



GT-Series

Terminal User's Guide



This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and, if not installed and used in accordance with the Installation Manual, may cause unwanted interference to radio communications.

Operation of this equipment in a residential area is likely to cause unwanted interference, in which case the user will be required to correct the interference at the user's own expense.

This Class A digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numérique de la classe A respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.

© 2012 Ingersoll Rand – ALL RIGHTS RESERVED

Document Part Number: 70100-7500 – Revision D – March 2012

Recognition Systems Company, LLC (dba Schlage Biometrics)

Schlage, GT-400, HandKey, HandReader, HandPunch and BackHand are trademarks of Schlage Lock Company LLC, Ingersoll-Rand Company, and/or their affiliates.

All other trademarks are owned by their respective owners.

Schlage Biometrics reserves the right to change, without notice, product offerings or specifications.

No part of this publication may be reproduced in any form without the express written permission of an Officer of Schlage Biometrics.

Table of Contents

- Chapter 1: Introduction 11**
- Using the GT-Series Terminal 11
 - Using Biometrics 11
 - How GT-Series Terminals Operate 11
 - Verification with GT-Series Terminals 12
 - 12
 - GT-Series Terminal Features. 13
 - GT-Series Terminal Specifications. 14
- Reviewing GT Series Terminal Operations 15
 - Command Menus. 15
 - Using the GT Series Terminal Keypad. 15
- Chapter 2: Important Information for Installers and Terminal Administrators 17**
- Network Setup and Ethernet Switches 17
- Power-on and Shutdown Precautions 17
- Using the Terminal Command Menu 17
- Synchronizing the Reader Before Enrolling Any Users 18
- Terminal Configuration Options 19
- Start-up Sequence 20
- Server Network Considerations With Firewalls/Security Software 21
- Clearing Interactions 22
- Precautions When Moving a Terminal Between Different Hosts 22
- Chapter 3: Terminal Installation 23**
- GT-Series Terminal Installation 23
 - Terminal Placement 23
 - Removing the Terminal from the Box. 24
 - Wall Preparation. 25
- Attaching the Wall Plate 28
- Hang Terminal and Run Wires 29
- Making Back Board Connections 31
- Attaching the Ferrite Clip 32
- Printer Setup (Optional) 33
- Removing/Installing Side Covers 34
- Removing Side Covers 34
- Installing Side Covers 35
- Attaching the Terminal to the Wall Plate 36
- Chapter 4: Setting Up the GT-Series Terminal 37**
- Network Mode Configuration 37
 - Using the Terminal's Command Menus for Configuration 37

Using the Terminal's Web Server for Terminal Configuration	38
Using Your Customized Host Application (GManager) for Terminal Configuration	40
Verifying Synchronization with the Host Application	40
Check the Terminal Status in the Terminal Command Menus	40
Change the Ready Screen Message	40
Check the RSITerm.log File From a Telnet Session	40
Demo Mode Configuration	42
Creating the Terminal Administrator Account	44
Shutting Down the Terminal	44
Shutting Down the Terminal Using the Terminal Interface	44
Shutting Down the Terminal Using Telnet	44
Chapter 5: Basic Operations	45
Reviewing the Terminal Front Panel and Interface	45
Startup Screen	46
GT-Series Terminal Startup Screen	46
Terminal Operation Tips and Tricks	46
Terminal Time-Outs	46
Entering Text	46
Navigating a Long List	47
Accessing Command Menus	47
Administrator Authentication	47
Recommendation: Create an EPIN for the Terminal Administrator	47
GT-Series Terminal Authentication	47
Creating and Enrolling Users	48
Creating an ID Numbering System	48
Creating a User from the Terminal	48
Enrolling a User	48
Setting User Data	49
Edit Timezone	49
Edit Authority	49
Add Credential	50
Edit Threshold	50
Edit Name	51
Remove a User	51
Setting Date and Time	52
Set Locale Timezone	52
Set Terminal Date	52
Set Terminal Time	53
User Authentication	53
Checking the Terminal Software Version	53
Updating the Terminal Software	53
Rebooting the Terminal Using the Terminal Interface	53

Chapter 6: Command Menu Reference 55

- Reviewing the Command Menu 55
- Command Menu Structure 56
- Setup Menu 57
 - Timezone Menu 57
 - Edit Timezone. 57
 - List Timezones 58
 - Add Timezone. 59
 - Print Setup 59
 - Set PrintBookings 60
 - Set Baud Rate. 60
 - General Setup 61
 - Set Terminal Date. 61
 - CmdLine Setup. 62
 - Set Time&Attend. 62
 - Set Terminal Time. 63
 - Set LocaleTimezone 63
 - Set ID Length 64
 - Set LogFile Size Factor. 65
 - Set CR Num of Prefix Chars. 66
 - Set Door Unlock Time. 66
 - Set CR Terminator String 67
 - Set Beeper 67
 - Set Duration to Retain Sent 68
 - Set Lunch Punch Lockout Secs 68
 - Holiday Menu 69
 - Edit Holiday. 69
 - List Holidays 70
 - Add Holiday. 70
 - Network Setup 71
 - Set Logical Name 71
 - Set Host Username. 72
 - Go to StandAlone or Demo Mode. 73
 - Set WebServer 74
 - Set Host Password 74
 - Set Host URL 75
 - Set CLISvr Port. 76
 - Set XMLRPCSvr Port 77
 - XMLRPC Svr Setup 78
 - Set WebSvr Port. 79
 - Set Static/DHCP 80
 - Set RealTimeInteraction 81
 - Display Setup 81
 - Set Company Name 81
 - Set Time Format. 82

Set Date Format	82
Set Ready String	83
Set Language	83
User Management	84
Edit User	84
List Users	84
Edit Name	85
Enroll Status	85
Edit Authority	86
Last Score	87
Edit Threshold	88
Verify Status	89
Edit Timezone	89
Edit User Status	90
Enroll User	90
Last Booking	91
Generate Punch	91
Remove User	92
List Credentials	93
Add Credential	94
No Hand Enroll	95
Edit EPIN	96
Edit Access Grant	97
List Access Grants	98
Add Access Grants	99
List Bookings	100
Add User	100
Security Menu	101
Clear Setup	101
Biometric Setup	101
Placements Per Try	102
Number of Tries	103
Set Passwords	104
Clear UserDB	105
Factory Settings	105
Reject Threshold	106
Set Credential Logging Flag	107
Restore Factory Password	107
Maintenance Menu	108
Partial Sync Now	108
Sync Now	108
Reboot	109
Terminal Status	110
Delete Sent Interactions	111
Shutdown	112

Last Punch	112
FKScript List Menu	113
Activating the Function Key Script	113
FKScript List	113
Activating the Function Key Script (FKScript List option)	113
Timecard Approval	115
Accrual Balances	115
Cancel Meal	116
Lunch Punch (Meal Compliance)	116
Time Off Request	117
Transfer-ValidList	118
Chapter 7: Understanding GT-Series Biometric	
Terminals	119
Reviewing Hand Geometry Basics	119
Hand Geometry Considerations	119
Proper Hand Placement	119
Understanding Hand Read Scores	120
Understanding Verification Messages	120
Reviewing LED Bar Indications	121
When Terminal is Idle	121
During Verification	122
During Enrollment	122
Cleaning the Terminal and Platen	123
Chapter 8: Troubleshooting	125
Viewing Terminal Status	125
Using the Terminal	125
Using a Web Browser	125
Using Telnet	125
Choosing a Telnet Client	125
Logging In and Out of Telnet	126
Using a Telnet (PuTTY) Session	127
Changing the Telnet Password	128
Navigating the File System	128
Changing Directories Using the cd Command	128
Viewing Terminal Processes Using the ps Command	129
Rebooting the Terminal Via Telnet	129
Shutting Down the Terminal Via Telnet	129
Shutting Down The Application Via Telnet	129
Starting the Application in Verbose Mode	130
Accessing a Terminal in Demo Mode Through Telnet	130
Using the Terminal Log File	131
Viewing the Log File Using the cat Command	131
Viewing the Last Few Lines of the Log File Using the tail	
Command	131

Saving the Log File to Your Computer	131
Returning the Terminal to Its Factory Settings	132
Through Telnet	132
Through the Terminal Interface	132
Using the Terminal Command Line Interface (CLI)	133
Logging in and out	133
Starting the CLI	133
Exiting the CLI	133
Viewing Help	133
Saving the Output to a Text File On Your Computer	133
Retrieving Sent/Unsent Interactions From Terminal	134
Troubleshooting Summary	135
Index	137

Introduction

1

Using the GT-Series Terminal

The GT-Series Terminal is the first member of the Schlage G-Series biometric hand geometry time and attendance terminals. The GT-Series Terminal records and stores the three dimensional shape of the human hand for comparison and identity verification. Upon verification, the terminal records the time, date, user ID number and collected time and attendance data and makes this information available for collection by a host computer. The terminal can produce an output to operate an auxiliary device, such as an electronic door lock or signal bell, and it can communicate with a host computer. The terminal also has auxiliary inputs that can be used to control other systems.

A third-party/custom host application communicates with GT-Series Terminals across a TCP/IP network, maintaining and storing data collected by the terminals, analyzing and updating data, maintaining security and initiating alarms as necessary. Access to this data is achieved through a web browser or custom application. The GT-Series Terminal provides employee identification verification and includes the sophisticated operating features one expects in a time and attendance terminal. Because of this unique combination of capabilities, the GT-Series Terminal provides the most accurate and flexible time and attendance data collection terminal available.

Using Biometrics

As with the GT-Series Terminals, Schlage offers hand geometry terminals which are one of the most widely used biometric technologies for time and attendance applications. Hand geometry technology uses the size and shape of the person's hand to verify the user's identity. Schlage biometric solutions also offer multi-authentication options. Smart card, proximity and magnetic stripe readers can be integrated into the terminals to provide an extra layer of security customized to the application requirements. Some of the world's largest providers of time and attendance systems recommend Schlage HandPunch terminals as part of their total solution. By using biometric technology, corporations reduce payroll costs and eliminate "buddypunching" fraud.

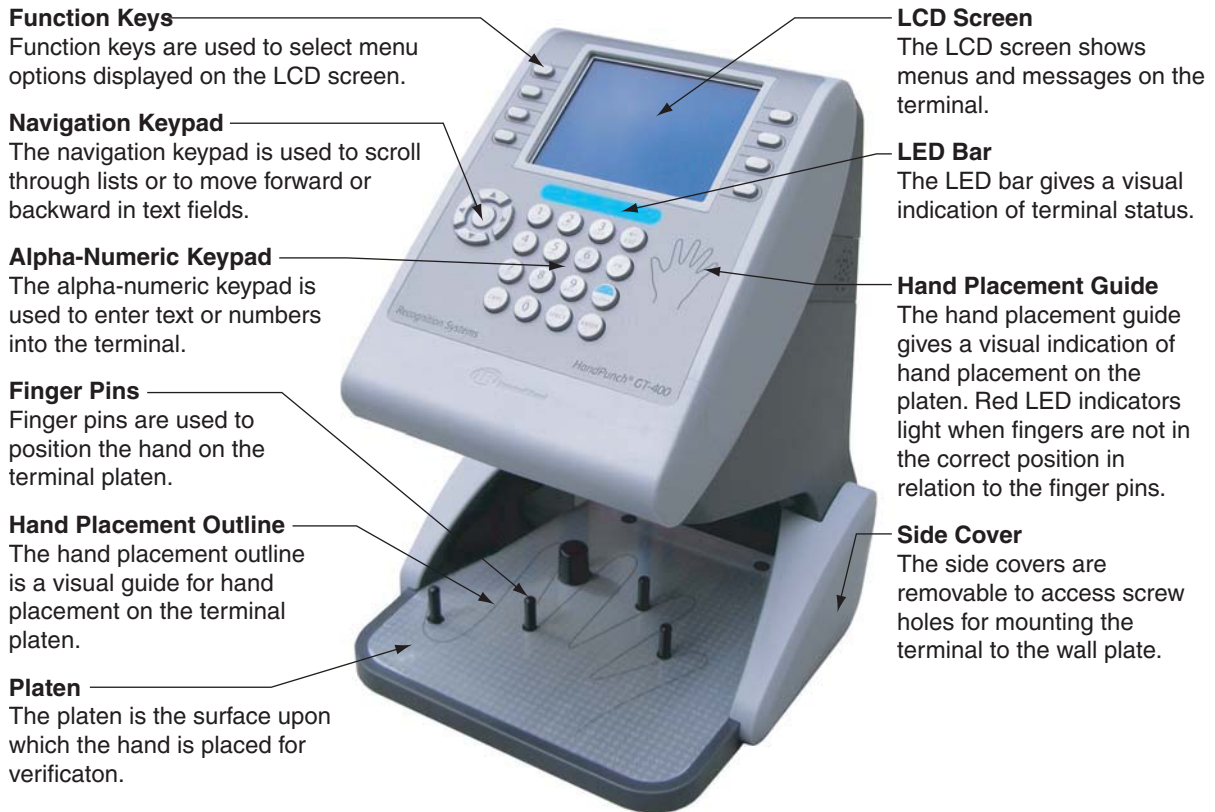
How GT-Series Terminals Operate

The GT-Series Terminal uses low-level infrared light, optics and a CMOS (IC chip) camera to capture a three-dimensional image of the hand. Using advanced microprocessor technology, the terminal converts the image to an encrypted electronic template. It stores the template in a database with the user's ID number. To gain access, the user enters his or her ID number using the terminal keypad or uses an optional, built-in card reader. The terminal prompts the user to place his or her hand on the terminal's platen. The terminal compares the hand on the platen with the user's unique template. If the templates match, the terminal records the transaction for processing.

Verification with GT-Series Terminals

Verification refers to the process of placing the hand on the terminal platen as a part of the authentication process. Authentication consists of entering a user identification number on the terminal's alpha-numeric keypad and verification of the hand.

GT-Series Terminal Features





GT-Series Terminal Specifications

Table 1-1: GT-Series Terminal Specifications

Specification	Description
Size	8 inches (20.32 cm) wide by 11.18 inches (28.40 cm) high by 7.52 inches (19.10 cm) deep
Weight	5.60 lbs (2.54 kg) – 6.90 lbs (3.13 kg) with optional backup
Power	12 VDC nominal (10.8 to 13.5 VDC), 4.5 Watts max. linear power supply recommended
Transient Protection	8,000 volts – all terminals
Reverse Voltage	on power input
Environment	Operating: 32°F to 113°F (0°C to 45°C) Relative Humidity: 5% to 95%, non-condensing Non-operating (storage): -40°F to 185°F (-40°C to 85°C)
Verification Time	less than one second
Date Retention	3 years using a standard internal lithium battery
Transaction Buffer	memory card-dependant
Baud Rate	9600 to 115200 bps
Communications	TCP/IP over Ethernet – 10/100 Base T
Function Keys	8 programmable soft keys
Alarm Monitoring	Unit Tamper
Relay Output	1 – 250 VAC @ 10A
Battery Backup (optional)	2 hour minimum run time

Reviewing GT Series Terminal Operations




Command Menus

Command menus are the menus in the terminal that are used to configure the terminal. The command menus can be accessed by pressing  and then  from the Ready screen. If the terminal is a new terminal and has no users, the command menus will immediately appear. After the administrator has been created and enrolled, verification will be required to access the command menus.

Using the GT Series Terminal Keypad

There are three types of keys used to make entries into the terminal. Each will be indicated in this guide as shown below.

Table 1-1: Types of Terminal Keys and Corresponding Symbols

Type of Key	Location and Purpose	Symbol
Function Key	These keys are located on both sides of the terminal screen. They are used to navigate through the command menus	
Alpha-Numeric Key	These keys are located in the terminal keypad. They are used to enter letters and numbers into the terminal.	
Navigation Pad	These keys are located to the left of the terminal keypad. They are used to navigate through lists displayed on the terminal screen. The middle key can be used as an “Enter” or “Select” key.	

Important Information for Installers and Terminal Administrators

2

NOTE: Field installers and terminal administrators should read this section thoroughly before attempting to install or configure a GT-Series Terminal site. It explains important concepts and lists required administrative terminal operations.

Network Setup and Ethernet Switches

For best performance, it is recommended that you use ethernet switches to connect the terminal(s) to the host, rather than ethernet hubs. Using ethernet hubs to connect the terminal(s) to the host may lead to terminal instability. If instability is encountered while using ethernet hubs, you may need to reboot the terminal(s).

➔ See *“Rebooting the Terminal Using the Terminal Interface”* on page 53 for more information.

Power-on and Shutdown Precautions

- If your terminal is equipped with a backup battery, it should be connected after power has been applied to the terminal.
- ➔ See *“Making Back Board Connections”* on page 31 for more information.
- The network (ethernet) cable must be connected to the terminal before applying power. The terminal establishes itself on the network during start-up. You will not be able to communicate with the terminal if the cable is not connected before applying power. Other connections, including optional USB, or serial or auxiliary relay connections, should also be made before applying power.

 **The terminal must not be disconnected from its power source without shutting down the application first. See “Shutting Down the Terminal” on page 44 for more information.**

Using the Terminal Command Menu

The terminal command menu allows you to manage your terminal and perform a variety of associated administrative tasks. To be able to access command mode you must be enrolled with administrative level privileges (level 5).

➔ ***It is assumed that the first person to use a new terminal would be the administrator. As such, the first person to access the Command Menu will by default be able to access this menu.***

➔ See *“Command Menu Reference”* on page 55 for more information.

Synchronizing the Reader Before Enrolling Any Users

The reader must be synchronized with a host server before creating any content, such as enrolling users. If users are created on a reader before the first synchronization, those users will be deleted from the reader.

➔ See ***“Sync Now” on page 108 for more information.***

Terminal Configuration Options

There are three ways to configure a new terminal. The table below lists each of the three methods for terminal network setup, as well as information on which situations to which each method best applies.

➔ **Terminal configuration tasks are described in more detail in “Network Mode Configuration” on page 37.**

 **When the terminal is configured for network connection any existing data (including users) will be deleted.**

Figure 2-1 Terminal Configuration Options




Setup Option	Do I need to use this?	When do I use it?	Usage Guidelines
GManager or equivalent. (Your customized Host Application which uses the Discovery feature)	<p>Yes, if:</p> <ol style="list-style-type: none"> The terminal has application software installed on it <p>OR</p> <ol style="list-style-type: none"> The default BSP or application software that comes on the terminal needs to be updated <p>No, if</p> <ol style="list-style-type: none"> The terminal already has the BSP and application software on it <p>AND</p> <ol style="list-style-type: none"> No upgrades to the terminal’s BSP or application software are required 	During terminal software updates or terminal start-up with a computer.	When there are a number of terminals in varying physical or geographical locations (but on the same LAN) the GManager Discovery feature can set them up quickly and efficiently.
Terminal Web Server	<p>Yes, if the GManager discovery feature was not used to configure the terminal.</p> <p>No, if the GManager discovery feature was used to configure the terminal.</p>	After the terminal application has started, from a web browser.	The web server is one of the is the fastest ways to set up terminals, provided that the application is already present on the terminal.
Terminal Command Menus	<p>Yes, if the GManager discovery feature was not used to configure the terminal.</p> <p>No, if the GManager discovery feature was used to configure the terminal.</p>	After the terminal application has started, using the terminal’s keypad.	If the GManager discovery feature and the terminal web server are not viable options, then the terminal’s user interface can be used.

Start-up Sequence

When you apply power to a terminal, it goes through the start-up sequence. First the operating system loads. Then the terminal checks to see if there are any software updates (from the host application). Finally, the terminal application loads.

The table below describes the stages of the start-up sequence and the available options for configuration (shown in the red columns):

Configuration Options

Stage	Description	Terminal Behavior	GManager Discovery Feature	Command Menus	Web Server	Options
1	Operating System Loading	LED Flash Cycle				N/A
2	Software Update	Single beep, followed by messages on the terminal screen	Yes**			Press  for more time Press  and  to skip this stage.
3	Terminal Application	"Enter ID", date and time displayed on the terminal screen		Yes	Yes	N/A
4	Terminal Synchronization					N/A

**Each connection attempt may take up to three (3) minutes. During that time, the terminal may appear to be unresponsive. Wait for three (3) minutes for the terminal's processes to time out before attempting to perform any other actions.

The following steps describe the stages of the start-up sequence:

1. Operating System Loading

- Description: Terminal screen illuminates and LED bar cycles through its colors
- Duration: 30 seconds
- Completion: the LED bar turns blue

2. Software Update

➔ ***If you are opting to use the GManager Discovery feature to configure your terminal, you would use it during this stage. This feature is not available if you are using a new “out-of-the-box” terminal which has not yet been configured in GManager.***

- Description: The terminal checks the host server to see if it needs to download any updates to its software. This application functions only if the terminal is connected to a network that is also running a host application. Software updates should be loaded into the host application.
- Duration: 1 second (if skipped) up to 10 minutes (if configured here and software is downloaded)
- Completion: if not skipped, it is completed when no updates are found on the host server

3. Terminal Application loads

➔ ***If you are opting to use the terminal’s web server or terminal command menus to configure your terminal, you would use one or the other after this stage.***

- Description: The time and attendance application starts
- Duration: approximately 2+ minutes
- Completion: the date and time are displayed on the terminal LCD

4. Terminal Synchronization

- The terminal performs a full synchronization with the host application.
➔ ***See “Sync Now” on page 108 for more information.***

Server Network Considerations With Firewalls/Security Software

Your network configuration may be configured with firewalls or security software that is designed to report or deny certain operations. For this reason, certain features and commands in the GT-Series Terminal (listed below) may not work, or cause the terminal to be inoperable if your network denies those actions. These include:

- The terminal’s XML-RPC server
➔ ***See “XMLRPC Svr Setup” on page 78 and “Set XMLRPCSvr Port” on page 77 for more information.***
- The terminal’s web server
➔ ***See “Set WebSvr Port” on page 79 for more information.***
- The terminal’s CLI server (if accessed outside of telnet)
➔ ***See “CmdLine Setup” on page 62 for more information.***
➔ ***If the CLI is accessed with telnet, it will function normally.***

If you want to use any of these features, it is recommended that you test them on your network to make sure that they function before using them in a live installation. If any of

these features do not work, they can easily be disabled through the terminal command menus, or through your host application. None of these features are required for database synchronization.

Clearing Interactions

Interactions that have *not* been sent are saved on the terminal indefinitely. Therefore, interactions must be periodically purged in order to make room for new interactions. The terminal administrator should create a schedule for purging interactions.

If interactions are not cleared on a schedule, and the SD card gets close to being full, the terminal will display the message, “SD Card Capacity Low”. This message will occur first when the SD Card capacity is 30% full. When this message is displayed, interactions should be cleared immediately. The reader will stop accepting punches when it is 45% full.

! *If the SD card becomes full, users will not be able to punch until the interactions are cleared. Administrator operations and command menu accesses are not affected when SD card is full*

The Delete Sent Interactions function will clear only those interactions that have been sent to the host application. See “Delete Sent Interactions” on page 111 for more information.

Precautions When Moving a Terminal Between Different Hosts

➔ *The following information assumes that you, as the administrator, have familiarized yourself with OBJIDs and managing a terminal’s database. For more information on these topics, see the GT-Series Terminal Terminal Network Guide.*

Before disconnecting a terminal from one host and connecting to another host, the terminal’s database must be reset.

IMPORTANT: *If you do not delete a terminal’s database, it will have objects with OBJIDs assigned in a range that the previous host application assigned, and which the new (current) host application has no knowledge. As such, you could potentially corrupt your new host database with objects that have duplicate OBJIDs.*

Use one of the following options when moving a reader to another host:

1. Delete the reader database before changing the host.
2. Reset the reader database to factory settings using the reader GUI.
3. Change the logical name of the reader on the new host to which you will connect the reader.

Terminal Installation

GT-Series Terminal Installation

Terminal Placement

The recommended height for the terminal's platen is between 40 and 48 inches (102 - 122 cm) from the finished floor. This height conforms to the Americans with Disabilities Act (ADA) standards (40 inches is recommended for ADA standards). All terminals within a site should be placed at the same height.

The terminal should be out of the path of pedestrian and vehicular traffic.

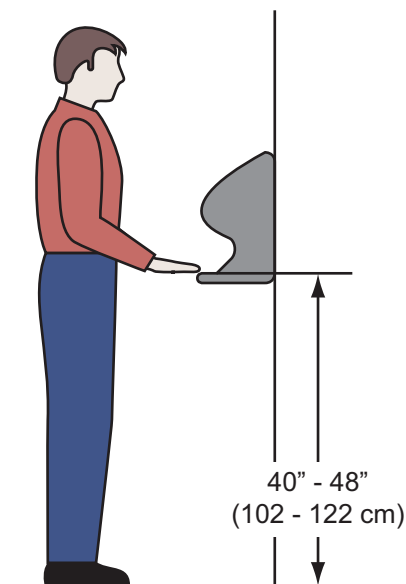


Figure 3.2— GT-Series Terminal Installation Height

Make sure that the terminal is not exposed to excessive airborne dust, direct sunlight, water or chemicals.

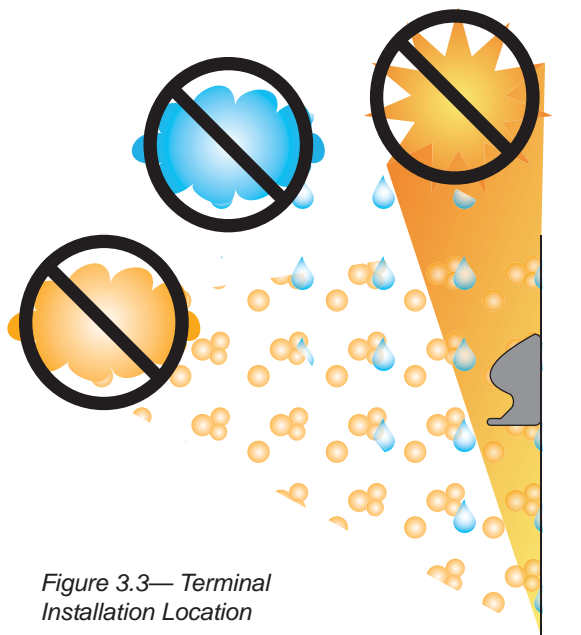


Figure 3.3— Terminal Installation Location

Removing the Terminal from the Box

1. Remove any accessories from the box.
2. Remove the packing materials from the top of the terminal.
3. Lift the terminal from the box. Do not touch the underside of the terminal face.

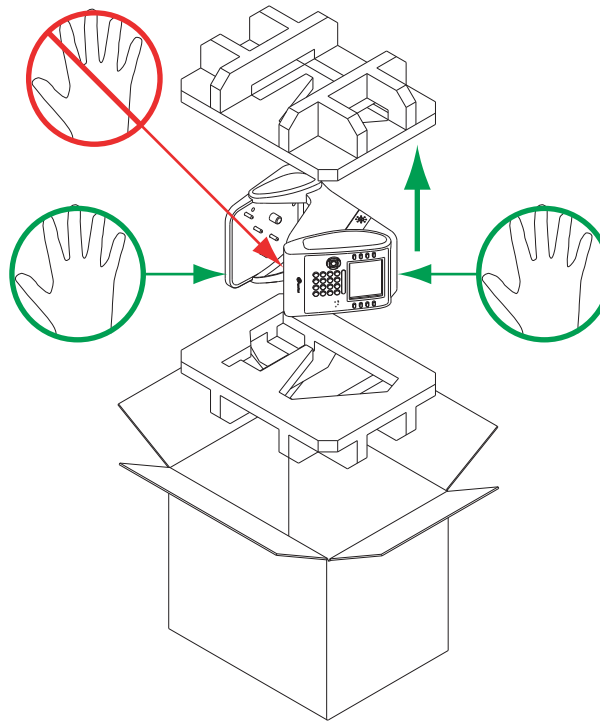


Figure 3.4— Removing the Terminal from the box

Wall Preparation

! *These directions and provided hardware are for installation on a hollow wall only. For installation on a solid wall, other means should be used.*

1. Measure and mark a point 49 inches (124.5 cm) from the surface of the finished floor.

→ *This point is used by the leveling hole where the top-center point of the terminal should be mounted. At 49 inches, the unit's platen will be 40 inches from the floor.*

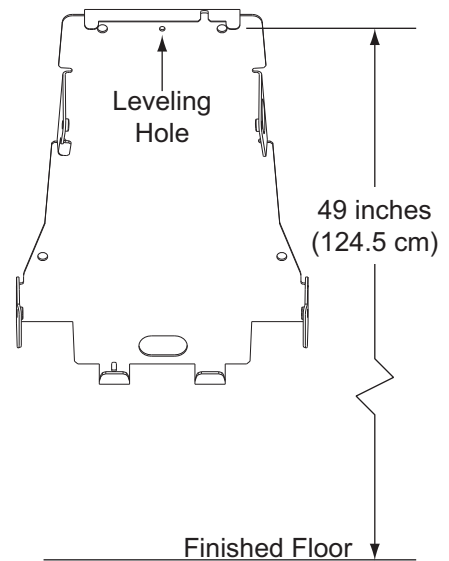


Figure 3.5— Measurements for Terminal Installation

2. Drive a small nail into the wall at the mark.

→ *For a solid wall, pre-drill a 1/8" hole. Insert nail into the hole.*

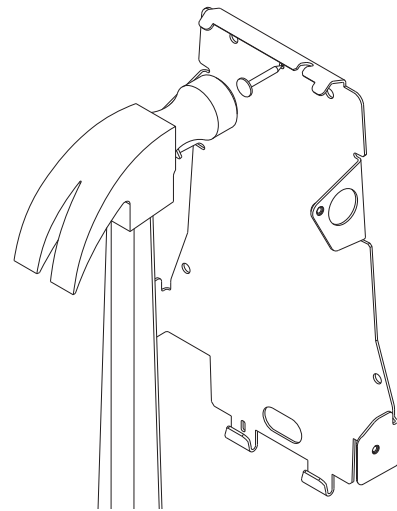


Figure 3.6— Leveling the Terminal (Step 1)

3. Hang the wall plate from the leveling hole located near the top of the wall plate.
4. Use a bubble level to ensure that the wall plate is level.

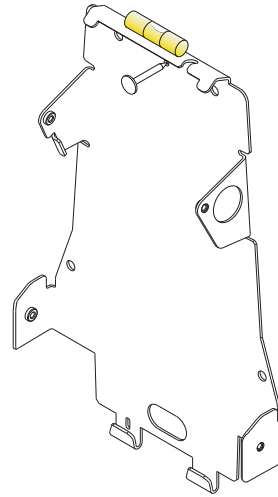


Figure 3.7— Leveling the terminal (step 2)

5. Mark the location of the two upper mounting holes and the two lower mounting holes.
- ➔ **For a concealed wiring connection through the wall, mark the rear cable entry hole on the wall plate.**

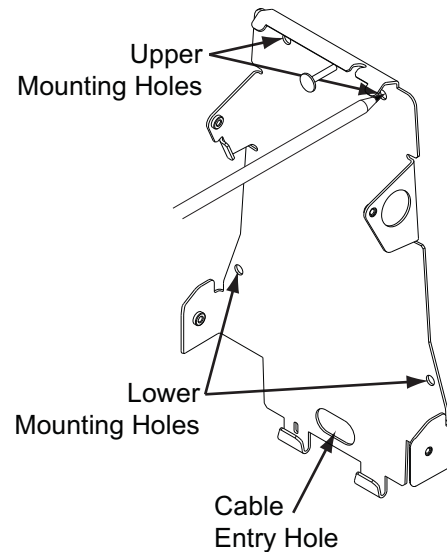


Figure 3.8— Marking to mount the holes

6. Remove the wall plate and nail.
7. Drill upper and lower mounting holes.
For a concealed wiring connection, drill a 1/2" hole in the center of the outlined rear cable entry hole.
- ➔ **Additional holes may be drilled to enlarge the hole for concealed wiring connection if necessary.**
8. Clear all dust and debris away from the terminal mounting location.

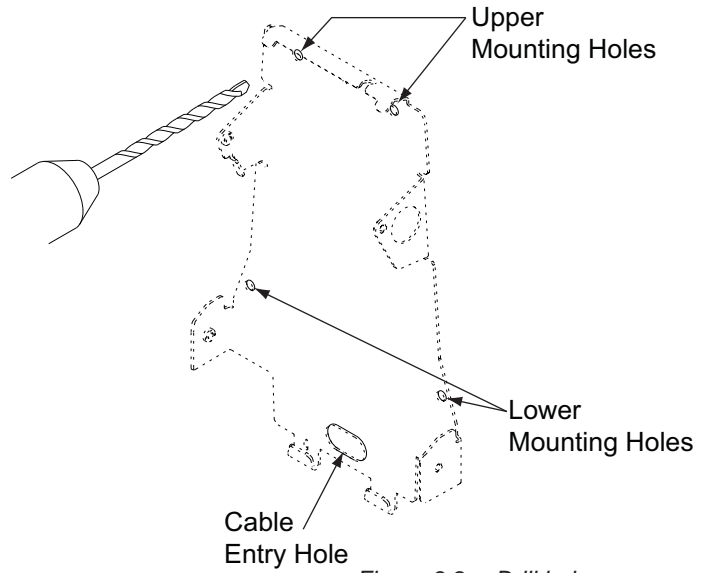


Figure 3.9— Drill holes

Attaching the Wall Plate

! *These directions and provided hardware are for installation on a hollow wall only. For installation on a solid wall, other means should be used.*

1. Pull all wires through holes in wall (if necessary) and make sure wires are clear of wall plate.
2. Install the four fasteners that have been provided into the mounting hole locations. Then use the four provided screws to attach the plate to the wall.

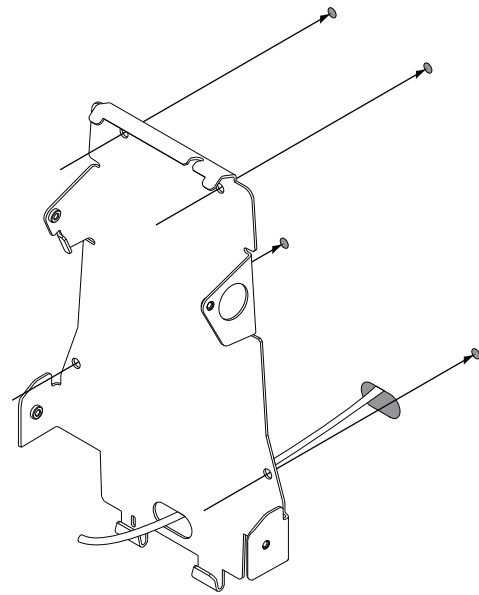


Figure 3.10— Attaching the Wall Plate

Hang Terminal and Run Wires

1. If the side covers are attached to the terminal, they must be removed before hanging the terminal on the wall plate.

➔ See “*Removing/Installing Side Covers*” on page 34 for more information.

2. Slide slots in terminal over hooks on wall plate. Allow terminal to rest against the wall while performing the following steps.

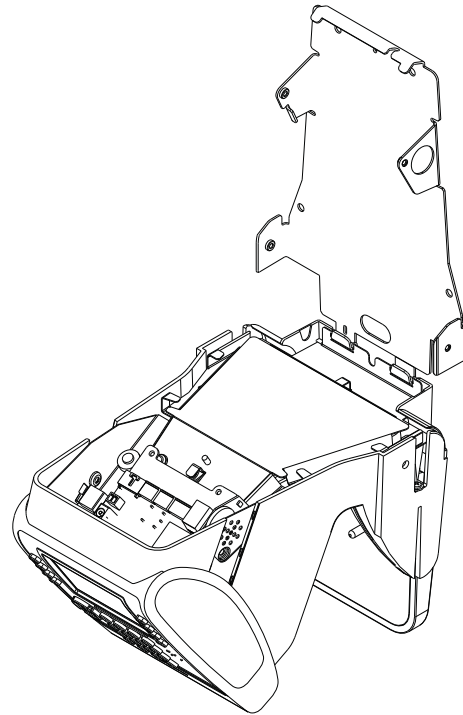


Figure 3.11— Hang the terminal from the Wall Plate

3. There are several options for running the wiring a. Run wiring through hole in wall plate.
 - a. Run wiring through hole in wall plate.
 - b. Run wiring through slot in terminal.
 - c. Run wiring through battery cover (material removal required).

➔ **If using option c, locate indentation in battery cover, drill 1/4" hole in battery cover indentation and use utility knife to remove excess material.**

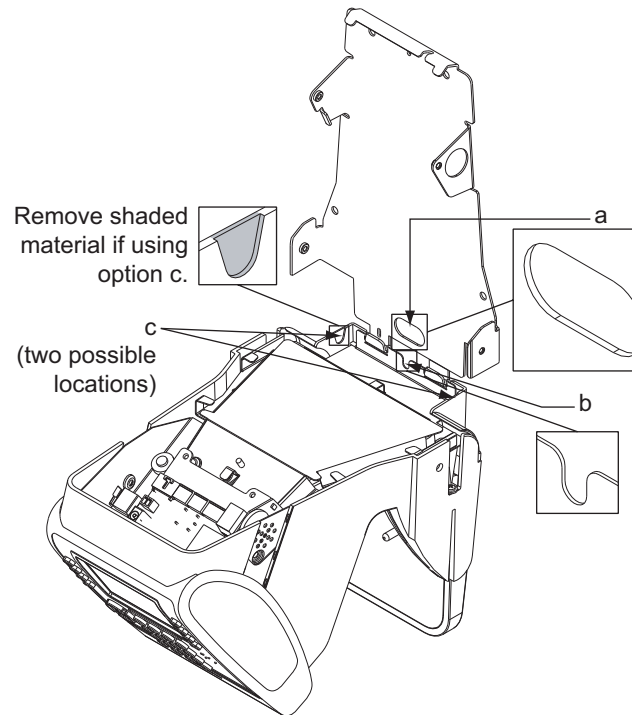


Figure 3.12— Terminal Wiring Options

4. Tuck wires under tabs on terminal to minimize risk of crimping wires.
5. Follow all local electrical codes when routing wire and making the terminal connections.

➔ **For concealed wiring, pull the terminal wiring through the 1/2" cable entry hole.**

➔ **Ensure there is at least twelve inches of extra cable beyond what is needed to make the required connections to the back board.**

➔ **For conduit wiring, pull an extra twelve inches of cable through the conduit beyond what is needed to make the required connections to the back board.**

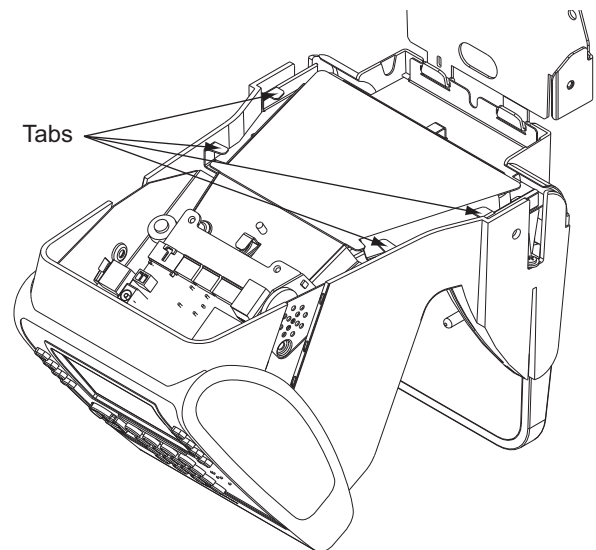


Figure 3.13— Wire Tabs

➔ **You may need to run the cable and then attach the connectors in order to fit cables through necessary holes and/or slots.**

Making Back Board Connections

! Use caution when making connections to the back board to avoid damage. Be aware of possible damage due to electrostatic discharge (ESD). ESD is of particular concern when working on carpeted surfaces and in dry environments. Use a ground strap to minimize ESD concerns.

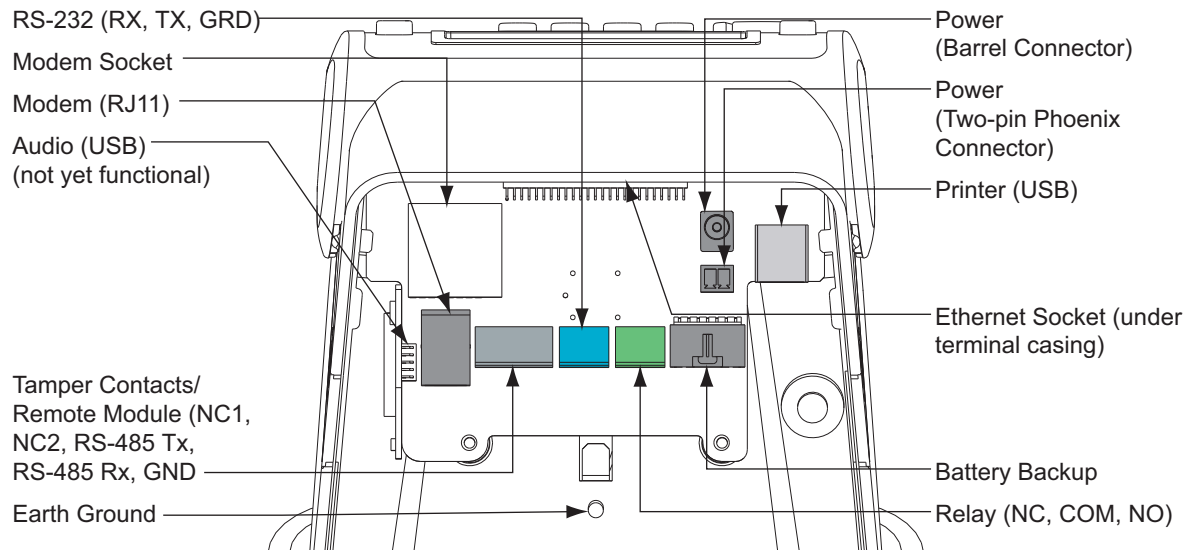
! DO NOT apply power until you are ready to configure the terminal!

! DO NOT connect backup battery (if using) until after main power has been supplied!

1. Connect the earth ground. The earth ground connection is made to the ground pin on the terminal. Bundle all ground connections into one crimp lug and attach the lug to the ground pin with a 8-32 nut.
2. Connect the ethernet cable to the ethernet connection socket inside the terminal casing.
3. DO NOT apply power until you are ready to configure the terminal! Connect the P1 plug to the twisted pair per the following: Pin 1: Ground, Pin 2: Power.

➔ See “Important Information for Installers and Terminal Administrators” on page 17 for details.

4. If using the optional backup battery, locate the backup battery relay, but DO NOT connect backup battery until after the main power has been connected.
5. Make other back board connections as necessary. Use the diagram below as a reference.



Back Board Connections

Attaching the Ferrite Clip

The ferrite clip must be attached to the terminal's power cord in order to be FCC-compliant.

1. Make a loop in the power cord approximately six (6) inches from the power supply.
→ The loop will keep the clip from sliding on the power cord.
2. Clamp the ferrite clip over the loop. Make sure the tabs fully engage.

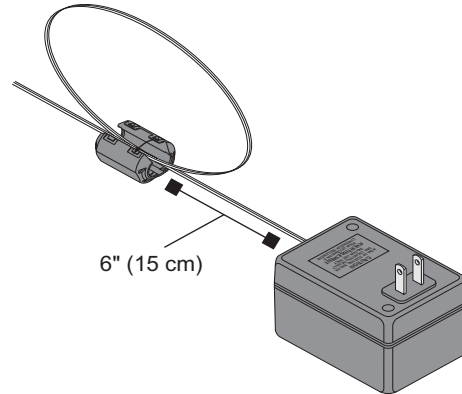


Figure 3.14— Attaching the Ferrite Clip

Printer Setup (Optional)

You may want to install a printer to provide a paper receipt of each user booking. A booking is the interaction that is recorded each time a user punches in or out of the terminal.

- ➔ ***The print format on the booking receipt can be customized. See “Print Setup” on page 59 for more information.***
- ➔ ***If you want to install a printer after initial terminal setup, you will need to shut down the terminal first and then perform the following steps. See “Shutting Down the Terminal” on page 44 for more information.***
- ➔ ***At the time this user’s guide was printed, only the Epson USB Receipt printer is supported.***

1. Connect the receipt printer to the terminal’s USB port.
2. Power on the receipt printer.

 ***The receipt printer must be powered on and connected to the terminal via the USB port before the terminal is powered on.***

After you have powered on and configured the terminal, perform the following:

1. Enable PrintBookings.
 - ➔ ***See “Set PrintBookings” on page 60 for more information.***
2. Set the baud rate.
 - ➔ ***See “Set Baud Rate” on page 60 for more information.***
3. Enable printing on the host application.

By default, the terminal will print the following on the receipt:

- Date and time of booking
- User name
- User’s credential ID
- Verification result
- Punch status (in or out)

Removing/Installing Side Covers

The side covers must be removed in order to attach the terminal to the wall plate.

➔ **The terminal may be shipped without the side covers attached.**

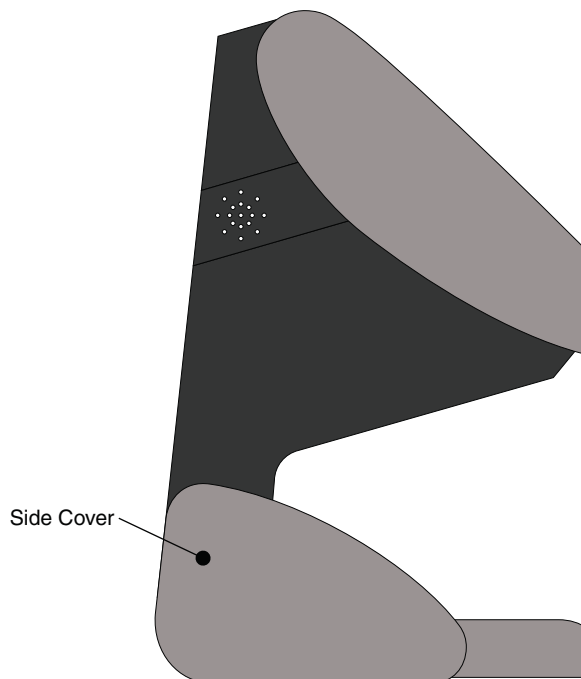


Figure 3.15— Terminal covers

Removing Side Covers

1. Locate slot on bottom of side cover. Insert a small screwdriver into slot.
2. Rotate screwdriver gently. Side cover will pop off.

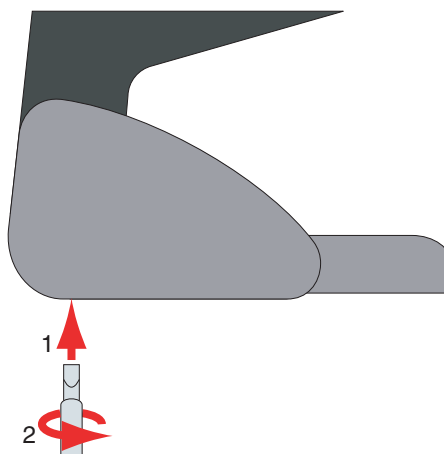


Figure 3.16— Removing the side covers

Installing Side Covers

1. Place outside ridge of side cover under edge of terminal body.
2. Rotate side cover toward terminal body and snap into place.

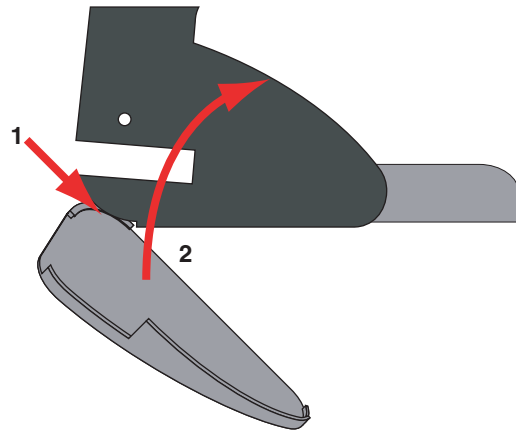


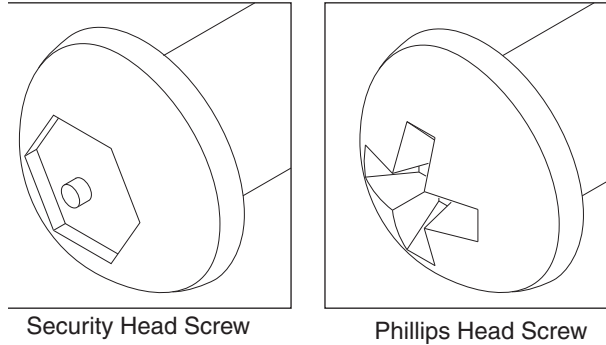
Figure 3.17— Installing the side covers

Attaching the Terminal to the Wall Plate

! Remove any dust and debris from the mounting site before attaching the terminal. Dust and debris can seriously affect the performance of the terminal.

1. Choose the standard Phillips head screws or the security head screws for installation.

➔ A special tool is required to install and remove a security head screw.



2. Terminal should already be hanging from wall plate.
3. Rotate terminal toward the wall plate. Make sure not to pinch or damage any wiring.
4. Make sure that the screw holes in the body of the terminal are aligned with the screw holes in the wall plate.
5. Install two (2) screws into the lower screw holes.
6. Attach side caps.

➔ See "Installing Side Covers" on page 35 for more information.

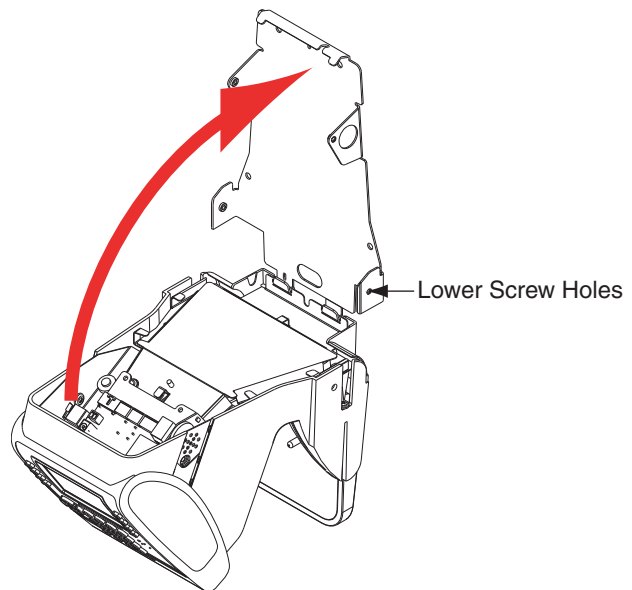


Figure 3.18— Closing the Terminal

Setting Up the GT-Series Terminal

4

Network Mode Configuration

You can configure terminals for network mode in 3 ways, as described in this chapter:

- Using the terminal command menus from the terminal user interface
- Using the terminal's web server
- Using your host application's customized interface (if provided)

➔ **For a comparison of the three options, see “Terminal Configuration Options” on page 19 for more information.**

After configuring the terminal, you can then verify that the reader is configured properly to synch with the host. This is described in “Verifying Synchronization with the Host Application” on page 40.

NOTE: Make sure that your host application is running and your terminal is powered up before configuring the terminal. You must logged in as the administrator in order to configure a terminal.



Do not apply power to the terminal until you understand the network setup procedures.

NOTE: The terminal should be synchronized with the host application before creating any content on the terminal. If content is created on the terminal before it is synchronized with the host application, content may be lost when synchronization occurs.

Using the Terminal's Command Menus for Configuration



If the terminal is not yet configured, only the command menus that are needed to configure a terminal for synchronization will be displayed when  and  are pressed. See Figure 4-1.

Figure 4-1 Using the Network Setup Menu for Terminal Configuration



1. Configure the following terminal network settings using the terminal interface:
 - **Set Host Password**

Use the alpha-numeric keypad to enter the host password. The password must match the password of a valid host account.

See “Set Host Password” on page 74 for more information.
 - **Set Host URL**

Use the alpha-numeric keypad to enter the host URL (Host Server’s IP address). The entire address must be entered (including “http://”).

Example: http://192.168.1.25.

See “Set Host URL” on page 75 for more information.
 - **Set Logical Name**

Use the alpha-numeric keypad to enter the name of the terminal. It must match the name of the terminal created on the host server.

See “Set Logical Name” on page 71 for more information.
 - **Set Host Username**

Use the alpha-numeric keypad to enter the username. It must match a username of a valid host account.

See “Set Host Username” on page 72 for more information.
2. Wait until the terminal LED turns blue, indicating host application has been found.
3. Verify the date and time on the terminal. They will agree with the host logical terminal locale time setup if the terminal is synchronizing.
4. If necessary, verify database synchronization.

See “Verifying Synchronization with the Host Application” on page 40 for more information.

Using the Terminal’s Web Server for Terminal Configuration

1. Open an internet browser.
2. Enter the terminal’s IP address in the URL address bar using the format:

`http://<terminal IP address>`

Example: `http://100.73.100.193`

 - If the terminal has never been on a network the terminal default IP address is 192.168.1.110.
 - If the terminal has previously been on a network, it will have been automatically assigned an IP address through DHCP. You can find this information by using the terminal status menu option on the reader. (See “Check the Terminal Status in the Terminal Command Menus” on page 40).

- The web server home page will prompt you for a Credential ID and an EPIN. On initial startup, the default Credential ID is `root` and the EPIN is `Schlage538`.

NOTE: This login account (root, Schlage538) will automatically self-destruct when the terminal completes its first synchronization or when there is a valid Administrator created for the reader. Any future attempts to log in to the terminal's web server must be with a valid administrator user record, and the user record must contain a user-determined EPIN.

- From the web server main page (Figure 4-2) set the terminal logical name, which must be the identical logical name set during terminal creation on the host application. The logical name can be found through the host or by checking the terminal status on the reader (see “Check the Terminal Status in the Terminal Command Menus” on page 40).

Figure 4-2 Terminal Web Server Main Page



Configuration Settings

Welcome . You may check the terminal status, factory settings or configure the host synchronization settings.

Terminal Logical Name : (EXERCISE CAUTION BEFORE MODIFYING)

Host URL :

Host User Name:

Host Password:

- Set the Host URL to `http://host machine's IP address`.
- Set the Host User Name to the user name set during the host application installation.
- Set the Host password to the password set during the host application installation.
- Click **Submit**.
- An update confirmation should appear indicating that the entered fields were updated.
- Click **Back**.

11. Check the LED bar to ensure it has turned blue. (This may take a minute.)
12. Click on **Display Terminal Status**.
13. Check the DB Synchronization Status field to verify that a DBSync was completed successfully.

Using Your Customized Host Application (GManager) for Terminal Configuration

If your site has a customized host application (similar to the sample GManager host application provided with the GT-Series Integration Package) you can use this interface to configure your terminals. See your host application documentation for details.

Verifying Synchronization with the Host Application

There are a number of ways to quickly verify that your terminal is synchronizing with the host application, as described in the following sections.

Check the Terminal Status in the Terminal Command Menus

1. Press Maintenance Menu.
2. Press Terminal Status.
3. Scroll down until you can view DBSync Status and confirm that it displays *DBSync Completed*.

Change the Ready Screen Message

From the host application:

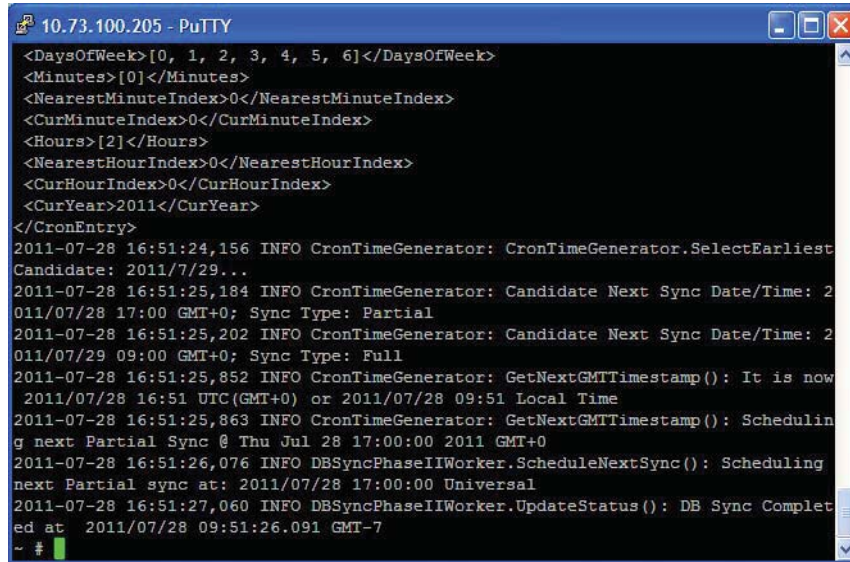
1. Change the ready string for the terminal
2. Run Sync Now.

At the terminal, look at the LCD and verify that the ready string has changed

Check the RSITerm.log File From a Telnet Session

1. Start a telnet session with the terminal.
See “Using Telnet” on page 125 for more information.
2. Type `cd /RecogSys/ZODB` and press **Enter**.
3. Type `cat RSITerm.log` and press **Enter**. Figure 4-3 shows an example of a successful DB Sync of the terminal.

Figure 4-3 Terminal Log File After Successful DB Sync



```
10.73.100.205 - PuTTY
<DaysOfWeek>[0, 1, 2, 3, 4, 5, 6]</DaysOfWeek>
<Minutes>[0]</Minutes>
<NearestMinuteIndex>0</NearestMinuteIndex>
<CurMinuteIndex>0</CurMinuteIndex>
<Hours>[2]</Hours>
<NearestHourIndex>0</NearestHourIndex>
<CurHourIndex>0</CurHourIndex>
<CurYear>2011</CurYear>
</CronEntry>
2011-07-28 16:51:24,156 INFO CronTimeGenerator: CronTimeGenerator.SelectEarliest
Candidate: 2011/7/29...
2011-07-28 16:51:25,184 INFO CronTimeGenerator: Candidate Next Sync Date/Time: 2
011/07/28 17:00 GMT+0; Sync Type: Partial
2011-07-28 16:51:25,202 INFO CronTimeGenerator: Candidate Next Sync Date/Time: 2
011/07/29 09:00 GMT+0; Sync Type: Full
2011-07-28 16:51:25,852 INFO CronTimeGenerator: GetNextGMTTimestamp(): It is now
2011/07/28 16:51 UTC(GMT+0) or 2011/07/28 09:51 Local Time
2011-07-28 16:51:25,863 INFO CronTimeGenerator: GetNextGMTTimestamp(): Scheduling
next Partial Sync @ Thu Jul 28 17:00:00 2011 GMT+0
2011-07-28 16:51:26,076 INFO DBSyncPhaseIIWorker.ScheduleNextSync(): Scheduling
next Partial sync at: 2011/07/28 17:00:00 Universal
2011-07-28 16:51:27,060 INFO DBSyncPhaseIIWorker.UpdateStatus(): DB Sync Complet
ed at 2011/07/28 09:51:26.091 GMT-7
~ #
```

Demo Mode Configuration

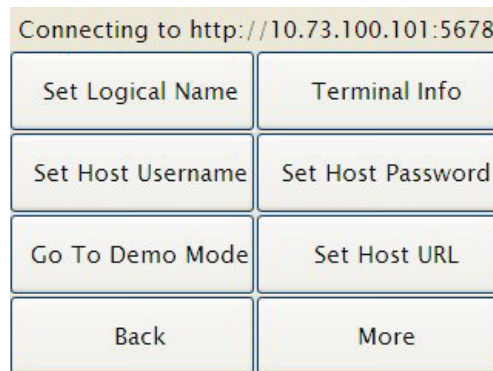
➔ *If a terminal has never been connected to a host, you can switch directly from Terminal Mode to Demo Mode. If a Terminal has already been connected to a host and synchronized successfully, you can only switch directly to StandAlone Mode.*

NOTE: *When the terminal is started for the first time, the Network Connection Setup screen will be displayed. When the terminal is not connected to a host application, synchronization will not occur and the terminal can be switched to Demo mode. For more information about using Demo Mode, see “Go to StandAlone or Demo Mode” on page 73.*

You must logged in as the administrator in order to configure a terminal in Demo Mode.

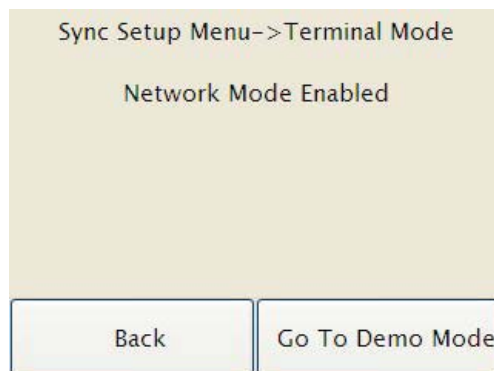
1. Press  and then  to access the Network Setup Screen. See Figure 4-4.

Figure 4-4 Network Setup Screen



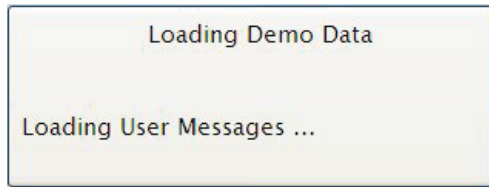
2. Press  Go to Demo Mode.
3. Press  Go to Demo Mode again. See Figure 4-5.

Figure 4-5 Selecting the Go To Demo Mode Option



4. Wait until the Terminal screen displays messages informing you that the reader is loading the pre-load Terminal databases, after which the terminal returns to the ready screen. See Figure 4-6.

Figure 4-6 Demo Mode Confirmation Message



5. Configure the following terminal settings:

➔ ***The following settings can only be used when the terminal is in Demo mode or Standalone. Once you leave Demo Mode, these setting values will not be used in Network mode; instead they will be set by your host application.***

- a. Set Locale Time Zone.

See “Set LocaleTimezone” on page 63 for more information.

- b. Set the date.

See “Set Terminal Date” on page 61 for more information.

- c. Set the time.

See “Set Terminal Time” on page 63 for more information.

Creating the Terminal Administrator Account



The first time the terminal is booted up, there are no user accounts. The first user account that is assigned to the terminal will be the terminal administrator account (with an authority level of 5). This can be changed later, but this account must be created before any other actions can be performed.

- ➔ ***The first user can be created using the host application. Once the user is assigned to the terminal, the user will be added to the terminal when the terminal synchronizes for the first time.***
- ➔ ***It is recommended that you create an EPIN for the terminal administrator account at this time. This will allow the terminal's web server to be used once the terminal is online. "Edit EPIN" on page 96 for more information.***

The terminal administrator account is created in the same way as other user accounts. This account can be created either from the terminal or from the host application. To create the terminal administrator account from the terminal, use the following instructions:

1. Add and enroll yourself as the administrator.
 - ➔ ***See "Creating and Enrolling Users" on page 48 for more information.***
2. Change the authority level to 5.
 - ➔ ***See "Edit Authority" on page 49 for more information.***

Shutting Down the Terminal

-  ***DO NOT remove power without completing the shut down sequence!***
-  ***If you have a terminal with the backup battery option, disconnect the main power first, then disconnect the battery.***

Shutting Down the Terminal Using the Terminal Interface

1. Log in to the terminal as an administrator.

See "Creating the Terminal Administrator Account" on page 44 for more information.
2. Press Maintenance Menu.
3. Press Shutdown.
4. Wait until the LED bar is no longer lit.
5. You can now safely remove power from the terminal.

Shutting Down the Terminal Using Telnet

If the terminal cannot be shut down using the terminal interface use telnet to do so. See "Shutting Down the Terminal Via Telnet" on page 129.

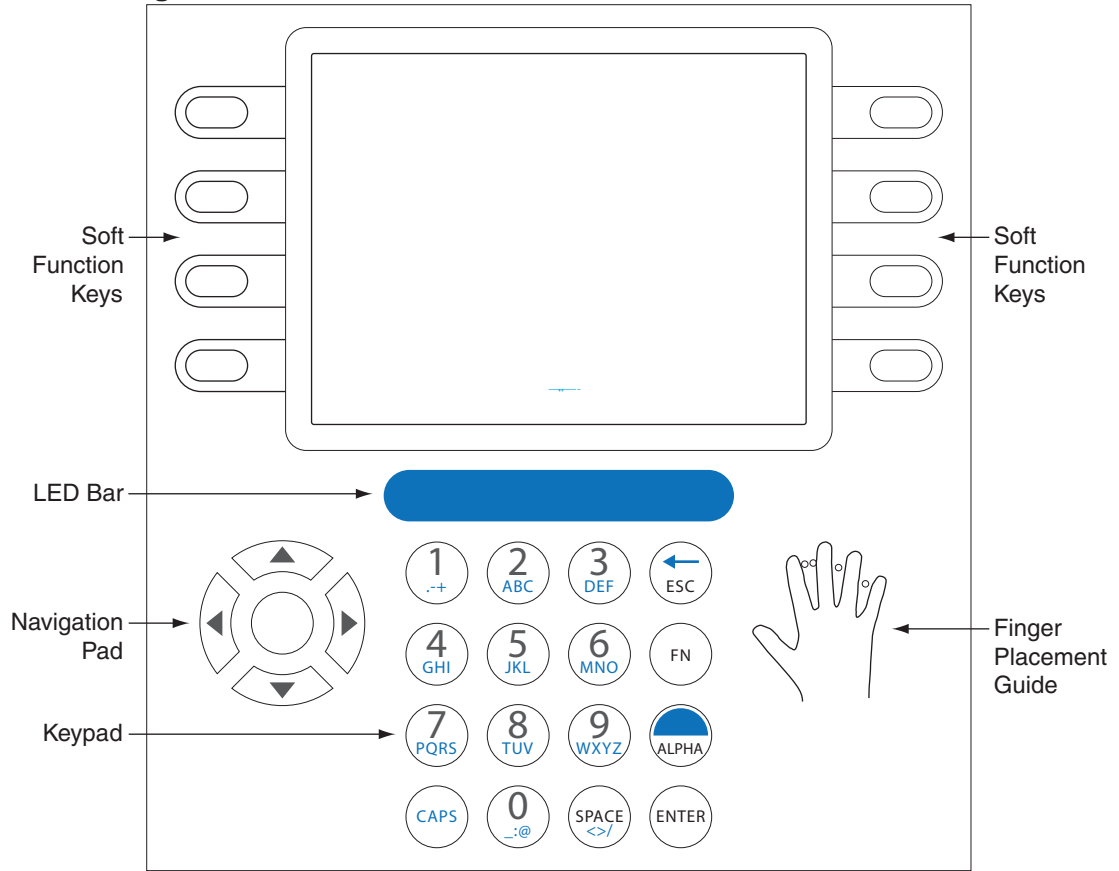
Basic Operations

5

Reviewing the Terminal Front Panel and Interface

Figure 5-1 shows the front panel of the GT-Series terminal.

Figure 5-1 Front Panel of the GT-Series Terminal



Startup Screen

GT-Series Terminal Startup Screen

The first time you boot up the terminal, the “Hand” logo will appear. The hand logo will disappear after the terminal is completely booted. →









Terminal Operation Tips and Tricks

Before using the terminal for basic operations, it is recommended that you review the following tips and tricks for a more successful experience with the GT-Series Terminal.

Terminal Time-Outs









The terminal will go back one screen level after ten (10) seconds of inactivity. The terminal will return to the default screen after thirty (30) seconds of inactivity. If you have been performing a function and fail to press a key for thirty (30) seconds, you will need to log in as an administrator again and start over.

Entering Text

- When you are using the keypad to enter text, such as a last name, press  to switch to alpha mode. Press  to switch to capital letters. If you need to enter the same letter twice, wait a few seconds to proceed to the next letter, or use the navigation keys  to proceed to the next letter.
- The navigation keys  can be used to move between characters in alpha-numeric entry fields.
- Press  and  from any command menu to return to the default screen.

Navigating a Long List

The terminal can sometimes contain long lists of items, such as time formats or users. There are some shortcuts that are useful for navigating through these lists.

- Press  and  to skip to the top of the list.
- Press  and  to skip to the end of the list.
- Press  and  to page down.
- Press  and  to page up.

Accessing Command Menus

Before performing any programming operations, you must be logged into the terminal as an administrator.



Administrator Authentication

Depending on the GT-Series Terminal model/configuration, use the appropriate set of instructions below.

Recommendation: Create an EPIN for the Terminal Administrator

As a best practice, you should create an EPIN for the terminal administrator. If the biometric camera encounters a failure, the terminal administrator will be able to access the command menus through use of the EPIN.

GT-Series Terminal Authentication

1. Press  and then .
2. When prompted, enter your Credential ID for the administrator account.
3. Place your hand for verification.
4. After successful verification, the COMMAND STRUCTURE menu will display from which you can make the appropriate menu selections.

Creating and Enrolling Users

Creating an ID Numbering System

An ID numbering system should be created before entering the first user into the terminal. ID Numbers (RPINs) are used during user enrollment and verification. Use the following guidelines when designing an ID numbering system.

- Each user must have a unique ID number (RPIN).
- All RPINs should be the same length.
 - ➔ **By making all RPINs the same length, users will not have to press ENTER after entering their RPIN, which can expedite processing. To do so, use the Set ID Length option as described in “Set ID Length” on page 64 for more information.**
- The RPIN should be as short as possible so users can remember their ID number. To make sure you will have enough unique RPINs, determine the length of RPIN by determining the number of users needed.
 - ➔ **For example, if you have 10,000 or less users, use a four-digit RPIN. If you have more than 10,000 users, use a five-digit RPIN.**

Creating a User from the Terminal

➔ **If possible, it is more efficient to create users by using your host application. Refer to your host application documentation for more information.**


➔ **See “Add User” on page 100 for more information.**

1. Log into the terminal as an administrator.
See “Administrator Authentication” on page 47 for more information.
2. Press User Management.
3. Press Add User.
4. Enter the user’s RPIN and press .
5. If the terminal is running in standalone mode, the screen will display “Host Unavailable/Create New User/Are You Sure?” Press YES.
6. If you are ready to enroll the user at this time, go to the next section “Enrolling a User”.

Enrolling a User

1. Ensure the user has been created in the terminal.
See “Add User” on page 100 for more information.
2. Log into the terminal as an administrator.

See “Administrator Authentication” on page 47 for more information.

3. Press User Management.
4. Press List Users.
5. Scroll to the name of the user you wish to enroll using . Press the middle navigational key to select the user.
6. Press Enroll User.
7. Follow the prompts on the terminal screen for hand placements. You will be prompted to place your hand three times.




➔ ***If needed, a user can also be enrolled without using hand verification. See “No Hand Enroll” on page 95 for more information***

Setting User Data

Most user data can be set at the host application and passed to the terminal through synchronization. See your host application documentation for more information.

Edit Timezone

➔ ***See “Edit Timezone” on page 57 for more information.***



1. Log into the terminal as an administrator.
See “Administrator Authentication” on page 47 for more information.
2. Press User Management.
3. Press List Users.
4. Scroll to the name of the user you wish to edit using . Press the middle navigational key to select the user.
5. Scroll to the timezone listing using . Press the middle navigational key to change the timezone.
6. Press List Timezone.
7. Scroll to the timezone you want to add to the user profile using . Press the middle navigational key to select the timezone.

Edit Authority

➔ ***See “Edit Authority” on page 86 for more information.***


1. Log into the terminal as an administrator.

See “Administrator Authentication” on page 47 for more information.

2. Press User Management.
3. Press List Users.
4. Scroll to the name of the user you wish to edit using . Press the middle navigational key to select the user.
5. Scroll to the authority listing using . Press the middle navigational key to edit the authority level.
6. Enter the appropriate authority level for the user (1-5).

Add Credential



➔ See “Add Credential” on page 94 for more information.

1. Log into the terminal as an administrator.
See “Administrator Authentication” on page 47 for more information.
2. Press User Management.
3. Press List Users.
4. Scroll to the name of the user you want to edit using . Press the middle navigational key to select the user.
5. Press More.
6. Press Credential Menu.
7. Press Add Credential.
8. Press RPIN.
9. Press Enter.

Edit Threshold



➔ See “Edit Threshold” on page 88 for more information.

1. Log into the terminal as an administrator.
See “Administrator Authentication” on page 47 for more information.
2. Press User Management.
3. Press List Users.

4. Scroll to the name of the user you wish to edit using . Press the middle navigational key to select the user.
5. Scroll to the threshold listing using . Press the middle navigational key to edit the threshold level.
6. Enter the threshold.
7. Press Enter.


Edit Name

➔ See “Edit Name” on page 85 for more information.

1. Log into the terminal as an administrator.
See “Administrator Authentication” on page 47 for more information.
2. Press User Management.
3. Press List Users.
4. Scroll to the name of the user you wish to edit using . Press the middle navigational key to select the user.
5. Scroll to the name field you want to edit (First Name or Last Name) using . Press the middle navigational key to select the name field.
6. Edit the name.
7. Press Enter to accept the changes.

Remove a User


➔ See “Remove User” on page 92 for more information.

1. Log into the terminal as an administrator.
See “Administrator Authentication” on page 47 for more information.
2. Press User Management.
3. Press List Users.
4. Scroll to the name of the user you wish to remove using . Press the middle navigational key to select the user.
5. Press More.
6. Press Remove User.
7. Press YES.

Setting Date and Time

- ➔ **Setting a terminal's date and time using the terminal can only be done when the terminal is in Demo mode; otherwise these settings are made by the host application when in Network mode.**

Set Locale Timezone

- ➔ **See “Set LocaleTimezone” on page 63 for more information.**
1. Log into the terminal as an administrator.
See “Administrator Authentication” on page 47 for more information.
 2. Press Setup Menu.
 3. Press General Setup.
 4. Press Set Locale Timezone.
 5. Press Set Locale TZ.
 6. Scroll to the appropriate time zone using . Press the middle navigational key to select the time zone.

Set Terminal Date

- ➔ **See “Set Terminal Date” on page 61 for more information.**
- NOTE: Set Terminal Date is available only when you are in Demo mode or Standalone mode.**
1. Log into the terminal as an administrator.
See “Administrator Authentication” on page 47 for more information.
 2. Press Setup Menu.
 3. Press General Setup.
 4. Press More.
 5. Press Set Terminal Date.
 6. Enter the current date.
 7. Press Enter.

Set Terminal Time

➔ See “Set Terminal Time” on page 63 for more information.

NOTE: Set Terminal Time is available only when you are in Demo mode or Standalone mode.

1. Log into the terminal as an administrator.
See “Administrator Authentication” on page 47 for more information.
2. Press Setup Menu.
3. Press General Setup.
4. Press More.
5. Press Set Terminal Time.
6. Enter the current time.
7. Press Enter.

User Authentication

1. When prompted, enter your Credential ID for the administrator account.
2. Place your hand for verification.

Checking the Terminal Software Version

The terminal software version can be obtained using the Terminal Status command menu.

➔ See “Terminal Status” on page 110 for more information.

Updating the Terminal Software

Updates to the terminal software can be applied to the terminal using the host application (if permitted by your custom host application). Refer to your host application documentation for more information.

Rebooting the Terminal Using the Terminal Interface

1. Log in to the terminal as an administrator.
See “Administrator Authentication” on page 47 for more information.
2. Press Maintenance Menu.
3. Press Reboot.

The terminal will shut down and reboot automatically. If the terminal cannot be rebooted using the terminal interface, use telnet. See “Rebooting the Terminal Via Telnet” on page 129.

Command Menu Reference

6

Reviewing the Command Menu

The following page is a map of all the commands that can be accessed on the terminal. Each command is described in detail in the following sections of this guide.

Command Menu Structure

Setup Menu

Timezone Menu

- Edit Timezone
- List TZIDs
- List Timezones
- Add Timezone

Print Setup

- Set PrintBookings
- Set Baud Rate

General Setup

- Set Beeper
- CmdLine Setup
- Set Time&Attend
- Set Door Unlock Time
- Set LocaleTimezone
- Set LocaleTZ
- Set ID Length
- More
 - Set Duration to Retain
 - Sent
 - Set CR Terminator String
 - Set Lunch Punch
 - Lockout Secs
 - Set Terminal Date**
 - Set Terminal Time**
 - Set LogFile Size Factor
 - Set CR Num of Prefix Chars

Holiday Menu

- Edit Holiday
- List Holidays
- List Holidays
- Add Holiday

Network Mode Setup

- Set Logical Name
- Set Host Username
- Go to Demo Mode***
 - Go to Demo Mode
- Go to StandAlone Mode
 - Go to StandAlone Mode
- Set Web Server
- Set Host Password
- Set Host URL
- More
 - Set CLISrv Port
 - Set XMLRPCsvr Port
 - XMLRPC Svr Setup
 - Set WebSvr Port
 - Set Static/DHCP
 - StaticIP
 - IPADDR
 - DNS1
 - DNS2
 - NETMASK
 - GATEWAY
 - Set RealTime Interaction

Display Setup

- Set CompanyName
- Date Time Format
- Set Time Format
- Set Date Format
- Set Ready String
- Set Language

User Management

Edit User

- First Name
- Last Name
- Enroll Status
- Authority
- Last Score
- Threshold
- Verify Status
- Timezone
- User Status
- Enroll User
- Last Booking
- More
 - Generate Punch
 - Remove User
 - Credential Menu
 - List Credentials
 - Add Credentials
 - No Hand Enroll
 - Edit EPIN
 - Access Grant Menu
 - Edit Access Grant
 - List Access Grant
 - Add Access Grant
 - List Bookings

List Users (see *Edit User* for submenus)

Add User (see *Edit User* for submenus)

Security Menu

Clear UserDB

Factory Settings

Set Reject Threshold

- Set Reject Threshold
- Credential Logging Enabled
- Restore Factory Password

Clear Setup

Biometric Setup

- Min High Res Update Count
- Placements Per Try
- Number of Tries
- Template Resolution

Set Passwords

- Set CLI Access Pwd

More

- Set Credential Logging Flag
- Restore Factory Password

Maintenance Menu

Partial Sync Now

Sync Now

Reboot

Terminal Status

Delete Sent

Interactions

Shutdown

Last Punch

FKScript List*

Timecard Approval

Accrual Balances

Cancel Meal

Lunch Punch

Time Off Request

Transfer-ValidList

Command Menu Notes:

*Available in Demo Mode only

**Available in Demo Mode or Stand Alone Mode only.

*** The **Go to Demo Mode** command is available only when you have not yet gone into Network Mode.



Setup Menu

Timezone Menu

A timezone is a period of time during which user access to the terminal is granted.

Every user must have a timezone assigned, either directly or through a group, in order to access the terminal. The timezones 0 (Always) and 61 (Never) are created by default. If a user is assigned timezone 0 (Always), the user always has access to the terminal. If the user is assigned timezone 61 (Never), the user never has access to the terminal.

Timezones are created with intervals. An interval is defined by start time, duration and days of week. Each timezone may have multiple intervals.

Edit Timezone	
<p>Edits a timezone that already exists on the terminal. Select the timezone and then edit the designed interval(s) to change the timezone.</p>	<p>Default: None Range: None Dependencies: None Who: A terminal administrator can edit a timezone at any time</p>
<ol style="list-style-type: none"> 1. Log into the terminal as an administrator. ➔ See “Administrator Authentication” on page 47 for more information. 2. Press <input type="radio"/> Setup Menu. 3. Press <input type="radio"/> Timezone Menu. 4. Press <input type="radio"/> List Timezones. 5. Highlight the timezone you want to edit using . Press the middle key to select the timezone. 6. Press <input type="radio"/> List TZIntervals. 7. Scroll to the interval you want to edit using . Press the middle key to select the interval. 8. To remove the interval, press <input type="radio"/> Remove TZInterval, then press <input type="radio"/> YES. 9. To edit the start time of the interval, press <input type="radio"/> Edit StartTime. Enter the start time and Press <input type="radio"/> Enter. 10. To edit the days of the week for which the interval is effective, Press <input type="radio"/> Edit DOW. 11. Press to toggle each day of the week desired. Then press <input type="radio"/> ENTER. 12. To edit the duration, press <input type="radio"/> Edit Duration. Enter the duration and press <input type="radio"/> Enter. 	

List Timezones	
Lists all the timezones for the terminal.	Default: None Range: None Dependencies: None Who: A terminal administrator can list a timezone at any time.
<ol style="list-style-type: none">1. Log into the terminal as an administrator. ➔ See “Administrator Authentication” on page 47 for more information.2. Press <input type="radio"/> Setup Menu.3. Press <input type="radio"/> Timezone Menu.4. Press <input type="radio"/> List Timezones.5. From here, many other functions can be accessed. See the other topics in this section for more information.	

Add Timezone	
<p>Creates an access timezone for the terminal. To create a timezone, first enter an ID, and then add the start time, duration and days to create an interval. Timezones can have many intervals.</p>	<p>Default: 0 (Always) Range: None Dependencies: None Who: A terminal administrator can add a timezone at any time.</p>
<ol style="list-style-type: none"> 1. Log into the terminal as an administrator. ➔ See “Administrator Authentication” on page 47 for more information. 2. Press <input type="radio"/> Setup Menu. 3. Press <input type="radio"/> Timezone Menu. 4. Press <input type="radio"/> Add Timezone. 5. Enter the timezone ID (any positive number not previously used). 6. Press <input type="radio"/> Enter. 7. Press <input type="radio"/> AddTZInterval. 8. Enter the start time. 9. Press <input type="radio"/> Enter. 10. Enter the duration. 11. Press <input type="radio"/> Enter. 12. Press <input type="radio"/> for each day of the week to add to the interval. (Each press toggles the day on or off.) 13. Press <input type="radio"/> <input type="radio"/> ENTER. 	

Print Setup

The Print Setup menu is used to configure print settings. This information is only necessary when a printer is connected to the terminal.

➔ **See “Printer Setup (Optional)” on page 33 for more information.**

Set PrintBookings	
<p>Enables or disables printing of each booking. A booking is the interaction that is recorded when a user punches in or out of the terminal. The display of this menu will indicate the current state of the Set PrintBookings option. If it is disabled, press Enable to enable PrintBookings. If it is enabled, press Disable to disable it.</p>	<p>Default: Disabled Range: None Dependencies: A printer must be connected to the terminal in order to print bookings. Who: A terminal administrator should set this option during initial terminal setup. his option can be changed at any time</p>
<ol style="list-style-type: none"> 1. Log into the terminal as an administrator. ➔ See “Administrator Authentication” on page 47 for more information. 2. Press <input type="radio"/> Setup Menu. 3. Press <input type="radio"/> Print Setup. 4. Press <input type="radio"/> Set PrintBookings. 5. Press <input type="radio"/> Enable/Disable. 	

Set Baud Rate	
<p>Sets the baud rate (data transmission speed) to be used for the printer. Enter the proper baud rate for your printer. Consult the documentation that came with your printer to determine the proper baud rate.</p> <p>➔ This setting must match the baud rate setting of the printer that is used to print data from the terminal.</p>	<p>Default: 9600 Range: None Dependencies: None Who: A terminal administrator should set this option to match the printer’s baud rate during initial terminal setup.</p>
<ol style="list-style-type: none"> 1. Log into the terminal as an administrator. ➔ See “Administrator Authentication” on page 47 for more information. 2. Press <input type="radio"/> Setup Menu. 3. Press <input type="radio"/> Print Setup. 4. Press <input type="radio"/> Set Baud Rate. 5. Scroll to the baud rate that matches the baud rate of the printer. 6. Press <input type="radio"/> Enter. 	


General Setup

Set Terminal Date	
Sets the date. This setting can only be made in Demo mode.	Default: None Range: None Dependencies: None Who: A terminal administrator should set the date of a terminal in Demo mode during initial setup.
<p>➔ The terminal must be in Demo Mode in order to use the following instructions.</p> <ol style="list-style-type: none">1. Log into the terminal as an administrator. ➔ See “Administrator Authentication” on page 47 for more information.2. Press <input type="radio"/> Setup Menu.3. Press <input type="radio"/> General Setup.4. Press <input type="radio"/> More.5. Press <input type="radio"/> Set Terminal Date using the format MM DD YYYY (Example: 23 32 59.)6. Enter the current date.7. Press <input type="radio"/> Enter.	

CmdLine Setup	
<p>Enables or disables command line interface (CLI) access to the terminal. The display of this menu will indicate the current state of the CmdLine Setup option. If it is disabled, press Enable to enable CLI access. If it is enabled, press Disable to disable it. This option should normally be disabled for security reasons.</p>	<p>Default: Enabled Range: None Dependencies: None Who: A terminal administrator, application developer/tester or any individual under the guidance of a technical support representative can disable or enable CLI for troubleshooting, testing or debugging purposes.</p>
<ol style="list-style-type: none"> 1. Log into the terminal as an administrator. ➔ See “Administrator Authentication” on page 47 for more information. 2. Press <input type="radio"/> Setup Menu. 3. Press <input type="radio"/> General Setup. 4. Press <input type="radio"/> CmdLine Setup. 5. Press <input type="radio"/> Enable/Disable. 	

Set Time&Attend	
<p>Enables or disables time and attendance mode for the terminal. When enabled, the user will be prompted to punch in or out before the hand verification. When disabled, the user will not be given the choice to punch in or out and the terminal or host will automatically punch the user in or out. This menu will display the current state of the Time and Attendance Mode option.</p>	<p>Default: Disabled Range: None Dependencies: None Who: A terminal administrator should set this option during initial setup of the terminal.</p>
<ol style="list-style-type: none"> 1. Log into the terminal as an administrator. ➔ See “Administrator Authentication” on page 47 for more information. 2. Press <input type="radio"/> Setup Menu. 3. Press <input type="radio"/> General Setup. 4. Press <input type="radio"/> Time&Attend. 5. Press <input type="radio"/> Enable/Disable. 	

Set Terminal Time	
<p>NOTE: <i>Set Terminal Time is used to set the time only on a terminal running in Demo mode. Otherwise, the terminal will acquire the time from the host application.</i></p> <p>Using the keypad, enter the time using the following format: hh mm ss based on a 24-hour clock.</p>	<p>Default: None</p> <p>Range: None</p> <p>Dependencies: None</p> <p>Who: A terminal administrator should set the time of a terminal running in Demo mode during initial terminal setup.</p>
<ol style="list-style-type: none"> 1. Log into the terminal as an administrator. ➔ See “Administrator Authentication” on page 47 for more information. 2. Press <input type="radio"/> Setup Menu. 3. Press <input type="radio"/> General Setup. 4. Press <input type="radio"/> More. 5. Press <input type="radio"/> Set Terminal Time using the format HH MM SS. (Example: 23 35 59.) 6. Enter the current time. 7. Press <input type="radio"/> Enter. 	

Set LocaleTimezone	
<p>Sets the time zone of a terminal based on the locality of the terminal itself. Otherwise, the terminal will acquire the time zone from the host application. Select the time zone from the menu that matches your locality.</p>	<p>Default: GMT-8 (Pacific Standard Time)</p> <p>Range: None</p> <p>Dependencies: None</p> <p>Who: A terminal administrator should set the LocaleTZ of a terminal during initial terminal setup.</p>
<ol style="list-style-type: none"> 1. 1. Log into the terminal as an administrator. ➔ See “Administrator Authentication” on page 47 for more information. 2. Press <input type="radio"/> Setup Menu. 3. Press <input type="radio"/> General Setup. 4. Press <input type="radio"/> Set Locale Timezone. 5. Scroll to the time zone you want to use by using . Press the middle key to select the time zone. 	

Set ID Length	
<p>If you set an ID length, the terminal will automatically accept an ID entry once the correct number of digits have been entered. This setting can help expedite the processing of users, especially when user volume is high.</p> <p>➔ All IDs in the system cannot exceed this length. If an ID exceeds this length, a user will not be able to enter the ID.</p>	<p>Default: 6</p> <p>Range: None</p> <p>Dependencies: None</p> <p>Who: A terminal administrator can set this feature to the desired length at any time.</p>
<ol style="list-style-type: none">1. Log into the terminal as an administrator. ➔ See “Administrator Authentication” on page 47 for more information.2. Press <input type="radio"/> Setup Menu.3. Press <input type="radio"/> General Setup.4. Press <input type="radio"/> Set ID Length.5. Press <input type="radio"/> the ID length.6. Press <input type="radio"/> Enter.	

Set LogFile Size Factor

Defines a percentage of disk space (the SD card) to be used for the log file. When that size is exceeded the terminal will automatically create a backup of that log file and a new log file will be generated. The backup log will be located in the same directory (RecogSys/ZODB).

Default: 3%

Range: 0%-80%

Dependencies: None

Who: A terminal administrator can define the disk space used by the log file to optimize the memory management in the terminal. An administrator may wish to increase the logging capacity if the overall database is small, or decrease the logging capacity if the database is large.

1. Log into the terminal as an administrator.
➔ **See “Administrator Authentication” on page 47 for more information.**
2. Press Setup Menu.
3. Press General Setup.
4. Press More.
5. Press Set LogFile Size Factor.
6. Enter the LogFile Size Factor.
7. Press Enter.

Set CR Num of Prefix Chars	
<p>Defines the number of prefix characters in a barcode credential ID.</p>	<p>Default: 2 Range: None Dependencies: None Who: A terminal administrator may set the prefix characters to comply with site specifications.</p>
<ol style="list-style-type: none"> 1. Log into the terminal as an administrator. ➔ See “Administrator Authentication” on page 47 for more information. 2. Press <input type="radio"/> Setup Menu. 3. Press <input type="radio"/> General Setup. 4. Press <input type="radio"/> More. 5. Press <input type="radio"/> Set CR Num of Prefix Chars. 6. Enter the CR Num of Prefix Chars. 7. Press <input type="radio"/> Enter. 	

Set Door Unlock Time	
<p>Defines the time, in seconds, that the relay (J5 connector) will fire and remain active after verification. Press Set Door Unlock Time and define the time in seconds, starting from verification, that the relay will fire and remain active. This may be used to unlock a door to which a terminal is attached or to activate any other device attached to the relay</p>	<p>Default: 0 Range: None (0 is defined as OFF) Dependencies: None Who: A terminal administrator can set the amount of time the relay will fire and remain active.</p>
<ol style="list-style-type: none"> 1. Log into the terminal as an administrator. ➔ See “Administrator Authentication” on page 47 for more information. 2. Press <input type="radio"/> Setup Menu. 3. Press <input type="radio"/> General Setup. 4. Press <input type="radio"/> Set Door Unlock Time. 5. Enter the door unlock time in seconds. 6. Press <input type="radio"/> Enter. 	

Set CR Terminator String	
<p>Defines a barcode credential's terminator string. Press Set CR Terminator String and set the string as necessary.</p>	<p>Default: 3232000</p> <p>Range: None</p> <p>Dependencies: None</p> <p>Who: A terminal administrator can define barcode terminator strings to comply with site specifications.</p>
<ol style="list-style-type: none"> 1. Log into the terminal as an administrator. ➔ See "Administrator Authentication" on page 47 for more information. 2. Press <input type="radio"/> Setup Menu. 3. Press <input type="radio"/> General Setup. 4. Press <input type="radio"/> More. 5. Press <input type="radio"/> Set CR Terminator String. 6. Enter the CR terminator string. 7. Press <input type="radio"/> Enter. 	


Set Beeper	
<p>Enables or disables the audible beep on the terminal. The display of this menu will indicate the current state of the beeper. If it is disabled, press Enable to enable the beeper. If it is enabled, press Disable to disable it.</p>	<p>Default: Enabled</p> <p>Range: None</p> <p>Dependencies: None</p> <p>Who: A terminal administrator can enable or disable the beeper at any time.</p>
<ol style="list-style-type: none"> 1. Log into the terminal as an administrator. ➔ See "Administrator Authentication" on page 47 for more information. 2. Press <input type="radio"/> 3. Press <input type="radio"/> Setup Menu. 4. Press <input type="radio"/> General Setup. 5. Press <input type="radio"/> Set Beeper. 6. Press <input type="radio"/> Enable or Disable. 	

Set Duration to Retain Sent	
<p>Defines the length of time (in days) to retain sent interactions in the terminal.</p>	<p>Default: 30 Range: None Dependencies: None Who: Terminal administrators can set the amount of time to retain sent interactions on the terminal.</p>
<ol style="list-style-type: none"> 1. Log into the terminal as an administrator. ➔ See “Administrator Authentication” on page 47 for more information. 2. Press <input type="radio"/> Setup Menu. 3. Press <input type="radio"/> General Setup 4. Press <input type="radio"/> More 5. Press <input type="radio"/> Set Duration to Retain Sent 6. Enter the Duration to Retain Sent Interactions. 7. Press <input type="radio"/> Enter. 	

Set Lunch Punch Lockout Secs	
<p>Defines number of seconds to lock out lunch punches after a user executes a lunch punch.</p>	<p>Default: 0 Range: 0 - 7200 (in seconds) Dependencies: None Who: A terminal administrator can set the lunch punch lockout duration at any time.</p>
<ol style="list-style-type: none"> 1. Log into the terminal as an administrator. ➔ See “Administrator Authentication” on page 47 for more information. 2. Press <input type="radio"/> Setup Menu. 3. Press <input type="radio"/> General Setup 4. Press <input type="radio"/> More 5. Press <input type="radio"/> Set Lunch Punch Lockout Secs. 6. Enter Lunch Punch Lockout Duration in Seconds. 7. Press <input type="radio"/> Enter. 	

Holiday Menu

Holidays are used to provide a break in a normal timezone.

Edit Holiday	
<p>Edits holidays already set up in the terminal. The holiday end date, begin date, end time, begin time and name may all be edited.</p>	<p>Default: 30 Range: None Dependencies: None Who: A terminal administrator can edit a holiday at any time.</p>
<ol style="list-style-type: none"> 1. Log into the terminal as an administrator. ➔ See “Administrator Authentication” on page 47 for more information. 2. Press <input type="button" value="O"/> Setup Menu. 3. Press <input type="button" value="O"/> Holiday Menu. 4. Press <input type="button" value="O"/> List Holidays. 5. Scroll to the appropriate holiday using . Press the middle key to select the holiday. 6. Press <input type="button" value="O"/> Edit End Date, Edit Begin Date, Edit End Time, Edit Begin Time or Edit Name. 7. Enter a new value for the field you have selected. 8. Press <input type="button" value="O"/> Enter. 9. Repeat step 6 through step 8 until all desired fields have been edited. 	

List Holidays	
Lists all holidays defined for the terminal.	<p>Default: None</p> <p>Range: None</p> <p>Dependencies: None</p> <p>Who: A terminal administrator can list holidays at any time.</p>
<ol style="list-style-type: none"> 1. Log into the terminal as an administrator. ➔ See “Administrator Authentication” on page 47 for more information. 2. Press <input type="radio"/> Management Menu. 3. Press <input type="radio"/> Holiday Menu. 4. Press <input type="radio"/> List Holidays. 5. From here, many other functions can be accessed. See the other topics in this section for more information. 	

Add Holiday	
Sets and configures holidays for the terminal. Enter the holiday name, start time and end time to build a holiday.	<p>Default: None</p> <p>Range: None</p> <p>Dependencies: None</p> <p>Who: A terminal administrator can add holidays at any time.</p>
<ol style="list-style-type: none"> 1. Log into the terminal as an administrator. ➔ See “Administrator Authentication” on page 47 for more information. 2. Press <input type="radio"/> Management Menu. 3. Press <input type="radio"/> Holiday Menu. 4. Press <input type="radio"/> Add Holidays. 5. Enter the name of the holiday. 6. Press <input type="radio"/> Enter. 7. Enter the holiday start date and time. 8. Press <input type="radio"/> Enter. 9. Enter the holiday end date and time. 10. Press <input type="radio"/> Enter. 	

Network Setup

The Network Setup menu is used to configure information that will be used by the terminal to communicate with the host application. This information is only necessary when the terminal is used in network mode.

Set Logical Name	
Sets the name of the terminal on the TCP/IP network. If the terminal will be running in network mode, this name must match the logical name for the terminal recorded in the host application for synchronization to occur.	Default: G-Series-Handreader Range: 6-25 alphanumeric characters Dependencies: None Who: An administrator should set a logical name during initial terminal setup.
<ol style="list-style-type: none">1. Log into the terminal as an administrator. ➔ See “Administrator Authentication” on page 47 for more information.2. Press <input type="radio"/> Setup Menu.3. Press <input type="radio"/> Network Setup.4. Press <input type="radio"/> Set LogicalName.5. Enter the logical name for the terminal.6. Press <input type="radio"/> Enter.	

Set Host Username	
<p>The host user name is used to authenticate with the host application. This user name must match a valid user account user name on the host application in order for synchronization to occur.</p>	<p>Default: None Range: None Dependencies: None Who: A network administrator should set the host user name during initial terminal setup</p>
<ol style="list-style-type: none">1. Log into the terminal as an administrator. ➔ See “Administrator Authentication” on page 47 for more information.2. Press <input type="radio"/> Setup Menu.3. Press <input type="radio"/> Network Setup.4. Press <input type="radio"/> Set HostUser.5. Enter the user name for the host application.6. Press <input type="radio"/> Enter.	

Go to StandAlone or Demo Mode	
<p>The display of this menu indicates the current mode of the terminal as follows:</p> <ul style="list-style-type: none">• Go To StandAlone Mode is only displayed when the terminal is running in network mode. To put the terminal in standalone mode, press Go To StandAlone Mode. When the terminal is in standalone mode, no synchronization with the host application will occur.• Go To Demo Mode is only displayed when the terminal is running in standalone or networked mode. To put the terminal in Demo mode, press Go To Demo Mode. when the terminal is in Demo mode, no synchronization with the host application will occur.• Go To Network Mode is only displayed when the terminal is running in standalone mode or Demo mode. To put the terminal in network mode, press Go To Network Mode. When the terminal is in network mode, the terminal will attempt to synchronize with the host application.	<p>Default: None</p> <p>Range: None</p> <p>Dependencies: None</p> <p>Who: A network administrator can change this setting at any time.</p>
<ol style="list-style-type: none">1. Log into the terminal as an administrator. ➔ See “Administrator Authentication” on page 47 for more information.2. Press <input type="radio"/> Setup Menu.3. Press <input type="radio"/> Network Setup.4. Press <input type="radio"/> Go To Demo Mode/StandAlone Mode/Go To Network Mode.5. Press <input type="radio"/> Go To Demo Mode/StandAlone Mode/Go To Network Mode (again).	

Set WebServer	
<p>Enables or disables the terminal's web server. If the terminal will be used in network mode, the web server should be enabled. The display of this menu will indicate the current state of the web server.</p>	<p>Default: Enabled Range: None Dependencies: None Who: A network administrator should set the WebServer during initial terminal setup.</p>
<ol style="list-style-type: none"> 1. Log into the terminal as an administrator. ➔ See “Administrator Authentication” on page 47 for more information. 2. Press <input type="radio"/> Setup Menu. 3. Press <input type="radio"/> press Network Setup. 4. Press <input type="radio"/> Set WebServer. 5. Press <input type="radio"/> Enable or Disable. 6. Reboot the terminal. (The new setting will not take effect until the terminal is rebooted.) ➔ See “Rebooting the Terminal Using the Terminal Interface” on page 53 for more information. 	

Set Host Password	
<p>The host password is used to authenticate with the host application. This password must match a valid user account password on the host application in order for synchronization to occur.</p>	<p>Default: None Range: None Dependencies: None Who: A network administrator should set the host password during initial terminal setup.</p>
<ol style="list-style-type: none"> 1. Log into the terminal as an administrator. ➔ See “Administrator Authentication” on page 47 for more information. 2. Press <input type="radio"/> Setup Menu. 3. Press <input type="radio"/> Network Setup. 4. Press <input type="radio"/> Set HostPassword. 5. Enter the host password. 6. Press <input type="radio"/> Enter. 	


Set Host URL	
<p>The HostURL is used to authenticate with the host application. This URL must match URL of the host application in order for synchronization to occur.</p>	<p>Default: http://127.0.0.1</p> <p>Range: None</p> <p>Dependencies: None</p> <p>Who: A network administrator should set HostURL during initial terminal setup.</p>
<ol style="list-style-type: none">1. Log into the terminal as an administrator. ➔ See “Administrator Authentication” on page 47 for more information.2. Press <input type="radio"/> Setup Menu.3. Press <input type="radio"/> Network Setup.4. Press <input type="radio"/> Set HostURL.5. Enter the host URL (complete URL, starting with “http://”).6. Press <input type="radio"/> Enter.	

Set CLISvr Port	
Set CLISrv Port defines the port that will be used connect to the terminal's Command Line Interface (CLI).	Default: 8090 Range: None Dependencies: Site's network specifications Who: A terminal administrator may change the port from the default to comply with site specifications.
<ol style="list-style-type: none">1. Log into the terminal as an administrator. ➔ See "Administrator Authentication" on page 47 for more information.2. Press <input type="radio"/> Setup Menu.3. Press <input type="radio"/> Network Setup.4. Press <input type="radio"/> More.5. Press <input type="radio"/> Set CLISrv Port.6. Enter the CLI server port.7. Press <input type="radio"/> Enter.8. Reboot the terminal. ➔ See "Rebooting the Terminal Using the Terminal Interface" on page 53 for more information.	

Set XMLRPCsvr Port	
Set XMLRPCsvr Port defines the port that will to connect to the terminal's XMLRPC server.	Default: 8085 Range: None Dependencies: Site network specifications Who: A terminal administrator may change the port from the default to comply with site specifications.
<ol style="list-style-type: none">1. Log into the terminal as an administrator. ➔ See “Administrator Authentication” on page 47 for more information.2. Press <input type="radio"/> Setup Menu.3. Press <input type="radio"/> Network Setup.4. Press <input type="radio"/> More.5. Press <input type="radio"/> Set XMLRPCsvr Port.6. Enter the XMLRPC server port.7. Press <input type="radio"/> Enter.8. Reboot the terminal. <p>➔ See “Rebooting the Terminal Using the Terminal Interface” on page 53 for more information.</p>	

XMLRPC Svr Setup	
<p>XMLRPC Svr Setup enables or disables the XMLRPC server. The display of this menu will indicate the current state of the XML-RPC server. If it is disabled, press enable to enable the XML-RPC server. If it is enabled, press disable to disable it.</p>	<p>Default: Enabled Range: None Dependencies: None Who: A network administrator should set the XML-RPC server during initial terminal setup.</p>
<ol style="list-style-type: none">1. Log into the terminal as an administrator. ➔ See “Administrator Authentication” on page 47 for more information.2. Press <input type="radio"/> Setup Menu.3. Press <input type="radio"/> Network Setup.4. Press <input type="radio"/> More.5. Press <input type="radio"/> Set XMLRPC Svr Setup Port.6. Press <input type="radio"/> to Enable (or Disable).7. Reboot the terminal. ➔ See “Rebooting the Terminal Using the Terminal Interface” on page 53 for more information.	

Set WebSvr Port	
Set WebSvr Port defines the port you will use to connect to the terminal's Web Server.	Default: 80 Range: None Dependencies: None Who: A terminal administrator may change the web server port from default to comply with a site's network specifications.
<ol style="list-style-type: none">1. Log into the terminal as an administrator. ➔ See "Administrator Authentication" on page 47 for more information.2. Press <input type="radio"/> Setup Menu.3. Press <input type="radio"/> Network Setup.4. Press <input type="radio"/> More.5. Press <input type="radio"/> Set WebSvr Port.6. Enter the web server port.7. Press <input type="radio"/> Enter.8. Reboot the terminal. ➔ See "Rebooting the Terminal Using the Terminal Interface" on page 53 for more information.	


Set Static/DHCP	
<p>Set Static/DHCP is used to either set a static IP address for the terminal or to use DHCP. If DHCP is enabled, enter an IP address to switch to static. If static is enabled, press DHCP to switch to DHCP.</p> <p>NOTE: Switching from DHCP to Static IP (or vice versa) will force a reboot.</p>	<p>Default: DHCP</p> <p>Range: 0-255</p> <p>Dependencies: None</p> <p>Who: A network administrator should set Static/DHCP during initial terminal setup.</p>
<ol style="list-style-type: none"> 1. Log into the terminal as an administrator. <ul style="list-style-type: none"> ➔ See “Administrator Authentication” on page 47 for more information. 2. Press <input type="radio"/> Setup Menu. 3. Press <input type="radio"/> Network Setup. 4. Press <input type="radio"/> More. 5. Press <input type="radio"/> Static/DHCP. 6. Do one of the following: <ol style="list-style-type: none"> a. At this point, DHCP is enabled. The IP address will be displayed on the screen. b. To enable a static IP address, press <input type="radio"/> Static IP. <ol style="list-style-type: none"> 1. To edit the IP address, highlight IPADDR using . Press the middle key to select the IPADDR list item. 2. Press <input type="radio"/> Edit and enter the IP Address. Press <input type="radio"/> Confirm. 3. To edit the DNS1, DNS2, NETMASK, or GATEWAY values, repeat the previous 2 steps. (in b.1 and b.2). 	


Set RealTimeInteraction	
<p>When Set Real Time Interaction is enabled, the terminal will send interactions as they happen (in real time). When Real Time Interaction is disabled, the terminal will send interactions only when a synchronization takes place. The display of this menu will indicate the current state of Real Time Interactions. If it is disabled, press enable to enable Real Time Interactions. If it is enabled, press disable to disable it.</p>	<p>Default: Enabled Range: None Dependencies: None Who: A terminal administrator should enable or disable Real Time Interaction to conform to the site design requirements.</p>
<ol style="list-style-type: none"> 1. Log into the terminal as an administrator. ➔ See “Administrator Authentication” on page 47 for more information. 2. Press <input type="radio"/> Setup Menu. 3. Press <input type="radio"/> Network Setup. 4. Press <input type="radio"/> More. 5. Press <input type="radio"/> RealTimeInteraction. 6. Press <input type="radio"/> to Enable (or Disable). 	

Display Setup

The Display Setup menu is used to configure information that is displayed on the LCD screen.

Set Company Name	
<p>The Company Name is the first line of text that is displayed on the terminal screen. It can be changed to any line of text.</p>	<p>Default: Schlage Biometrics Range: None Dependencies: None Who: A terminal administrator can set the company name at any time.</p>
<ol style="list-style-type: none"> 1. Log into the terminal as an administrator. ➔ See “Administrator Authentication” on page 47 for more information. 2. Press <input type="radio"/> Setup Menu. 3. Press <input type="radio"/> Display Setup. 4. Press <input type="radio"/> Set Company Name. 5. Enter the company name and press <input type="radio"/> Enter. 	

Set Time Format	
<p>Sets the time format that will be used to display the time on the terminal screen.</p>	<p>Default: HH:MM:SS</p> <p>Range: None</p> <p>Dependencies: None</p> <p>Who: A terminal administrator can set a time format at any time.</p>
<ol style="list-style-type: none"> 1. Log into the terminal as an administrator. ➔ See “Administrator Authentication” on page 47 for more information. 2. Press <input type="radio"/> Setup Menu. 3. Press <input type="radio"/> Display Setup. 4. Press <input type="radio"/> Date Time Format. 5. Press <input type="radio"/> Set Time Format. 6. Scroll to the format you want to use by using . Press the middle key to select the time format. 	

Set Date Format	
<p>Sets the date format that will be used to display the date on the terminal screen.</p>	<p>Default: MM/DD/YYYY</p> <p>Range: None</p> <p>Dependencies: None</p> <p>Who: A terminal administrator can set a date format at any time.</p>
<ol style="list-style-type: none"> 1. Log into the terminal as an administrator. ➔ See “Administrator Authentication” on page 47 for more information. 2. Press <input type="radio"/> Setup Menu. 3. Press <input type="radio"/> Display Setup. 4. Press <input type="radio"/> Date Time Format. 5. Press <input type="radio"/> Set Date Format. 6. Scroll to the format you want to use by using . Press the middle key to select the date format. 	

Set Ready String

The Ready String is the line of text that is displayed below the company name on the terminal screen. It can be changed to any line of text.

Default: ***Enter ID***

Range: None

Dependencies: None

Who: A terminal administrator can set a ready string at any time.

1. Log into the terminal as an administrator.
 ➔ **See “Administrator Authentication” on page 47 for more information.**
2. Press Setup Menu.
3. Press Display Setup.
4. Press Set Ready String.
5. Enter the ready string.
6. Press Enter.

Set Language


Set Language is used to change language on the terminal. Note: English (EN) is the only supported language for this release.

Default: EN


Range: None

Dependencies: None



Who: A terminal administrator should set this value during initial configuration of the terminal.


1. Log into the terminal as an administrator.
 ➔ **See “Administrator Authentication” on page 47 for more information.**
2. Press Setup Menu.
3. Press Display Setup.
4. Press Set Language..
5. Scroll to the format you want to use by using . Press the middle key to select the desired language.



User Management




Edit User	
Edits a user that is already entered in the terminal.	<p>Default: None</p> <p>Range: None</p> <p>Dependencies: None</p> <p>Who: A terminal administrator can edit a user in the terminal at any time.</p>
<ol style="list-style-type: none"> Log into the terminal as an administrator. ➔ See “Administrator Authentication” on page 47 for more information. Press <input type="radio"/> User Management Press <input type="radio"/> Edit User. Press <input type="radio"/> List Users. Scroll to the appropriate user using . Press the middle key to select the user. From here, many other functions can be accessed. See the other topics in this section for more information.. 	






List Users	
<p>List Users displays a table showing all users associated with the terminal. The table also displays the RPIN, user authorization and in/out status.</p> <p style="color: red; text-align: center;">➔ This information is only accurate to within the last host synchronization.</p>	<p>Default: None</p> <p>Range: None</p> <p>Dependencies: None</p> <p>Who: A terminal administrator can list a user in the terminal at any time.</p>
<ol style="list-style-type: none"> Log into the terminal as an administrator. ➔ See “Administrator Authentication” on page 47 for more information. Press <input type="radio"/> User Management Press <input type="radio"/> List Users. From here, many other functions can be accessed. See the other topics in this section for more information.. 	

Edit Name	
<p>Edit Name is used to change a user's name. First name, last name and middle name are edited separately.</p>	<p>Default: None</p> <p>Range: None</p> <p>Dependencies: None</p> <p>Who: A terminal administrator can change a user's name in the terminal at any time.</p>
<ol style="list-style-type: none"> 1. Log into the terminal as an administrator. ➔ See "Administrator Authentication" on page 47 for more information. 2. Press <input type="button" value="○"/> User Management 3. Press <input type="button" value="○"/> List Users. 4. Scroll to the appropriate user using . Press the middle key to select the user. 5. Scroll to the name you want to edit and use  to select the name. 6. Make any necessary changes to the name. 7. Press <input type="button" value="○"/> Enter. 	

Enroll Status	
<p>This option displays the user's enroll status information such as high/low resolution template and EPIN usage.</p>	<p>Default: None</p> <p>Range: None</p> <p>Dependencies: None</p> <p>Who: A terminal administrator can view a user's enrollment status at any time.</p>
<ol style="list-style-type: none"> 1. Log into the terminal as an administrator. ➔ See "Administrator Authentication" on page 47 for more information. 2. Press <input type="button" value="○"/> User Management 3. Press <input type="button" value="○"/> List Users. 4. Scroll to the appropriate user using . Press the middle key to select the user. 5. Scroll to the Enroll Status option to view enrollment information for this user. 	

Edit Authority	
<p>Changes the authority level of a user. Authority level determines which level of command menu a user may access. The terminal administrator account must have level 5 authority. Users have authorization based on their authority level as follows:</p> <ul style="list-style-type: none">• Last Punch• Last Punch, User Management• Last Punch, User Management, Maintenance• Last Punch, User Management, Maintenance, Setup• Last Punch, User Management, Maintenance, Setup, Security	<p>Default: 1 Range: 1-5 Dependencies: None Who: A terminal administrator can change the authority level associated with a user's profile at any time.</p>
<ol style="list-style-type: none">1. Log into the terminal as an administrator. ➔ See "Administrator Authentication" on page 47 for more information.2. Press <input type="button" value="F2"/> User Management3. Press <input type="button" value="F3"/> List Users.4. Scroll to the name of the user for which you want to change the authority using . Press the middle key to select the user.5. Scroll to the authority listing using . Press the middle key to select the authority.6. Enter the authority level.7. Press <input type="button" value="Enter"/> Enter.	

Last Score	
<p>This option displays the user's last score, which reflects how accurately the user's hand is placed on the platen.</p> <p>For more information about hand scores, see "Understanding Hand Read Scores" on page 120.</p>	<p>Default: None</p> <p>Range: Scores above 50 may indicate improper hand placement</p> <p>Dependencies: None</p> <p>Who: A terminal administrator can view a user's last hand score at any time.</p>
<ol style="list-style-type: none">1. Log into the terminal as an administrator. ➔ See "Administrator Authentication" on page 47 for more information.2. Press  User Management3. Press  List Users.4. Scroll to the appropriate user using . Press the middle key to select the user.5. Scroll to the Last Score option to view hand score information for this user.	

Edit Threshold	
<p>Each time a user verifies at the terminal, a number that represents the closeness of the match between the template (created at enrollment) and the actual hand is recorded. The threshold is a number that represents how close the match must be for successful verification. The threshold is generally set at the terminal level. If a particular user cannot verify under the terminal's threshold, a personal threshold may be set at the user level. In this way, the level of security is not compromised for all users on the terminal.</p> <p>→ A threshold set at the user level will override the threshold set at the terminal level.</p> <p>→ If a threshold is set at the user level to be a value of "0", the terminal threshold level will be set to the default value of "75" automatically.</p>	<p>Default: 75</p> <p>Range: 10-255</p> <p>Dependencies: None</p> <p>Who: A terminal administrator can edit the threshold at any time.</p>
<ol style="list-style-type: none"> 1. Log into the terminal as an administrator. → See "Administrator Authentication" on page 47 for more information. 2. Press  User Management 3. Press  List Users. 4. Scroll to the name of the user for which you want to edit the threshold using . Press the middle key to select the user. 5. Scroll to the authority listing using . Press the middle key to edit the threshold. 6. Enter the threshold. 7. Press  Enter. 	

Verify Status


This option displays the user's status. A value of true indicates that the user is active; a value of false indicates that the user is inactive.

Default: None

Range: None

Dependencies: None

Who: A terminal administrator view a user's status at any time.

1. Log into the terminal as an administrator.
 ➔ **See "Administrator Authentication" on page 47 for more information.**
2. Press User Management
3. Press List Users.
4. Scroll to the appropriate user using . Press the middle key to select the user.
5. Scroll to the Verify Status option to view user status.

Edit Timezone




Changes the timezone that is associated with a user's profile. Select the user. Then select the timezone you want to associate with that user's profile.


Default: None


Range: None


Dependencies: None


Who: A terminal administrator can change the timezone associated with a user's profile at any time.


1. Log into the terminal as an administrator.
 ➔ **See "Administrator Authentication" on page 47 for more information.**
2. Press User Management
3. Press List Users.
4. Scroll to the name of the user for which you want to edit the timezone using . Press the middle key to select the user.
5. Scroll to the timezone option using . Press the middle key to edit the timezone.
6. Enter the desired timezone and press Enter.
7. Scroll to the timezone you want to associate with the user using . Press the middle key to select the timezone.


Edit User Status	
<p>Changes a user's status from active to inactive. (Inactive users are those which are not able to use a terminal until their status is changed to active.)</p>	<p>Default: Active Range: None Dependencies: None Who: A terminal administrator can change a user's status at any time.</p>
<ol style="list-style-type: none"> 1. Log into the terminal as an administrator. ➔ See "Administrator Authentication" on page 47 for more information. 2. Press <input type="radio"/> User Management 3. Press <input type="radio"/> List Users. 4. Scroll to the name of the user for which you want to edit the user status using . Press the middle key to select the user. 5. Press <input type="radio"/> Disable to change a user's status to Inactive, or press <input type="radio"/> Enable to change a user's status to active. 	








Enroll User	
<p>Enroll User records a user's hand template for verification. After the user has been entered into the terminal, a terminal administrator should instruct the user on correct hand placement.</p>	<p>Default: None Range: None Dependencies: User must be entered into the terminal before enrollment. The user must be present for enrollment. Who: A terminal administrator can enroll a user after the user has been entered into the terminal.</p>
<ol style="list-style-type: none"> 1. Log into the terminal as an administrator. ➔ See "Administrator Authentication" on page 47 for more information. 2. Press <input type="radio"/> User Management 3. Press <input type="radio"/> List Users. 4. Scroll to the name of the user you want to enroll using . Press the middle key to select the user. 5. Press <input type="radio"/> Enroll User. 6. Follow the prompts on the terminal screen for hand placement. 	

Last Booking	
<p>Shows information about the user’s last booking, or log- in.</p> <p>➔ This information is only accurate to within the last host synchronization.</p>	<p>Default: None</p> <p>Range: None</p> <p>Dependencies: None</p> <p>Who: A terminal administrator can display the last booking at any time.</p>
<ol style="list-style-type: none"> 1. Log into the terminal as an administrator. ➔ See “Administrator Authentication” on page 47 for more information. 2. Press <input type="radio"/> User Management 3. Press <input type="radio"/> List Users. 4. Scroll to the name of the user for which you want to view the last booking using . Press the middle key to select the user. 5. Press <input type="radio"/> Last Booking. 	

Generate Punch	
<p>Generates a punch for a given user.</p>	<p>Default: None</p> <p>Range: None</p> <p>Dependencies: None</p> <p>Who: A terminal administrator can generate a punch for a user at any time.</p>
<ol style="list-style-type: none"> 1. Log into the terminal as an administrator. ➔ See “Administrator Authentication” on page 47 for more information. 2. Press <input type="radio"/> User Management 3. Press <input type="radio"/> List Users. 4. Scroll to the name of the user for whom you want to generate a punch using . Press the middle key to select the user. 5. Press <input type="radio"/> More. 6. Press <input type="radio"/> Generate Punch. 	

Remove User	
<p>Removes a user from the terminal if the user no longer requires access.</p> <p>➔ <i>When using this function to remove a user, user is not removed from the host application database. See the documentation that came the host application for more information.</i></p>	<p>Default: None</p> <p>Range: None</p> <p>Dependencies: None</p> <p>Who: A terminal administrator can remove a user at any time.</p>
<ol style="list-style-type: none">1. Log into the terminal as an administrator. ➔ <i>See “Administrator Authentication” on page 47 for more information.</i>2. Press <input type="radio"/> User Management3. Press <input type="radio"/> List Users.4. Scroll to the name of the user you which to enroll using . Press the middle key to select the user.5. Press <input type="radio"/> More.6. Press <input type="radio"/> Remove User.7. Press <input type="radio"/> YES.	

List Credentials	
Lists all credentials associated with a user. Select the user and then select List Credentials.	Default: None Range: None Dependencies: None Who: A terminal administrator can list the credentials for a user at any time.
<ol style="list-style-type: none">1. Log into the terminal as an administrator. ➔ See “Administrator Authentication” on page 47 for more information.2. Press <input type="radio"/> User Management3. Press <input type="radio"/> List Users.4. Scroll to the name of the user you wish to want to list credentials using . Press the middle key to select the user.5. Press <input type="radio"/> More.6. Press <input type="radio"/> Credential Menu.7. Press <input type="radio"/> List Credential.8. Credentials can be edited from this menu. See the other topics in this section for more information.	

Add Credential	
<p>Adds any type of credential to a user's profile. Select the user. Then select the type of credential to add to the profile.</p> <p>➔ A user can have multiple credential IDs of different types, provided that the user has only 1 credential ID for a given credential type.</p>	<p>Default: None</p> <p>Range: None</p> <p>Dependencies: None</p> <p>Who: A terminal administrator can add a new credential at any time.</p>
<ol style="list-style-type: none">1. Log into the terminal as an administrator. ➔ See "Administrator Authentication" on page 47 for more information.2. Press  User Management3. Press  List Users.4. Scroll to the name of the user for which you want to add a credential using . Press the middle key to select the user.5. Press  More.6. Press  Credential Menu.7. Press  Add Credential.8. Scroll to the type of credential you want to add using . Press the middle key to select the credential type.	

No Hand Enroll

Enrolls a user who cannot perform the standard hand enrollment or verification, or to enroll a user who is not present. If the user has previously enrolled using the standard enrollment procedures, the hand template will be deleted after no hand enrollment. If the user needs to go back to using hand verification, the user must be re-enrolled using the normal enrollment process.


➔ See **“Enroll User”** on page 90 for more information.



Default: None

Range: None

Dependencies: User must be entered into the terminal before the user can be enrolled.

Who: A terminal administrator can enroll a user using no hand enroll at any time.

1. Log into the terminal as an administrator.
➔ See **“Administrator Authentication”** on page 47 for more information.
2. Press User Management
3. Press List Users.
4. Scroll to the name of the user you wish to enroll using . Press the middle key to select the user.
5. Press More.
6. Press No Hand Enroll.
7. Enter the EPIN.
8. Press Enter.

Edit EPIN	
<p>An EPIN is used for verification if the HPU becomes non-functional. Select the user. Then add an EPIN to the user.</p> <p> <i>An EPIN should be used as an emergency backup function only when the HPU fails. EPIN is not intended for regular use as it will compromise security.</i></p>	<p>Default: None</p> <p>Range: None</p> <p>Dependencies: User must be entered into the terminal before an EPIN can be added.</p> <p>Who: A terminal administrator can add an EPIN to any user's profile.</p>
<ol style="list-style-type: none">1. Log into the terminal as an administrator. ➔ See “Administrator Authentication” on page 47 for more information.2. Press <input type="radio"/> User Management3. Press <input type="radio"/> List Users.4. Scroll to the name of the user you wish to add an EPIN using . Press the middle key to select the user.5. Press <input type="radio"/> More.6. Press <input type="radio"/> Edit EPIN.7. Enter the EPIN.8. Press <input type="radio"/> Enter.	

Edit Access Grant

Edits an access grant for particular user. Access grants are used to grant access to a user for a particular, recurring time period. Access grants override timezones. Select the user. Then select the access grant you want to edit.



➔ **Access grants and timezones should not be used in the same site.**







Default: None

Range: None

Dependencies: None

Who: A terminal administrator can edit an access grant at any time.

1. Log into the terminal as an administrator.
➔ **See “Administrator Authentication” on page 47 for more information.**
2. Press User Management
3. Press List Users.
4. Scroll to the name of the user for which you want to edit the access grant using . Press the middle key to select the user.
5. Press More.
6. Press Access Grant Menu.
7. Press List Access Grants.
8. Scroll to the access grant you want to edit using . Press the middle key to select the access grant.
9. Choose one of the following:
 - a. Press Remove AccessGrant to remove the access grant. Press YES.
 - b. Press Edit StartTime to edit the start time. Enter the start time and press Enter.
 - c. Press Edit DOW to edit the day of the week. Press to toggle each day of the week and/or holiday.
 - d. Press Edit Duration to edit the duration. Enter the duration and press Enter.

List Access Grants	
<p>Lists all access grant for a particular user. Access grants are used to grant access to a user for a particular, recurring time period. Access grants override timezones.</p> <p>➔ Access grants and timezones should not be used in the same site.</p>	<p>Default: None</p> <p>Range: None</p> <p>Dependencies: None</p> <p>Who: A terminal administrator can list access grants at any time.</p>
<ol style="list-style-type: none">1. Log into the terminal as an administrator. ➔ See “Administrator Authentication” on page 47 for more information.2. Press  User Management3. Press  List Users.4. Scroll to the name of the user for which you want to list access grants using . Press the middle key to select the user.5. Press  More.6. Press  Access Grant Menu.7. Press  List Access Grants.8. From here, many other functions can be accessed. See the other topics in this section for more information.	

Add Access Grants

Adds an access grant particular user. Access grants are used to grant access to a user for a particular, recurring time period. Access grants override timezones. Select the user. Then add an access grant to the user.


➔ **Access grants and timezones should not be used in the same site.**


Default: None

Range: None

Dependencies: None

Who: A terminal administrator can add access grants at any time.

1. Log into the terminal as an administrator.
➔ **See “Administrator Authentication” on page 47 for more information.**
2. Press User Management
3. Press List Users.
4. Scroll to the name of the user for which you want to edit access grants using . Press the middle key to select the user.
5. Press More.
6. Press Access Grant Menu.
7. Press Add Access Grants.
8. Enter the start time using the format HH MM SS (Example: 13 22 59.)
9. Enter the duration using the format HH MM SS.
10. Press Enter.
11. Press to toggle each day of the week and/or holiday.

List Bookings	
<p>Lists all of the bookings (such as punches) for a particular user.</p> <p>➔ <i>This information is only accurate to within the last host synchronization.</i></p>	<p>Default: None</p> <p>Range: None</p> <p>Dependencies: None</p> <p>Who: A terminal administrator can list bookings for a user at any time.</p>
<ol style="list-style-type: none"> 1. Log into the terminal as an administrator. ➔ <i>See “Administrator Authentication” on page 47 for more information.</i> 2. Press <input type="radio"/> User Management 3. Press <input type="radio"/> List Users. 4. Scroll to the name of the user for whom you want to list bookings using . Press the middle key to select the user. 5. Press <input type="radio"/> More. 6. Press <input type="radio"/> List Bookings. 	

Add User	
<p>Creates a new user profile in the terminal. Enter the user’s RPIN credential. Other properties may be configured after the user is added.</p>	<p>Default: None</p> <p>Range: None</p> <p>Dependencies: None</p> <p>Who: A terminal administrator can add users at any time.</p>
<ol style="list-style-type: none"> 1. Log into the terminal as an administrator. ➔ <i>See “Administrator Authentication” on page 47 for more information.</i> 2. Press <input type="radio"/> User Management 3. Press <input type="radio"/> Add User. 4. Enter the RPIN. 5. Press <input type="radio"/> Enter. ➔ <i>The terminal must check the host system at this point to ensure that the RPIN is not already in use. This process can sometimes take a while to complete. Wait until the next screen appears before pressing any other buttons.</i> 6. At this point, the user has been added. To configure other properties for this user (or to enroll the user) see the other topics listed in this section. 	

Security Menu

Clear Setup

Clear Setup	
<p>! <i>Use caution when performing this function!</i> <i>All settings will be restored to factory settings. This action cannot be undone!</i></p> <p>Clear Setup can be used to restore all of the settings on the terminal back to their original state. Clear Setup will perform the following actions:</p> <ul style="list-style-type: none"> • All setup values will be returned to defaults (including sync settings) • All databases will be cleared (for example, user database, interaction databases, etc.) 	<p>Default: None</p> <p>Range: None</p> <p>Dependencies: None</p> <p>Who: A terminal administrator can use Clear Setup at any time.</p>
<ol style="list-style-type: none"> 1. Log into the terminal as an administrator. ➔ See “Administrator Authentication” on page 47 for more information. 2. Press <input type="radio"/> Security Menu. 3. Press <input type="radio"/> Clear Setup. 4. Press <input type="radio"/> YES. 	


Biometric Setup

The Biometric Setup Menu is used to configure the level of security at the terminal. Biometric security is determined by a combination of template resolution and the number of access tries.

Min High Res Update Count	
<p>**Indicates the minimum number of time the terminal must update its high resolution template before switching to high resolution template verifications automatically.</p> <p>➔ **This option is currently not in use since all supported terminals are high resolution terminals.</p>	<p>Default: NA</p> <p>Range: NA</p> <p>Dependencies: NA</p> <p>Who: NA</p>
<ol style="list-style-type: none"> 1. Log into the terminal as an administrator. <p style="margin-left: 20px;">➔ See “Administrator Authentication” on page 47 for more information.</p> 2. Press <input type="radio"/> Security Menu. 3. Press <input type="radio"/> Biometric Setup. 4. Press <input type="radio"/> Min High Res Count. 5. Enter the Set Min High Resolution Update Count. 6. Press <input type="radio"/> Enter (or Clear to cancel). 	

Placements Per Try	
<p>Placements Per Try defines the number of hand placements allowed during a verification attempt.</p> <p>➔ A “try” is the presentation of a credential ID during a verification attempt. A “placement” is the presentation of a hand to the GT-Series terminal during a verification attempt.</p>	<p>Default: 3</p> <p>Range: 1-99</p> <p>Dependencies: None</p> <p>Who: A terminal administrator specifies this value in coordination with Number of Tries to indicate how forgiving the terminal will be during verification.</p>
<ol style="list-style-type: none"> 1. Log into the terminal as an administrator. <p style="margin-left: 20px;">➔ See “Administrator Authentication” on page 47 for more information.</p> 2. Press <input type="radio"/> Security Menu. 3. Press <input type="radio"/> Biometric Setup. 4. Press <input type="radio"/> Placements/Try. 5. Enter the number of placements per try. 6. Press <input type="radio"/> Enter. 	

Number of Tries	
<p>Number of Tries defines the number of verification attempts allowed for a user. Once the number of tries has been exceeded, the credential ID will be locked out until a terminal administrator verifies at the terminal. For increased security, use a lower number. For increased convenience, use a higher number.</p> <p>➔ A try is the presentation of a credential ID during a verification attempt. A placement is the presentation of a hand to the hand reader during a verification attempt.</p>	<p>Default: 3</p> <p>Range: 1-99</p> <p>Dependencies: None</p> <p>Who: A terminal administrator specifies this value in coordination with Placements Per Try to indicate how forgiving the terminal will be during verification.</p>
<ol style="list-style-type: none"> 1. Log into the terminal as an administrator. <p>➔ See “Administrator Authentication” on page 47 for more information.</p> 2. Press <input type="radio"/> Security Menu. 3. Press <input type="radio"/> Biometric Setup. 4. Press <input type="radio"/> Number of Tries. 5. Enter the number of tries. 6. Press <input type="radio"/> Enter. 	

Template Resolution	
<p>Sets the template resolution to High or Non-biometric. Set this option to High for Biometric terminals. Set this option to non-biometric for those terminals you run in Non-biometric mode (those terminals which do not use hand recognition in order to use the terminal). In non-biometric mode, terminals can use both an RPIN and EPIN (if an EPIN has been created) or an RPIN only (if an EPIN has not been created).</p>	<p>Default: NA</p> <p>Range: NA</p> <p>Dependencies: NA</p> <p>Who: An administrator can use this setting at any time, as needed.</p>
<ol style="list-style-type: none"> 1. Log into the terminal as an administrator. <p>➔ See “Administrator Authentication” on page 47 for more information.</p> 2. Press <input type="radio"/> Security Menu. 3. Press <input type="radio"/> Biometric Setup. 4. Press <input type="radio"/> Template Resolution. 5. Scroll to and select High or Non-biometric by using . 	

Set Passwords

Set Passwords	
<p>Sets the password for command line access to the terminal. CLI access is only available if all other conditions for enabling CLI access have been met.</p>	<p>Default: Schlage538</p> <p>Range: Must match host application password</p> <p>Dependencies: Other conditions for CLI access be met before command line access to the terminal will be available.</p> <p>Who: An application developer can change the CLI access password to enhance security, or as a troubleshooting, testing or debugging step.</p>
<ol style="list-style-type: none">1. Log into the terminal as an administrator. ➔ See “Administrator Authentication” on page 47 for more information.2. Press <input type="radio"/> Security Menu.3. Press <input type="radio"/> Set Passwords.4. Press <input type="radio"/> Set CLI Access Pwd.5. Enter the CLI access password.6. Press <input type="radio"/> Enter.	

Clear UserDB

Clear UserDB	
<p>Clear UserDB will remove all users from the terminal.</p> <p>! <i>This function cannot be undone. However, all users will be restored to the terminal the next time the terminal synchronizes with a host application.</i></p>	<p>Default: None</p> <p>Range: None</p> <p>Dependencies: None</p> <p>Who: A terminal administrator can use Clear UserDB to remove all users from the terminal.</p>
<ol style="list-style-type: none"> Log into the terminal as an administrator. ➔ See “Administrator Authentication” on page 47 for more information. Press <input type="radio"/> Security Menu. Press <input type="radio"/> Clear UserDB. Press <input type="radio"/> YES. 	

Factory Settings

Factory Settings	
<p>Factory Settings is a list of useful information about the factory settings of the terminal. Factory settings cannot be edited. The following list will be displayed:</p> <ul style="list-style-type: none"> User Capacity: number of users that can be stored BPUType: type of biometric processing unit BoardRevision: version of the internal hardware MemorySizeMB: total capacity of the SD card SerialNum: serial number Model: model number Credential Reader Type: all available credential reader types 	<p>Default: None</p> <p>Range: None</p> <p>Dependencies: None</p> <p>Who: A terminal administrator can use Factory Settings to view the factory settings of the terminal, most likely as a troubleshooting step.</p>
<ol style="list-style-type: none"> Log into the terminal as an administrator. ➔ See “Administrator Authentication” on page 47 for more information. Press <input type="radio"/> Security Menu. Press <input type="radio"/> Factory Settings. 	

Reject Threshold

At each verification attempt, the hand placement is compared to the user template. A score that reflects how closely the placement and the template match is assigned. The lower the score, the closer the match. The reject threshold defines the minimum score that must be attained for verification.

Reject Threshold	
<p>Sets the global biometric reject threshold for all users enrolled in the terminal who do not have an individual reject threshold.</p> <p>For increased security or decreased FAR (False Acceptance Rate), use a lower number. For increased convenience or decreased FRR (False Rejection Rate), use a higher number.</p> <p style="text-align: center;">➔ A reject threshold set at the user level will override this setting.</p>	<p>Default: 75</p> <p>Range: 30-255</p> <p>Dependencies: None</p> <p>Who: A terminal administrator should set this value during initial configuration of the terminal. A terminal administrator can also change this value at an existing site if there is a need to increase security or user convenience.</p>
<ol style="list-style-type: none"> 1. Log into the terminal as an administrator. ➔ See “Administrator Authentication” on page 47 for more information. 2. Press <input type="button" value="○"/> Security Menu. 3. Press <input type="button" value="○"/> Set Reject Threshold. 4. Enter the reject threshold. 5. Press <input type="button" value="○"/> Enter. 	

Set Credential Logging Flag

Set Credential Logging Flag	
<p>This setting is mainly used for debugging purpose. When enabled, the credential/Barcode information of all users will logged into the Terminal log file.</p>	<p>Default: Enabled Range: None Dependencies: None Who: A terminal administrator can set Credential Logging Enabled at any time.</p>
<ol style="list-style-type: none"> Log into the terminal as an administrator. ➔ See “Administrator Authentication” on page 47 for more information. Press <input type="radio"/> Security Menu. Press <input type="radio"/> More. Press <input type="radio"/> Set Credential Logging Flag. Press <input type="radio"/> to Enable (or Disable). 	

Restore Factory Password




Restore Factory Password	
<p>Use this option to restore the factory password for a given terminal.</p>	<p>Default: Enabled Range: None Dependencies: None Who: A terminal administrator can restore the factory password at any time.</p>
<ol style="list-style-type: none"> Log into the terminal as an administrator. ➔ See “Administrator Authentication” on page 47 for more information. Press <input type="radio"/> Security Menu. Press <input type="radio"/> More. Press <input type="radio"/> Restore Factory Password and press <input type="radio"/> YES to confirm. 	

Maintenance Menu

Partial Sync Now	
<p>If changes to users are made to the terminal that need to be immediately implemented, Partial Sync Now can be used. Partial Sync Now will start a database synchronization process between the terminal and host application as soon as possible. Only user adds and edits are transferred during Partial Sync Now. No users will be removed during Partial Sync Now. Note that only changes made after previous sync will be synchronized</p>	<p>Default: None Range: None Dependencies: None Who: A terminal administrator can use Partial Sync Now to synchronize user data immediately.</p>
<ol style="list-style-type: none"> 1. Log into the terminal as an administrator. ➔ See “Administrator Authentication” on page 47 for more information. 2. Press <input type="radio"/> Maintenance Menu. 3. Press <input type="radio"/> Partial Sync Now. 	

Sync Now	
<p>If changes are made to the terminal that need to be immediately implemented, Sync Now can be used. Sync Now will start a database synchronization process between the terminal and host application as soon as possible.</p>	<p>Default: None Range: None Dependencies: None Who: A terminal administrator can use Sync Now to synchronize user data immediately.</p>
<ol style="list-style-type: none"> 1. Log into the terminal as an administrator. ➔ See “Administrator Authentication” on page 47 for more information. 2. Press <input type="radio"/> Maintenance Menu. 3. Press <input type="radio"/> Sync Now. 	

Reboot	
Reboot will perform a CPU reset of the terminal. Pressing Reboot will start the reboot process. The reader will appear to power down and then start the boot-up process.	Default: None Range: None Dependencies: None Who: An application developer/tester (or any individual under the guidance of a technical support representative) can reboot the terminal as a troubleshooting, testing or debugging step.
<ol style="list-style-type: none">1. Log into the terminal as an administrator. ➔ See “Administrator Authentication” on page 47 for more information.2. Press <input type="radio"/> Maintenance Menu.3. Press <input type="radio"/> Reboot.4. Press <input type="radio"/> Yes to reboot (or <input type="radio"/> No to discontinue reboot request).	

Terminal Status	
<p>The information contained in the Terminal Status menu is tremendously important in troubleshooting a terminal problem. The first step of determining the cause of nearly any problem with the terminal is knowing what software versions the terminal is running and verifying that those versions are expected or up to date.</p>	<p>Default: None</p> <p>Range: None</p> <p>Dependencies: None</p> <p>Who: A terminal administrator can access this information at any time.</p>
<p>The following information will be displayed:</p> <ul style="list-style-type: none"> • TerminalIP: the IP address of the terminal • LogicalName: the unique logical named assigned to the terminal • AppVersion: the application software version. • BSPVersion: the version of the board OS used by this terminal. • CommLibVer: the version of the communications library used by this terminal software. • HPUVersion: the version of the HPU • SyncProtocolVersion: the sync protocol version number for the terminal. • UserCount: the number of users that are stored in this terminal. • Interactions: the number of interactions that have not yet been sent to the host. • SentInteractions: the number of interactions that have been sent by the terminal to the host. • AcceptingPunches: Specifies if the terminal is accepting punches. • LastSyncTimeStamp: the last DB Sync timestamp. • NextScheduledDBSync: the next time the terminal is to sync • BackupBatteryOn: indicates whether the Terminal is running on Battery power • TotalDiskSpace: the total amount of space on the SD card. • UsedDiskSpace: the amount of space that has been used on the SD card. • AvailableDiskSpace: the amount of space left on the SD card. • 1aWkrStatus: Status of the DBSync worker thread used to send Interactions to the host • PhaseIIWkrStatus: Status of the DBSync worker thread used to pull the updates from the host • PurgeEvalPackWkrStatus: Status of the DBSync worker thread used to evaluate the sent interactions for purging purposes • BootPartition: current (Primary/Secondary) partition from which the Terminal is booted • BootedGolden: indicates whether the Terminal has booted from a partition set in the factory • PrimaryPartitionVersion: Version of the BSP on Primary partition • SecondaryPartitionVersion: Version number of the Secondary Partition • GoldenPartitionVersion: Version number of the Golden Partition • APSVersion: Version number of the APS • XMLLIBVersion: Version number of the XMLLIB partition • UBootVersion: Uboot version 	
<ol style="list-style-type: none"> 1. Log into the terminal as an administrator. ➔ See “Administrator Authentication” on page 47 for more information. 2. Press  Maintenance Menu. 3. Press  Terminal Status. 4. You can navigate though the status list by using . 	

Delete Sent Interactions

Delete Sent Interactions also clears sent interactions from the database on the terminal. The database contains all interactions with the terminal. Only interactions that have been sent to the host application will be cleared from the database when Delete Sent Interactions is used.

! *Delete Sent Interactions MUST be performed on a regular basis. If not, the SD card could become too full and cause the terminal to discontinue receiving user punches. You will start to see warnings when the card is 30% full. At 45% full, the terminal will no longer accept punches.*

Default: None

Range: None

Dependencies: None

Who: A terminal administrator can use Delete Sent Interactions to remove old information that is no longer necessary in order to create room on the SD card for new information.

1. Log into the terminal as an administrator.
➔ **See “Administrator Authentication” on page 47 for more information.**
2. Press Maintenance Menu.
3. Press Delete Sent Interactions.
4. Enter the number of days to retain sent interactions. A value of 0 deletes all sent interactions.
5. Press Enter.

Shutdown	
<p>Shutdown is used to properly shut down the terminal. The terminal screen will indicate that the terminal is shutting down. Wait until the LED bar is no longer illuminated before removing power.</p>	<p>Default: None</p> <p>Range: None</p> <p>Dependencies: None</p> <p>Who: A terminal administrator must use the shutdown operation before removing power from the terminal.</p>
<ol style="list-style-type: none">1. Log into the terminal as an administrator. ➔ See “Administrator Authentication” on page 47 for more information.2. Press <input type="radio"/> Maintenance Menu.3. Press <input type="radio"/> Shutdown.4. Press <input type="radio"/> Yes to shutdown (or <input type="radio"/> No to discontinue the shutdown request).5. Wait until the LED bar is no longer lit.6. You can now safely remove power from the terminal if needed.	

Last Punch

Last Punch	
<p>Last Punch shows the last punch into the terminal. The user’s last name, status (IN or OUT) and date and time of punch is displayed.</p> <p>➔ This information is only accurate to within the last host synchronization.</p>	<p>Default: None</p> <p>Range: None</p> <p>Dependencies: None</p> <p>Who: A terminal administrator can view the last punch into the terminal at any time.</p>
<ol style="list-style-type: none">1. Log into the terminal as an administrator. ➔ See “Administrator Authentication” on page 47 for more information.2. Press <input type="radio"/> Last Punch.	

FKScript List Menu

➔ *This menu is available only when you are in Demo Mode.*

Activating the Function Key Script

The FKScript List menu uses an example script that was designed to show you some of the types of application you may want to implement at your own site. The sample applications access the Demo mode database which has been preloaded with a list of users and user messages.

➔ *For more information about Demo Mode and the preloaded user database it uses, see the [GT-Series Integration Package Quick Start Guide](#).*

FKScript List

Activating the Function Key Script (FKScript List option)	
After you log in as an Administrator and go to Demo Mode, you can use the FKScript List option to activate the Function Key script.	<p>Default: None</p> <p>Range: None</p> <p>Dependencies: None</p> <p>Who: A terminal administrator can activate this option any time from Demo Mode only.</p>

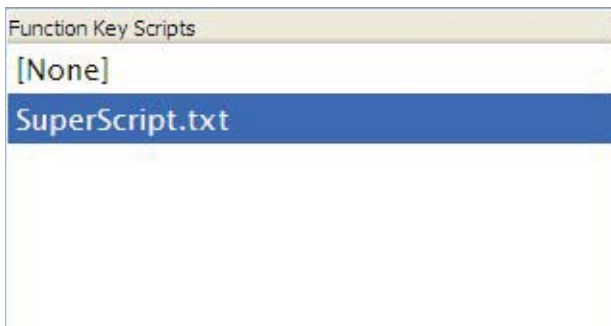
1. From Demo Mode, log into the terminal as an administrator.
 ➔ **See “Administrator Authentication” on page 47 for more information.**
2. Figure shows the COMMAND STRUCTURE menu in Demo Mode.:

Figure 6-1 Function Key Script List Option Accessible in Demo Mode



3. Press FKScript List. The script selection list displays as shown in Figure 6-2.

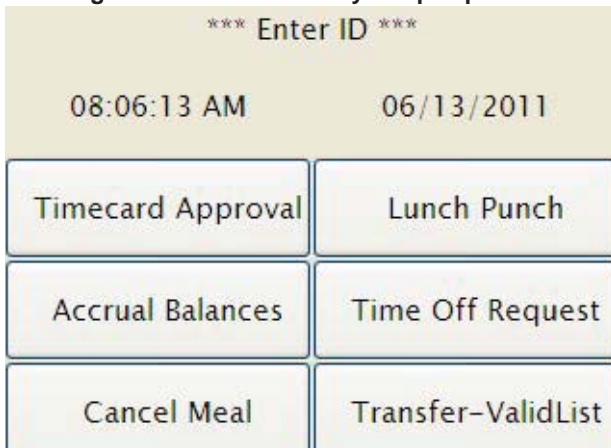
Figure 6-2 Selecting the Function Key script



4. Scroll to the SuperScript option using . Press the middle key to select the Function Key script.

The list of available Function Key script options displays. See Figure 6-3.

Figure 6-3 Function Key Script Options



Timecard Approval

Timecard Approval	
<p>After the Function Key script has been activated in Demo Mode, you can log in and select the Timecard Approval option to view any unapproved timecards you may have.</p>	<p>Default: None Range: None Dependencies: None Who: Any user can use this option any time after logging into the Terminal in Demo Mode</p>
<ol style="list-style-type: none"> 1. Press <input type="radio"/> Timecard Approval. 2. When prompted, log into the terminal. 3. If you have any unread messages (such as any new unapproved timecards) you will be prompted whether you want to read them. If so, press <input type="radio"/> YES. 4. After reviewing the timecard, press <input type="radio"/> Approve to approve the timecard, or press <input type="radio"/> Back to disapprove (or defer approving) the timecard. 	

Accrual Balances

Accrual Balances	
<p>After the Function Key script has been activated in Demo Mode, you can log in and select the Accrual Balance option to view any used and available vacation and sick leave you may have.</p>	<p>Default: None Range: None Dependencies: None Who: Any user can use this option any time after logging into the Terminal in Demo Mode</p>
<ol style="list-style-type: none"> 1. Press <input type="radio"/> Accrual Balances. 2. When prompted, log into the terminal. 3. Your accrued and available vacation and sick leave time displays. 	


Cancel Meal

Cancel Meal	
<p>After the Function Key script has been activated in Demo Mode, you can log in and select the Cancel Meal option to cancel a meal deduction.</p>	<p>Default: None Range: None Dependencies: None Who: Any user can use this option any time after logging into the Terminal in Demo Mode</p>
<ol style="list-style-type: none"> 1. Press <input type="radio"/> Cancel Meal. 2. When prompted, log into the terminal. 3. You will receive a meal cancellation notification. 	




Lunch Punch (Meal Compliance)

Lunch Punch (Meal Compliance)	
<p>Lunch Punch is typically used to enforce break/meal law regulations. You must be an Administrator to set Lunch punch lockout values. A user can then use the Function Key script's Lunch Punch option to punch back in from a meal break.</p> <p>If the user punches in earlier than the specified Lunch Punch lockout setting, the user will receive a message indicating that he/she has attempted to log in earlier than the specific lockout session. The number of minutes/seconds the user must wait to punch back in is also specified.</p>	<p>Default: None Range: None Dependencies: A lunch punch lockout setting must be activated by the Administrator prior to using this option. Who: Any user can use this option any time after logging into the Terminal in Demo Mode.</p>
<ol style="list-style-type: none"> 1. Press <input type="radio"/> Lunch Punch. 2. When prompted, log into the terminal. 3. If successful, the user will receive a message indicating successful lunch punch. 	

Time Off Request

Time Off Request	
After the Function Key script has been activated in Demo Mode, you can log in and select the Time Off Request option to request to take vacation or sick leave time.	Default: None Range: None Dependencies: None Who: Any user can use this option any time after logging into the Terminal in Demo Mode
<ol style="list-style-type: none">1. Press <input type="button" value="F1"/> Time Off Request.2. When prompted, log into the terminal.3. Scroll to the desired option in the list (AvailableVacation or AvailableSickHours) using . Press the middle key to select the desired option.4. Enter the start date, using the format mm dd yyyy. (Example: 12 22 2011) and press <input type="button" value="Enter"/>.5. Enter the total number of hours you want to take off. Press <input type="button" value="Enter"/>.6. After the request is accepted, you will see updated balances reflecting the requested time off.	

Transfer-ValidList

Transfer-ValidList	
<p>After the Function Key script has been activated in Demo Mode, you can log in and select the Transfer-ValidList option to transfer a user from one department and job to another (based on a predefined list of valid departments and jobs that have already been set up for that user).</p>	<p>Default: None</p> <p>Range: None</p> <p>Dependencies: The administrator must first set up the list of valid departments for a given user to transfer. In Demo Mode, a list of valid departments has already been set up.</p> <p>Who: Any user can use this option any time after logging into the Terminal in Demo Mode</p>
<ol style="list-style-type: none">1. Press  Transfer-ValidList.2. When prompted, log into the terminal.3. Scroll to the desired department to which you want to transfer . Press the middle key to select the department.4. Scroll to the desired job to which you want to transfer . Press the middle key to select the job.5. You will see a transfer confirmation which displays the department and job to which you are to transfer.	

Understanding GT-Series Biometric Terminals

7

Reviewing Hand Geometry Basics

This chapter will provide some basic information for those users who have never used a biometric terminal.

Hand Geometry Considerations

The terminal reads the shape of the hand, not the fingerprints or palm prints. Also note the following:

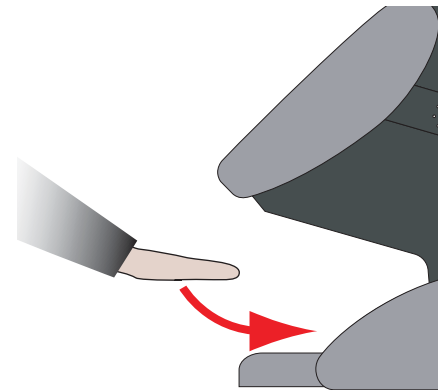
- It does not identify people. It verifies people's identity.
- It scans with an invisible light of the type used in TV remote controls.
- It does not transfer germs any more than a doorknob or money.
- It does not invade privacy; it guarantees it.
- The enrollment process requires three or more reads to collect enough information to create a template.

NOTE: For users with special needs that require a no hand enrollment, see “No Hand Enroll” on page 95.

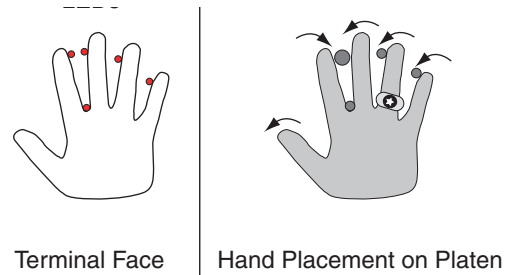
Proper Hand Placement

For correct, consistent hand reads it is very important that your hand is placed on the platen in the same manner every time. The following rules apply for proper hand placement on the platen.

1. If you are wearing a ring, rotate the ring so the stone faces up in its normal position.
2. Slide your right hand onto the platen rather like an airplane landing at the airport.
3. Slide your hand forward until the web between your index and middle finger stops against the web pin.
4. Keep your hand flat. You should feel the surface of the platen on your palm and the underside of your fingers.



5. Close your fingers together until they touch the finger pins and watch the hand diagram on the terminal display. There are small LEDs on the hand diagram that correspond with the finger pins. Your thumb should be held wide to the side.
6. The LEDs turn off when you have properly placed your fingers. If an LED remains on, a finger is not in proper contact with a finger pin.



Understanding Hand Read Scores

When a user verifies his/her hand, a score of the verification quality is generated. The score is displayed on the terminal's display after a successful verification.

The score can be found in the interaction data for the verification. This information is viewable in the Host Application.

The score number on the display reflects how accurately the user's hand is placed on the platen. Scores that vary greatly between low and high numbers are indicative of inconsistent hand placement. Scores above 50 are indicative of improper hand placement or of a drastic change in the physical appearance of the hand.

When this occurs, emphasize the importance of sliding the hand onto the platen and keeping the hand flat. Re-training and practice should lower a user's score. It might be necessary to assign an individual user reject threshold if the user has a mild disability. Re-enrollment might be necessary to create a new user template.

Understanding Verification Messages

Various messages can appear on the terminal's display during hand verification, as listed in Table 7-1.

NOTE: *If you enter your ID number, but do not place your hand on the platen, the terminal will time-out in approximately 25 seconds. You can immediately end this timeout by pressing (ENTER).*

Table 7-1: Messages Displayed During Verification

Message	Definition
PLACE HAND	The platen is ready to receive your hand for verification.
OK <user name>	You are verified, proceed.

Table 7-1: Messages Displayed During Verification (Continued)

Message	Definition
REMOVE HAND	Remove your hand and place it on the platen again. Follow proper hand placement rules.
TRY AGAIN	Your attempt was rejected. Repeat verification following proper hand placement rules.
TIME RESTRICTION	You are not authorized to punch in at this time. If this seems to be in error, contact your supervisor about time restrictions.
ID INVALID	Your rejections exceeded the maximum number of tries allowed. Wait until a supervisor has verified and try again or call your supervisor.
ENTER ID	You entered your ID number incorrectly or your access time is restricted.
MOVE THUMB	Your thumb is interfering with the read attempt. Slide your thumb to the side of the terminal.
LIFT UP SLEEVE	Your sleeve is interfering with the read attempt. Slide your sleeve away from the body of the terminal.

Reviewing LED Bar Indications

When Terminal is Idle

Table 7-1: LED Bar Indication When Terminal is Idle

Event	LED
Connected to the terminal	Blue
Not connected to the terminal	Amber
Not connected to host application	Red

During Verification

Table 7-2: LED Bar Indications During Verification

Operation	Event	Beeps*	LED
During Keypad Entry	Keystroke accepted	1 per keystroke	no change
After ID Entry	OK-place hand	1	Slow blinking amber
	ID number not in database	2	No change
	User locked out Timezone violation		
After Hand Placement	Hand image captured	1	White/Purple
	ID verified	1	Green
	ID not verified - try again	2	Red
	ID refused	2	Red
* Beeper will only sound if beeper is enabled. See “Set Beeper” on page 67 for more information.			

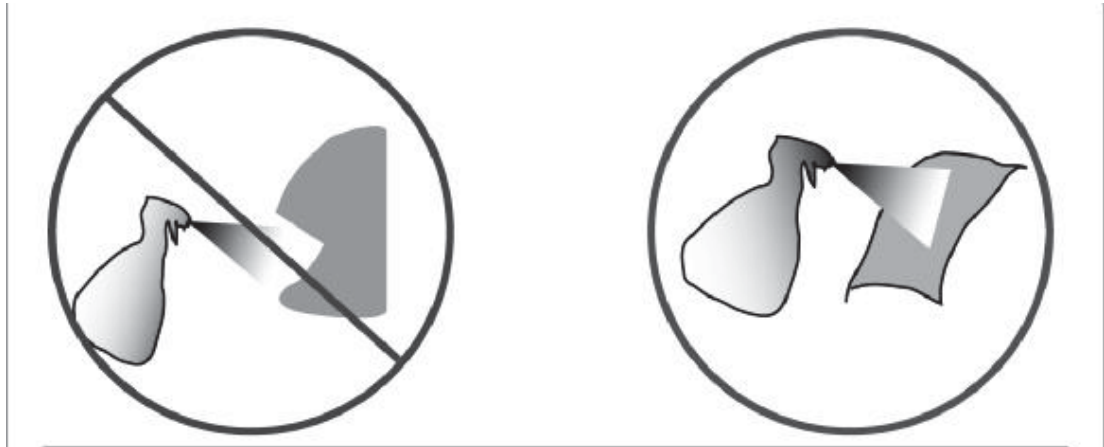
During Enrollment

Table 7-3: LED Bar Indications During Enrollment

Event	Beeps*	LED
OK - place hand	1	Slow blinking amber
Hand image captured	1	White/Purple
Bad hand placement, try again	1	Blinking red
* Beeper will only sound if beeper is enabled. See “Set Beeper” on page 67 for more information.		

Cleaning the Terminal and Platen

Inspect and clean the terminal regularly to maintain optimum performance. Clean the platen, side mirror, reflector, and the window above the platen using a clean cloth dampened with ordinary, nonabrasive window cleaner. Start at the rear corners of the platen and work your way forward.



! *DO NOT SPRAY CLEANING FLUID DIRECTLY INTO OR ON THE TERMINAL.*

! *There are NO user-serviceable parts inside the terminal.*

Troubleshooting

8

Viewing Terminal Status

Using the Terminal

The easiest step to take for any problem is to view the terminal status. It is useful to see the last network activity in which the terminal was involved. If you call technical support you will be asked to provide this information, since it lists all of the software versions running in the terminal. Terminal status lists such information as software versions, user database information, network information, and sync status.

To access the terminal status screen, see “Terminal Status” on page 110.

Using a Web Browser

➔ ***The administrator must have an EPIN assigned to him/her in their user record in order to use the terminal's web browser.***

1. From a computer on the same network as the terminal, open a web browser.
2. Enter the IP address of the terminal in the address bar of the web browser, and press Enter or click Go. The welcome screen should appear.
3. Log in with the ID and EPIN of an administrator.
4. Click the Terminal Status button. The same information that appears in the Terminal Status command menu is listed here.

Using Telnet

Telnet will likely be the single most useful maintenance and diagnostic tool you will use with GT-Series terminals. It provides a command line-style interface to the actual terminal, identical to the DOS prompt in Windows. "Run a telnet session and check the log file" is the most commonly used phrase when troubleshooting a terminal.

Choosing a Telnet Client

➔ ***The DOS prompt cannot be used as a telnet client to connect to your terminal.***

HyperTerminal comes with Windows, and can be used to create a telnet connection to your terminal. However it is not recommended because it has limited viewing and saving capabilities.

It is strongly recommended that you use the telnet client PuTTY (pronounced "PUH-tee"). It has robust saving capabilities and configuration options. It can be downloaded (for free) at the following address:


<http://www.versiontracker.com/dyn/moreinfo/win/16985>

The PuTTY developer's site is located at the following address:

<http://www.chiark.greenend.org.uk/~sgtatham/putty/>

Logging In and Out of Telnet

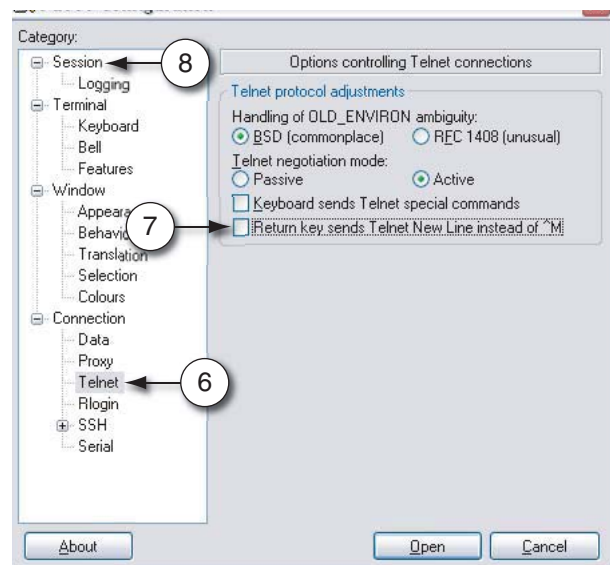
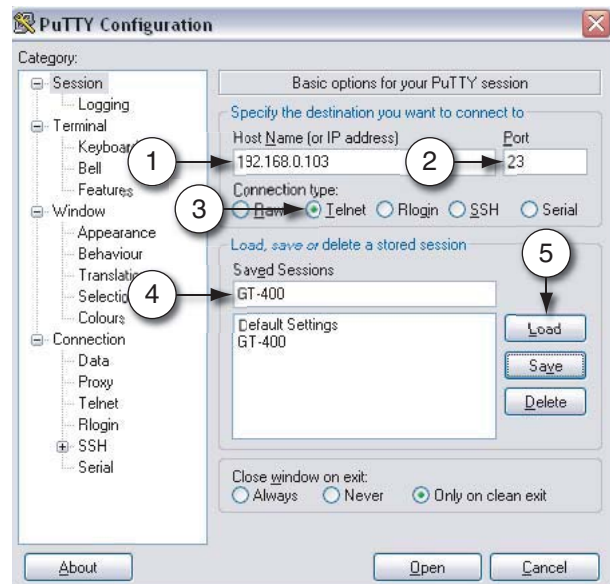
1. Enter the IP address of your terminal into your telnet client.
2. Click OK. A window will appear that displays the prompt
accordl login:
3. Enter the login name, which is root (it is case-sensitive).
4. Enter the password, which is 1520rsi by default (it is also case-sensitive).

 ***All directories, commands and files in Linux are case-sensitive. Pay very close attention to case when entering text because the difference between checking the status and deleting the entire file system can be a matter of using the wrong casing for a letter. Also, bear in mind that Linux is not as forgiving as other operating systems when it comes to making certain changes; if you delete a file, it is deleted forever; there is no undo or Recycle Bin. However, as long as you have a host connection, you need only reboot, and the host server will give back everything you deleted after it synchronizes.***

5. If the login is successful, the following prompt displays: ~#
This is the Linux shell prompt.
6. To logout of the telnet session, type exit and press enter from anywhere in the shell.

Using a Telnet (PuTTY) Session

1. Enter the IP address for the terminal.
 → See *“Terminal Status”* on page 110 for information on obtaining the terminal's IP address.
2. Enter the telnet port number: 23.
3. Click the Telnet radio button.
4. Enter a title for the new profile.
5. Click Save to save the profile. If you have created a profile for this terminal in the past, you can select the profile from the list and click Load.
6. Click Telnet.
7. Uncheck the box labeled Return key sends Telnet New Line instead of ^M.
8. Click Session.
9. Save the profile again by clicking Save before opening the telnet session by clicking Open.
10. Once the telnet session is open, you can enter commands into the telnet window as described in other sections of this guide.
11. If you want to log your telnet session, click Logging.



Changing the Telnet Password

Since all terminals come with a default telnet password (1520rsi), you will want to change it for security reasons.

1. At the prompt, type `passwd root`. This tells the shell you wish to change the password for the user root. The change password dialog will appear.
2. Enter the new password. Be sure to conform to the naming requirements.
3. Enter the password again. The password is now changed.

Navigating the File System

Once you are at the prompt, you are communicating with the terminal at a command-line level, similar to a DOS prompt in Windows. With DOS you can navigate the hard drive of your computer. With telnet you can navigate the SD card of the GT-Series Terminal. There are commands you can use to navigate the directories, view files and start or stop programs. Some of the most useful commands (such as `cd`, `tail`, `cat`, and `ps`) are described in this chapter; they are safe to experiment with as often as you want (as long as you keep in mind that commands are case sensitive).

Changing Directories Using the `cd` Command

The `cd` command is used to navigate from directory to directory. For example, if you type `cd RecogSys` at the first prompt, you will be moved to the RecogSys directory.

➔ *The main directory is called root, so if you are ever asked to "cd to root", simply type cd anywhere and you will be taken to the main directory.*

One of the most useful features in Linux is filename/directory auto-fill, which enables you to type in only a portion of a directory name. For example, to change directories to RecogSys, you need only type a portion of the directory name (the portion that makes it unique from other existing directory names) and then press the tab key to “fill in” the rest of the directory name.

For example, if you want to change directories to RecogSys/Src/Python/RSITerm, you can do the following:

1. Type `cd R` and press the Tab key on the keyboard. The remainder of the directory name “RecogSys” will display, since, in this example, the “R” is unique enough in the list of available directory names to distinguish it from other directory names.
2. Continuing on, you can type `S` (plus Tab key), `P` (plus Tab key), `RSIT` (plus Tab key). Just keep in mind that if there are multiple directories that start with the same letter, you'll need to fill in enough letters to uniquely identify to the shell what directory is it is that you want to auto-fill.

Viewing Terminal Processes Using the ps Command

The `ps` command is used to view a list of all the processes running in the terminal. If you have ever used the Task Manager in Windows, viewing the Processes tab is similar. If you execute the `ps` command on an active terminal, you will see a number of "python RSITerm.pyc" listings. These are all of the active processes (or threads) of the terminal application. If you do not see any "python RSITerm.pyc..." processes running, it means your terminal application has stopped.

To use the command, type `ps` at the prompt and press Enter.

Rebooting the Terminal Via Telnet

When you are having trouble with your PC, often the first thing to do to resolve the issue is to reboot it - the same is mostly true for the GT-Series Terminal. And just as you would not yank the power cable out of your PC to restart it, you should not power cycle the GT-Series Terminal before trying to reboot it gracefully. If you are unable to reboot through the command menus or the host server command, you can reboot it through the telnet session.

The command is `reboot` (and press Enter).

NOTE: After you have entered this command (and press Enter), the terminal may take up to a minute to shut itself down.

Shutting Down the Terminal Via Telnet

If you would rather shutdown the terminal as opposed to rebooting it, the command is `shutdown` (and press Enter).

Shutting Down The Application Via Telnet

If you shutdown the terminal with the `poweroff` argument (`shutdown poweroff`), you are telling the terminal to power down completely. However, if you run that same script, but give it the `nop` argument (`shutdown nop`), you are telling the terminal to shutdown only the application, but leave Linux running.

The command is `shutdown closeapp` (and press Enter).

This will shutdown the application and return you to the Linux shell prompt.

Starting the Application in Verbose Mode

After you have run the shutdown script with the `nop` argument, you can start the application again. If you start it in verbose mode, you will see a lot of messages during the start-up that should help you diagnose what is going on.

➔ ***When you're ready to take the terminal live again, you should reboot it. Avoid leaving a terminal on your live site running in verbose mode, because will put unnecessary strain on your terminal.***

The command is `vstartapp` (and press Enter).

Accessing a Terminal in Demo Mode Through Telnet

➔ ***These instructions ONLY apply to a terminal that has never been connected to a network.***

1. Using a cross-over cable, connect a computer to the terminal.
2. Access the Internet Protocol (TCP/IP) settings for your computer.
➔ ***See the documentation for your operating system for more information, or contact your system administrator for help.***
3. Set the IP address to 192.168.1.112.
➔ ***Your computer will not communicate with a network after changing this setting. You will need to write down your computer's TCP/IP settings and change them back when you are finished working with the terminal if you need to connect to a network.***
4. Open a telnet session to 192.168.1.110, or the IP address of your terminal, using a telnet client of your choice (a command prompt will not work properly).
➔ ***If the terminal has never been on a network, the IP address will be 192.168.1.110. If the terminal has been on a network, the IP address may be different. If you cannot determine your terminal's IP address, see "Returning the Terminal to Its Factory Settings" on page 132 to reset your terminal.***
5. At the `accord1 Login:` prompt, type `root`.
At the `password:` prompt, type `1520rsi`.

You are now accessing the root directory of the terminal.

Using the Terminal Log File

The terminal log file resides in the terminal and provides a clear picture as to what is going on in the terminal. If you are experiencing any kind of issue, your first step should be to check the terminal's log file. This can often point out the last task the terminal was working on before it encountered the problem.

You can view the log file from your telnet session.

1. `cd` to `RecogSys/ZODB`:
`cd RecogSys/ZODB`
2. Type `ls` (and press Enter) to see the list of files in this directory. The log file is named `RSITerm.log`.

Viewing the Log File Using the `cat` Command

There are a different ways to view the log file depending on your needs and circumstances. If the log file is small, the quickest way may be to use the `cat` command from the directory where the log file is located:

```
cat <log filename>
Example: cat RSITerm.log
```

At the prompt, type `entirelog` and press Enter.

This command provides the entire log file, which may exceed your window or buffer setting. However, the last line or last few lines are usually the most important. If you see a sync that did not complete, or an exception error message, you have likely found the source or your problem.

Viewing the Last Few Lines of the Log File Using the `tail` Command

The `tail` command can be used to look at just the last few lines of the log file.

The command is `recentlog`.

This will show the last 50 lines of the log file by default.

Saving the Log File to Your Computer

If you want to see the entire log file, or if your technical support representative requests it, you can easily save it to a file using PuTTY.

1. Before you start the telnet session, go to the Logging menu in the PuTTY setup window.

2. Select the radio button Log all output to a file and in the text field box, enter the name you want the log file to save. Click Browse to select the desired save location.
 - ➔ ***It is recommended as a best practice to name the saved log file by the terminal's name and the date and time that the log file was saved. Save the log file to your desktop.***
3. Go back to the Session category, and click Save.
 - ➔ ***This will create a log file for every telnet session you make to this terminal. Be careful not to over-write the log file (meaning if you close the session and create a new one, the log file from the previous session will be over-written). Before you start another telnet session, either move the log file or turn off logging in that session.***

Returning the Terminal to Its Factory Settings

If you have been using a terminal in Demo mode and want to convert it to network mode, you must first delete the database and log files on the terminal. This can be done either through telnet or through the terminal interface.

Through Telnet

1. Access the terminal through telnet.
 - ➔ ***See “Accessing a Terminal in Demo Mode Through Telnet” on page 130 on page 99 for more information.***
2. Type `cd RecogSys/ZODB` and press Enter.
3. Type `rm *` and press Enter. This removes all files (using the wildcard *) in this directory.

Through the Terminal Interface

1. Clear the terminal setup.
 - ➔ ***See “Clear Setup” on page 101 for more information.***
2. Clear the user database.
 - ➔ ***See “Clear UserDB” on page 105 for more information.***
3. Reboot the terminal.
 - ➔ ***See “Reboot” on page 109 for more information.***

Using the Terminal Command Line Interface (CLI)

The command line interface (CLI) is a program that runs within a telnet session. It allows you to explore the actual database of users, interactions, and so forth. If your log is not giving you very much information, you could choose to explore the terminal through the CLI for troubleshooting purposes.

There is integrated help within the CLI, which you can access by typing `h` at the prompt. The most useful basic activities are viewing interactions that have been sent to the host server, and viewing the total interaction list. If, for example, you are looking for a user's punch record, and there is no record of it in the host, you should be able to see if it actually happened by checking the interaction records through the CLI.

! *As with all telnet operations, the CLI is a place where care must be taken when entering commands.*

Logging in and out

! *Be sure to exit this client properly at all times. If you do not exit properly, it will still be running when you leave telnet, and you will not be able to get into it again without rebooting the terminal.*

Starting the CLI

1. `cd` to `RecogSys/Src/Python/RSITerm`
2. Type `python RSICLIclient.py` and press Enter. The login prompt will appear.
3. At the prompt, enter `Schlage538` (this is the default CLI password). The CLI prompt will then display.

Exiting the CLI

Type `close` at the prompt. Wait to be returned to the telnet prompt.

Viewing Help

The CLI comes with contextual help, which you can view by entering `h` at the prompt.

Saving the Output to a Text File On Your Computer

You can save output from the CLI session the same way you would save output from the telnet session; in fact, using the CLI is part of the same telnet session, so you need only enable logging for the telnet session and all CLI output will be saved there.

Retrieving Sent/Unsent Interactions From Terminal

When a host terminal connection is present, all interactions performed at terminal will be pushed to host and saved in host database. If host terminal connection is not present, interactions generated in terminal will be saved in the terminal and pushed to host whenever host terminal connection is resumed.

Figure 8-3 Terminal Status view that shows Sent/Unsent Interactions

Terminal Status	Value
CommLibVer	2.0.13
SentInteractions	41
Interactions	12
HPUVersion	0.0
TotalDiskSpace	UNKNOWN
AppVersion	2.1.14
TerminalIP	10.44.118.171
UsedDiskSpace	UNKNOWN
AvailableDiskSpace	UNKNOWN

In most cases, terminal interactions will make their way to host and be saved in host database. In case for some reason you are not able to retrieve interactions from host, you can retrieve them from terminal using the RSICLIClient.

To retrieve sent and/or unsent interactions from terminal, you can start an RSICLIClient by using the following steps:

1. Open a telnet session to terminal.
➔ See “Logging In and Out of Telnet” on page 126 for more information.
2. Change the working directory to `/RecogSys/Src/Python/RSITerm`
3. Start the RSICLIClient by typing the following command at the prompt:
`Python RSICLIClient.pyc 127.0.0.1 8090`
4. When prompted for password, enter Schlage538 (the default password).
5. You will see the `Ready >` prompt if you successfully started the CLI Client.
6. At the ready prompt, enter the following to list the sent interactions in the terminal, in XML format:
`Ready >sia`
7. At the ready prompt, enter the following command to list the unsent interactions in the terminal, in XML format:
`Ready >ia`
8. Save the output from executing steps 6 and 7 into a file and write an XML parser to parse the interactions and retrieve the information as necessary.

Troubleshooting Summary

The most common steps used to troubleshoot a terminal are:

- Using Telnet (to view the terminal's log file and check processes).
- Reviewing Terminal Status (either through the command menus or the terminal's web server)
- Using the CLI (to view specific database information records on the terminal)

Lastly, keep in mind that rebooting the terminal is a perfectly acceptable way of troubleshooting a problem. Just be sure to do it through the terminal command menus, or telnet - *do not power cycle the terminal to reboot the terminal*. Also, keep in mind that rebooting may only offer a temporary solution; if the problem continues to arise, accessing at the log file and trying to understand what the terminal is doing at the time of failure will be critical in resolving the problem.

INDEX

A

- Access Grants
 - adding 99
 - editing 97
 - listing 98
- Accrual Balances command (Demo Mode) 115
- Add Access Grants 99
- Add Credential 94
- Add Holiday 70
- Add Timezone 59
- Add User 100
- Administrator account creation 44
- Authenticating at the terminal 47
- Authentication, defined 12
- Authority, editing 86

B

- Basic Operations
 - Add Credential 50
 - Checking the terminal software version 53
 - Edit (user) Name 51
 - Edit Authority 49
 - Edit Threshold 50
 - Edit Timezone 49
 - Rebooting the terminal 53
 - Remove a User 51
 - Set Locale Timezone 52
 - Set Terminal Date 52
 - Set Terminal Time 53
- Baud Rate, setting 60
- Beeper, setting 67
- Biometric Setup Menu, description 101
- Biometrics, Hand Geometry 119
- Bookings, listing 100

C

- Cancel Meal command (Demo Mode) 116
- Cleaning terminal and platen 123
- Clear Setup 101
- Clear UserDB 105
- CLI (command line interface) 133

- Exiting 133
 - Saving output to your computer 133
 - Starting 133
 - Viewing Help 133
- CLISvr Port, setting 76
- CmdLine Setup 62
- Command line interface 133
 - exiting 133
 - saving output to your computer 133
 - starting 133
 - viewing Help 133
- Command menu structure, overview 56
- Command menus, defined 15
- Company Name, setting up 81
- Configuration options
 - Customized host configuration option 19
 - Terminal Command Menus configuration option 19
 - Terminal Web Server configuration option 19
- Configuring Demo Mode 42
- CR Num of Prefix Characters, setting 66
- CR Terminal String, setting 67
- Creating users from the terminal 48
- Credential Logging Flag, setting 107
- Credentials
 - adding 94
 - listing 93

D

- Date Format, setting 82
- Demo Mode configuration 42
- Display Setup Menu 81
- Door Unlock Time, setting 66

E

- Edit (user) Name 85
- Edit Access Grant 97
- Edit Authority 86
- Edit EPIN 96
- Edit Holiday 69

- Edit Threshold 88
- Edit Timezone 57, 89
- Edit User 84
- Edit User Status 90
- Enroll User 90
- Enrolling users 48
- EPIN, editing 96
- Ethernet switch usage 17

F

- Factory Settings (returning to)
 - Using Telnet 132
 - using the Terminal Interface 132
- Factory Settings command 105
- Feature description of terminal 13
- Ferrite clip attachment 32
- Firewalls and server network considerations 21
- FKScript List command 113
- FKScript List Menu, description 113
- Front panel overview 45

G

- Generate Punch 91
- GManager configuration option 40
- Go to StandAlone or Demo Mode 73

H

- Hand Geometry 119
- Hand Placement on the terminal 119
- Hand Read scores, description 120
- Holidays
 - adding 70
 - editing 69
 - listing 70
- Host (customized) configuration option 19
- Host application (customized) configuration option 40
- Host Password, setting 74
- Host URL, setting 75
- Host Username, setting 72

I

- ID Length, setting 64
- Installing the terminal
 - Backboard connections 31

- Ferrite clip attachment 32
- Hanging terminal and running wires 29
- Printer setup 33
- Removing terminal from the box 24
- Side cover removal or installation 34
- Terminal attachment to wall plate 36
- Terminal placement 23
- Wall plate attachment 28
- Wall preparation 25

Interactions

- clearing to save card space 22
- retrieving sent/unsent interactions from the terminal 134

K

- Keypad, overview of usage 15

L

- Language, setting 83
- Last Booking 91
- Last Punch 112
- LED Bar indications
 - During Enrollment 122
 - During Verification 122
 - Idle Terminal 121
- List Access Grants 98
- List Bookings 100
- List Credentials 93
- List Holidays 70
- List Timezones 58
- List Users 84
- LocaleTimezone, setting 63
- LogFile Size Factor, setting 65
- Logical Name, setting 71
- Lunch Punch (Meal Compliance) command (Demo Mode) 116
- Lunch Punch Lockout Seconds, setting 68

M

- Moving terminal to another host, precautions 22

N

- Name (user), editing 85
- Network Mode configuration

- Host Application (customized) 40
- Options description 37
- Terminal command menu option 37
- Web Server option 38

Network setup 17

No Hand Enroll 95

Number of Tries (at verification) 103

P

- Partial Sync Now 108
- Passwords, setting 104
- Placement of terminal during installation 23
- Placements Per Try 102
- Platen cleaning 123
- Power-on precautions 17
- Precautions when powering-on the terminal 17
- Precautions when shutting down the terminal 17
- Print Setup Menu 59
- PrintBookings, setting 60
- Printer setup during installation 33
- Purging interactions to save card space 22

R

- Ready String, setting 83
- RealTimeInteraction, setting 81
- Reject Threshold 106
- Remove User 92
- Restore Factory Password 107
- RPIN numbering system, creating 48
- Running terminal wires during installation 29

S

- Security software and network considerations 21
- Sent Interactions, setting duration to retain 68
- Set Baud Rate 60
- Set Beeper 67
- Set CLISvr Port 76
- Set Company Name 81
- Set CR Num of Prefix Chars 66
- Set CR Terminator String 67
- Set Credential Logging Flag 107
- Set Date Format 82
- Set Door Unlock Time 66

- Set Duration to Retain Sent (Interactions) 68
- Set Host Password 74
- Set Host URL 75
- Set Host Username 72
- Set ID Length 64
- Set Language 83
- Set LocaleTimezone 63
- Set LogFile Size Factor 65
- Set Logical Name 71
- Set Lunch Punch Lockout Seconds 68
- Set Passwords 104
- Set PrintBookings 60
- Set Ready String 83
- Set RealTimeInteraction 81
- Set Static/DHCP 80
- Set Terminal Date 61
- Set Terminal Time 63
- Set Time Format 82
- Set Time&Attendance 62
- Set WebServer 74
- Set WebSvr Port 79
- Set XMLRPCsvr Port 77
- Setup Menu, displaying 81
- Setup, clearing 101
- Shutdown (terminal) options
 - Telnet 44
 - terminal interface 44
- Shutdown precautions 17
- Side cover removal or installation 34
- Specifications of terminal 14
- Startup Screen 46
- Startup sequence of terminal 20
- Static/DHCP, setting 80
- Sync Now 108
- Synchronization verification with the host application 40

T

- Telnet
 - Accessing terminal in Demo Mode 130
 - Changing Directories (CD command) 128
 - Changing the password 128
 - Choosing a client 125
 - File system navigation 128
 - for troubleshooting 125

- Logging in and out 126
- Rebooting the terminal 129
- Returning terminal to factory settings 132
- running a session 127
- Running the command line interface (CLI) 133
- Saving the terminal log file to your computer 131
- Shutting down
 - terminal 129
 - terminal application 129
- Starting the application in verbose mode 130
- Viewing terminal processes (ps command) 129
- Viewing the terminal log file using cat command 131
- Viewing the terminal log file using ls command 131
- Viewing the terminal log file using tail command 131
- Template Resolution 103
- Terminal cleaning 123
- Terminal command configuration option 37
- Terminal Command Menus configuration option 19
- Terminal Date, setting 61
- Terminal interface, navigating long lists 47
- Terminal log file
 - saving to your computer 131
 - using the cat command 131
 - using the ls command 131
 - using the tail command 131
- Terminal shutdown options
 - Telnet 44
 - terminal interface 44
- Terminal Time, setting 63
- Terminal Web Server configuration option 19
- Terminal. precautions when moving a terminal to another host 22
- Text input at the terminal (tips and tricks) 46
- Threshold, editing 88
- Time Format, setting 82
- Time Off Request command (Demo Mode) 117
- Time&Attendance, setting 62
- Timecard Approval command (Demo Mode) 115
- Time-Outs (terminal) 46
- Timezone Menu, description 57
- Timezones
 - editing 57, 89
 - listing 58
- Transfer-ValidList command (Demo Mode) 118
- Troubleshooting tools
 - Viewing terminal status using Telnet 125
 - Viewing terminal status using the terminal 125
 - Viewing terminal status using Web Browser 125

U

- User Status, editing 90
- Users
 - adding 100
 - Creating at the terminal 48
 - editing 84
 - enrolling 48
 - listing 84
 - removing 92

V

- Verification messages, description 120
- Verification, defined 12

W

- Wall preparation during terminal installation 25
- Web Browser, for troubleshooting 125
- Web Server configuration option 38
- WebServer, setting 74
- WebSvr Port, setting 79

X

- XMLRPC Svr Setup 78
- XMLRPCSvr Port, setting 77



Ingersoll Rand's Security Technologies Sector is a leading global provider of products and services that make environments safe, secure and productive. The Sector's market-leading products include electronic and biometric access control systems; time and attendance and personnel scheduling systems; mechanical locks and portable security, door closers and exit devices, steel doors and frames, architectural hardware and technologies and services for global security markets.

www.securitytechnologies.ingersollrand.com