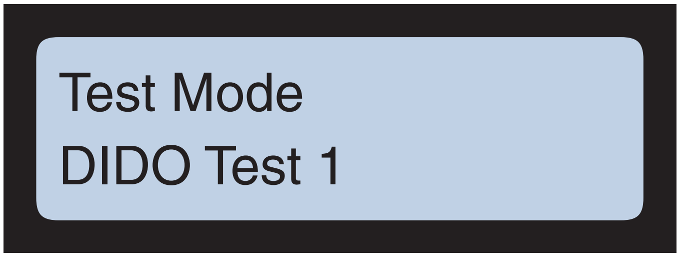
4. Press the **clear** key to exit to the **Test Mode** menu when finished.

DIDO Test 1

The DIDO test checks the functionality of the Data-In-Data-Out port on the terminal (also referred to as the Auxiliary Port). This test requires specific loopback “jumper” and is typically only performed by an ATS service technician. It’s noted here for reference purposes.

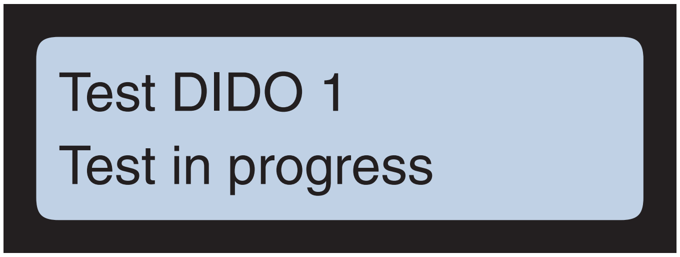
1. Insert the “loopback jumper” into the DIDO port on the terminal.

2. In the **Test Mode** menu, press the **clear** key until the **Test DIDO 1** option appears.



```
Test Mode
DIDO Test 1
```

3. Press the **enter** key to start the test. The terminal displays the result when the test is complete.



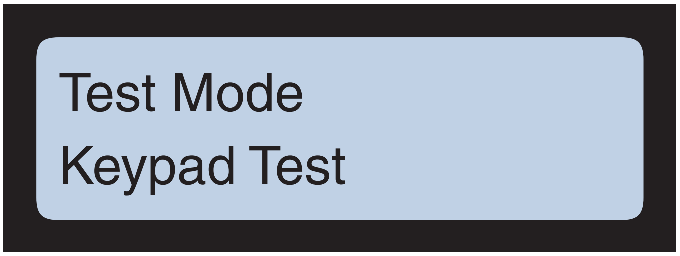
Test DIDO 1
Test in progress

4. When you are finished, press the **clear** key to exit and return to the start of the DIDO test. If you are finished, press the clear key to exit to the **Test Mode** menu (at the **Keypad Test** option). You may now remove the jumper from the terminal.

Keypad Test

The keypad test checks the functionality of the numeric and “alpha/function” keys on the keypad. Use the following procedure to test the keypad:

1. In the **Test Mode** menu, press the **clear** key until the **Keypad Test** option appears.



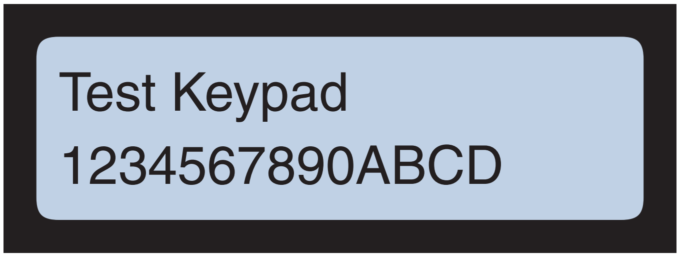
Test Mode
Keypad Test

2. Press the **enter** key to start the test.

3. Press the numeric keys in sequence from **1** to **9** then the **0** key. Next press the function keys in order (i.e., “F1” then “F2” and so forth to “F8”).

   If you press a button out of sequence, the terminal sounds an error tone and the “X / Error” LED illuminates for each incorrect press.

   If you press the buttons in sequence and the button functions correctly, the terminal confirms the key by displaying it on the screen while illuminating the “OK / check” LED for each correct key press.



Test Keypad
1234567890ABCD

4. If you pressed the keys in the correct sequence and all the keys are functioning correctly the test self-terminates and the system returns to the **Test Mode** menu (at the **DIDO Test 1** option).

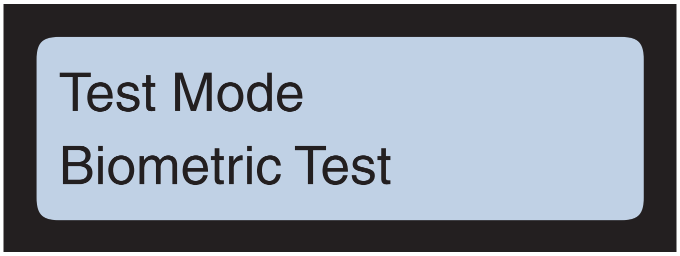
Biometric Test

The biometric test checks the functionality of an optional biometric fingerscan reader (if installed.

NOTE: If the terminal is not equipped with a biometric reader, this option does not appear in the **Test Mode** menu.

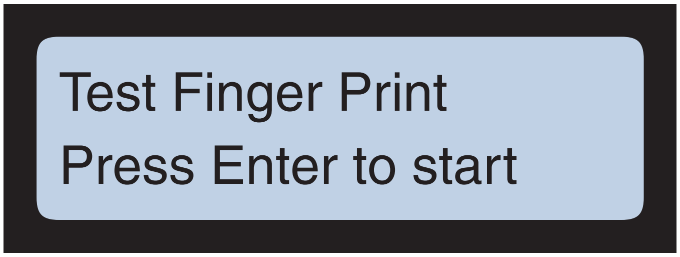
Use the following procedure to test an installed biometric fingerscan reader:

1. In the **Test Mode** menu, press the **clear** key until the **Biometric Test** option appears.



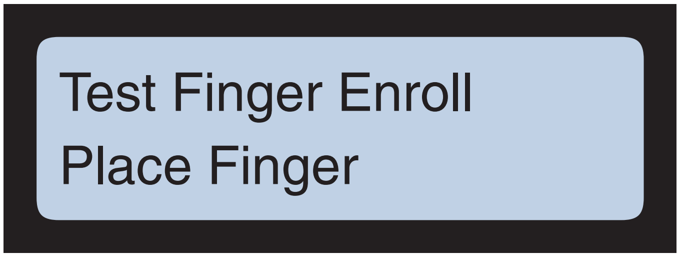
Test Mode
Biometric Test

2. Press the **enter** key to select the Biometric Test option. The terminal displays the **Test Finger Print** prompt.



Test Finger Print
Press Enter to start

3. Press the **enter** key to start the test. The system prompts you to place your finger on the reader.



Test Finger Enroll
Place Finger

4. Place your finger on the fingerscan reader sensor. The system scans your finger then displays the result when finished (e.g., **Enroll Score = 93**).

5. When you are finished, press the clear key to exit the biometric test and return to the start of the **Test Mode** menu (at the **Reader Test** option).

This page intentionally left blank.

Color Terminals

4

Chapter

About this Chapter

This section tells you how to use the color Maximus menus to set up your color terminal. (See Chapter 3, "Monochrome Terminals" to set up a monochrome Maximus.)

NOTE: If you have a Accu-Engine Serial terminal configured for Java programming, see the Advanced Development Manual for Accu-Time Terminals for additional information.

Chapter Contents

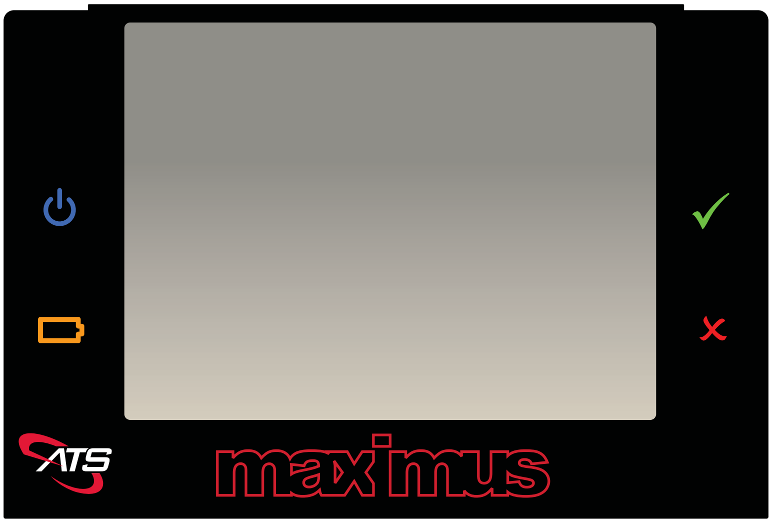
This chapter contains the following topics:

This page intentionally left blank.

Color Display

While the power and physical characteristics of a monochrome and color Maximus are the same, their setup menus are different. You can differentiate between the monochrome and color Maximus without turning on the terminal by looking at the lens. The color Maximus lens has a much larger window/LCD display than the monochrome lens. Figure 4-1 shows the color Maximus lens (see Figure 3-1 on page 3-3 for an illustration of the monochrome lens).

Figure 4-1 Color Maximus Lens

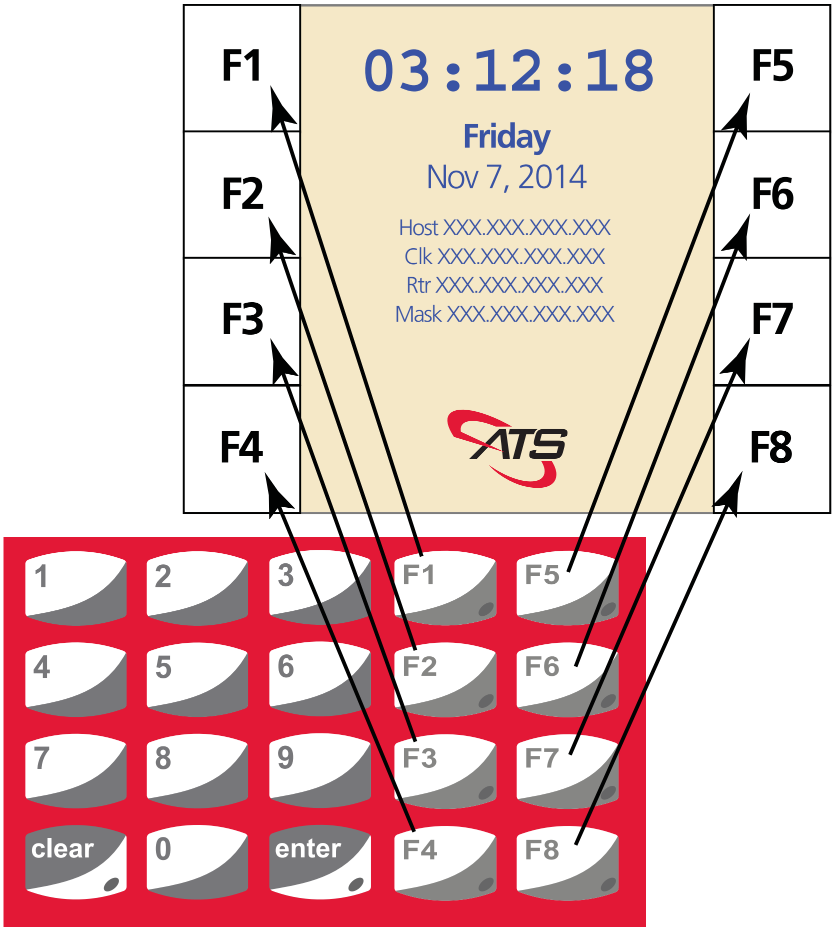


Using the Configuration Menu

The configuration menu lets you access some frequently used terminal functions. Figure 4-2 shows which function key corresponds to which menu selection.

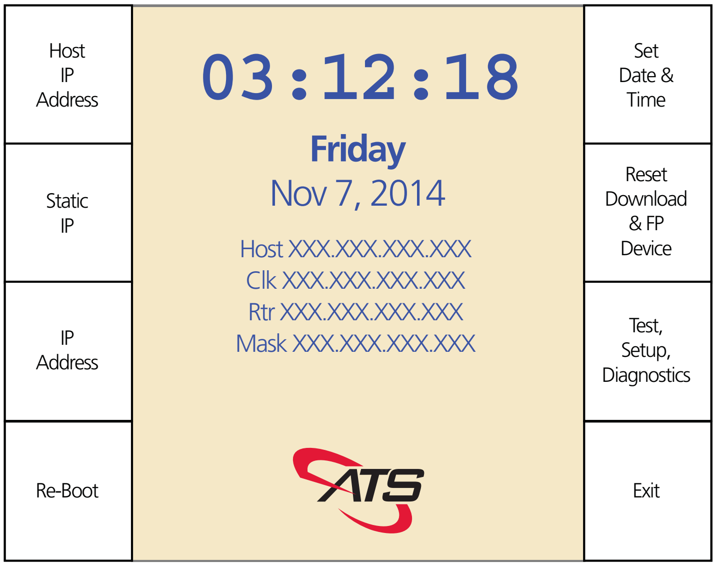
NOTE: The text on your keypad might not be the same as shown in Figure 4-2 (e.g., “In” instead of “F1”) but the positions and operation are the same.

Figure 4-2 Function Key Mapping to Configuration Menu Navigation



The Main Menu displays the selections you can make. To choose a selection, press the corresponding function button on the terminal. For example, if you compare Figure 4-3 and Figure 4-2, **F4** selects **Re-Boot**.

Figure 4-3 Color Maximus Configuration Menu (Initial Setup Menu Shown)



03:12:18

Friday

Nov 7, 2014

Host XXX.XXX.XXX.XXX

Clk XXX.XXX.XXX.XXX

Rtr XXX.XXX.XXX.XXX

Mask XXX.XXX.XXX.XXX

Initial Setup

The Initial Setup Menu, shown in Figure 4-3 on page 4-5, enables you to configure the basic parameters to quickly connect your Maximus to its host/network and to access other menus. Simultaneously press and hold down the **clear** and **enter** keys for about five seconds (and enter the password if prompted for it) to launch the Initial Setup menu.

NOTE: Maximus terminals leave the factory without a password to enter the configuration menus. You can set a password via the Setup menu as described in "Set Password" on page 4-17.

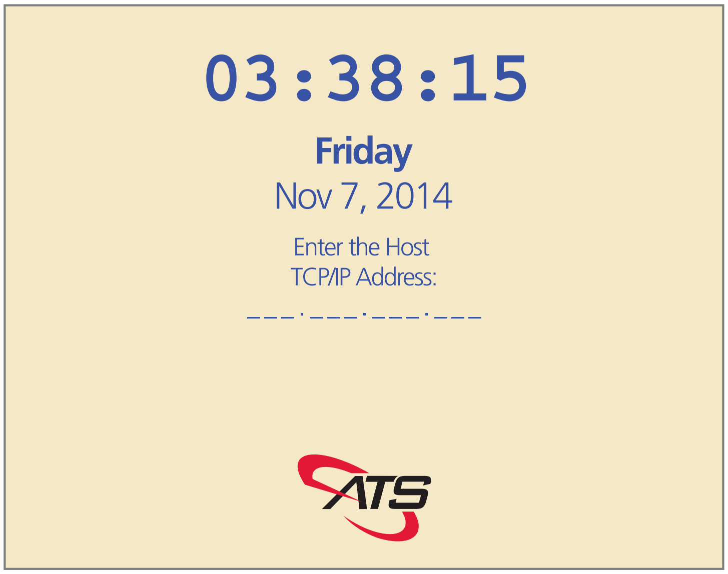
Initial Setup Menu Parameters

The following sections describe the Initial Setup Menu parameters (the Initial Setup Menu screen is shown in Figure 4-3 on page 4-5).

Host IP Address

This sets the IP address of the computer with which the terminal communicates. Press the "F1" key to select the **Host IP Address** parameter. The screen prompts you to enter an IP address for the host as shown in Figure 4-4.

Figure 4-4 Host IP Address Prompt (Initial Setup)



03:38:15

Friday

Nov 7, 2014

Enter the Host
TCP/IP Address:

___.___.___.___

NOTE: The IP selections display when host type is serial mode as well as when host type is Ethernet. If host type is serial, these settings are ignored. For more information, see "Host Type" on page 4-15.

Static IP / Dynamic DHCP

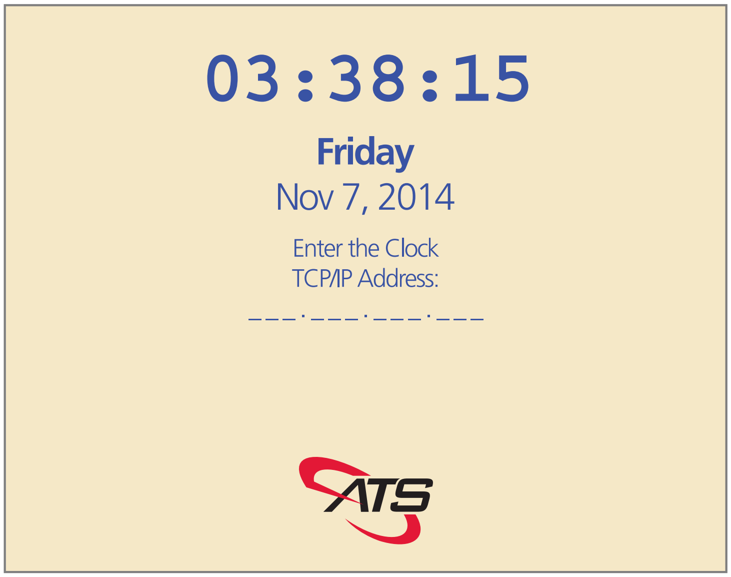
This parameter enables you to switch the IP mode of the Maximus terminal. When set to **Static IP**, the IP address of the terminal is fixed. Use the **IP Address** parameter to set a static IP address for the terminal (described in the following section). When set to **Dynamic DHCP**, the IP address of the terminal is determined by the DHCP server on the local network. The IP address of the terminal might change periodically, based on what the DHCP server assigns.

Use the “F2” key to toggle between **Static IP** and **Dynamic DHCP**. If you set the terminal to **Static IP** the Initial Setup menu displays the **IP Address** parameter that enables you to set the static IP address for the Maximus (described in the following section).

IP Address

The Initial Setup menu displays this parameter when set to **Static IP** (not available when set to **Dynamic DHCP**). It enables you to set a Static IP for the terminal (clock). If displayed, press the “F3” key to select the **IP Address** parameter. The screen prompts you to enter an IP address for the clock (terminal) as shown in Figure 4-5.

Figure 4-5 Clock (Terminal) IP Address Prompt (Initial Setup)



03:38:15

Friday

Nov 7, 2014

Enter the Clock
TCP/IP Address:

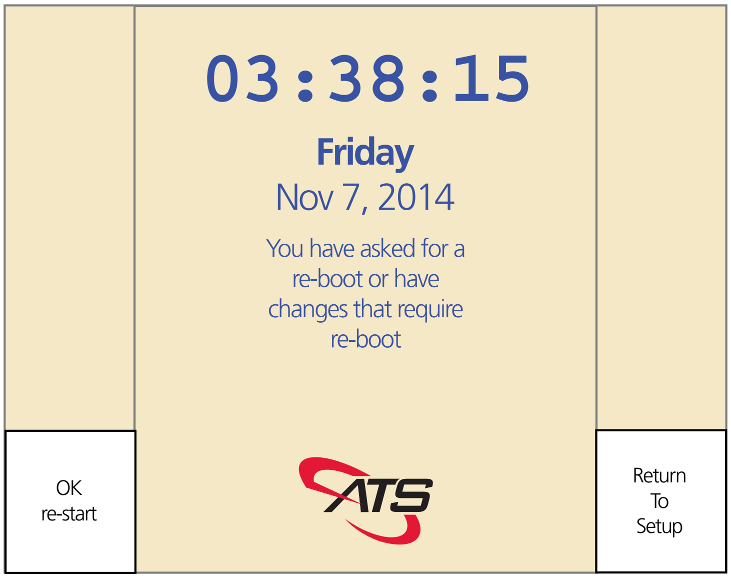
___.___.___.___

NOTE: Make sure you do not use the same IP address more than once on the network, as doing so can result in communication conflicts.

Re-Boot

Press the “F4” key to select the **Re-Boot** parameter. The system will prompt you to confirm as shown in Figure 4-6.

Figure 4-6 Reboot Confirmation Window



03:38:15

Friday

Nov 7, 2014

You have asked for a re-boot or have changes that require re-boot

The Reboot Confirmation window provides two options:

- Press the “F4” key to select **OK Re-start**. Selecting this option reboots the terminal and applies any changes you have made.
- Press the “F8” key to select **Return to Setup**. Selecting this option places the terminal in setup mode (described in "Setup Mode" on page 4-15).

NOTE: To return to the Initial Setup Menu, simultaneously press and hold down the **clear** and **enter** keys for about five seconds (and enter the password if prompted for it).

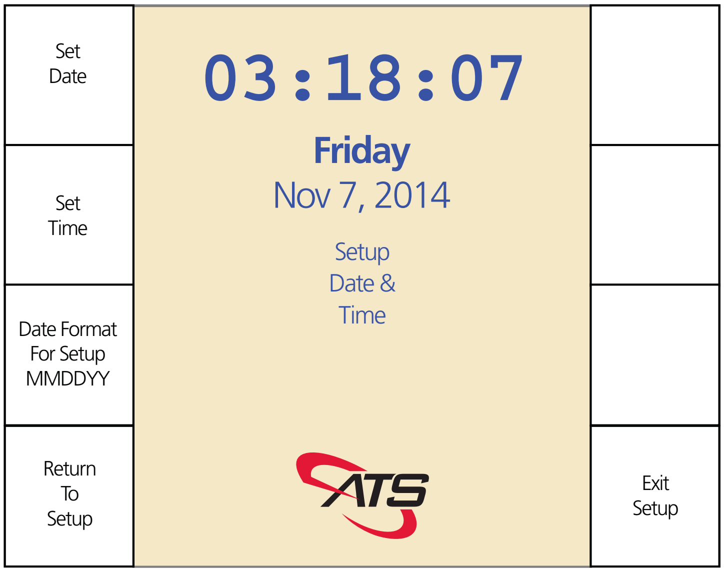
NOTE: There is a reset switch that you can push to reboot a terminal, as well. Use this switch if you cannot access the Re-Boot option in the terminal’s menu. This switch is called out in Figure 2-10 on page 2-11.

Set Date & Time

The **Set Date & Time** parameter enables you to manually set the current date, current time, and the date format used by the terminal. Press the "F5" key to access the Set Date & Time options screen as shown in Figure 4-7.

NOTE: The system has a timeout period for setting the date and time that automatically returns to the Setup Date & Time screen if the timer expires before a key press. If you enter invalid numbers or enter numbers when the timeout expires, an error message appears.

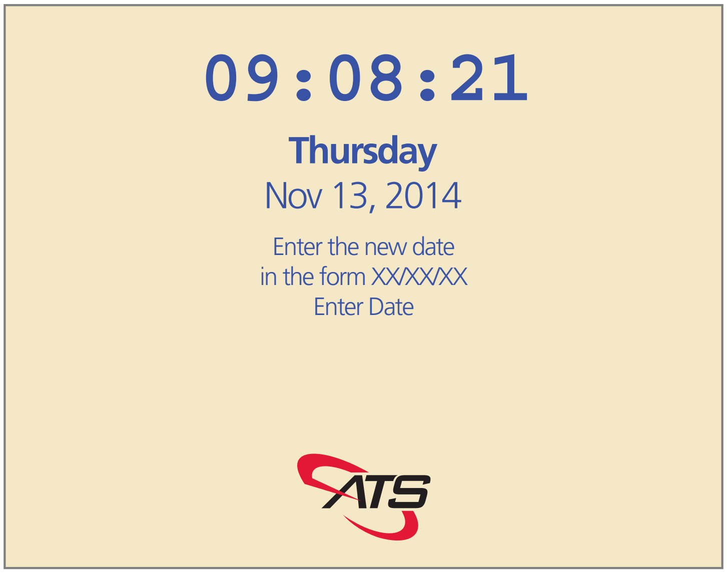
Figure 4-7 Setup Date & Time Options Screen



The following are descriptions of the Setup Date & Time options:

- **Set Date** – Press the "F1" key to display the **Enter Date** prompt screen as shown in Figure 4-8. Use the numbers on the terminal keypad to enter a new date then press the **enter** key. The date uses the selected date format as defined by the **DateFormat For Setup** parameter.

Figure 4-8 Enter Date Prompt Screen



09:08:21

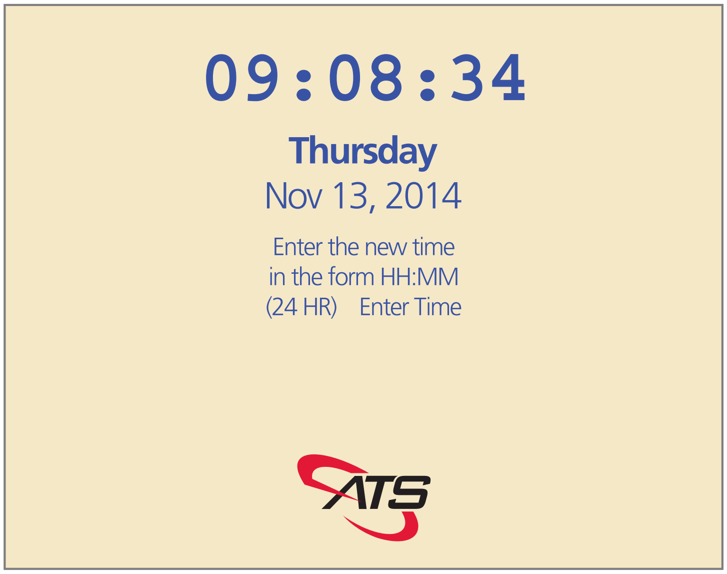
Thursday

Nov 13, 2014

Enter the new date
in the form XX/XX/XX
Enter Date

- **Set Time** – Press the "F2" key to display the **Enter Time** prompt screen as shown in Figure 4-9. Use the numbers on the terminal keypad to enter a new time then press the **enter** key. Use a 24-hour format to enter the time even if the terminal displays time in 12-hour format (e.g., key in 2105 for 9:05 PM).

Figure 4-9 Enter Time Prompt Screen



09:08:34

Thursday

Nov 13, 2014

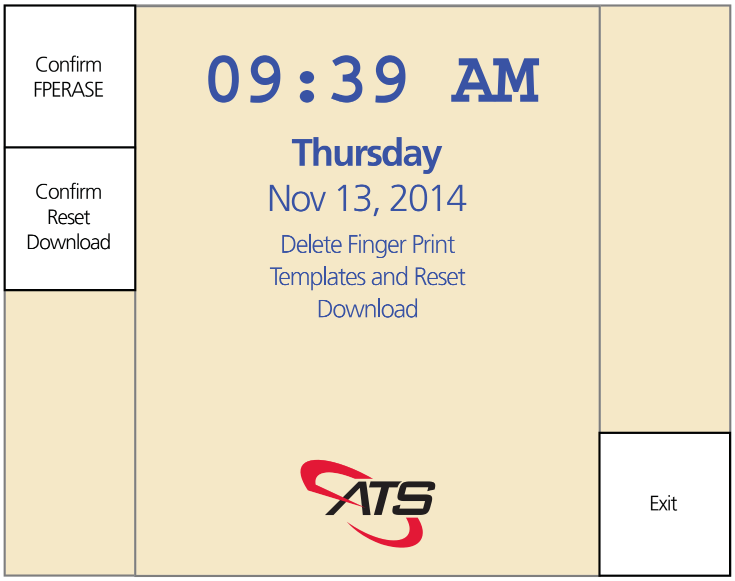
Enter the new time
in the form HH:MM
(24 HR) Enter Time

- **DateFormat For Setup**– Press the “F3” key to cycle through **MMDDYY**, **DDMMYY**, or **YYMMDD** for the date format. The selected format displays in real time on the option field.
- **Return To Setup** – Press the “F4” key to exit the **Set Date & Time** and **Initial Setup** menus and go directly to **Setup Mode**. See "Setup Mode" on page 4-15 for more information.
- **Exit Setup** – Press the “F8” key to exit the **Set Date & Time** and **Initial Setup** menus and display the reboot confirmation window as shown in "Reboot Confirmation Window" on page 4-8. The reboot confirmation window provides two options:
    - Press the “F4” key to select **OK Re-start**. Selecting this option reboots the terminal and applies any changes you have made.
    - Press the “F8” key to select **Return to Setup**. Selecting this option places the terminal in setup mode (described in "Setup Mode" on page 4-15).

Reset Download & FP Device

Press the “F6” key to access the **Reset Download & FP Device** confirmation screen as shown in Figure 4-10.

Figure 4-10 Delete Finger Print Templates and Reset Download Confirmation Screen



The options are:

- **Confirm FPERASE** - Press the “F1” key to reboot the Maximus terminal and erase all fingerscan templates. If the Maximus is not equipped with a biometric finger scan device or it is not configured in the **Setup Menu** (see "Device Setup" on page 4-16), the **Confirm FPERASE** option is disabled and the label reads **No FP Device**.

- **Confirm Reset Download** - Press the “F2” key to reboot the Maximus terminal and clear the terminal memory, including all prompts and data in any queues. After you reset the download, you need to download parameters to the terminal to make it functional.
- **Exit** - Press the “F8” key to exit the he **Delete Finger Print Templates and Reset Download** confirmation screen and return to the Initial Setup menu screen (as shown in Figure 4-3 on page 4-5).

Test Setup Diagnostics

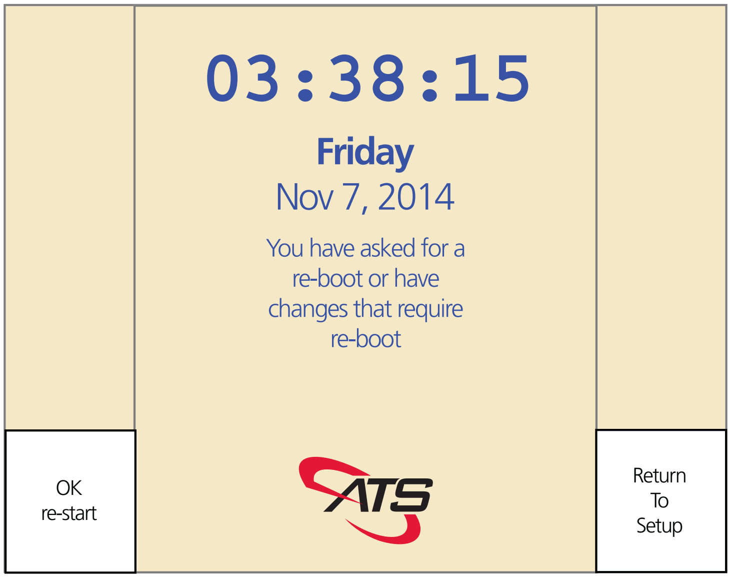
Press the “F7” key to exit the Initial Setup menu and go to the TSD mode screen (Test, Setup, Diagnostics) as shown in Figure 4-12 on page 4-13. This screen also enables you to access the Information Mode, the **Download from USB** command, and the **Restore Factory Settings** command. For more information, see "Test, Setup, Diagnostics (TSD) Menu" on page 4-13.

Exit

Press the “F8” key to access the re-boot confirmation window as shown in Figure 4-11. The options on the screen are:

- Press the “F4” key to select **OK re-start** and re-boot the Maximus terminal (saving any changes).
- Press the “F8” key to select **Return to Setup**. Selecting this option places the terminal in setup mode (described in "Setup Mode" on page 4-15).

Figure 4-11 Reboot Confirmation Window



03:38:15

Friday

Nov 7, 2014

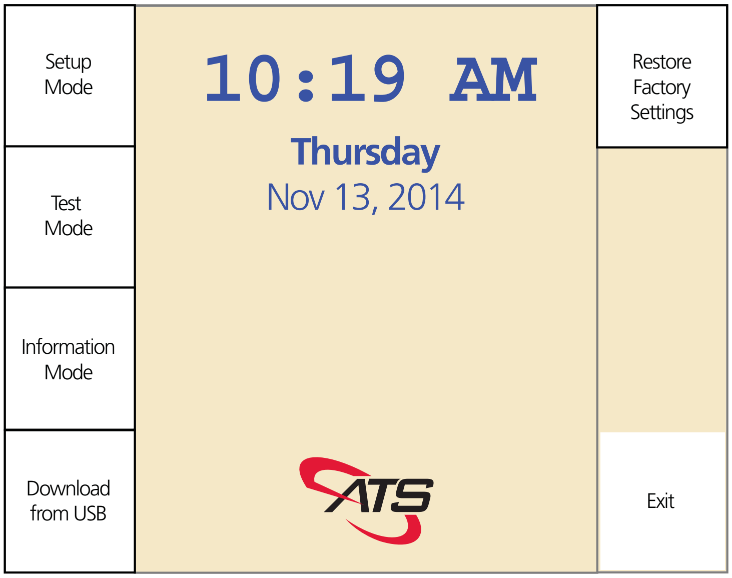
You have asked for a re-boot or have changes that require re-boot

Test, Setup, Diagnostics (TSD) Menu

The **Test, Setup, Diagnostics** menu enables you to access **Test Mode**, **Setup Mode**, **Information Mode**, the **Restore Factory Settings** command, and **Download from USB** command.

Press the "F7" key, when in the Initial Setup Menu screen (shown in Figure 4-3 on page 4-5), to open the **Test, Setup, Diagnostics** screen as shown in Figure 4-12.

Figure 4-12 Test Setup Diagnostics Menu



The TSD Screen provides access to the following selections:

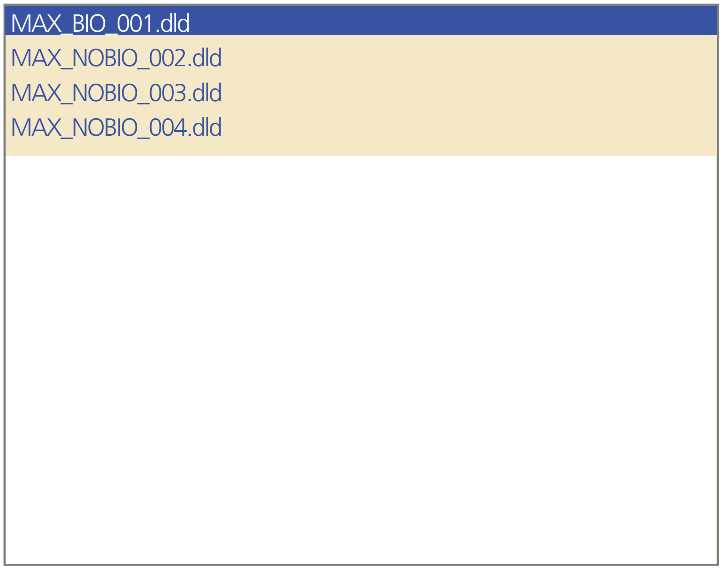
- **Setup Mode** – Setup Mode ("F1" key) provides access to all the configuration settings for the Maximus terminal (except for factory/service only settings). See "Setup Mode" on page 4-15 for a complete description of Setup Mode.
- **Test Mode** – Test Mode ("F2" key) provides access to the terminal built-in self tests. See "Test Mode" on page 4-30for a complete description of Test Mode.
- **Information Mode** – Information Mode ("F3" key) enables you to view the current settings and conditions on the Maximus Terminal. See "Information Mode" on page 4-34 for a complete description of Information Mode.

Download from USB – The **Download from USB** command ("F4" key) enables you to install downloads (applications) to the Maximus terminal from a USB flash drive. With a USB flash drive that contains download files (*.dld) installed in the Maximus USB port, press the "F4" key to access the download selection screen as shown in Figure 4-13 on page 4-14. Use the "F7" and "F8" keys to scroll between multiple download files (if applicable). With the desired download file highlighted, press the **enter** key to install the download file/application on the Maximus terminal.

NOTE: Ensure the desired download file is present on the USB flash drive before entering the download selection screen. Once you enter the list the terminal will install a download if one is present. You won't be able to exit without installing a download if one is on the flash drive (both the clear and enter keys install the highlighted download file). If you are forced to install an undesired download file, you can remove it using the **Reset Download** command as described on "Reset Download & FP Device" on page 4-11.

For more information about the USB see Appendix C, "Using the USB". For more information about the UCS applications (downloads and *.dld files) see the Universal Command Set Manual, MANU-UCS-01.

Figure 4-13 Selecting a Download File



MAX_BIO_001.dld
MAX_NOBIO_002.dld
MAX_NOBIO_003.dld
MAX_NOBIO_004.dld

- **Restore Factory Settings** - This function is reserved for specific applications. In typical Maximus configurations pressing the "F5" key to select **Restore Factory Settings** command results in the "**Unable to Restore Settings"** response.
- **Exit** – Press the "F8" key to go to the Reboot Confirmation Window as shown in Figure 4-11 on page 4-12. If you select **Return To Setup** ("F8" key) on the Reboot Confirmation Window you will proceed to Setup Mode (see "Setup Mode" on page 4-15 for more information). If you select **OK Re-start** ("F4" key) the system reboots.

Setup Mode

Use setup mode to configure the terminal, including setting serial or Ethernet host and parameters.

To enter setup mode, press the"F1" key to select **Setup Mode** when in the **Test, Setup, And Diagnostics** screen (see "Test Setup Diagnostics" on page 4-12). You can also enter Setup Mode by selecting **Exit Setup** (in multiple screens) then **Return To Setup** (from the Reboot Confirmation Window).

Setup mode has two screens, one for serial host setup and the other for Ethernet setup (see Figure 4-14 on page 4-15 and Figure 4-15 on page 4-16).

Host Type

Press the "F1" function key to toggle between **Host Type Serial** (see Figure 4-14) and **Host Type Ethernet** (see Figure 4-15). For more information, see either "Ethernet Setup" on page 4-22 and "Serial Setup" on page 4-18.

Figure 4-14 Setup Mode, Main Menu Screen – Host Type Serial

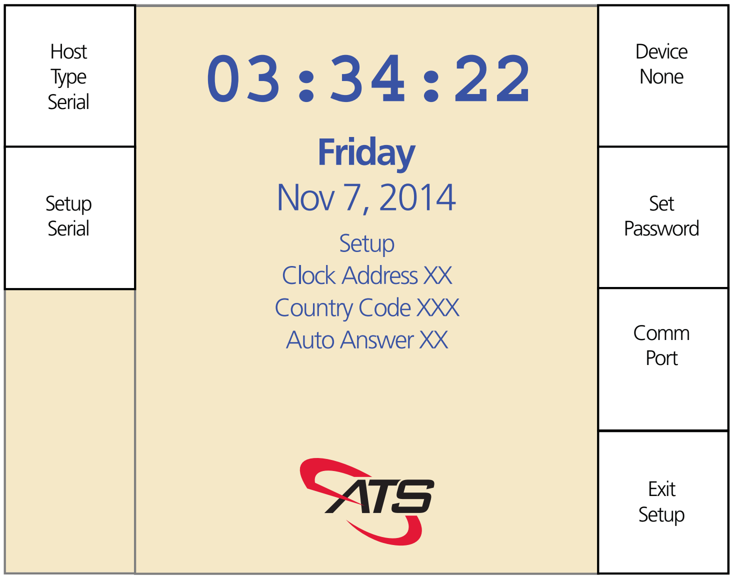
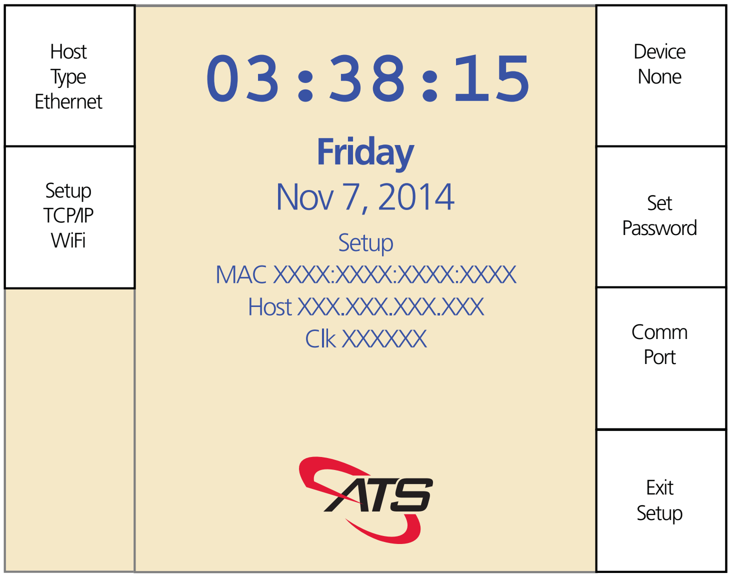


Figure 4-15 Setup Mode, Main Menu Screen – Host Type Ethernet



Common Settings

Several settings are common to both serial and Ethernet host types. This section lists those options and provides a description of each.

Device Setup

The **Device Setup** parameter enables you to setup the type of biometric fingerscan reader installed on the terminal. The options are:

- **Device None** - Select this option if your Maximus terminal is not equipped with a biometric fingerscan reader (or if you are not sure which reader is installed).
- **Fingerprint Cogent Verify** - Select this option if your Maximus terminal is equipped with a Cogent reader and you want it to operate in Verification Mode.
- **Fingerprint Cogent Identify** - Select this option if your Maximus terminal is equipped with a Cogent reader and you want it to operate in Identification Mode
- **Fingerprint Bioscrypt** - Select this option if your Maximus terminal is equipped with a Bioscrypt reader.
- **Fingerprint Suprema Verify** - Select this option if your Maximus terminal is equipped with a Suprema reader and you want it to operate in Verification Mode.
- **Fingerprint Suprema Identify** - Select this option if your Maximus terminal is equipped with a Suprema reader and you want it to operate in Identification Mode.

- **Fingerprint Lumidigm Verify** - Select this option if your Maximus terminal is equipped with a Lumidigm (Accu-Touch) reader and you want it to operate in Verification Mode.
- **Fingerprint Lumidigm ID 500x2** - Select this option if your Maximus terminal is equipped with a Lumidigm reader and you want it to operate in Identification Mode with two templates per user (with a maximum of 500 users).
- **Fingerprint Lumidigm ID 1Kx1** - Select this option if your Maximus terminal is equipped with a Lumidigm reader and you want it to operate in Identification Mode with one template per user (with a maximum of 1000 users).
- **Finger Geometry** - Do not select the **Finger Geometry** option. The Maximus does not support finger geometry readers. The **Finger Geometry** option is removed from Firmware Version 2.05.17(X) and greater.

NOTE: You must select the correct type of device installed in your terminal (or **Device None**). If you select an incorrect device type the terminal will continually reboot as it searches for the selected device type.

Do not let the system “time out” with an incorrect option highlighted unless it is **Device None**. If you’re unsure what device is installed in your Maximus scroll to **Device None** so that it is highlighted.

Set Password

Initially, there is no password set for the terminal, and there is no restriction on access to the setup functions. Use **Set Password** to set a numeric password of up to seven digits for access to the terminal setup screens.

NOTE: If you set a password, be sure to record the value in a safe place. If you lose the password, you cannot change the terminal setup.
(If you encounter this problem, contact ATS for recovery assistance.)

Use the following procedure to set a password:

1. Press the “F6”key to select **Set Password**.
2. At the **Enter New Password** prompt, type a new password up to seven digits long.
3. After you type the password, press the **enter** key to apply the password.
4. At the **Confirm Password** prompt, type the same password you just entered then press the **enter** key.
5. Press the “F8” key to select **Exit Setup** then press the “F4” key to select **OK Re-Start** to reboot the terminal. The password becomes active after the reboot.

To clear the current password:

1. Press the “F6”key to select **Set Password** (in Setup Mode).

2. At the **Enter New Password** prompt press the **Enter** key without typing any numbers.

3. At the **Confirm Password** prompt press the **Enter** key without typing any numbers.

4. Press the “F8” key to select **Exit Setup** then press the “F4” key to select **OK Re-Start** to reboot the terminal. The password clears after the reboot.

Exit Setup

Press **Exit Setup** to leave setup mode. You have two choices:

- **OK Re-start** – Selecting this option (“F4” key) reboots the terminal and applies any changes you made.
- **Return To Setup** – Selecting this option (“F8” key) brings you to the Setup Mode, Main Menu screen.

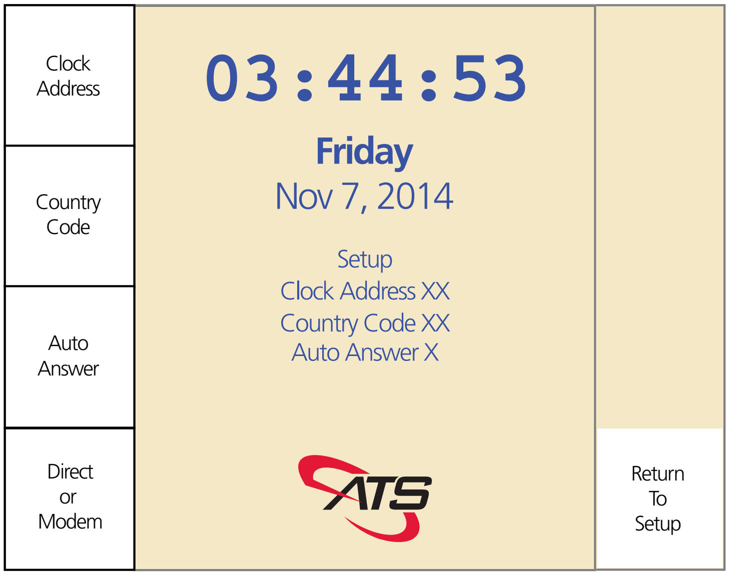
Serial Setup

The **Setup Serial** and **Comm Port** menus enable you to customize the serial connection setting for a Maximus connected to the host via a serial interface. Use the following procedure to configure the Maximus serial interface settings:

1. Press the “F1” key when in the Setup Mode Main Menu screen to toggle the terminal host type to **Host Type Serial** as shown in Figure 4-14 on page 4-15. If your Maximus connects directly to the serial device (not via a modem) proceed to Step 6. on page 4-19.

2. If the Maximus connects to a serial modem, press the “F2” key to select **Setup Serial**. The Serial Setup menu screen appears as shown in Figure 4-16.

Figure 4-16 Serial Setup Menu Screen



03:44:53

Friday

Nov 7, 2014

Setup
Clock Address XX
Country Code XX
Auto Answer X

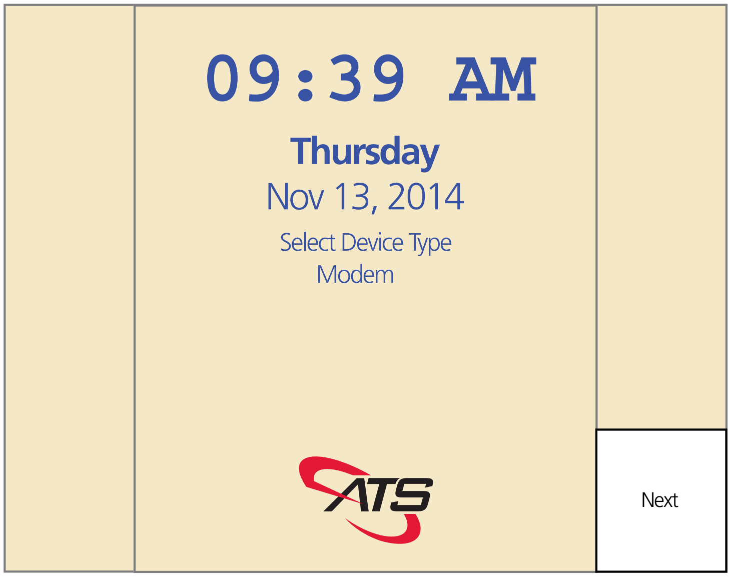
3. If the Maximus connects to a serial modem, press the “F1” key to select **Clock Address**. This parameter enables you to enter a number from 01–99 using the numeric keys with the value displayed in the enter of the screen. You can press the “**clear**” key to delete a number. With the desired number displayed, press the “**enter**” key to accept the number. This selection does not time out.

4. If the Maximus connects to a serial modem, press the “F2” key to select **Country Code**. This parameter enables you to enter a number from 00–FF using the numeric keys for numbers and the function keys for letters. The value is displayed in the enter of the screen. You can press the “**clear**” key to delete a number. With the desired number displayed, press the “**enter**” key to accept the number. This selection does not time out.

5. If the Maximus connects to a serial modem, press the “F3” key to select **Auto Answer**. This parameter enables you to select **1 Ring**, **2 Rings**, **3 Rings**, or **None** (no rings) by pressing the “F3” key to scroll through the options that are displayed in the center of the screen.

6. The **Direct Or Modem** parameter enables you select if the Maximus connects to the host using a serial modem or if it connects directly using a serial cable. The center of the screen shows the current setting (**Direct** or **Modem**) in the **Serial Setup:** field. If you want to change the displayed setting, press the “F4” key to select **Direct Or Modem** and display the **Select Device Type** screen (shown in Figure 4-17) then press the “F8” key to select **Next** (this changes the setting). If you pressed the “F8” key and the Select Device Type screen displays the desired setting, press the **clear** key to return to the Serial Setup menu screen without changing the setting.

Figure 4-17 Select Device Type Screen (Shown with Modem Option Selected)



09:39 AM

Thursday

Nov 13, 2014

Select Device Type

Modem

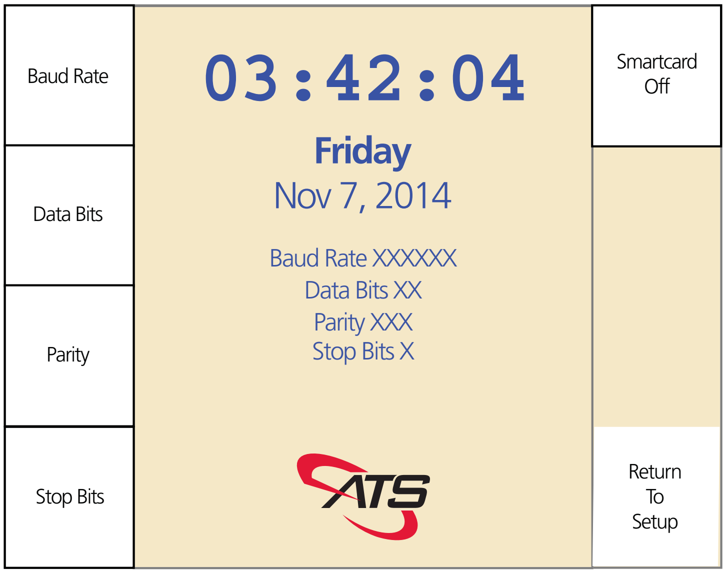
7. If the Maximus connects to a serial modem, press the"F2" key to select appropriate **Country Code** for your modem (e.g., the T.35/D1/J1 country code for the United States is B5 while the S1 code is 22). This parameter enables you to enter a number from 00–FF using the numeric keys for numbers and the function keys for letters. The value is displayed in the enter of the screen. You can press the "**clear**" key to delete a number. With the desired number displayed, press the "**enter**" key to accept the number. This selection does not time out.

8. Press the "F8" key to select **Return To Setup**. Selecting this option returns you to the Setup Mode, Main Menu Screen – Host Type Serial (see Figure 4-14 on page 4-15).

Comm Port

The Comm Port menu enables you to configure the serial communication port settings. These settings must match the communication software and hardware you are using to connect to the terminal. Press "F7" from the "Setup Mode, Main Menu Screen, Host Type Serial screen" (see Figure 4-14 on page 4-15) to access the Comm Port menu screen as shown in Figure 4-18.

Figure 4-18 Comm Port Menu Screen



03:42:04

Friday

Nov 7, 2014

Baud Rate XXXXXX

Data Bits XX

Parity XXX

Stop Bits X

Use the following procedure to configure the serial communications settings:

1. To change the **Baud Rate** press the “F1” key to scroll through the available rates. The currently selected value displays in the middle of the screen. The default value is **9600** baud. The options are **1200**, **4800**, **9600**, **19200**, **38400**, **57600**, and **115200** baud (bps).

2. To change the value for the **Data Bits** parameter press the “F2” key to toggle the data bits between **7** and **8**. The currently selected value displays in the middle of the screen. The default value is **7** data bits.

3. To change the value for the **Parity** parameter, press the “F3” key to scroll between the parity options of **odd**, **even**, and **none**. The currently selected value displays in the middle of the screen. The default value is **odd**.

4. **T**o change the value for the **Stop Bits** parameter, press the “F4” key to toggle between **1** or **2** stop bits. The currently selected value displays in the middle of the screen. The default value is **2** stop bits.

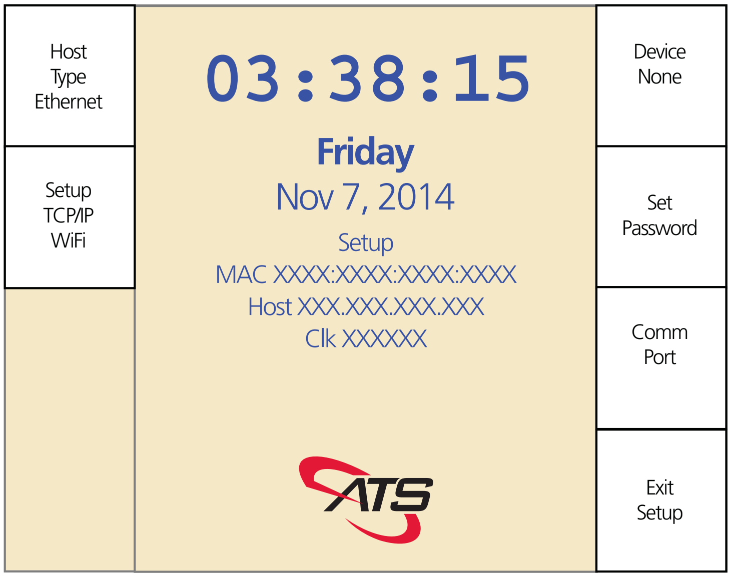
5. **T**o change the value for the **Smartcard**, press the “F5” key to scroll between **off**, **1k** or **4k**. The currently selected value displays in the middle of the screen. Set this selection to match the storage capacity of an installed smartcard or set it to **off** if the Maximus is not equipped with a smartcard.

6. Press the “F8” key to select **Return To Setup** and go to the Setup Mode Main Menu screen.

Ethernet Setup

The **Setup TCP/IP WiFi** and associated sub-menus enable you to customize the Ethernet and WiFi settings for a Maximus connected to the host via an Ethernet interface.

Figure 4-19 Ethernet Setup Screen – Ethernet Host Type



03:38:15

Friday

Nov 7, 2014

Setup

MAC XXXX:XXXX:XXXX:XXXX

Host XXX.XXX.XXX.XXX

Clk XXXXXX

Use the following procedure too set up Ethernet host type:

1. Use the “F1” key to toggle the host type setting to **Host Type Ethernet** (if the screen displays **Host Type Serial**).

2. Press the “F2” key to select **Setup TCP/IP Wifi**. The TCP/IP Setup screen appears (for either Dynamic mode as shown in Figure 4-21 on page 4-26 or Static mode as shown in Figure 4-22 on page 4-27). The TCP/IP Setup screen enables you to specify the parameters for the Maximus Ethernet connection.

3. On the TCP/IP Setup screen, use the “F1” key to select between **TCP/IP Client** and **TCP/IP Server**. In client mode, the terminal makes the TCP/IP connection to the designated host computer. When in this mode, the terminal does not accept a connection request from any outside device.

   In server mode, the terminal awaits a connection initiated by the host as follows:

   - The terminal waits for a host server to initiate a connection. The terminal does not attempt to connect to any host server, so it is the responsibility of the host server to make the connection request with a terminal. The terminal is set up to accept a single connection that can come from any host.
   - A terminal connection needs to be maintained only when the host server needs to, which reduces network traffic, such as Keep Alives.

- You can change the host server without needing to set up your terminals.
- Since any host on the network can try to make a connection with the terminal, any host that knows how to communicate with the terminal can read data from the terminal.

4. The terminal displays the current Socket Port setting in the center of the screen. The default value is **2500**. To change the displayed value:

   - Press the “F5” key to select **Socket Port** and display the **Enter the Socket Port** prompt screen.
   - Use the numeric keys to type the new socket port number, up to five digits (You can press the “**clear**” key to delete a number) then press the **enter** key to apply the socket port change. The terminal returns to the TCP/IP Setup screen and displays the new value for the **Socket Port** field in the center of the screen.
     If you type an invalid socket port number the terminal displays **Invalid Socket Port** and returns you to the saved/default value.

5. **Append EOT Yes** adds an end-of-transmission (EOT) character to the end of the communication packet. The default value is **Append EOT No**. Turning this option on helps to eliminate the possibility of large packets being lost. There are some networks that limit the size of a packet that can be transmitted between devices. The **Append EOT No** selection does not add (append) EOT numbers.

CAUTION

*Set “**Append EOT”** to **No** unless your communication software or networking software specifically support EOT (End Of Transmission).*
*If you set this to **Append EOT Yes** and EOT is unsupported, the terminal could behave unpredictably, including not responding to input.*

To change the displayed Append EOT value, press the “F6” key to select between **Append EOT No** and **Append EOT Yes**.

6. To change between **Dynamic DHCP** and **Static IP** modes press the “F2” key. If you selected **Dynamic DHCP**, proceed to "Dynamic Mode Settings" on page 4-25. If you selected Static IP proceed to "Static Mode Settings" on page 4-26.

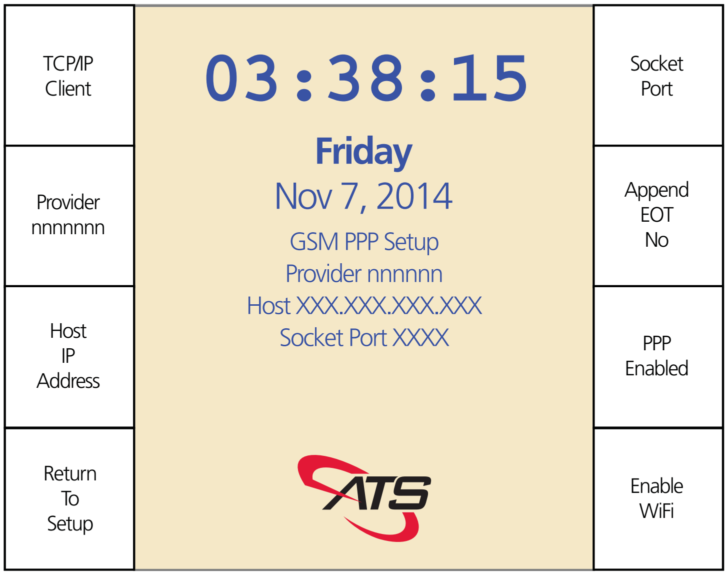
7. You can use the “F7” key to select between **PPP Disabled** and **PPP Enabled**.
   WiFi must be disabled before you can enable PPP.
   Use **PPP Enabled** to set up a GSM/GPRS terminal PPP communication for connectivity with a host server over a cellular wireless data network.
   To set up for GSM/GPRS support, you need a GSM/GPRS-modem-equipped terminal and a data plan from a wireless carrier.
   When you set this parameter to **PPP Enabled**, the **GSM PPP Setup** screen appears as shown in Figure 2 on page 4-24 with the current settings displayed in the center of the screen.

   To change the GSM / GPRS provider press the “F2” key to cycle through the provider options. The available providers are; **stream**, **proximus**, **o2**, **etisalat**, **datalink**, **att-gold**, **att**, **ats-tm**, **O2UK**, **ATS-t-mobil**, **Wlogic-ATT**, **wlogic**, **AIS**, **vodafoneUK**, **vodafone**, **vodacom**, **vodaPAYG**, **telenor**, **t-mobil-uk**, **t-mobile**.

In addition, the **GSM PPP Setup** screen displays the GSM/GPRS Host IP address in the center of the screen (the IP address of a public-facing server that communicates with the terminal using the wireless data network). To change this IP address, press the “F3” key to select **Host IP Address** and go to the **Enter the Host TCP/IP Address** prompt screen.

Use the numeric keys to type the new Host IP address (You can press the “**clear**” key to delete a number) then press the **enter** key to apply the change. The terminal returns to the **GSM PPP Setup** screen and displays the new value for the **Host IP Address** in the center of the screen.

Figure 4-20 GSM PPP Setup Screen



03:38:15

Friday

Nov 7, 2014

GSM PPP Setup

Provider nnnnnn

Host XXX.XXX.XXX.XXX

Socket Port XXXX

Configuring WiFi

1. To configure the WiFi interface (if installed), press the “F8” key to select **Setup WiFi**. PPP must be disabled before you can enable WiFi. The center of the screen displays the WiFi Signal and Version.
   For more information on setting up GSM/GPRS terminals, see Appendix D, "GSM/GPRS Setup".

2. Select **Next** (“F8” key). The center of the screen displays the **Set SSID** prompt. Press the enter key to set the SSID. This will enable WiFi (if disabled). The center of the screen displays the Set SSID prompt. Use the numeric keys for numbers and the function keys for letters to define the SSID. Press the enter key when finished.

3. The center of the screen displays the **Set Type of Security** prompt. Press the enter key to set the security protocol type. Select Next ("F8" key) or use the clear key to scroll between the **WPA2**, **WPA**, **WEP**, and **None** options. When the terminal displays the desired option, press the **enter** key to set the encryption type.

NOTE:

We recommend using the **WPA2** security protocol.
WEP has many security flaws and is easily broken.
WPA was introduced as an interim security enhancement over WEP and uses Temporal Key Integrity Protocol (TKIP) which is not secure and vulnerable to attack.

If the terminal is set to **WPA2** it may not connect to routers set to WPA/WPA2 (mixed mode). It will connect to a router set to "WPA2 Personal".

4. The center of the screen displays the **Set Security Key** prompt. Press the enter key to set a security key (password). Use the numeric keys for numbers and the function keys for letters to define the security key (password). Press the enter key when finished. The center of the screen displays **Disable WiFi**.

5. If you want to diable the WiFi press the enter key at the **Disable WiFi** prompt. Press the clear key or select **Next** ("F8" key) to proceed while leaving WiFi enabled. The center of the screen displays **Exit WiFi Setup**.

6. Press the enter key if you want to exit the WiFi setup menu and return to the previous menu or select **Next** ("F8" key) to proceed. If you selected Next the center of the screen displays **Set Factory Defaults**.

7. If you want to return the WiFi interface to the factory default settings press the enter key (a confirmation prompt will appear). Otherwise you can select **Next** ("F8" key) to go to the start of the WiFi menu or select **Prev** ("F7" key) or the clear key to return to the **Exit WiFi Setup** prompt.

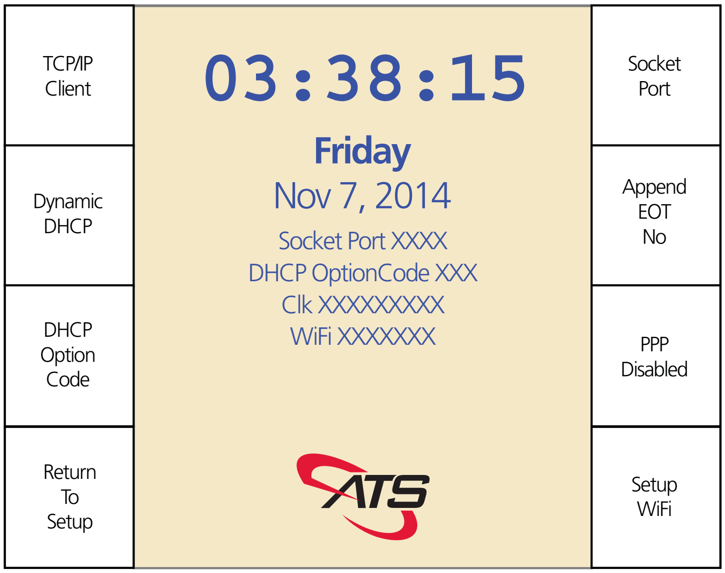
8. When you are finished, press the enter key to go back to the TCP/IP Setup screen.

9. When you are finished with the **Setup TCP/IP WiFi** menu select **Return To Setup** ("F4" key).

Dynamic Mode Settings

In DHCP mode, the IP address of the terminal is determined by the DHCP server on the local network. The IP address of the terminal might change periodically, based on the DHCP server. The center of the display shows the current DHCP settings.

Figure 4-21 TCP/IP Setup – Dynamic Mode



Use the following procedure to configure the Dynamic Mode Ethernet settings:

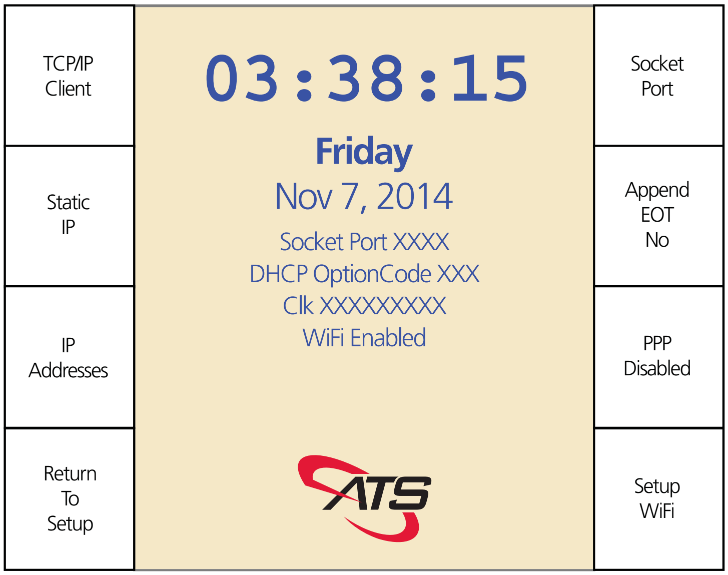
1. Press the “F3” key to select the **DHCP Option Code** parameter. At the **Enter the DHCP Option Code** prompt screen, use the numeric keys to type an option code then press the **enter** key (You can press the “**clear**” key to delete a number).
   The DHCP Option Code allows for customizable configurations beyond the standard DHCP options. Different option codes could be used to provide information to and from the terminal, provided the terminal is programmed to use the information and the DHCP server is configured to transmit the information.

   - Options 1–127 are reserved for definition by the Internet Assigned Numbers Authority (IANA) for public standardization. Some are used and some are not. For example, option 117 specifies the order in which name services should be consulted when resolving host name and other information.
   - Options in the range of 128–254 are user configurable and have no standard definition. For example, the terminal supports a list of up to five additional hosts that can be specified using the UCS command ENETHOST.
   - Alternatively, the terminal could send the DHCP server a DHCP request with option code 128, and if the server were configured appropriately, the server would respond with a list of hosts for the terminal to connect to.

Static Mode Settings

In static mode, the IP address of the terminal is entered at the terminal and does not change unless changed at the terminal. The center of the display shows the current socket port.

Figure 4-22 TCP/IP Setup – Static Mode



03:38:15

Friday

Nov 7, 2014

Socket Port XXXX

DHCP OptionCode XXX

Clk XXXXXXXXX

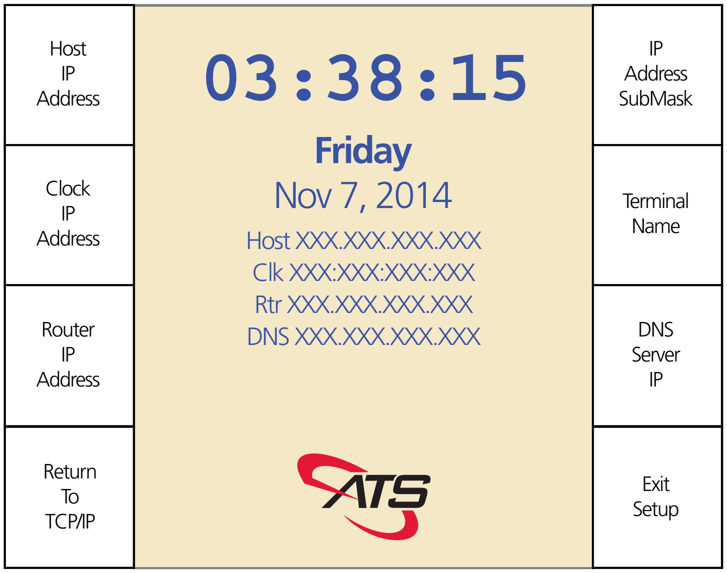
WiFi Enabled

Use the following procedure to configure the Static Mode Ethernet settings:

1. Press the “F3” key to select **IP Addresses** access the Secondary TCP/IP Setup screen (shown in Figure 4-23).
   The center of the Secondary TCP/IP Setup Screen displays:

   - **Host**: the host IP address.
   - **Clk**: the IP address for the terminal.
   - **Rtr**: the IP address for the “router” (Gateway).
   - **DNS**: The IP address of the DNS server.

Figure 4-23 Secondary TCP/IP Setup Screen, Static Mode



03:38:15

Friday

Nov 7, 2014

Host XXX.XXX.XXX.XXX
Clk XXX:XXX:XXX:XXX
Rtr XXX.XXX.XXX.XXX
DNS XXX.XXX.XXX.XXX

Use the following procedure to change the Static IP settings (if desired):

1. To change the Host IP address press the “F1” key to select the **Host IP Address** parameter and access the **Enter the Host TCP/IP Address** prompt screen. Use the numeric keys to type in the desired IP address then press the **enter** key to return to the Secondary TCP/IP Setup screen (You can press the “**clear**” key to delete a number).

2. To change the Maximus terminal (clock) IP address press the “F2” key to select the **Clock IP Address** parameter and to access the **Enter the Clock TCP/IP Address** prompt screen. Use the numeric keys to type in the desired IP address then press the **enter** key to return to the Secondary TCP/IP Setup screen (You can press the “**clear**” key to delete a number).

3. To change the IP address for the Gateway (router) press the “F3” key to select the **Router IP Address** parameter and to access the **Enter the Router TCP/IP Address** prompt screen. Use the numeric keys to type in the desired IP address then press the **enter** key to return to the Secondary TCP/IP Setup screen (You can press the “**clear**” key to delete a number).

4. To change the Maximus terminal (clock) subnet mask (SubMask) press the “F5” key to select the **IP Address SubMask** parameter and access the **Enter the SubMask** prompt screen. Use the numeric keys to type in the desired subnet mask then press the **enter** key to return to the Secondary TCP/IP Setup screen (You can press the “**clear**” key to delete a number).

5. To change the name for the Maximus terminal, press the "F6" key to select the **Terminal Name** parameter and access the **Enter the Terminal Name** prompt screen. The **Terminal Name** parameter enables you to set a unique up-to-20 character administrative name for the terminal. The default name is "ATS" plus the last 6-digits of the terminal MAC address (e.g., **ATS000001**).

NOTE: Applications such as Accu-Engine require "ATS" as the first three characters of the Terminal Name. If not, Accu-Engine will only display the terminal IP address (that can change with DHCP enabled).

NOTE: Firmware Versions prior to 2.05.11(X) do not save any changes to the Terminal Name. If you make any changes the terminal reverts to the default Terminal Name after a re-boot.

Common Settings for Dynamic and Static IP Modes

- **Return to Setup** – This function appears in different menus and returns the terminal to the previous menu screen. For example, press the "F4" key when in the TCP/IP WiFi setup screen to return to the Host Type Ethernet menu screen or press the "F8" key when in the Comm Post setup menu to return to the Host Type configuration screen.

Test Mode

To enter Test Mode, press the "F7" key to select **Test, Setup, Diagnostics** from the main Configuration Menu screen (shown in Figure 4-24) and enter the Test, Setup Diagnostics menu screen as shown in Figure 4-25.

Figure 4-24 Color Maximus Configuration Menu (Initial Setup Menu Shown)

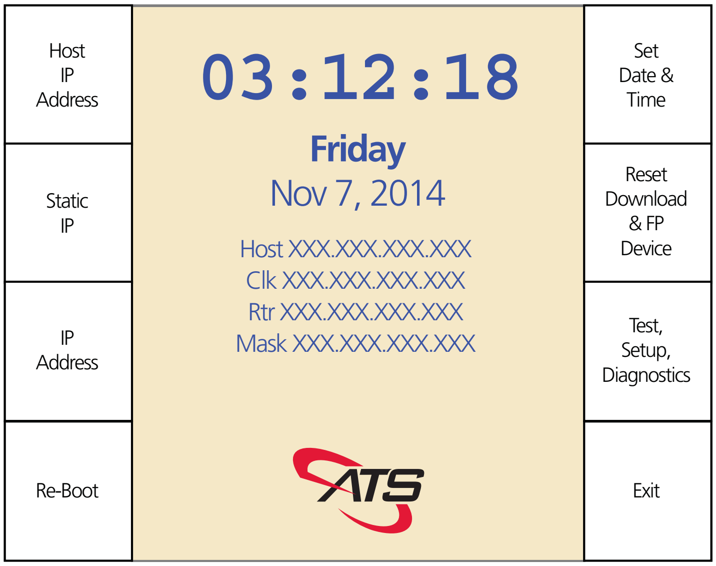
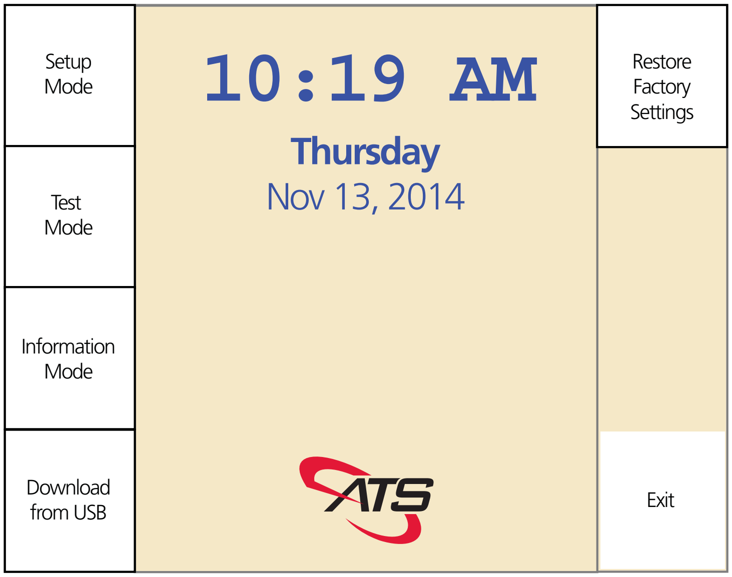
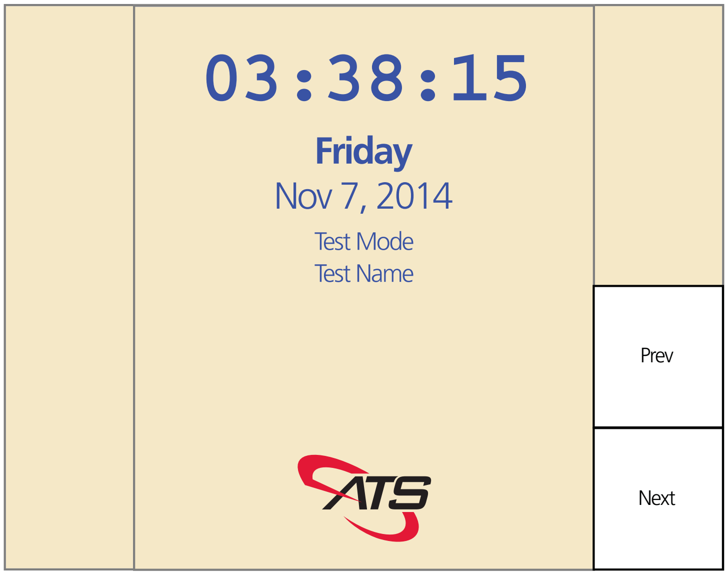


Figure 4-25 Test Setup Diagnostics Screen



Press the “F2”Function key to enter Test Mode and display the Test Mode screen as shown in Figure 4-26.

Figure 4-26 Test Mode


03:38:15

Friday

Nov 7, 2014

Test Mode

Test Name

NOTE: To exit Test Mode, cycle through the test selections until the Exit option appears, then press the enter key.

- Use the **Next** function (“F8” key) to cycle through the tests.
- Use the **Prev** function (“F7” key) to cycle through the tests in the reverse order.
- Press the **enter** key to start the currently displayed test.

You can select the tests in the following sections (some require optional hardware and configuration to activate the test in the menu).

Reader Test

This test enables you to test a card reader or wand. Press the enter key when the display reads “**Test Mode Reader Test**” to start the test. When the display reads “**Test Reader or Wand**” use a card (e.g., swipe) or activate the wand. Press the **clear** key or select **Next** to exit the test when finished.

Biometric Test

Press the **enter** key when the display reads “**Test Mode Biometric Test**” to start the test. The display changes to read “**Test Finger Print Press Enter to start**”. Press the **enter** key and follow the directions on the screen (steps through an enrollment test followed by a verification test). If the test fails, you can press the **enter** key to reselect the Biometric Test. Press the **clear** key or select either **Next** or **Prev** to exit the test when finished.

Keypad Test

This tests each numeric and function key on the terminal. If you press an incorrect key the system will beep and the red LED (X) flashes. When you successfully complete the test the system exits to the next test. You can press the **clear** key to exit before completing the test. Press the **enter** key when the display reads "**Test Mode Keypad Test**" to start the test then:

- Press the numbers **1**–**9** then **0** in order.
- Press the function buttons, starting at the top on the left in order down to the bottom on the left ("F1" to "F4"), then the top on the right down to the bottom on the right ("F5 to "F8"). These display as A through H.

DIDO Test 1

Press the **enter** key when the display reads "**Test Mode DIDO Test 1**" to start the test. The test runs then displays the result. Press the **clear** key to exit the test before it finishes.

- **DIDO Test 2** – Press the **enter** key when the display reads "**Test Mode DIDO Test 2**" to start the test. Press the clear key to exit the test before it finishes.

GSM Signal Strength

This option only appears with a GSM / GPRS module installed and used primarily when installing a 5-meter antenna (see "GSM Long Cable Antenna" on page 2-14). Press the **enter** key when the display reads "**Test Mode GSM Signal Strength**" to start the test. The test displays the signal strength of the cellular data network received by the GSM antenna. Move the terminal, antenna, or both to change the received signal strength. You need a signal strength of at least 15 for a GSM/GPRS module. Press the **clear** key to exit when finished.

NOTE: Signal strength measures from 0 to 32 with 15 or higher being best.

RTC Test

Press the **enter** key when the display reads "**Test Mode RTC Test**" to start the test. This tests the real-time clock (HW and SW) and beeps every second. Press the **clear** key to exit the test when finished.

Battery/Charger Test

Press the **enter** key when the display reads "**Test Mode Battery/Charger Test**" to enter the test and display the "**Battery/Charger Test Press Enter to Test**" prompt. Press the **enter** key to test the components of the optional backup battery and proceed to the next test. The status of each component displays on the screen each time you press the enter key. The tests are for the UPS (Present or not), Battery (OK or Not OK), and AC (Present or not). Press the **clear** key to exit when finished

USB Test

Press the **enter** key when the display reads "**Test Mode USB Test**" to enter the test and display the "**USB Storage Test Attach drv, tap Enter**" prompt. Open the terminal and install a USB flash drive into the USB port then press the **enter** key. The results appear on the screen when the test completes (e.g., **Passed**). Remove the USB flash drive and press the **clear** key to exit.

System Test

This does a quick check on the integrity of the RAM, FLASH, and EEPROM installed on the terminal. Press the **enter** key when the display reads “**Test Mode System Test**” to enter the test and display the “**System Test Press Enter to Test**” prompt. The results of the test appear on the screen when the test completes, including notification of any failures. Press the enter key when the system displays “**Enter to continue**” to exit the test.

Speaker/Beep Test

Press the **enter** key when the display reads “**Test Mode Speaker/Beep Test**” to start the test. The terminal initiates three increasing frequency beeps to verify that the speaker works correctly. Press the **clear** key or select either **Prev** or **Next** to exit the test.

Display Test

Press the **enter** key when the display reads “**Test Mode Display Test**” to start the test. The display turns all the pixels off then on. Press the **clear** key or select either **Prev** or **Next** when finished.

LED Test

Press the **enter** key when the display reads “**Test Mode LED Test**” to start the test. This lights all the LEDs on the terminal one at a time, including those behind the lens and those on the keypad. Press the **clear** key or select either **Prev** or **Next** when finished.

Serial Test: Printer

This test is a loopback and reserved for service personnel. It tests the auxiliary port and requires a specific hardware jumper.

Serial Test: Direct

This test is a loopback and reserved for service personnel. It tests the serial port and requires a specific hardware jumper.

System Diag Dump

This is a test done under the direction of a service technician to help troubleshoot the terminal. This test saves the results of your tests to a text file on a USB flash drive installed in the Maximus USB port.

Press the **enter** key when the display reads “**Test Mode System Diag Dump**” to start. When the system displays the “**Attach USB Drive then press Enter**” prompt, open the Maximus cover and insert a USB flash drive into the USB port then press the enter key. The system displays “**Results copied to USB**” when complete. You can review the results with the technician by opening the text file (on a PC). Press the **clear** key or select either **Prev** or **Next** when finished.

Exit

Press the enter key when the display reads “**Test Mode Exit**” to exit to the Test, Setup, Diagnostics menu (see "Test, Setup, Diagnostics (TSD) Menu" on page 4-13).

Information Mode

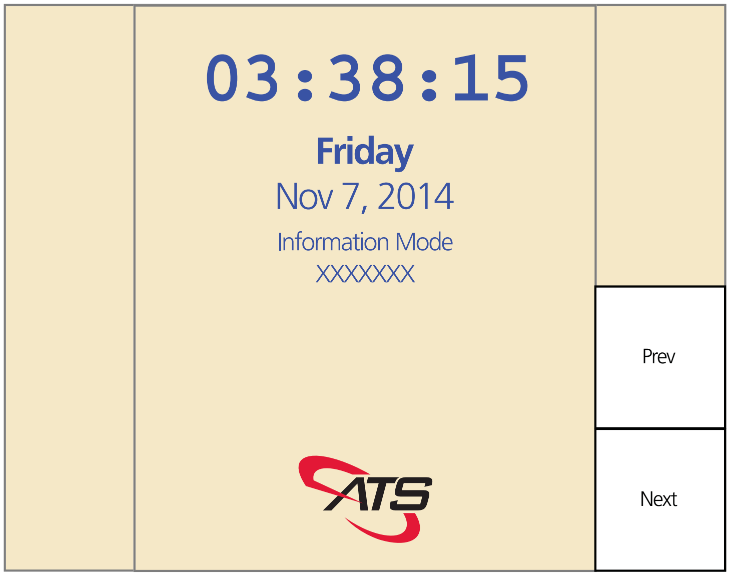
To enter Information Mode, select **Information Mode** (“F3” key) from the Test, Setup, Diagnostics menu (see "Test, Setup, Diagnostics (TSD) Menu" on page 4-13).

To navigate Information Mode:

- Use the **Next** function (“F8” key) to cycle through the tests.
- Use the **Prev** function (“F7” key) to cycle through the tests in the reverse order.
- Press the **enter** key to view the currently displayed information settings/status.
- Use the “up/down” functions (“F7” key and “F8” key) to scroll through the items (if the list is longer than the number of lines on the display).
- Press the **clear** key to return to the Information Mode selections.

To exit Information Mode and return to the Test, Setup, Diagnostics menu, cycle through the selections to the **Exit** selection, then press the **enter** key.

Figure 4-27 Information Mode Screen



03:38:15

Friday

Nov 7, 2014

Information Mode

XXXXXXX

You can select and view the following information categories:

- **Version Info** – Press the **enter** key when the display reads “**Information Mode Version Info**” to view hardware, firmware, and software version information. Depending on the Maximus configuration the information can include:
  - **U-Boot** (boot-loader version information)
  - **U-Boot** (date of the boot-loader version)
  - **Kernel** (main operating system version)
  - **Kernel** (main operating system version date)
  - **Eeprom** (hardware driver version)

  - **Eeprom** (hardware driver version date)
  - **Speaker** (speaker driver version)
  - **Speaker** (speaker driver version date)
  - **AtsLeds** (LED driver version)
  - **AtsLeds** (LED driver version date)
  - **BarRdr** (barcode reader driver version)
  - **BarRdr** (barcode reader driver version date)
  - **Keypad** (keypad driver version)
  - **Keypad** (keypad driver version date)
  - **UCS** (Universal Command Set software version)
  - **UCS** (Universal Command Set software version date)
  - **glibc** (C library version for customization)
  - **glibc** (C library branch information)
  - **Java** (version found – on Java systems, reports the date of the latest component of the java library)
  - **Biometric** (device found – provides information about any connected fingerprint reader
  - **Smartcard** (provides information about any connected smartcard)
- **Ethernet Info** – Press the **enter** key when the display reads "**Information Mode Ethernet Info**" to view the following network information:
  - **Host IP** (IP address of the host computer that the terminal connects to)
  - **Local IP** (IP address of the terminal)
  - **Subnet Mask** (IP subnet mask used by the terminal)
  - **Gateway IP** (IP address of the gateway/router)
  - **DHCP OptionCode** (DHCP option code, e.g., **0** for pad, set by protocol)
  - **Mac Address** (Media Access Control address of the terminal)
  - **PHY** (Ethernet controller type, e.g., **Micrel KS8721 PHY**)
- **Misc Info** – press **ENTER** to view the following miscellaneous information:
  - **Serial Number** (the terminal serial number)
  - **Customer Number** (customer number as noted at the ATS factory)
  - **G-10 Number** (PC board assembly number)
  - **CPU** (terminal CPU type and version)
- **Memory Info** – Press the **enter** key when the display reads "**Information Mode Memory Info**" to view the following memory information:
  - **RAM Total** (the total Random Access Memory installed on the terminal)
  - **RAM Free** (the amount of RAM available/unused on the terminal)
  - **Flash Total** (the total flash memory installed on the terminal)
  - **Flash Free** (the amount of flash memory available/unused on the terminal)

Setting Up the Screensaver

The Color Maximus terminal features an automatic screen saver that is disabled by default. The screen saver is designed to protect the terminal screen from burn-in during periods of inactivity. After a preset period of time, the screen dims (becomes gray), and then the time and optionally an image display and move around the terminal's screen.

The screen saver is only controlled through a configuration file installed on the terminal: **/etc/ssaver.conf**.
You can use this to set the time to idle, sleep, roving duration, and 12/24 hour mode, and the location of the logo. Open the **ssaver.conf** file in a text editor to view and change it.

Screen saver images must be ASCII raster files and stored in a specific location on the terminal. Use the **ZZDLOAD** UCS command (see the *UCS Reference Guide*) or system-level commands to add and remove these graphics files.

The logo must be a Windows bitmap (.BMP) file that is 250 pixels wide and 150 pixels high, or smaller. The BMP must be saved as an 8-bit color palette but a maximum of 224 colors can be used. (Some colors in the map are reserved for drawing the time digits, which use 32 shades of gray.)

The **ssaver.conf** file has the following settings:

- **idletime** – Sets the number of seconds before idle mode activates after the last time the terminal was used. Set this to 0 to disable idle mode. In idle mode, the terminal's display dims, but touch screen and key presses and badge swipes are processed immediately. The default is 45 seconds.
- **sleeptime** – Sets the number of seconds after idle mode activates that sleep mode activates. Set this to 0 to disable sleep mode. In sleep mode, the terminal's display turns black and displays a clock. To use the terminal, press a key (or a touch screen, if applicable) to take the terminal out of sleep mode, and then enter your keypad transactions. Unlike key presses, badge transactions are processed immediately in sleep mode. The default is 45 seconds.

NOTE: Set both idletime and sleeptime to 0 to turn off the screen saver.

- **rovetime** – Rovetime sets how quickly the displayed moves around the terminal screen when the terminal is in sleep mode. The default is 25 seconds.
- **mode** – Sets the display mode of the terminal. Set this to 12 to display a 12-hour clock with an am or pm suffix. Set this to 24 to display a 24-hour clock. By default or if an invalid entry is made, the clock displays in 12-hour format.

Maintenance

5

Chapter

About this Chapter

This section tells you about power, maintenance, and troubleshooting for your Maximus terminal.

NOTE: If you have a Accu-Engine Serial terminal configured for Java programming, see the *Advanced Development Manual for Accu-Time Terminals* for additional information.

Chapter Contents

This chapter contains the following topics:

This page intentionally left blank.

Verifying Installation

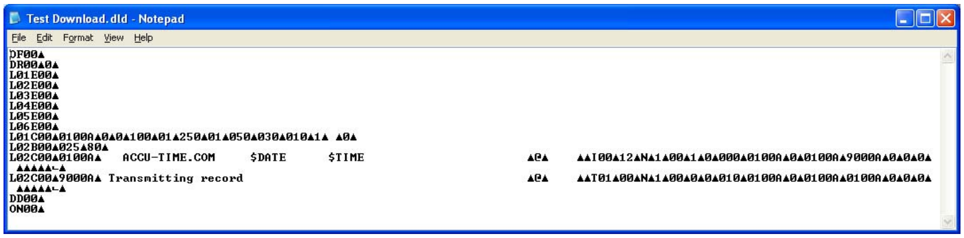
This section tells you how to verify that the installation is correct by performing a query and answerback sequence between a Maximus terminal and its host.

Accu-Time Systems, Inc., has two sample host applications available: Accu-Engine and Accu-Engineer. Your ATS representative can provide a copy. Use these to send a program download file to a terminal and monitor the terminal's response.

Test Download File

Use a text editor capable of inserting control characters (000 through 031_{10}, 000 through 17_{16}) to create a download file containing the lines. The following commands set the terminal offline, reset the terminal, specify a message to display, terminate the download, and put the terminal online. Figure 5-1 shows a sample download file.

Figure 5-1 Sample Download Test File



```
DF00▲
DR00▲0▲
L01E00▲
L02E00▲
L03E00▲
L04E00▲
L05E00▲
L06E00▲
L01C00▲0100A▲0▲0▲100▲01▲250▲01▲050▲030▲010▲1▲ ▲0▲
L02B00▲025▲80▲
L02C00▲0100A▲   ACCU-TIME.COM     $DATE      $TIME                    ▲@▲     ▲▲I00▲12▲N▲1▲00▲1▲0▲000▲0100A▲0▲0100A▲9000A▲0▲0▲0▲
 ▲▲▲▲▲∟▲
L02C00▲9000A▲ Transmitting record                                     ▲@▲     ▲▲T01▲00▲N▲1▲00▲0▲0▲010▲0100A▲0▲0100A▲0100A▲0▲0▲0▲
 ▲▲▲▲▲∟▲
DD00▲
ON00▲
```

The » symbol represents a record separator character, 30_{10} or $1E_{16}$. For more information about control character symbols, see "Control Character Representation" on page P-4.

Use Accu-Engine to send that download file to the terminal. The terminal should respond with a beep and display the text.

Maintenance

The Maximus is a low-maintenance data collection terminal. The only required procedure is periodic cleaning of the badge reader, finger sensor, or other input device.

Cleaning the Terminal

To clean a terminal's exterior, moisten a cleaning cloth with a commercial or domestic hard-surface cleaner and wipe the terminal exterior to clean it.

Since dried residue of cleaning product could become a future problem for the terminal's electrical and mechanical connections, avoid gross application of cleaning product and do not spray cleaning product directly onto the terminal.

These instructions do not apply to the interior of the terminal. See the following instructions for cleaning badge and fingerprint readers.

Cleaning the Badge Reader

To clean the badge reader, swipe a cleaning card premoistened with isopropyl alcohol (rubbing alcohol) through the reader several times. Low-usage readers should be cleaned monthly. High-usage readers should be cleaned weekly.

Although the finger sensors used in ATS terminals have few maintenance and handling requirements, a few basic precautions help ensure a high level of performance over the life of the sensor.

Deposits from fingers accumulate on the surface of the finger sensor after repeated use. These deposits may be from natural oils from the finger or from dirt, grease, or lotions. These deposits may effect sensor operation, so you should clean the sensor as required by your environment. In normal use, we recommend cleaning the sensor once a month, or any time a residue is visible on the sensor surface or when the reader performance degrades.

Cleaning the Biometric Sensor

Use the following procedure to clean the Biometric sensor surface (all sensor technologies):

1. Remove electrical power from the finger sensor by disconnecting the terminal from its power source.

2. Use an alcohol prep wipe or dampen (not soaking or dripping wet) a clean cotton swab, a clean cotton ball, or a non-abrasive cloth with isopropyl alcohol.

⚠ **Caution**

Do not directly spray the sensor.
Do not use nylon brushes or scouring pads, abrasive cleaning fluids or powders, or steel wool. These items can damage the sensor.

Do not use bleach or chlorine-based cleaners, non-chlorine bleach, or chlorine-based bathroom or mildew cleaners.
Chlorine-based cleaners do not necessarily affect the functionality of the fingerprint sensor, but they can discolor and could damage the surrounding enclosure and peripheral components.
Do not use any solvents such as acetone, MEK, TCE, paint thinner, turpentine, etc.

Do not allow cleaner to drip or run down into the enclosure.

3. Gently rub the sensor surface and surrounding bezel with the damp cotton swab, rotating the swab to keep exposing a clean surface to the sensor.

4. If the sensor is very dirty, you may need to repeat the cleaning operation using a new clean swab.

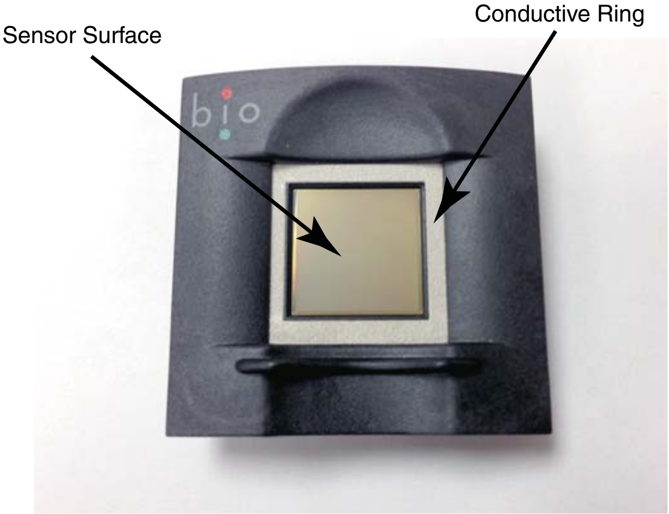
5. After cleaning with the damp swab, gently rub the surfaces again with a clean dry cotton swab.

6. Reconnect the terminal power when cleaning is complete.

Cleaning an E-Field Conductive Ring (Bioscrypt)

After an extended period of use, the conductive ring, surrounding the sensor, may become tarnished or accumulate deposits that can degrade performance (see "E-Field Sensor (Bioscrypt)" on page A-9 for how the conductive ring operates with the sensor).

Figure-6 Bioscrypt E-Field Sensor Conductive Ring



Use the following procedure to clean the E-Field conductive ring:

1. Remove electrical power from the finger sensor by disconnecting the terminal from its power source.
2. Using a new pink rubber pencil eraser, remove the deposits/tarnishing from the surface of the conductive ring - do not use the eraser on the sensor surface.
3. Use compressed air to remove the eraser dust from the reader. Alternately you can remove the eraser dust with a clean dry cotton ball.
4. Clean the sensor surface using the procedure described in "Cleaning the Biometric Sensor" on page 5-5.
5. Reconnect the terminal power when cleaning is complete.

Caution *Do not remove eraser dust with wet or damp material. Do not scratch the sensor surface. Do not rub the sensor surface with the eraser. Do not use an eraser to clean the sensor.*

Caring for the Biometric Sensor

The sensor is designed to perform well even under harsh conditions. Nevertheless, some precautions should be taken to avoid damaging the sensor:

- Do not place the finger sensor close to a heat source, such as a radiator or hot plate.
  - In addition, the sensor should not be exposed to rain or excessive moisture.
  - With the exception of the procedure as described in "Cleaning the Biometric Sensor" on page 5-5, do not put any liquids on the sensor. Never spray or pour liquids directly on the sensor.
- Do not subject the finger sensor to heavy shocks or vibrations.
- Do not allow the sensor to come in contact with metallic objects.
- Periodically clean the sensor as described in "Cleaning the Biometric Sensor" on page 5-5 as appropriate for your specific site (different sites may require different cleaning schedules).

Troubleshooting Guide

CAUTION

The terminal has no user-serviceable parts. Accu-Time terminals must be operated within the parameters described in this document. Any operation performed contrary to these parameters voids the warranty.

Table 6-1 Troubleshooting Diagnostic Table

Symptom	Possible Cause	Solution
Terminal does not power up, the display and none of the status LEDs are lit.	No DC power applied.	Ensure primary side of DC power pack assembly is plugged into a live AC outlet. Ensure secondary side of DC power pack assembly is plugged into the Time and Data Collection Terminal (DCT).
		Test the outlet by plugging in another appliance.
		If all else fails, replace the power pack assembly.
Terminal is not communicating with host computer.	Terminal to Host communication cable is defective or unplugged on either end.	Verify cable is tested and plugged into both ends. Ensure that cable termination guidelines and lengths are observed.
		Ensure the application package is loaded and running on the host.
Terminal does not accept badge data.	Bar code badge is not manufactured to the proper specification.	See the vendor’s specifications for manufacturing criteria.
	Badge is being swiped in the wrong direction.	Ensure media faces the correct direction: turn the card around and try again.
	Badge code format is not supported.	Ensure badge code is among those supported. Supported codes include most standard bar code formats including UPCA, 128, 3 of 9, Interleave 2 of 5 and more, as well as IATA Track I and ABA Track II magnetic stripe input (reader dependent).
	Badge reader needs cleaning.	Swipe a pre-moistened (isopropyl alcohol) cleaning card through the reader several times.
	Badge number does not exist in validation file.	See a supervisor.

Table 6-1 (page 1 of 2)

Table 6-1 Troubleshooting Diagnostic Table

Symptom	Possible Cause	Solution
Terminal does not accept keypad input.	Keyed data does not exist in validation file	See a supervisor
	Keypad connector is unplugged.	Test the keypad in Test Mode (for monochrome terminals, see "Test Mode" on page 3-46, and for color terminals, see “Test Mode” on page 4-30).

Table 6-1 (page 2 of 2)

If the suggested solutions have been tried and the problem still exists, contact the Accu-Time Systems Product Service Department at (860) 870-5000 during normal business hours: 9 am to 5 pm Eastern time, Monday through Friday. Before contacting Accu-Time, please be prepared to provide the serial number and the configuration number of the product.

Power-Related Troubleshooting

Table 6-2

Symptom	Possible Cause	Solution
The terminal display is blank.	The primary of the power pack assembly is not plugged into an AC-wall outlet, is not plugged into the terminal, or is the wrong voltage.	Check the outlet, both power pack connections, and that it is a 12 VDC power pack.
		Replace the power pack.
The low power (yellow) indicator LED is lit.	Outlet or power pack problem.	Check the outlet, both power pack connections, and that it is a 12 VDC power pack.
		Replace the power pack.

NOTE: If the battery backup option is installed, the terminal operates for approximately 1.5 hours after the primary voltage source is lost. After this, the terminal turns off. When the terminal is in battery backup mode, the yellow low-power indicator LED is lit. before the terminal display goes blank.

Communication-Related Troubleshooting

Table 6-3

Symptom	Possible Cause	Solution
The terminal is not communicating with the host.	Communication parameters were not previously set.	Use Setup Mode to setup the terminal (for monochrome terminals, see "ATS Setup Mode" on page 3-15, and for color terminals, see "Setup Mode" on page 4-15). Your network administrator needs to provide the following: IP address to be assigned to the terminal IP address of the host to which the terminal can connect Network Mask (example 255.255.255.0) Port number (try 2500 by default) Gateway or router address (if required)
		Reboot the terminal to see if it connects.
		If parameters are set, ping the terminal.
		Verify that the cable is plugged into both ends (terminal and hub) and terminated to the appropriate eight-position modular connector.
		Verify that the single segment cable length is equal or less than 100 meters (328 feet). The cable should also be a 10/100BASE-T category 5, twisted pair high-speed data transmission cable with both ends properly crimped.
		Ensure application package is loaded and running on the host. Check the Ethernet diagnostic LEDs: BUSY: This amber or yellow light indicates the terminal is busy processing. LINK: This green light indicates the terminal is receiving network traffic, though the traffic might not be from the host.
A previously working terminal is not operational.	Cables not plugged in or host application software not operational.	Ensure that all connections are made and that the host software application is functional. If possible, take a known working terminal and readdress it for this particular node to determine whether the problem is related to the terminal, installation, or host.

If neither the standard nor Ethernet troubleshooting guide is of any help, please contact the Accu-Time Product Service Center, (860) 870-5000, for further assistance.

This page intentionally left blank.

Biometrics

A

Appendix

About this Appendix

This Appendix describes the differences in biometric fingerscan readers, operating modes, and proper finger placement.

Appendix Contents

This Appendix contains the following topics:

This page intentionally left blank.

Why Use Biometrics?

Biometric identification provides several advantages over traditional methods that require ID cards/tokens or Password/PIN numbers. Some of the advantages biometric devices provide are:

- Eliminates buddy punching - the person must be physically present at the point-of-identification.
- Provides the ability to eliminate badges/tokens/PINs - identification based on biometric techniques alleviates the need for users to remember a password or carry a token.
- Improves security - protects sensitive and personal data by replacing PINs, eliminates credentials that can be stolen, and prevents unauthorized access to systems or facilities.

User Confidentiality

ATS offers fingerscan biometric devices. Fingerscans are not fingerprints. Many people refer to fingerscans as "fingerprints," but the data of a fingerscan template is not suitable for law enforcement fingerprint matching. In addition, the reader does not create or save the type of image file required by the Integrated Automated Fingerprint Identification System (IAFIS). The IAFIS is the national fingerprint and criminal history system maintained by the Federal Bureau of Investigation (FBI), Criminal Justice Information Services division (CJIS).

The ATS fingerscan products produce a template that represents points along the unique features and minutia found in a fingerprint pattern. The template files cannot be reverse-engineered to reproduce a fingerprint because the reader does not save the necessary information.

Reliability Rules

Successful biometric installation and use typically requires:

- Management Support (commitment to a maintenance schedule, etc)
- Training of Supervisors and Employees
- Satisfactory Environmental Conditions

Even if all these requirements are met it's important to note:

- Not all users can be enrolled (for various physiological reasons).
- Biometric devices are susceptible to vandalism.
- Environmental conditions can affect operation (e.g., moisture, dust, cold).

ATS uses these fingerscan technologies for their proven reliability given a few simple rules:

1. All terminals within a facility are installed correctly (installation height observed, obstructions avoided).

2. The employee enrollment procedure is closely followed.
3. The sensor is maintained on a scheduled basis.

ATS Biometric Operational Options

Users may enroll on any terminal and templates can be stored on the scanning terminal or on a host. Templates stored on a host may be distributed to other terminals.

ATS fingerscan readers and terminals provide the following special features:

- Enroll Two Fingers - ATS terminals enable you to configure the fingerscan device to require more than one fingerscan (e.g., index and middle finger).
- Override Verification for Individuals - ATS terminals enable you to disable or set special conditions for certain individuals (in Verification Mode). For example, you can configure the terminal so an amputee can identify/verify without a fingerscan. Alternately, you can configure a user profile to accept any live fingerscan from an individual. This may be necessary if the reader cannot obtain a “good fingerscan” due to physiological issues.
- Adjust False Acceptance Rate - ATS terminals enable you to set the threshold for fingerscan matching accuracy.

Verification and Identification Modes

Verification and Identification Modes are used in time & attendance. During the enrollment process an employee's fingerprint is scanned and converted to a mathematical code, or template. There are no actual "fingerprints" stored anywhere, merely an arithmetic representation of certain minutiae points.

ATS biometric devices have two modes of operation:

- 1:1 Mode (one-to-one mode) or Verification Mode
- 1:N Mode (one-to-many mode) or Identification Mode

NOTE: 1:1 and 1:N templates are not transferable between modes on E-Field readers (Bioscrypt). The E-Field readers come in either 1:1 Mode or 1:N Mode. You can send templates between E-Field readers but the template only works in the original mode (1:1 or 1:N).

Verification Mode

1:1 Mode is also called Verification Mode. It confirms or denies a person's claimed identity. In this mode the user identifies him or herself using an ID card/token or by entering a password (PIN) at the terminal. Then the person uses the biometric reader to confirm their identity. This process is quick since the terminal/reader recalls the template for the claimed identity and compares it to the current scan.

When an employee presents their identity card/badge or enters their PIN at a terminal the reader retrieves that person's fingerscan template. The terminal then prompts the employee to place their finger on the sensor. The reader compares that person's fingerprint to the template held on file and called up by the person's ID. If the fingerprint being presented matches the one on file for that employee then the match is accepted (good). This is called Verification Mode. It answers the question "Am I the person I say I am?"

Identification Mode

1:N Mode is also called Identification Mode. This method confirms a person's identity by comparing the current fingerscan against a number of enrolled templates (N). This method eliminates the need for ID cards/tokens or passwords/PINs but takes longer to confirm/deny the fingerscan as the number of enrolled templates (N) increases. In addition, a 1:N template is larger than a 1:1 template (file size).

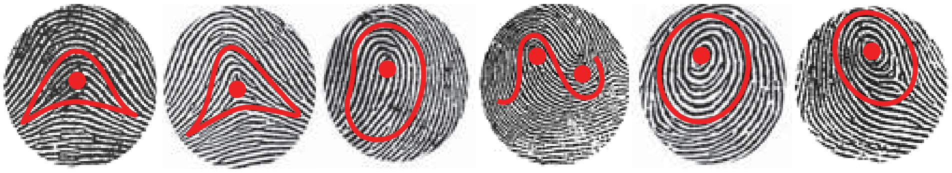
In Identification Mode the employee simply approaches the terminal, presents their finger for scanning, and the entire template database is searched for a matching template. Identification Mode answers the question "Who am I?" This process is simple for the employee and relies on the human body, specifically the fingerprint, as the credential. The company does not need to issue credentials (badges, swipe cards, barcode cards, RFID cards), the employee does not need to carry a card, and the back office infrastructure is less complicated. However, Identification Mode can be a slow process if the template database is large; a problem for enterprises with several hundred or several thousand employees. In large companies Verification Mode may take less than 2 seconds while Identification Mode may take 8 seconds. Multiply 8 seconds by thousands of employees lined up waiting to "punch in" and many hours are wasted.

How it Works

At enrollment, the biometric reader scans the user's fingerprint and creates a numeric data template from the fingerprint image. Once it creates the template it discards the fingerprint image/scan. Templates are used for comparison to live fingerscans and are either stored at the terminal or on a host. Templates stored on a host can be distributed to additional terminals.

When a person places his or her finger on the sensor the reader captures an image of the fingerprint. From this point the reader finds unique patterns within the fingerprint. The starting point of this is the fingerprint core. A fingerprint core is a point located within the inner most re-curving ridge. Normally it is located in the middle of the fingerprint as shown in Figure A-1.

Figure A-1 Location of Fingerprint Core

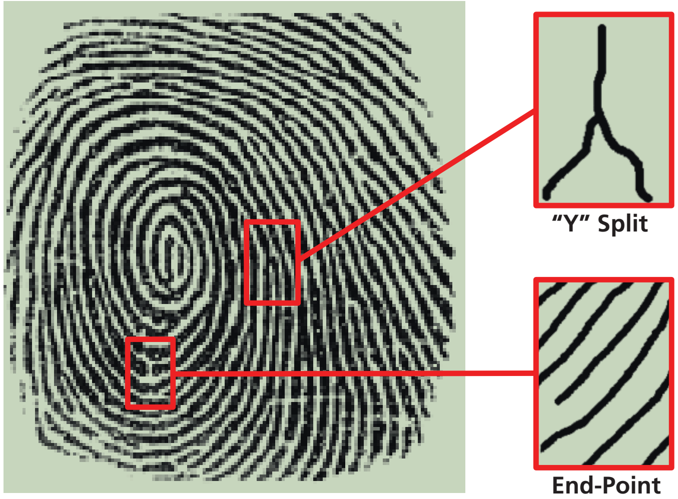


Most frequent types of cores are:

- Arches (plain and tented)
- Loops (singular and twinned)
- Whorl and Central Pocket Loop

The reader also looks for points within the image such as a "Y" split or an end-point as shown in Figure A-2.

Figure A-2 Identifying Points Within Image



Most biometric units only look at the skin surface. These readers are more susceptible to misreads caused by damage on the top layer of the skin. Furthermore, if only the surface layer of skin is examined, the readers can also fall prey to gelatin duplicates of fingerprints.

Recommended Fingers

We recommend users enroll their index, middle or ring fingers. Avoid using the thumb and pinky finger since they are difficult to position on the sensor consistently.

Fingerprint Scanner Types

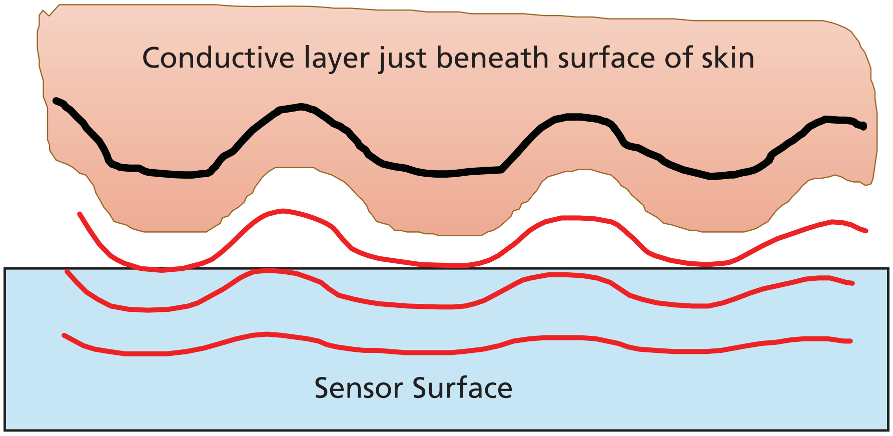
Accu-Time Systems uses one of three types of finger scanning technologies:

- E-Field Technology (Bioscrypt) - E-Field sensors send a radio wave through the finger to measure the ridges and valleys of the sub-dermal live skin layer. This technology is desirable for environments where fingerprint “spoofing” is a concern.
- Capacitive Technology (Cogent, Suprema) - Capacitive sensors use a system of amplifiers to measure the ridges and valleys of the sub-dermal live skin layer. During enrollment the capacitive reader takes three images of the user’s fingerprint and converts all three into a single stored template. Thereafter, the reader verifies the user’s subsequent fingerscans using the template. This technology is desirable for high-resolution/low-cost imaging in normal environments.
- Multi-Spectral Imaging Technology (Lumidigm) - The multi-spectral reader uses different light wavelengths (430, 530, 630 nm, and “white light”) to capture multiple authentication images of the topical fingerprint and structures beneath the skin (e.g., blood vessels and oxygenated hemoglobin, collagen). This technology is desirable for difficult environmental conditions where fingerprints are subject to moisture, dirt, dry/arid conditions, as well as genetic or physiological challenges. In addition, it defeats spoofing by measuring the subcutaneous structures in the finger.

Image Creation

In general, the sensor detects the ridges and the valleys on the fingerprint as shown in Figure A-3. The reader then uses the image to create a numerical fingerscan template or to compare against a template on file. The reader then deletes the scanned image.

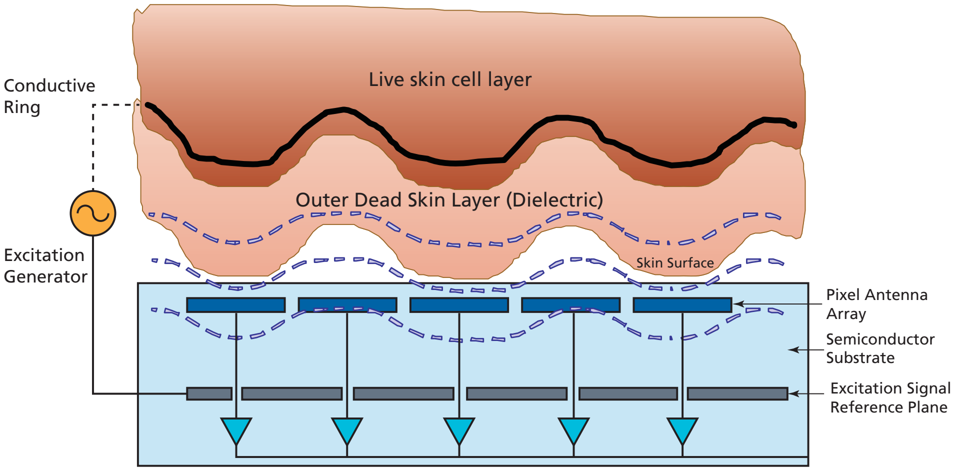
Figure A-3 Sensor Detecting Fingerprint Ridges & Valleys



E-Field Sensor (Bioscrypt)

Figure A-4 illustrates how an E-Field sensor operates to create a fingerprint image. It shows a cross-section of an E-Field sensor array reading the skin layers of a finger.

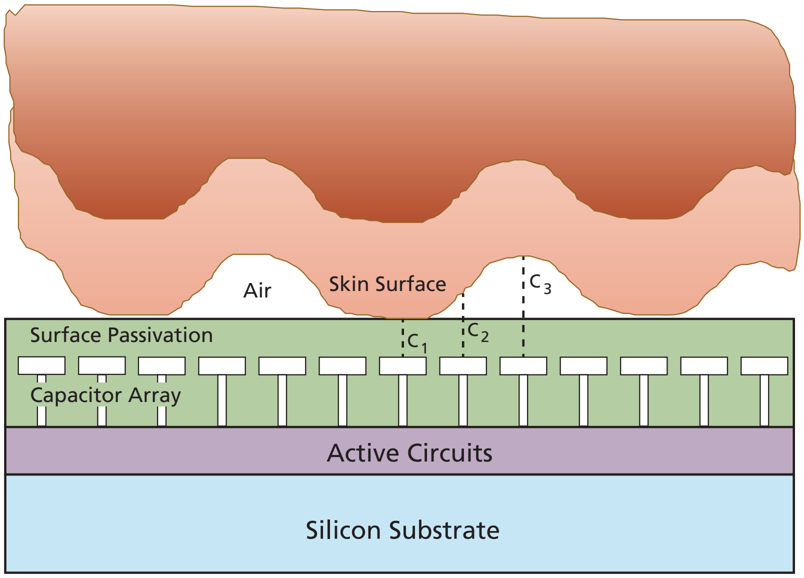
Figure A-4 E-Field Sensor Image Creation



Capacitive Sensor (Cogent, Suprema, Crossmatch/Digital Persona)

Capacitive sensors use active capacitive pixel-sensing technology to detect the finger ridge and valley patterns. They measure the capacitance of the finger to obtain an image. The capacitance of the finger changes as the distance between the finger and the array changes, C1, C2 and C3, as show in Figure A-5.

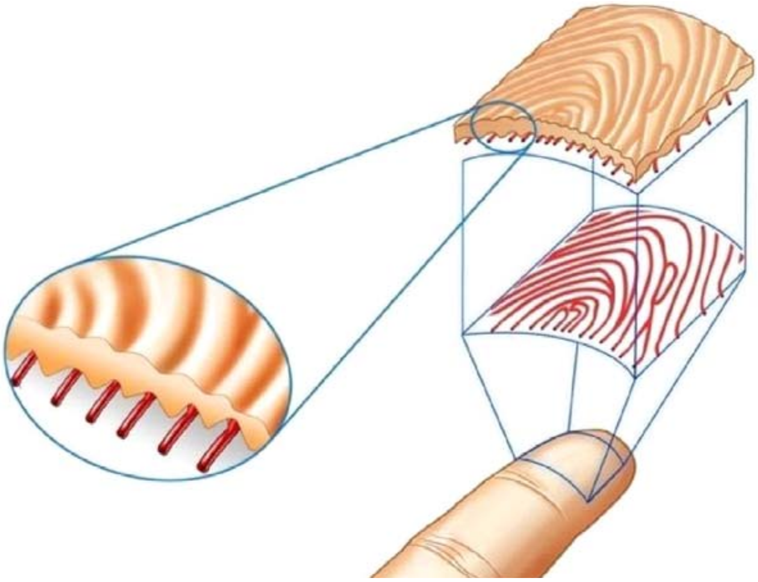
Figure A-5 Capacitive Sensor Image Creation



Multi-Spectral Imaging Sensor (Lumidigm)

The AccuTouch reader uses multi-spectral imaging to authenticate fingerscans. The multispectral sensor has the ability to “see” structures beneath the skin surface (subcutaneous structures). Your “internal fingerprint” is identical to your external fingerprint as illustrated in Figure A-6.

Figure A-6 Internal and External Fingerprint (Source: Lumidigm Corporation)



The blood vessels and other skin structures are easily imaged with the multispectral approach. Figure A-7 shows how oxygenated hemoglobin in blood affects absorption depending on the wavelength of light.

Figure A-7 Optical Absorption Due to Blood (Source: Lumidigm Corporation)

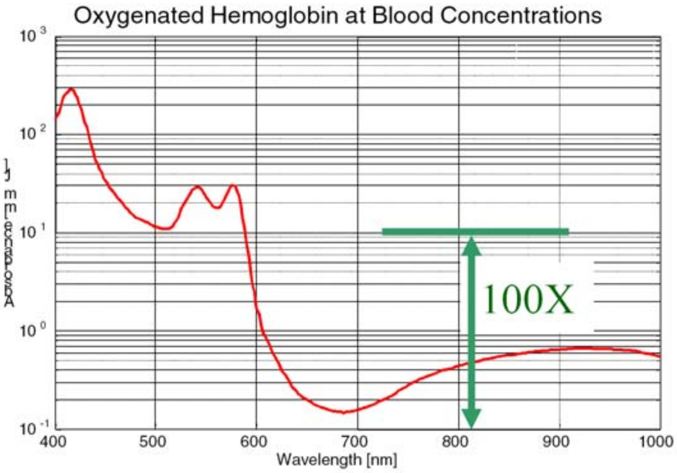
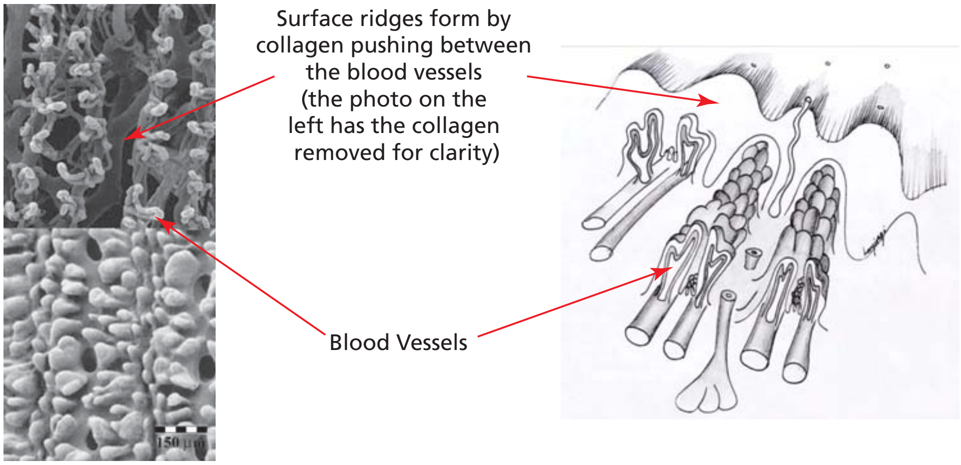


Figure A-8 shows how collagen pushing between blood vessels creates ridges in the finger tip.

Figure A-8 Relevant Fingertip Physiology (Simone Sangiogi 2006, Source: Lumidigm Corporation)


Surface ridges form by collagen pushing between the blood vessels (the photo on the left has the collagen removed for clarity)
Blood Vessels
150 µm

Multi-spectral optical fingerprinting using multiple, different images taken on a single reader during a single finger placement offers the following advantages:

- Multiple authentication images at enrollment and during authentication
- Multiple scanning wavelengths
- Different optical geometries
- Surface and subsurface feature identification
- Surface penetration up to 1500 microns deep (1.5 mm)
- "Single reader, single finger placement" for authentication
- No extra user actions

Finger Placement

Filling the sensor area with the fingerprint provides the best performance. Touching the sensor with a fingertip, as if pressing a button, creates scan that lacks information-rich fingerprint data resulting in a rejected authentication.

Caution

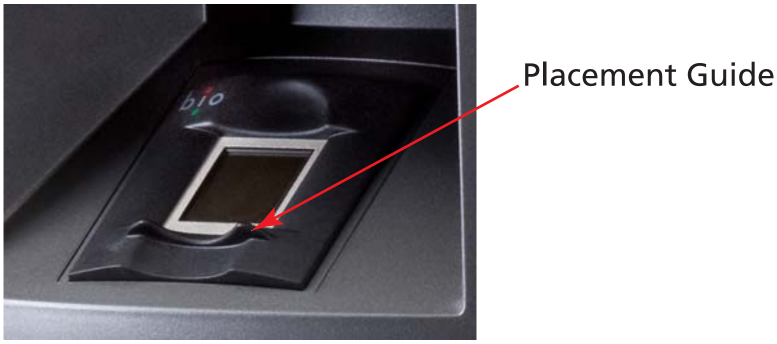
Don't slide your finger onto the finger scanner, as this can push debris onto the sensor.

NOTE: For finger scans, we recommend you use an index finger, middle finger, or a ring finger, in that order. We do not recommend using a thumb.

Placement Guides

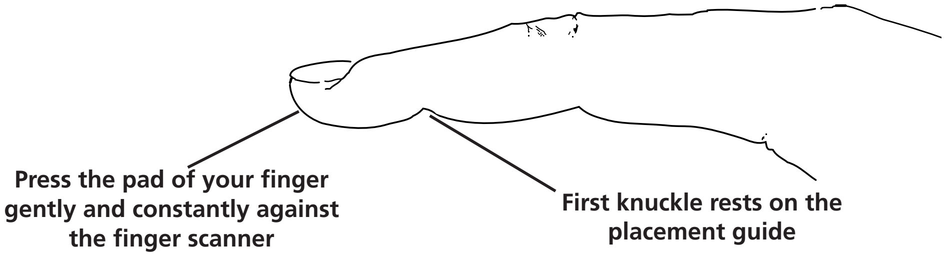
E-Field (Bioscrypt) and Capacitive (Suprema and Cogent) sensors are equipped with a placement guide. The placement guide is a raised area located in front of the sensor to aid in finger positioning. Users should center the bottom of their first joint on the placement guide before lowering their finger onto the sensor. Figure A-9 shows the placement guide in front of an E-Field sensor.

Figure A-9 Placement Guide in Front of a Sensor (E-Field shown)



When the terminal displays a message such as "Place finger on reader" or "Present Finger", slide your finger across the placement guide without touching the sensor until the first joint is centered on the placement guide.

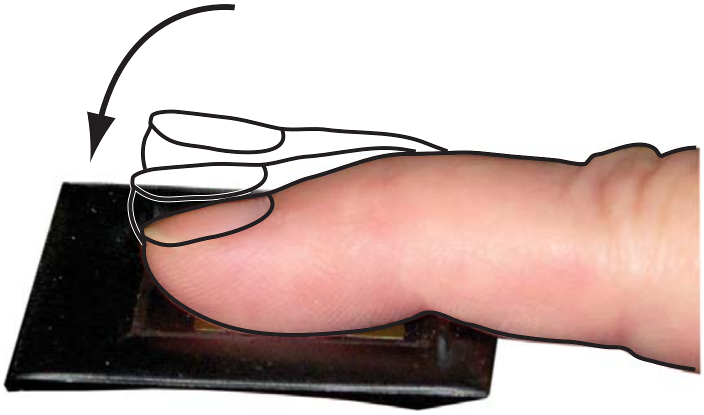
Figure A-10 Knuckle Placement for Finger Scanner


Press the pad of your finger gently and constantly against the finger scanner
First knuckle rests on the placement guide

Use the following procedure to authenticate your fingerprint:

- Align: Position the finger where the center of the first joint meets the center of the placement guide as shown in Figure A-10.
- Drop: Lower the finger evenly onto the sensor using moderate pressure as shown in Figure A-11.
- Hold: Keep the finger on the sensor until the display shows the acceptance/ rejection message (e.g., "Your finger has been accepted").

Figure A-11 Correct Finger Placement on a Finger Scanner – Side View



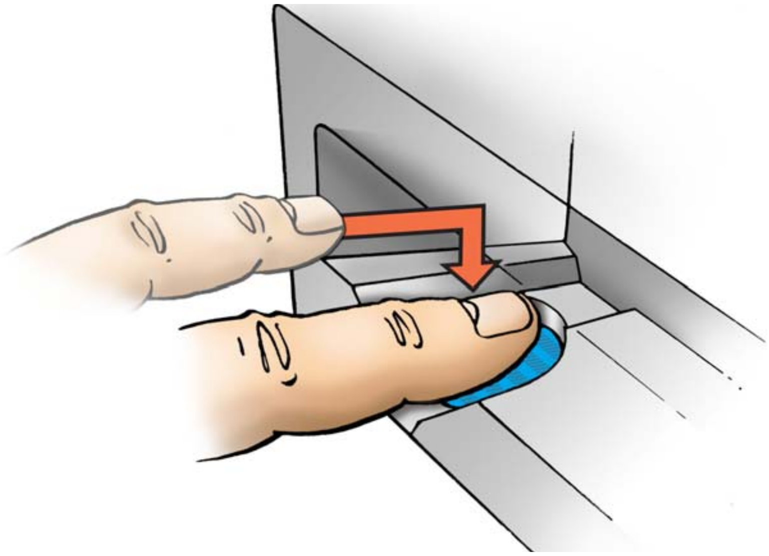
Sensors Without Placement Guides

Many multi-spectral sensors, such as the AccuTouch (Lumidigm), do not have a placement guide. Use the following procedure to enroll on a multi-spectral sensor (refer to Figure A-12):

1. Straighten your finger.
2. Position the pad of your finger above the center of the sensor.
3. Keep your finger straight and lower the pad of your finger evenly onto the center of the sensor.

4. Without moving or rolling your finger, hold the pad of your finger on the sensor with moderate pressure until the system reads and verifies/identifies the scan.

Figure A-12 Correct Finger Placement on an AccuTouch Finger Scanner



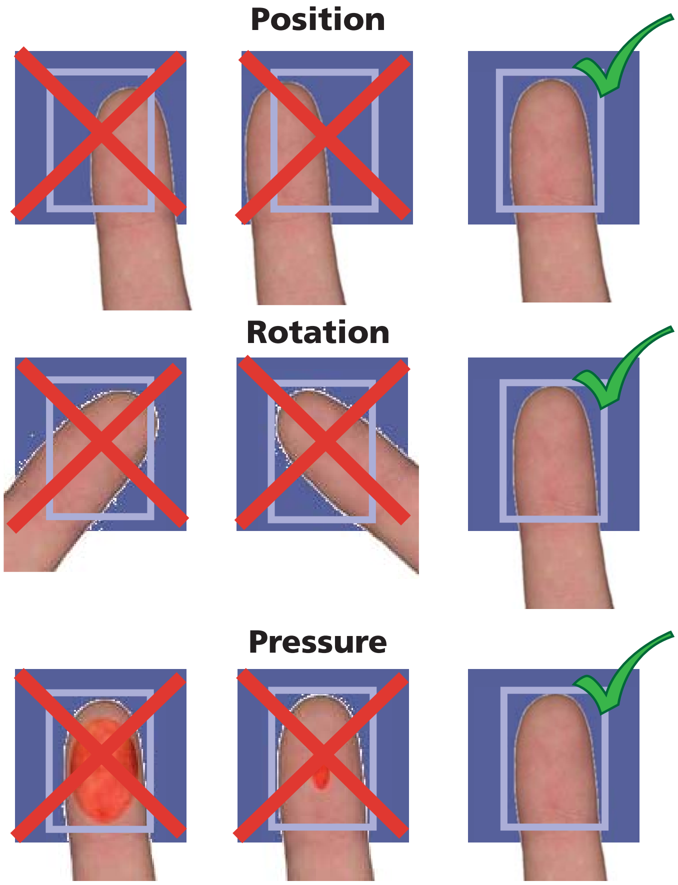
Authentication Issues

Common issues that produce a rejected authentication are:

- Position: Placing your finger far from the center position of the sensor will increase the rejection rate.
- Rotation: Finger rotation should be kept to a minimum during enrollment and verification.
- Pressure: Apply moderate pressure when making contact with the sensor. Too much pressure may cause smudging of the fingerprint. Too little pressure may not allow the sensor to recognize the presence of a finger.

Figure A-13 shows correct and incorrect finger placements.

Figure A-13 Correct and Incorrect Finger Placements



This page intentionally left blank.

Badge Specifications

B

Appendix

About this Appendix

This Appendix provides specifications for employee badges used with Maximus terminals that can be equipped with optical barcode and/or magnetic stripe readers.

Appendix Contents

This Appendix contains the following topics:

This page intentionally left blank.

Optical Barcode Badges

Guidelines

This section provides recommendations and requirements for Maximus optical badge readers. This is not meant as a comprehensive specification, but as a guideline, which ensures high read rates. This section pertains solely to the printing of Code 3 of 9 barcodes.

Physical Specifications

The following are the physical specifications for an optical barcode badge:

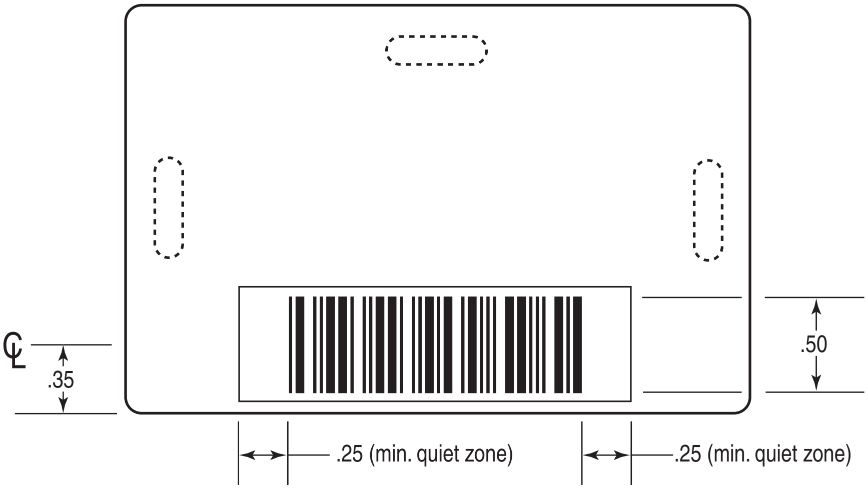
- The maximum badge thickness is 0.040 inch.
- The laminate covering the barcode must be no thicker than 0.010 inch and transparent to light in the 600 to 880 nanometer wavelength range. The external surface of the material may have a matte finish.

Printing Specifications

Refer to Figure B-1 for an illustration of a typical optical badge barcode size and position. The following are the detailed printing specifications for an optical barcode badge:

- The print contrast ratio (PCR) of the barcode should be greater than 75% for light in the 600 to 880 nanometer wavelength range.
- The minimum width of a narrow barcode element should be 0.010 inch.
- The ratio of wide to narrow bar code elements depends on the barcode. For Code 3 of 9 the ratio is in the range of 2.2:1 to 3:1.
- A quiet zone of at least 0.250 inch is required on each end of the barcode. There can be no transitions in this are such as a stock to stock seam or the beginning of the blocking pattern.
- Any vertical cutouts designed to accommodate attachments clips or devices must be located no lower than one (1) inch from the bottom edge of the badge to prevent interference with the bar code reader slot.
- A blocking pattern may be used over the barcode to resist copying. Red is typically used for IR badges. The blocking pattern must be transparent to light in the 600 to 880 nanometer wavelength range. Some IR badges have a copy protection layer.
- The barcode height should be at least 0.500 inch.
- The barcode should be located such that it is parallel to one side of the card and the center-line of the code is 0.350 inch.
- A high quality printing method should be used which will limit bar imperfections (voids, smears) to 0.005 inch diameter or less.

Figure B-1 Typical Barcode Position & Sizes (optional holes for clips shown as dotted lines)



Magnetic Stripe Badges

This section provides recommendations and requirements for magnetic stripe badges used with the Maximus magnetic stripe readers. This is not meant as a comprehensive specification, but as a guideline, which ensures high read rates. Table B-1 lists the ISO Specifications for magnetic stripe badges used on the Maximus terminals.

Table B-1 ISO Specifications for Magnetic Stripe Badges

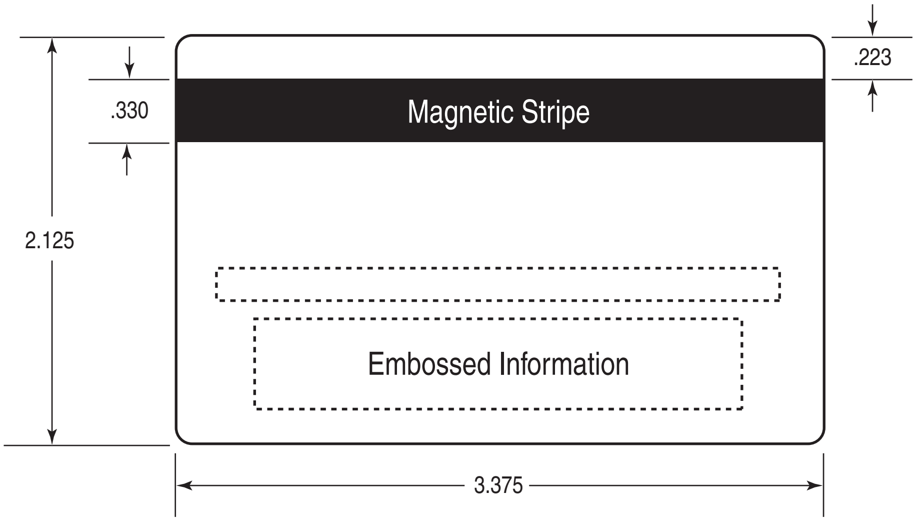
ISO #	Description
7810	Physical characteristics of credit card size document
7811-1	Embossing
7811-2	Magnetic stripe - low coercivity
7811-3	Location of embossed characters
7811-4	Location of tracks 1 & 2
7811-5	Location of track 3
7811-6	Magnetic stripe - high coercivity
7813	Financial transaction cards

Table B-1

Physical Specifications

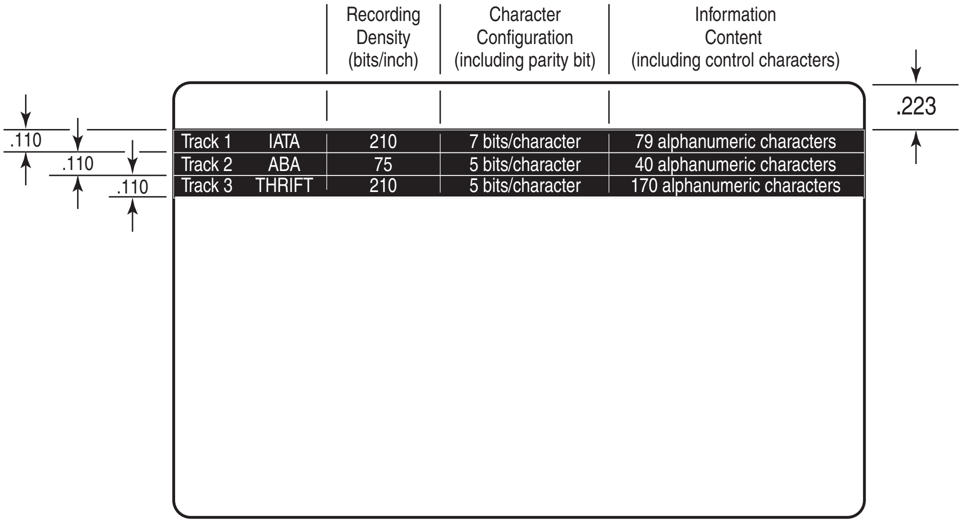
Figure B-2 shows the physical dimensions and positions for magnetic stripe badges used with the Maximus terminals.

Figure B-2 Typical Magnetic Stripe Position and Size



The track formats in this document are based on ISO Standards, however, other formats may be used. Figure B-3 shows the locations of the encoding tracks typical in financial transaction cards (format used by the Maximus terminals).

Figure B-3 Magnetic Stripe Encoding (financial transaction cards)



		Recording Density (bits/inch)	Character Configuration (including parity bit)	Information Content (including control characters)
Track 1	IATA	210	7 bits/character	79 alphanumeric characters
Track 2	ABA	75	5 bits/character	40 alphanumeric characters
Track 3	THRIFT	210	5 bits/character	170 alphanumeric characters

Track Encoding Specifications

This section provides details for Track 1 from Figure B-3.

Track 1 (Card Data Format)

Figure B-4 provides a graphical representation of the fields in Track 1 and Table B-2 provides a description of the fields.

Figure B-4 Card Data Format, Track 1

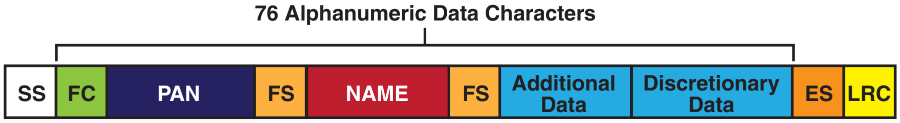


Table B-2 Card Data Format, Track 1 Field Descriptions/Lengths

Field	Description/Length
SS	Start Sentinel (%)
FC	Format Code
FS	Field Separator (^)

Table B-2 (page 1 of 2)

Table B-2 Card Data Format, Track 1 Field Descriptions/Lengths

Field	Description/Length	
ES	End Sentinel (?)	
LRC	Longitudinal Redundancy Check character	
PAN	Primary Account Number (19 digits maximum)	
Name	Name (25 alphanumeric characters maximum)	
Additional Data	**Number of characters**	
	Expiration Date (YYMM)	4
	Service Code	3
Discretionary Data	**Number of characters**	
	PVKI - Pin Verification Key Indicator	1
	PVV (or Offset) - Pin Verification Value	4
	Card Verification Value (CVV) or Card Validation Code (CVC)	3
	Some or all of the PVKI, PVV, CVV, and CVC, fields may be found with the Discretionary Data.	

Table B-2 (page 2 of 2)

Track 2 (Card Data Format)

Figure B-5 provides a graphical representation of the fields in Track 2 and Table B-3 provides a description of the fields.

Figure B-5 Card Data Format, Track 2

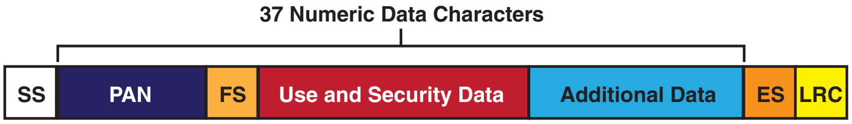


Table B-3 Card Data Format, Track 2 Field Descriptions/Lengths

Field	Description/Length
SS (control character)	Start Sentinel, Hex B, ;;
FS (control character)	Field Separator, Hex D, =
ES (control character)	End Sentinel, Hex F, ?
LRC	Longitudinal Redundancy Check character

Table B-3 (page 1 of 2)

Table B-3 Card Data Format, Track 2 Field Descriptions/Lengths

Field	Description/Length	
PAN	Primary Account Number (19 digits maximum)	
Additional Data	Number of characters	
	Expiration Date (YYMM)	4
	Service Code	3
Discretionary Data	Number of characters	
	PVKI - Pin Verification Key Indicator	1
	PVV (or Offset) - Pin Verification Value	4
	Card Verification Value (CVV) or Card Validation Code (CVC)	3
	Some or all of the PVKI, PVV, CVV, and CVC, fields may be found with the Discretionary Data.	
Table B-3 (page 2 of 2)		

Track 3 (Card Data Format)

Figure B-6 provides a graphical representation of the fields in Track 3 and Table B-4 provides a description of the fields.

Figure B-6 Card Data Format, Track 3 (ISO 4909)

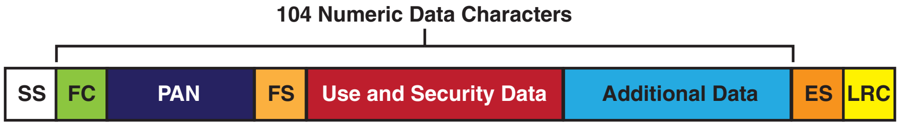


Table B-4 Card Data Format, Track 3 (ISO 4909) Field Descriptions/Lengths

Field	Description/Length
SS (control character)	Start Sentinel (%)
FS (control character)	Field Separator (^)
ES (control character)	End Sentinel (?)
FC	Format Code (2 digits)
LRC	Longitudinal Redundancy Check character
PAN	Primary Account Number (19 digits maximum)
Name	Name (25 alphanumeric characters maximum)
Table B-4 (page 1 of 2)	

Table B-4 Card Data Format, Track 3 (ISO 4909) Field Descriptions/Lengths

Field	Description/Length	
Use and Security Data	**Number of characters**	
	Country Code (*optional)	3
	Currency Code	3
	Currency Exponent	1
	Amount Authorized per Cycle	4
	Amount Remaining per Cycle	4
	Cycle Begin (Validity Date)	4
	Cycle Length	2
	Retry Count	1
	PIN Control Parameters (optional)	6
	Interchange Controls	1
	PAN Service Restriction	2
	SAN-1 Service Restriction	2
	SAN-2 Service Restriction	2
	Expiration Date (optional)	4
	Card Sequence Number	1
	Card Security Number (*optional)	9
Additional Data	**Number of characters**	
	First Subsidiary Account Number (*optional)	
	Secondary Subsidiary Account Number (*optional)	
	Relay Marker	1
	Cryptographic Check Digits (*optional)	6
	Discretionary Data	
	*A Field Separator (FS) must be used if an optional field is not used.	

Table B-4 (page 2 of 2)

Proximity Badges

By default, ATS Supports 26-bit Wiegand™ and 34-bit standard binary data format for proximity badges and readers, such as those provided by HID.

The 26-bit format is an open format, which means the format description is not proprietary but is available publicly for any manufacturer to use. The 26-bit format is a widely used industry standard. The 26-bit format includes:

- The maximum facility code is 255, which is the decimal equivalent of setting all eight facility code bits to one.
- The maximum card number is 65,535, which is the decimal equivalent of setting all sixteen card number bits to one.
- A parity bit is used to check the accuracy of transmitted binary data.

Additionally, ATS offers a service that allows a structured data string to be sent to the terminal to support additional binary data formats up to 75 bits. To use this service, a customer provides ATS with the decoding format and ATS creates and provides a custom string for use with their terminal.
Please contact ATS technical support at 860-870-5000 if you need additional assistance.

Using the USB

C

Appendix

About this Appendix

This Appendix describes how to use a portable USB drive with your terminal.

Appendix Contents

This Appendix contains the following topics:

This page intentionally left blank.

Overview

What You Need

To use a USB drive with your terminal, you need a portable USB drive and access to the USB port on the terminal.

Functions

You can use a portable USB drive to do the following:

- Apply a download (.dld file) to the terminal – see “Applying a Download” on page C-4
- Store punches and transactions when the terminal is disconnected from the network – see “Storing Punches” on page C-5
- Update UCS – see “Updating UCS” on page C-7.

Additionally, you can use a standard USB keyboard with the terminal’s USB port. See “Using a USB Keyboard with the Terminal” on page C-8.

Applying a Download

A download file is a text file used to configure a terminal. Typically, a download file has a **.dld** file extension (for example, GlobalDownload.dld). To apply the download to a terminal using a portable USB drive:

1. Create the download file on a computer. Name it using a **.dld** extension.

NOTE: **Download files must have a .dld extension. Also, they cannot be in folders or directories on your USB drive; they must be in the root of the USB drive. Otherwise, the terminal cannot find the download file.**

2. Copy the download file from the computer to the root of your portable USB drive.

3. Safely remove the USB drive from your computer.

NOTE: **A terminal that is in Setup, Test, or Information Mode will not mount the USB drive. Make sure you exit those modes before plugging the USB drive into the terminal.**

4. Plug the USB drive into the USB connector on the terminal.

5. Access and select the **Download from USB** option.

6. Select **Download from USB**.

   - If there is only one .dld file in the root directory of your USB drive, the terminal downloads and applies it to the terminal.
   - If there are more than one .dld file in the root directory of your USB drive, the terminal lists the download files for you to navigate between. Press **E** to select the download you want to use.

NOTE: If you unplug the USB drive from the terminal while the list of downloads displays on the terminal, you can select a download from the menu but the download is neither downloaded nor applied. You must then reboot the terminal before you can retry downloading from the USB drive.

7. After you finish, unplug the USB drive from the terminal.

Storing Punches

The download your terminal uses must support saving punches and transactions to a portable USB drive. The download must define a function key on the terminal to save punches and transactions to a USB drive. Also, your terminal must be offline.

- You cannot use this feature if the terminal is online with the network.
- If you have reset the download or are using a download that doesn't support storing punches to USB, then you cannot use this feature.
- You cannot use this feature if you have applied a download but have not yet rebooted; reboot a terminal to which you applied a new download if you want to store punches to the USB drive.
- Use the S40 prompt in the L02C00 command in UCS to define a function key for this selection. For more information on L02C00 and S40, see the Universal Command Set (UCS) Reference Manual, Part Number MANU-UCS-01.

If the terminal is disconnected from the network, then you can save the following transactions and punches to the USB drive: pending status commands (such as AG00 or AG01), any pending status generated by a USB download load, any fingerprint template enrolls, and any pending punches.

NOTE: **You can use Accu-Engine Ethernet to view the online status of a terminal on the network.**

To save punches to the USB drive:

1. Make sure the terminal is offline and not connected to the network. You must wait a short time after the connection is lost.

NOTE: **A terminal that is in Setup, Test, or Information Mode will not mount the USB drive. Make sure you exit those modes before plugging the USB drive into the terminal.**

2. Plug the USB drive into the USB connector on the terminal.
3. After transactions have been processed by the terminal (employees punching in or out, etc.), press the function key that is set up to send data to the USB drive.
4. A message displays whether the data was saved successfully to the USB drive.

If the data is not saved successfully to the USB drive:

- Follow up on any messages displayed by your terminal.
- Reboot the terminal and try again to save data to the USB drive.
- From the USB drive, send a download that supports saving files to USB to the terminal.

To review the transactions and punches that were saved to the USB drive:

1. Unplug the USB drive from the terminal.
2. Plug the USB drive into a computer.
3. Review the contents of the USB drive using the computer.

   The file that the terminal puts on the USB drive is named using 18 numbers and the extension “**.usb**”, such as *yymmddhhmmssNNNNNN.usb*, such as 080229150528000090.usb, where:

   - yy = the last two digits of the year the file was created
   - mm = the month the file was created
   - dd = the day the file was created
   - hh = the hour of the time the file was created
   - mm = minutes of the time the file was created
   - ss = seconds of the time the file was created
   - NNNNNN = the last six digits of the terminal’s MAC address
4. Open the “**.usb**“ file using a text editor, such as Notepad.exe.

   If you are prompted convert the file to DOS format, select **Yes**. Converting to DOS format does not change any of the data in the download, it just makes the .usb file easier to read for Windows.
5. The file contains a list of transactions and punches. See the Universal Command Set Reference Manual for more information about the contents of the .usb file.

Updating UCS

You can update UCS using a USB drive.

1. Copy the download file from the computer to the root of your portable USB drive.

2. Safely remove the USB drive from your computer.

NOTE: **A terminal that is in Setup, Test, or Information Mode will not mount the USB drive. Make sure you exit those modes before plugging the USB drive into the terminal.**

3. Plug the USB drive into the USB connector on the terminal.

4. Put the terminal in Setup Mode.

5. Reboot the terminal.

6. The updates are applied as the terminal reboots.

Using a USB Keyboard with the Terminal

With UCS version 2.04.05, the terminal lets you plug any standard USB keyboard into a terminal and perform all the same functions on it as you can on the terminal keypad.

On the standard USB keyboard, F1 through F8 operate the terminal's F keys, the Backspace key operates the terminal's Clear key, Enter operate's the terminal's Enter key, and all numbers and letters correspond to numbers and letters on the terminal keypad. Additionally, for an OPTIMUS terminal, the USB keyboard's arrow keys function as the arrow keys on the terminal.

GSM/GPRS Setup

D

Appendix

About this Appendix

This Appendix describes details about setting up a GSM/GPRS Modem.

Appendix Contents

This Appendix contains the following topics:

Introduction

This Appendix describes to ATS VARs how to set up a GSM modem on Global series terminals.

Currently, GSM modems are available for use with T-Mobile in the USA and a variety of carriers in Europe and Asia, including O2. Check with your strategic account manager (SAM) for the latest list of carriers supported.

Hardware

Using a GSM modem on a Global terminal requires these items:

- SIM card (subscriber identity module) enabled for use with a supported carrier at GPRS modem speeds (approximately 50 kbps – faster speeds are unsupported)
- Antenna to plug into the GSM modem
- GSM modem that plugs into the terminal's serial port

Installing the Hardware

Install the hardware:

1. Insert the SIM into the socket in the GSM modem.
2. Open the terminal and plug the GSM modem into the serial connection.
3. Feed the antenna cable from the outside of the terminal case through the antenna hole into the interior of the terminal case.
4. Plug the antenna cable into the receptacle on the GSM modem board.
5. Secure the antenna on the outside of the terminal case using double-sided tape.
6. Close the terminal.

Software

GSM modems require version 2.03 or later of the ATS operating system (UCS, Java, etc.). After you make sure that version 2.03 is installed, configure the terminal for use with the GSM modem.

Using the Setup Menu on the Terminal

If the terminal is preconfigured with your wireless service provider, you can select PPP and the provider using the terminal's menus. To select a terminal's menu mode, press the **Clear** and **Enter** keys together on a terminal's keypad. (For more information on Setup Mode and Test Mode, see the terminal's datastation manual or user guide.)

1. Enable **Ethernet** instead of serial communication.
2. Enable **PPP**.

3. Select your wireless service provider in the **Provider** or **Service Provider** menu.

The host computer needs to have an Internet-facing IP address and any firewall needs to permit communication on the port selected for the terminal, which is 2500 by default.

4. Set the **Host IP** to the IP address of the host computer with which your terminal will communicate.

Manually Configuring a GSM Terminal

If your provider is not preconfigured in the terminal, you must configure the GSM terminal.

- Enable PPP
- Set up a provider peer configuration file
- Set up provider authentication

Enable PPP

PPP can be selected from the terminal's setup menu as well as enabled at the command-line level.

The underlying networking system that manages a cellular data connection is the Point-to-Point Protocol (PPP). This system handles connection dialing, authentication, data rate negotiation, and the core data exchange process. The PPP system needs some basic information in order to interact with the hardware and communicate with the end server. This information is stored in peer files and chat scripts in these directories on your terminal:

- /etc/ppp/peers
- /etc/ppp directories

To enable PPP, log on to the terminal and use the following command:

```
/ # echo pppEnabled = 1 > /dev/atsconfig
```

To disable PPP, log on to the terminal and use the following command:

```
/ # echo pppEnabled = 0 > /dev/atsconfig
```

You can also enable and disable PPP using the setup menu on the terminal.

Set up a Provider Peer Configuration File

When PPP is enabled it automatically loads the peer configuration file located in the /etc/ppp/peers/peer directory. This file is actually just a symbolic link pointing to the intended PPP peer. To configure the PPP for a new service provider, modify by modifying this link.

For example, to set up a clock to use T-Mobile as the provider we see the following in our peers directory, go to the peers directory:

```
/ # cd /etc/ppp/peers
```

Then, run the –sf option to the ln (link command) that identifies T-Mobile as the provider. Note that you can also set the provider using the Setup Menu on the terminal.

```
/etc/ppp/peers # ln -sf t-mobile peer
```

If you list the peer configurations, notice that T-Mobile is set as the current provider but other links are defined. For example, in this case ATT could be set as the provider by using the –sf switch because a link for ATT is defined.

```
/etc/ppp/peers # ls -l
-rw-r--r-- 1 500 500 215 Jan 12 21:16 att
-rw-r--r-- 1 500 500 198 Jan 12 21:16 o2
lrwxrwxrwx 1 root root 8 Feb 3 20:23 peer -> t-mobile
-rw-r--r-- 1 500 500 195 Jan 12 21:16 proximus
-rw-r--r-- 1 500 500 202 Jan 12 21:16 t-mobile
-rw-r--r-- 1 500 500 207 Jan 12 21:16 t-mobile-uk
```

Set up a New Provider

If the provider you want isn’t already a link, you can set up the new provider. There are three components that make up a complete provider configuration: the peer file, the chat script, and the authentication information. In order to create these files you will need to obtain this essential information from your service provider:

- Username and password
- Connection endpoint or access point name (APN)
- Frequency band of operation

Then, you will need to create and modify three files:

- Peer file
- PPP password file
- Chat file

Creating a Peer File

Peer files are in the /etc/ppp/peers directory. Copy an existing one then modify the first two lines to create a new peer file.

- Modify the first line to set the username, such as “t-mobile.”
- Modify the second line to use the name of your new chat script.

```
/etc/ppp/peers # cat nameofpeerfile
user "enter-a-username-here"
connect "/usr/sbin/chat -v -f /etc/ppp/connect-yourchatfile-
name"
/dev/ttyS2 115200
persist
maxfail 0
```

```
modem
#noipdefault
usepeerdns
defaultroute
ipcp-accept-local
ipcp-accept-remote
lock
crtscts
debug
```

Editing the PPP Password File

The PPP password file is found here: /etc/ppp/pap-secrets. Open and modify this file to include the username and password combination you want for your connection. The username is the same one you set in the first line of the peer file.

```
/etc/ppp # cat pap-secrets

# Secrets for authentication using PAP

# client    server secret IP addresses

* * "" *

"tm" * "tm"*

"user" * "one2one" *

"isp@cingulargprs.com" "CINGULAR1" *

"mobileweb" *"password"*

"enter-a-username-here" * "enter-password" *
```

Editing a Chat File

The chat files are found here: /etc/ppp. Open and modify an existing chat file. You need to provide the endpoint information, or access point name (APN), which is provided by your service provider, as well as the frequency of the signal.

- The endpoint is placed in the second set of quotes in the AT+CGDCONT command. In this case, the endpoint begins with **wap** but does not have to.
- Frequency is set in the AT+WMBS command based on the provider frequency.
  - A value of 850MHz or 1900MHz requires you enter **4,1**
  - 900MHz or 1800MHz requires you enter **5,1**

```
/etc/ppp # cat connect-yourchatfilename

ABORT 'BUSY'

ABORT 'NO CARRIER'

ABORT 'ERROR'

" " ATV1

OK AT+WOPEN=0

OK AT+WMBS=5,1

OK AT+CGDCONT=1,"IP","wap.endpoint.somewhere"

OK ATD*99***1#

CONNECT " "
```

Communication Speed

It takes about one second to transmit one line of an ATS UCS download. You can speed up your transmission of downloads by compacting the download. Compact downloads have these features:

- Up to 1500 characters in one line
- Each command must begin with this string (where ➲ is a group separator)
  - \A!➲
- Each command must end with a record separator (where ^ is a record separator)
  - \A!➲ON00A^
- Each line up to 1500 characters must end with an end-of-transmission character (where EOT represents that end-of-transmission character)
- Use of EOT must be enabled in the terminal's Setup menu

Verifying Wireless Connectivity

To verify wireless connectivity, use the setup menu on the terminal to test for signal strength. This tells you how strong the wireless signal is for the terminal in its current location. Signal strength needs to be a value of 10 or higher for connectivity and better connectivity—15 or higher—is required for troubleshooting connections.

To test for signal strength and wireless connectivity:

1. Make sure **PPP** is enabled for the terminal.

2. Make sure a configured provider has been selected for the terminal.

NOTE: You do not need to install a SIM card to test signal strength. A SIM card can be installed later for communication.

3. Select **Test Mode** on the terminal.

4. In Test Mode, select **GSM Signal Strength.**
GSM Signal Strength displays a number, from 0 to 32, that displays the signal strength of the wireless connection with the terminal's antenna in its current location.

5. Move the antenna (and the terminal, if necessary) to achieve a signal strength of at least 10. If you are going to troubleshoot a connection, a signal strength of at least 15 is required.

Index

This page intentionally left blank.

Your Trusted Partner for Time and
Attendance Terminals and Integrated Solutions

Reference Manual

Maximus Reference Manual

Part Number: MANU-MAXIMUS-02
Revision-02