Omni 3750 Help Desk Training Guide

Release Date: 9/16/05

Version 2.01

IMPORTANT NOTICE

NO WARRANTY. ALTHOUGH VERIFONE HAS ATTEMPTED TO ENSURE THE ACCURACY OF THE CONTENTS OF THIS MANUAL, THIS MANUAL MAY CONTAIN ERRORS OR OMMISSIONS. THIS MANUAL IS SUPPLIED "AS-IS", WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED. INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

LIMITED LIABILITY. IN NO EVENT SHALL VERIFONE BE LIABLE FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES (INCLUDING DAMAGES FOR LOSS OF BUSINESS, PROFITS, OR THE LIKE) EVEN IF VERIFONE OR ITS REPRESENTATIVES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

OMNI 3750 Help Desk Training Guide

Version 2.01

Published 9/16/05
VeriFone, Inc.
2455 Augustine Drive
Santa Clara, CA 95054

By: Karen Mingle

www.verifone.com

Table Of Contents

VeriFone Timeline

1981 VeriFone founded and incorporated in Hawaii on April 14, 1981.

VeriFone launches its first product - VeriFone (stands for VERIFication telephONE). Performed check verification and credit authorization. The VeriFone device was one of first terminals designed to replace voice authorization with electronic authorization of credit card transactions.

1982 First official VeriFone office opens in downtown Honolulu, HI.

1983 ZON ("son" of VeriFone) is born (uses Zilog Z80 microprocessor). Performs check verification and credit authorization only.

1984 VeriFone launches the ZON Jr – the first low-cost authorization terminal. It was the most successful credit verification terminal of its time. Initial shipment to Visa. Ships over 50,000 units in the first year.

1985 VeriFone launches ZON Jr PLUS – first "soft" terminal (programmable keys).

VeriFone introduces the VeriFone PIN Pad 201.

1986 VeriFone launches ZON Jr XL – first electronic data interchange (EDI) capable terminal for the industry, allowing network transmission of data to host computers, and supporting printers, PIN pads and other peripherals.

1987 TRANZ 330 terminal introduced – becomes world's best selling transaction payment terminal. It is the first VeriFone terminal that accepts both credit and debit cards, allowing electronic draft capture and settlement with banks.

1988 Handheld PIN Pad 101 debuts – becomes the best selling PIN Pad in the world.

1989 VeriFone ships its 1 millionth terminal system.

Printer 250 launched – now a fixture in many retail locations.

1990 VeriFone announces that it has products installed in 40 countries worldwide.

VeriFone goes public; stock opens on NASDAQ stock exchange.

1991 Two millionth system ships.

VeriFone introduces first smart card reader.

Tranz 380 and Omni 480 terminals launched.

1992 Ruby SuperSystem for Petroleum/C-store market launched.

Omni 490 for customer-activated multi-lane retail market launched.

1993 Three millionth system ships.

VeriFone introduces first smart card product of its own design, the CM 450, in Singapore and France.

1994 VeriFone expands service offering with VeriFone Finance.

VeriFone delivers industry's first low-cost high-security smart card PIN Pads – which are certified in the Netherlands and Germany.

1995 Moved from NASDAQ to New York Stock Exchange-listed as VFI.

Industry-leading SC55x consumer activated smart card PIN Pad launched.

Everest payment terminal for customer-activated multi-lane market launched.

1996 **Five millionth system ships.**

Company debuts on World Wide Web.

VeriFone introduces suite of Internet commerce products for consumers, merchants, and processors.

VeriFone enters its 100th country.

1997 CR 600 MICR check reader launched.

VeriSmart and Personal ATM used in largest smart card pilot in U.S.

Six millionth system ships.

1998 **Seven millionth system ships.**

Integrated Payment Solution launched.

1999 **Eight millionth system ships.**

Omni 3200 payment terminal launched – becomes VeriFone's best selling terminal.

2000 **VeriFone exceeds 9 million payment systems in over 110 countries worldwide.**

Global payment platform featuring Verix multi-application architecture, VeriShield security architecture, SoftPay payment software, VeriCentre Appliance Management Suite, Omni 3300/3350 terminals, and the Verix Developer Toolkit launched.

Internet connectivity introduced via direct TCP/IP communications.

EverestPlus multi-lane customer activated terminal launched.

CR1000*i* check reader/imaging peripheral launched.

2001 Omni 3700 family of terminals introduced.

Omni 3600 wireless, multi-application payment terminal launched.

Omni 3210 terminal with internal PIN Pad launched.

VeriCentre Download Management Module, Message Management Module, Information Collection Module, and Remote Diagnostics Module launched.

VeriFone ships its 200,000th Omni 3200.

2002 **VeriFone celebrates 10 million shipments.**

VeriFone reaches 350,000 shipment mark for Omni 3200.

VeriFone reaches 200,000 EBT and government systems installations in 47 states.

VeriFone reaches 45,000 installations of Ruby SuperSystems in petro/c-store market.

VeriFone ships its 300,000th Everest.

2003 VeriFone introduces Pin Pad 1000SE to meet global triple DES and Visa International PED requirements.

VeriFone's Omni 3600 mobile wireless payment solution is first to utilize the benefits of CDMA 2000 IX, GPRS, and Wi-Fi.

VeriFone ships its 450,000th Omni 3750 payment terminal, now the most successful terminal in history.

VeriFone's best-selling Omni 3200 is improved with faster processing and a smaller footprint in the Omni 3200SE.

Lesson 1: What Is Multi-Application?

Lesson Objectives

After completing this lesson you will be able to:

- List five merchant objectives met by the multi-application architecture.
- Provide examples of various types of value-added applications.
- Describe the purpose of the VeriFone Value-added Partners Program.

Multi-Application — The Changing World of Payments

Only a decade ago, a merchant could accept a single type of credit card and satisfy most customers. That has changed dramatically with the proliferation of card-based payment and value-added options in the highly competitive retail marketplace. Today, many customers carry a variety of cards, and they expect merchants to readily accept whichever card they choose for a given purchase.

The Need To Accept Multiple Types Of Payment

To compete effectively in this environment, merchants have offered a growing variety of credit and debit services, electronic stored value cards, and loyalty programs designed to encourage customers to patronize their businesses. This has added significantly to the complexity of today's payment environment.

This changing environment has created a need for a single terminal capable of supporting multiple payment and value-added applications–efficiently, securely, and cost-effectively. As the leader in payment, VeriFone has addressed this by introducing terminal families, such as the Omni 3750, that run the powerful Verix multi-application architecture.

The Need to Increase Operational Efficiencies and Remain Competitive

As payment terminals have become more powerful and sophisticated, they offer the potential to move into the mainstream of retail operations – providing an ideal way to capitalize on untapped opportunities by supporting an array of value-added applications. Merchants are always looking for new ways to:

- Enhance convenience – offering customers multiple payment options and the ability to complete various transactions during a single visit (e.g., purchase a product/service, pay a bill, transfer money, purchase a pre-paid phone card, etc.) enhances the customer's overall experience.
- Increase sales – the ability to accept multiple payment methods attracts both new customers and repeat business, as well as, increases the average purchase amount.
- Reduce costs – the Omni 3750's ability to store multiple applications allows it to be used as both a payment device, as well as, perform tasks that improve the merchant's operational efficiency (e.g., time and attendance, age verification, pre-employment screening, medical benefits verification, etc.).
- Increase return on investment – utilizing a single terminal for multiple purposes reduces the merchant's overall investment in POS equipment - one terminal does it all.
- Reduce counter-top clutter – all applications reside within a single terminal. Merchants no longer have to use precious counter space for multiple terminals running multiple applications. Within a compact footprint, the Omni 3750 stores all of the applications required by the merchant.

Value-Added Applications

VeriFone has developed a comprehensive Value-added Partner Program (VAP) that provides value-added product and service providers in the United States and Canada with the resources and information they need to develop, certify, market and deliver a broad range of value-added applications that run on VeriFone terminals. Value-added applications foster growth. And growth expands possibilities. VeriFone value-added solution bundles are bringing endless possibilities to the point of sale.

VeriFone was the FIRST to deliver true multi-app architecture to the point of sale, fostering the use of value-added applications worldwide. And through our exclusive, membership-based Value-added Partner Program, we're expanding our lead in the number and variety of value-added applications certified to run on VeriFone terminals.

The opportunities are clear for banks, processors, ISO's and merchants in hosting the expanding array of payment and value-added applications on a single terminal. The tremendous potential in the area of value-added applications helps merchants.

Value-Added applications can:

- Increase customer loyalty
- Attract new customers
- Increase sales
- Generate new revenue streams
- Increase operational efficiency
- Reduce risk
- Gain competitive advantage

The VeriFone Value-Added Application (VAP) Program

VeriFone has worked closely with many different "value-added" service providers to create applications that allow merchants to offer additional services to their customers (e.g., gift card, pre-paid card, value card) or improve their operational efficiency (e.g., age verification, time and attendance).

In order to become a "VeriFone Approved Value Added Partner", all companies in the program must agree to adhere to strict rules regarding the functionality of their application, have the tools necessary to load their application into a specific memory area assigned by VeriFone, and have the ability to configure, download, and support their application. In fact, all VAPs must have their own "Class A" help desk.

For more information on the VAP Program, including a list of current program partners, go to: http://www.verifone.com/partners/vap/index.html

The SoftPay Application

Up to this point, you have learned about various value-added applications and how they can benefit a merchant. But, you may be asking yourself, just how does the merchant accept credit and debit card payments? This is where SoftPay comes into the picture. SoftPay is VeriFone's financial payment application designed to operate in a variety of *retail* and *restaurant* environments. It is highly configurable which allows you to customize the application for a particular merchant or group of merchants. Although VeriFone does not consider SoftPay to be a value-added application, it will more than likely be the financial payment application of choice in the terminals you will support.

Lesson 1: Review

- Five merchant objectives met by the multi-application architecture are:
  - **Enhance convenience** – offering customers multiple payment options and the ability to complete various transactions during a single visit (e.g., purchase a product/service, pay a bill, transfer money, purchase a pre-paid phone card, etc.) enhances the customer's overall experience.
  - **Increase sales** – the ability to accept multiple payment methods (check, gift, loyalty, etc.), in addition to the financial payment capability provided by SoftPay, attracts both new customers and repeat business, as well as, increases the average purchase amount.
  - **Reduce costs** – the Omni 3750's ability to store multiple applications allows it to be used as both a payment device, as well as, perform tasks that improve the merchant's operational efficiency (e.g., time and attendance, age verification, pre-employment screening, medical benefits verification, etc.).
  - **Increase return on investment** – utilizing a single terminal for multiple purposes reduces the merchant's overall investment in POS equipment - one terminal does it all.
  - **Reduce counter-top clutter** – all applications reside within a single terminal. Merchants no longer have to use precious counter space for multiple terminals running multiple applications. Within a compact footprint, the Omni 3750 stores all of the applications required by the merchant.
- Value-added applications developed for the Omni 3750 are grouped into the following categories:
  - Check Authorization and Conversion
  - Age Verification
  - Employment Pre-screening
  - Gift and Loyalty
  - Healthcare Insurance Eligibility
  - Money Transfer
  - Prepaid
  - Return Abuse/Fraud Protection
  - Time and Labor Management
- The SoftPay application provides financial transaction processing for credit and debit cards.

Lesson 1: Test Your Knowledge

1. If you were discussing the benefits of a multi-application environment to a merchant, what five benefits would you mention?

2. What does the SoftPay application do?

Lesson 2: Terminal Hardware

Lesson Objectives

After completing this lesson you will be able to:

- List the steps that must be performed to setup the terminal at the merchant site.
- List the hardware components that comprise the Omni 3750's integrated 3-in-1 design.
- Define TCP/IP.
- List the available communication modules.

Setting Up the Terminal At the Merchant Site

Step 1: Select a Location

Use the following guidelines described while selecting a location for the Omni 3750 terminal.

Ease of Use

- Select a location convenient for both merchant and cardholder.
- Select a flat support surface, such as a countertop or table.
- Select a location near a power outlet and a telephone/modem line connection.

NOTE For safety, do not string the power cable in a walkway or place across a walkway on the floor.

Environmental Factors

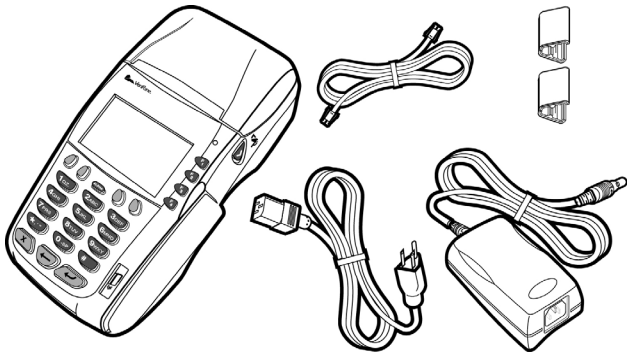
- Do not use the terminal where there is high heat, dust, humidity, moisture, or caustic chemicals or oils.
- Keep the terminal away from direct sunlight and anything that radiates heat, such as a stove or a motor.
- Do not use the terminal outdoors.

Electrical Considerations

- Avoid using this product during electrical storms.
- Avoid locations near electrical appliances or other devices that cause excessive voltage fluctuations or emit electrical noise (for example, air conditioners, electric motors, neon signs, high-frequency or magnetic security devices, or computer equipment).
- Do not use the terminal near water or in moist conditions.

CAUTION The terminal is not waterproof or dustproof, and is intended for indoor use only. Any damage to the unit from exposure to rain or dust may void any warranty.

Step 2: Unpack the Shipping Carton



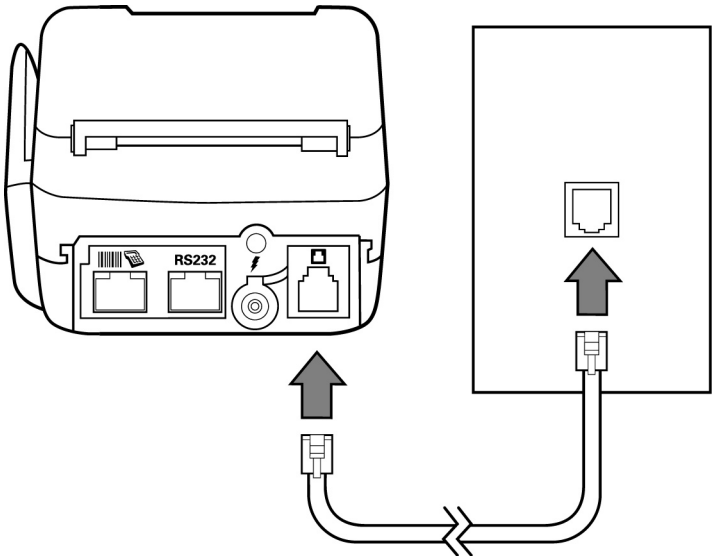
What's included:

- Omni 3750 terminal
- Power pack
- Telephone line cord
- Paper roll

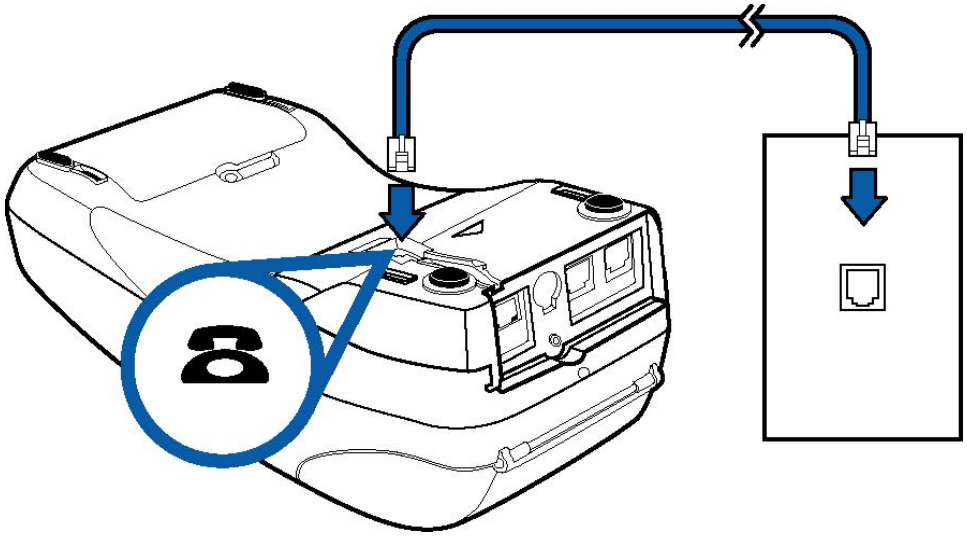
Step 3a: Plug In the Phone Line

The terminal is plugged into a phone line if the terminal dials into the host computer as its primary means of communication, as well as, if the terminal connects with the host computer via the Internet and uses the modem as a backup means of communication.

Connect the telephone cord to the RJ11 telco port on the terminal, and then route it directly to a telephone wall jack. This is a direct connection and the line is dedicated to the terminal.



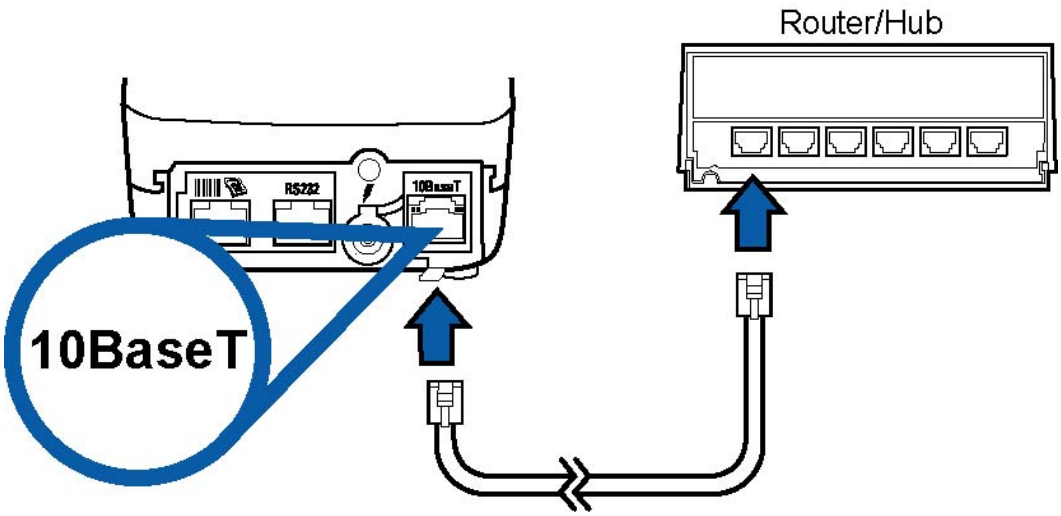
NOTE On the Omni 3750 with the dual-comm module, the RJ11 telco port is located on the bottom of the terminal.



NOTE If a DSL line is being used, every device sharing the DSL phone number (except for the DSL modem) needs a filter. Filters may be obtained from the DSL provider.

Step 3b: Connect the Ethernet Cable

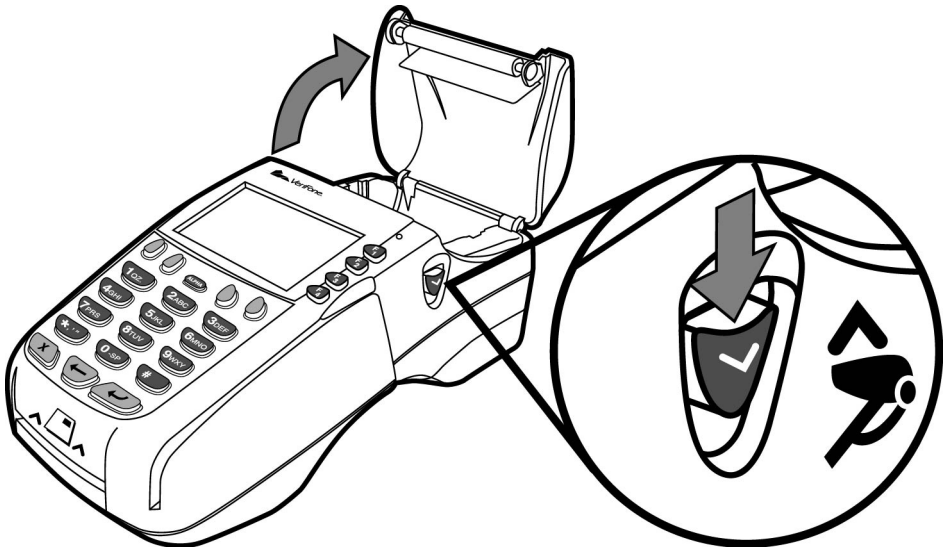
If the terminal has an Ethernet or dual-comm module, connect the CAT5 Ethernet cable from the 10BaseT port on the rear of the terminal to an available port on the router.



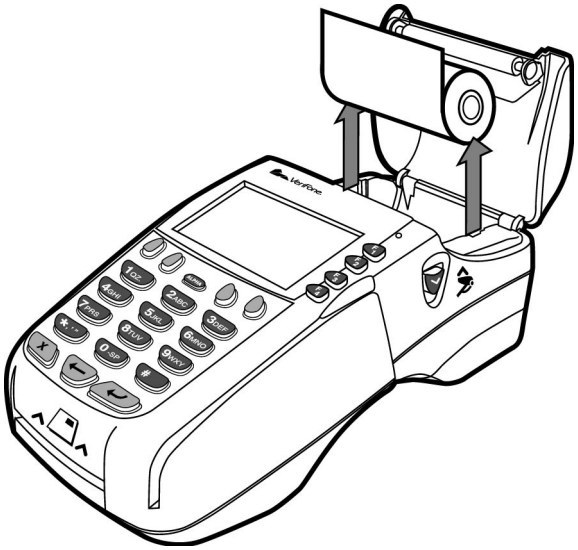
Step 4: Install the Paper

A fast, quiet thermal printer is built-in to the Omni 3750 terminal. Before processing transactions that require a receipt or record, you must install a roll of thermal-sensitive paper in the printer. The internal thermal printer (ITP) uses a roll of single-ply, thermal-sensitive paper 58 millimeters (2.25 inches) wide and approximately 25-33 meters (82-108 feet) long.

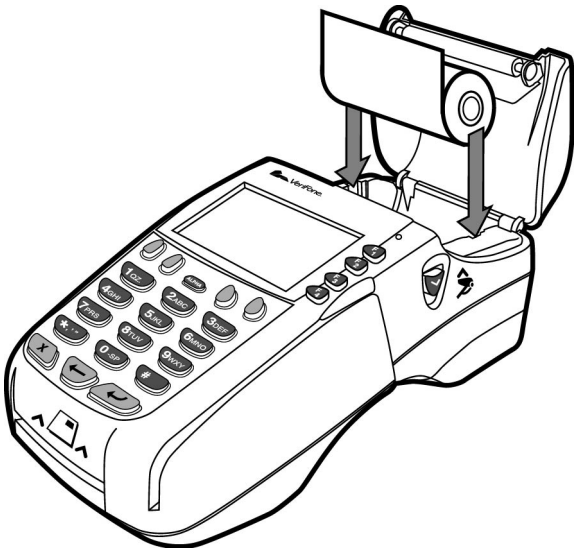
1. Turn on the terminal. The green LED indicator will blink on and off, indicating that the printer needs paper.
2. Press the button on the side of the terminal to unlatch the paper roll cover, then rotate the cover up and back.



3. Remove a partial roll of paper in the printer tray by lifting it up.

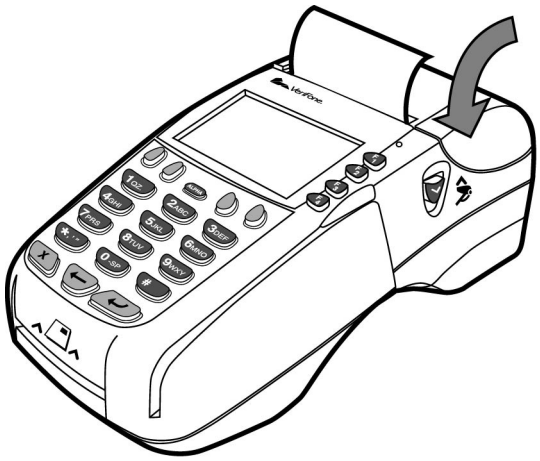


4. Loosen the glued leading edge of the paper or remove the protective strip from the new roll of paper and cut a straight edge across its leading end.
5. Hold the roll so the paper feeds from the bottom of the roll.
6. Drop the paper roll into the printer tray, leaving 7 centimeters (about two inches) of paper sticking up past the serrated metal tear strip.



NOTE There is no paper advance button on the Omni 3750. In the SoftPay application, advance the paper by pressing the [3] key.

7. Close the paper roll cover by gently pressing directly on the cover until it clicks shut. Allow a small amount of paper to extend outside the cover.



Step 5: Connect Other Peripherals

WARNING Before connecting any peripheral device, remove the power cord from the back of the terminal and be sure the LED is not lit. Reconnect the power cord only after you are finished connecting the peripheral device(s). For complete information about peripheral installation and use, refer to the user documentation supplied with those devices.

Optional devices:

- 2-D Bar Code Reader
- Check Reader
- Keyboard
- External PIN Pad
- Electronic Cash Register
- Router
- Biometric Device

The application program that utilizes each device determines to which port it is connected.

NOTE To protect against possible damage caused by lightening strikes and electrical surges, consider installing a surge protector. Also, only use the power supply provided with the terminal.

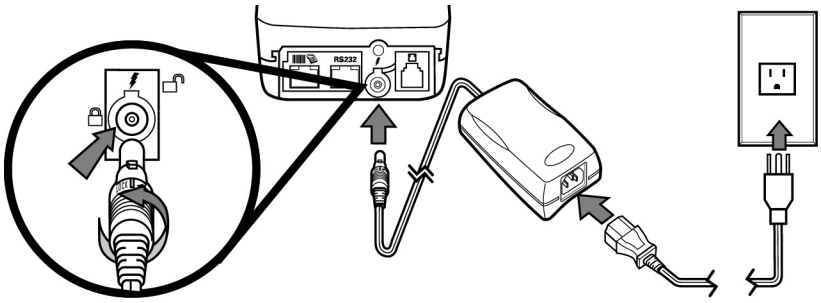
Step 6: Plug In the Terminal Power Pack

1. Insert the round barrel connector into the power port identified by the icon at right.

   To lock the connector into the power port, align the plastic lock tab so it points up. Insert the connector and twist to the left.

To unlock the connector, twist it to the right.

2. Insert the power cable into the power pack.
3. Plug the power pack cable into a wall outlet or surge protector.



When the terminal has power, the LCD screen lights and the green LED indicator flashes on and off if the printer has no paper, or remains lit if there is paper loaded.

If an application is loaded in the terminal, it starts after the initial VeriFone copyright screen and displays a unique copyright screen. If no application is loaded in the terminal, **DOWNLOAD NEEDED NO *GO PARAMETER** displays on screen after the initial VeriFone copyright screen.

DOWNLOAD NEEDED INVALID *GO PARAMETER	F1 F2 F3 F4

NOTE To protect against possible damage caused by lightning strikes and electrical surges, consider installing a power surge protector. Also, only use the power supply provided with the terminal.

Communication Module Options

The meteoric rise of the Internet and World Wide Web has been driven by the development of numerous enabling technologies. Among these is a broad spectrum of wired and wireless LAN and WAN alternatives, as well as, the various network protocols that make transparent communications possible. The most important of these protocols is IP.

What Is IP?

IP (Internet Protocol) comes in several forms. Transmission Control Protocol over IP, more often shown as TCP/IP, has emerged as a *de facto* standard. TCP/IP is the suite of protocols that connects all of the computers on the Internet.

Although IP technology was originally created for the Internet, it is now embedded in essentially all leading wired and wireless network communications.

This includes dial-up network services, as well as, a broad selection of high-speed networks, such as Digital Subscriber Line (DSL), cable modem, and T1/T3 services. IP is also at the heart of a proliferation of wireless services, such satellite, GPRS, CDMA, and 802.11.

To support this broad range of communication technologies, the Omni 37xx terminal was designed with a specific communications module for each technology. This module is field upgradeable (either by your deployment group, a merchant sales rep, or the actual merchant).

NOTE Keep in mind that the terminal may require a new operating system along with the selected module.

The currently available communication modules are:

- 14.4 modem
- Ethernet (10BaseT)
- Ethernet + 14.4 modem (10BaseT) – dual-comm module
- CDMA + 14.4 modem
- GPRS + 14.4. modem
- 802.11b + 14.4 modem

NOTE Communications performed via the modem utilize the host dial protocol.

Replacing the Module

Simply remove the power plug, remove the screw holding the module in place, and then remove the module itself. To install the Ethernet module, these steps are completed in reverse.

Application Support

In addition to installing the Ethernet module, the application(s) residing in the terminal must also have the ability to communicate over an IP or Ethernet connection. Do not assume that just because the merchant has the Ethernet module installed that all of the applications resident in the terminal have been updated to support this capability. Some applications may communicate via IP and others may communicate via the dial modem.

Integrated 3-In-1 Design

One of the most compelling features of the Omni 3750 is its integrated 3-in-1 design. A terminal with an integrated printer, internal PIN pad, and integrated smart card reader saves the merchant both counter space and money.

Although the Omni 3750 has an internal PIN pad (IPP), an external PIN pad may be attached if this is a merchant requirement.

Troubleshooting Tips

The terminal works, but the printer does not print.

Steps to resolve:

1. Check to be sure the merchant is using the correct power supply with the terminal (P/N CPS05791-3A DC power pack (universal), 21973-01 power cable (US))

   Note: The Omni 3200 power supply power pin will fit the Omni 3750, but does not supply enough power to the Omni 3750 for the printer to operate correctly.

2. Confirm the SoftPay printer enabled flag is set to ON.

   SoftPay > Other Setup > Printer > Enable Printer

   Note: Refer to your SoftPay reference manual for information on how to modify SoftPay parameters.

The terminal works, but the printer makes a grinding noise.

Steps to resolve:

Be sure to close the printer cover.

The printer feeds the paper, but nothing prints.

Steps to resolve:

Be sure the paper is installed correctly. Thermal paper has two sides, a dull side and a shiny side. The printer must be able to print on the shiny side.

To test which side is facing up, scratch the printer paper. If a mark appears, the paper is inserted correctly. If no mark appears, remove the paper roll, rotate it 180 degrees, and replace the paper roll.

Lesson 2: Review

- To setup a terminal at the merchant site, the following steps must be performed:
  1. Select an appropriate location for the terminal.
  2. Unpack the shipping carton.
  3. Plug in the phone line and/or CAT5 Ethernet cable.
  4. Install the paper.
  5. Connect other peripherals (if available).
  6. Plug in the terminal power pack.
- The hardware components that comprise the Omni 3750's integrated 3-in-1 design are:
  - Integrated clam-shell thermal printer.
  - Internal PIN pad.
  - Integrated smart card reader.
- TCP/IP is the suite of protocols that connects all of the computers on the Internet.
- TCP/IP is supported on a broad selection of high-speed networks, such as Digital Subscriber Line (DSL), cable modem, and T1/T3 services. IP is also at the heart of a proliferation of wireless services, such satellite, GPRS, CDMA, and 802.11.
- To support this broad range of communication technologies, the Omni 37xx terminal was designed with a specific communications module for each technology.

Lesson 2: Test Your Knowledge

1. List three features of the Omni 3750 that make it the terminal of choice?

2. On the back of the Omni 3750, what do the following icons mean?

   10BaseT

   HS

3. What are the advantages of having a dual-comm module?

4. What is TCP/IP?

Lesson 3: The Verix Operating System

Lesson Objectives

After completing this lesson you will be able to:

- List the key features of the Verix operating system.
- Explain the concept behind the Verix “apartment building”.
- Describe how Verix utilizes various GIDs.
- Explain what tasks VMAC performs.
- Print VMAC Summary and Detail reports.
- Explain dynamic memory allocation and why it is important.
- Identify the types of files that are stored in RAM and Flash memory.
- Describe how VeriShield provides enhanced security.

What Is Verix?

All Omni terminals prior to the Omni 33xx/37xx series were based on the TXO (Transaction Express Option) operating system. The Omni 33xx/37xx series is based on the Verix operating system that offers new functionality:

Application separation at both the hardware and software level.

Supports multiple, independent applications on a single terminal.

Applications can be added or modified without having to re-certify existing applications.

Applications and files may be compressed to reduce download time.

Applications and files are secured using the VeriShield security functionality.

What Are File Groups (GIDs)?

To support a multi-application environment in which applications and their associated data files are completely isolated from each other, the Verix operating system implements a file system in volatile, battery-backed RAM and non-volatile[1] Flash memory. Each file group is identified by a Group ID (GID).

The Rules

- Application and data files are assigned to one of fifteen (15) file groups for access control. These file groups are similar to directories on a computer. The files comprising a single application can be stored in a separate file group, just like different computer applications can be stored in separate directories.
- Each file group is protected by a separate password and each has a separate CONFIG.SYS[2] file (except GID 0).
- The primary application (e.g., VMAC) must be downloaded into File Group 1 (GID 1). On power-up and after system restarts, the terminal defaults to GID 1 as the controlling group. The GID 1 application has access to files stored in all other groups (except GID 0). If no application is found in GID 1, the terminal displays DOWNLOAD NEEDED INVALID *GO PARAMETER.
- Other applications may reside in GIDs 2 through 14. These applications only have access to themselves and files stored in GID 15.
- GID 15 is globally accessible. It is used to store files shared by multiple applications, such as shared libraries. GIDs 1 through 15 are empty until a download is performed.

[1] **Non-volatile memory**. A memory or storage medium that retains data in the absence of power so that data is available when power is restored.

[2] File where terminal and application parameters are stored.

File Group (GID)	Description
0	Contains information used by the Verix operating system. It is not accessible by any application.
1	 Contains a program called VMAC that stands for Verix Multi-Application Conductor. Think of VMAC as the apartment building superintendent. VMAC ensures that all of the applications that live in the apartments share and release system resources (e.g., modem, keypad, display). VMAC also builds a menu that displays a list of all VAP applications loaded in the terminal. When the terminal powers up or restarts from System Mode, the Operating System splash screen displays followed by the VMAC splash screen. **NOTE** If any application is IP-enabled, the Comm Server application will also reside in GID 1. **NOTE** The [*] (hot key) can be pressed from within any application to return to the VMAC menu.
2	Contains the SoftPay application. This application performs credit, debit, and EBT card processing.
3 - 12	Value-add applications, such as check, gift card, loyalty, age verification, etc.
13	Overflow. Used in case there is a need for two applications that fall in the same category. For example, if the merchant requires two gift card applications. The first one will reside in the standard GID 5 and the second one will reside in this GID.
14	Reserved for use by VeriFone.
15	Shared by all GIDs – used to store shared libraries and other common data.

Dynamic Memory Allocation

Unlike current terminal systems in which the same amount of memory is allocated for every application (whether it requires it or not), Verix utilizes dynamic memory allocation that allows an application to use only the amount of memory it requires. This is very important in a multi-application environment because all applications share the same memory pool.

Application 1	Application 2	Application 3	Available Memory
Total Terminal Memory (RAM + Flash)			

Because memory is allocated as needed, this impacts the number of applications and associated data that may be stored in the terminal. Do not assume that just because the terminal has 13 GIDs available, 13 applications can be stored.

RAM and Flash Memory

The Omni 3750 has two types of memory: RAM and Flash. A terminal with 4 Mb of memory has 2 Mb of RAM and 2 Mb of Flash.

Flash VS. RAM Memory

Flash — A solid-state, nonvolatile, rewritable memory that functions like a combination of RAM and hard disk. Flash memory is durable, operates at low voltages, and retains data when power is off.

When data is added to Flash memory, it is appended to existing data rather than overwriting it. For this reason, Flash memory must be cleared before new data is downloaded. Because Flash is not automatically cleared prior to a full download, it must be cleared manually using the System Mode Menu 2 Flash Files option.

RAM — Acronym for Random-Access Memory. A memory cell configuration that holds data for processing by a central processing unit (CPU). Random means the CPU can retrieve data from any address within RAM. In the Omni 3750, terminal RAM is commonly used to store temporary data (e.g., batch records) generated during a transaction.

How Flash and RAM Memory Are Used In the Terminal

The Omni 3750 has a RAM-based file system. Files can be stored in RAM (drive "I") or in the Flash (drive "F") memory area of any file group (GIDs 1 – 15).

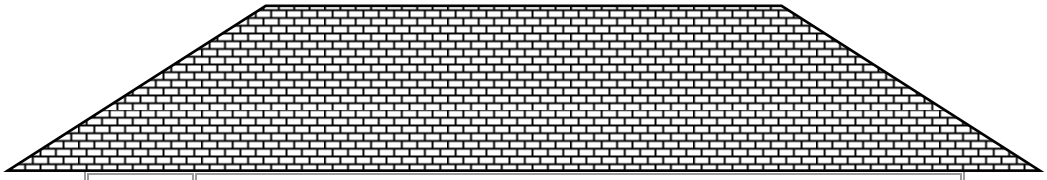
It is up to the application programmer to determine where to store application and data files. (RAM vs. Flash) depending upon how they will be used during the terminal's operation. Other file types, such as operating system files, digital certificates, and signatures files must be downloaded into RAM.

RAM (referenced as Drive I: in the file system)	Flash (referenced as Drive F: in the file system)
Batch records (.DAT)	Application library files (.LIB)
Digital certificates (.CRT)	Application code files (.OUT)
Digital signature files (.P7S)	Font files (.VFT - screen) or (.FON - printer)
	Printer template files (.FRM)

Typically, static data files (files that are not changed) are stored in Flash because it has a slower access speed than RAM and you can only write to it (update its contents) approximately one million times.

The Verix "Apartment Building"

In order to grasp the concept of multiple applications residing and running independently on a single terminal, it's helpful to think of the multi-application environment as an apartment building in which there are 15 different apartments that are managed by the operating system.



0	Used by the operating system
1	VMAC + Comm Server
2	SoftPay
3	Private Label
4	Age Verification
5	Gift Card
6	Check
7	Pre-Paid
8	Money Transfer
9	Atrana Micro-Portal Applications
10	Emerging Markets
11	Time and Attendance
12	Bill Payment
13	Overflow
14	Reserved
15	Used for shared data between all GIDs

In Verix, each "apartment" is referred to as a Group ID or GID.

What Is VMAC?

VMAC or Verix Multi Application Conductor is an independent application that resides in GID 1. It is not part of the terminal's operating system. The purpose of the VMAC application is to 1) dynamically build a menu that displays a list of all other applications resident in the terminal, and 2) manage the system resources (e.g., display, card reader, keypad, modem, RS232 port, etc.) by allocating them as each application make resource requests.

NOTE If VMAC and only one other application are loaded into the terminal, the VMAC menu does not display since this would add an unnecessary key press in order to select the application.

VMAC Reports

In VMAC version 1.4 (and higher) two VMAC reports have been added to aid in downloading and troubleshooting multiple applications. At the VMAC menu, press the right-most purple key.

VMAC REPORTS	F1	Press the [F2] key to print a Summary Report.
SUMMARY REPORT	F2	Press [F3] to print a Detail Report.
DETAIL REPORT	F3	After the selected reports prints, VMAC returns to the reports menu.
	F4	

Summary Report

The Summary Report prints a summary of the terminal configuration, as well as, a list of the application(s) that reside in each GID.

VMAC
SUMMARY REPORT
==========

09/21/04 **18:10**

VMAC Version 1.4.2
Terminal OS Version: Q50016A6
Terminal Type: O3750
Terminal Serial #: 207-311-954

Total RAM: 2048K
Available RAM: 924K
Total FLASH: 2048K
Available FLASH: 524K

GID Information

Group	Application Name
1	DEVMAN
1	FRONTEND
1	COMMSVR
2	SOFTPAY
3	----------
4	----------
5	GIFTCARD
6	----------
7	----------
8	----------
9	----------
10	----------
11	----------
12	----------
13	----------
14	----------
15	VMAC.LIB

Before assisting the merchant in downloading another application into the terminal, ask the merchant to print the VMAC Summary report to list all applications currently residing in the terminal.

Also, make note of the available RAM and Flash memory to ensure the terminal has enough memory to store the new application.

It's possible for more than one application to reside in each GID as long as they are compatible applications. For example, DEVMAN and FRONTEND are executable files that are part of the VMAC application. COMMSVR is the executable file that is part of the Comm Server application.

Detail Report

The Detail Report prints a summary of the terminal configuration, as well as, a list of all application files (for both RAM and Flash) that reside in the selected GID(s). Because this report lists all files in a GID, it can be very lengthy and is generally not printed unless requested by your VeriFone support representative.

1	VMAC REPORTS SUMMARY REPORT DETAIL REPORT		F1 F2 F3 F4	Press [F3] to print a Detail Report.
2	Select a Group: Group 1 DEVMAN, FRONTEND, COMMSVR	PREV NEXT SLCT ALL	F1 F2 F3 F4	Press [F1] to select the previous file group. Press [F2] to select the next file group. Press [F3] to select the current file group. Press [F4] to select all file groups.

VMAC
DETAIL REPORT

==========

09//21/04 **19:26**

VMAC Version 1.4.2
Terminal OS Version: Q50016A6
Terminal Type: O3750
Terminal Serial #: 207-311-954

Total RAM: 2048K
Available RAM: 924K
Total FLASH: 2048K
Available FLASH: 524K

FILENAME	DATE mm/dd/yy	SIZE Bytes

==========

GROUP: 1

Application: VMAC

RAM Files

COMMSVR.OUT	05/10/04	519130
CONFIG.SYS	06/21/04	432
ABOUT.TXT	05/10/04	78
COMMSVR.INS	03/24/04	61
COMMSVR.RES	05/10/04	40
CSVRRAM.P7S	06/17/04	392
FEMESSAG.INI	01/20/04	2654
FRONTEND.RES	05/23/04	40
IMM.INI	03/24/04	25
SSAVER.INI	04/11/04	680
IMM_VMAC.INI	06/24/04	348

FLASH Files 05/23/04 36966

DEVMAN.OUT	04/11/04	4112
FEENLRG.VFT	04/11/04	2064
FEENMED.VFT	04/11/04	784
FEENSML..VFT	04/11/04	36066
FRONTEND.OUT	05/23/04	10912
IMM.OUT	05/23/04	393
DEVMAN.P7S	05/23/04	395
FRONTEND.P7S	05/23/04	390
IMM.P7S	05/23/04	
Total Group 1 Memory:		615962

Because this report may use a lot of paper (depending upon which GIDs are selected), don't have the merchant print this report unless requested by your VeriFone support representative.

It's possible for more than one application to reside in each GID as long as they are compatible applications. For example, DEVMAN and FRONTEND are executable files that are part of the VMAC application. COMMSVR is the executable file that is part of the Comm Server application.

What Is VeriShield?

Almost everyday, you hear about another case of identity theft, computer viruses, and Internet worms. Because of this, anyone who uses a computer (including a POS terminal) is rightly concerned about the security of the device and the information stored in it. To address these concerns and to meet more stringent PIN Entry Device (PED) security standards required by Visa and MasterCard, VeriFone developed the VeriShield security architecture. For information about PED, go to www.visa.com/pin.

File Authentication

Security concerns must also be addressed in the multi-application architecture. Instead of a single application downloaded by a single download system, the terminal may house many different applications developed and downloaded by a variety of value-added application providers. To protect the integrity and privacy of each application, VeriShield provides logical security that includes the following elements:

- Restricts the GIDs to which each application has access.
- Prevents unauthorized data access and data modification between applications.
- Utilizes Public Key Encryption (PKI) technology to authenticate application executable and library files after a download. If the authentication fails, the application is not permitted to run in the terminal.

After an application download, you can see the file authentication process in action:

** VERIFYING FILES **	F1
Compare Signature	F2
G2	
SP2000.P7S	F3
F:sp2000.OUT	
** Authentic **	F4

Physical Security

VeriShield provides physical security designed to make the terminal tamper-resistant. This prevents an unauthorized individual from obtaining information by accessing internal electronic components. Elements of VeriShield's physical security are:

- Prevents electronic bugging or tapping of clear text PIN data.
- High security tamper detection eliminates the need for epoxy potting of the IPP (older PIN pads have a block of epoxy resin surrounding the IPP).
- Prevents correlation of tone or electro-magnetic emissions on the keypad (i.e., no one can determine which keys have been pressed by "listening" to each key press).
- Securely stores Master Session and DUKPT keys.
- Renders the terminal inoperative if tampering is detected.

Logical Security

In addition to the physical security required to protect PIN-based transactions, VeriShield also provides logical security elements, such as:

- Offers secure key management and PIN encryption.
- Adheres to current industry standards for key management and key loading.
- Supports the new 3DES (triple DES) key management standard.
- Performs file authentication on all downloaded application executable and library files.
- EMV level 1 and 2 certified for smart card transactions.

The features of VeriShield's physical and logical security architecture provide a comprehensive security system that provides real peace of mind by meeting and exceeding industry security standards.

Troubleshooting Tips

The terminal menu at the merchant location does not display what I expected.

If VMAC and only one other application are loaded into the terminal (e.g., SoftPay), VMAC is smart enough not to build a menu that only has a single selection. If the merchant downloads another value-added application, then VMAC will build the menu.

How do I know which version of VMAC I am using?

When the terminal initializes (after a power-cycle or restart from system mode), the VMAC splash screen displays that includes the VMAC version number.

Lesson 3: Review

- The key features of the Verix operating system are:
  - Application separation at both the hardware and software level.
  - Supports multiple, independent applications on a single platform.
  - Applications can be added or modified without having to re-certify existing applications.
  - Applications and files are secured using VeriShield.
- The Verix "apartment building" is a useful analogy for explaining the multi-application architecture provided by the Verix operating system. Each GID can be compared to an apartment in which an application resides. Specific GIDs are restricted for use by the operating system while others are used to house value-added applications.
- Verix strictly enforces how each GID is used:
  - GID 0 - used by the operating system.
  - GID 1 - used for the "main" application (i.e., VMAC) that has access to all GIDs. If any application is IP-enabled, the Comm Server application also resides in GID 1.
  - GID 15 – used to store shared data and libraries (accessible by all GIDs).
  - GIDs 2 – 14 – used to store value-added applications (applications stored in each GID cannot access any other GID except for GID 15).
- VMAC (Verix Multi Application Conductor) is the controlling application that resides in GID 1. It builds a menu of all resident applications, as well as, manages system resources.
- VMAC version 1.40 (and above) provides two reports: Summary and Detail that can be used prior to downloading additional applications into the terminal and as a troubleshooting tool.
- Dynamic memory allocation is an important feature of the Verix operating system because it ensures that each application only uses the amount of memory it requires, thus freeing the remaining memory for data (e.g., batch records) or additional value-added applications.
- The Verix operating system utilizes two types of memory:
  - RAM memory is used to store information that is frequently updated (e.g., batch records) or is used by the operating system (e.g., device drivers, digital certificates, digital signature files).
  - Flash memory is used to store information that is infrequently updated (e.g., application code files, application library files, font files, message files).
- VeriShield provides physical security designed to make the terminal tamper-resistant, as well, as logical security required to protect PIN-based transactions. One of the most important features of VeriShield is file authentication that prevents unauthorized applications from running.

Lesson 3: Test Your Knowledge

1. What key is used to exit an application and return to the VMAC menu?

2. What key is pressed to display the VMAC Reports menu?

3. When would you use the VMAC Summary Report?

4. Static files (that do not change) are stored in _____ memory.

5. Dynamic files (that do change) are stored in _____ memory.

6. Indicate the GID in which the following programs are stored:

   _____ VMAC

   _____ SoftPay

   _____ Shared Libraries/Data

   _____ Operating System

   _____ Comm Server

7. What are two important functions performed by VMAC?

8. What file is present in all GIDs except for GID 0?

Lesson 4: System Mode

Lesson Objectives

After completing this lesson you will be able to:

- Explain the difference between Normal Mode and System Mode.
- Edit parameters using the CONFIG.SYS editor.
- Clear RAM and Flash files prior to performing a full download.
- Perform full and partial telephone downloads.
- Explain the function of common CONFIG.SYS parameters.
- Describe the types of files that may be downloaded.
- Describe the benefits of file compression.

Operating Modes

Before you can use the keys on the front panel to enter ASCII characters, the Omni 3750 must be in a mode that accepts keyed data entry. There are two terminal operating modes; each enables you to press keys to enter data under specific circumstances:

- **Normal mode** – This is the terminal operating mode where an application program is present in RAM and currently running.
- If you turn on an Omni 3750 terminal that does not have an application stored in GID1 (i.e., VMAC), the system prompt **DOWNLOAD NEEDED INVALID *GO PARAMETER** displays. VMAC must be present to run any other applications in the terminal.
- **System mode** – This is a special, password-controlled terminal operating mode for performing a variety of test and configuration procedures that cannot be performed when an application is running.
- You can enter system mode by simultaneously pressing [F2] and [F4], and then entering the password. Once in system mode, you can configure the terminal as required and perform the necessary download.

System Mode

Because the Omni 3750 platform supports new features, such as multiple applications, the System Mode functions have been revised.

How To Enter System Mode

During power-up, the operating system version and copyright notice display.

VERIFONE O3750 Q50016A5 11/26/2002 Verix COPYRIGHT 1997 - 2002 VERIFONE ALL RIGHTS RESERVED	F1 F2 F3 F4

1. Press [F2] + [F4] at this time to enter System Mode.
2. Enter 1 [Alpha] [Alpha] 66831 as the default System Mode password.

The first System Mode menu displays.

In the following System Mode function descriptions:

= [Enter] key (Green)

= [BackSpace] key (Yellow)

X = [Cancel] key (Red)

= advance to the next screen/menu

= return to the previous screen/menu

System Mode Menu 1

SYS MODE MENU 1	F1
CONTRAST F2	F2
CLOCK F3	F3
RESTART F4	F4

Function Key	Description
[F2] – Contrast	[F2] – increase display contrast [F3] – decrease display contrast
[F3] – Clock	1. Press one of the following function keys to set the year, month or, day OR press ↓ to set the hour and minutes. After pressing the function key, enter the corresponding value. First screen [F2] – set year (YYYY) [F3] – set month (01 – 12) [F4] – set day (01 – 31) Second screen [F2] – set hour (00 – 23) [F3] – set minutes (00 – 59) 2. After pressing the function key, enter the new value. 3. Press X to return to System Mode Menu 1. 4. Press [F4] to restart the terminal.
[F4] – Restart	Exit System Mode and restart the terminal.

System Mode Menu 2

SYS MODE MENU 2	F1
DOWNLOAD F2	F2
RAM FILES F3	F3
FLASH FILES F4	F4

Function Key	Description
[F2] – Download	Initiates modem or direct downloads. 1. Enter the file group number (GID). 2. Enter the file group's password (default = 1 [Alpha] [Alpha] 66831). 3. Press [F3] for full or [F4] for partial. 4. Press [F2] for modem (dial) or [F3] for COM1 (direct). COM2 and COM3 are not currently supported. Press X to cancel the download.
[F3] – RAM Files	Clears RAM files. 1. Press [F2] to clear a single file group's RAM files or [F3] to clear RAM for all file groups. 2. Enter the file group's password (default = 1 [Alpha] [Alpha] 66831). 3. Press [F3] to cancel or [F4] to confirm. If you clear the RAM files for all groups, the CONFIG.SYS files for all groups are cleared except for GID 1. In GID 1, only the parameters that begin with * or # are retained.
[F4] – Flash	Clears Flash files. 1. Press [F2] to clear a single file group's Flash files, [F3] to clear Flash files for all file groups, or [F4] to Defrag. It is only necessary to Defrag if a single group's RAM or Flash files are cleared. 2. Enter the file group's password (default = 1 [Alpha] [Alpha] 66831). 3. Press [F3] to cancel or [F4] to confirm.

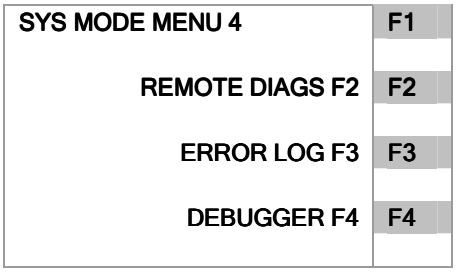
System Mode Menu 3

SYS MODE MENU 3	F1
CONFIG INFO F2	F2
EDIT F3	F3
PASSWORDS F4	F4

Function Key	Description
[F2] – Config Info	Displays information, such as: RAM files (in use + available) Flash files (in use + available) Total Kb RAM Total Kb Flash Serial number PTID Part number Hardware version Model number Country of manufacture Keypad type Display type Mag reader type Printer type PIN pad type Terminal life (in seconds) Latest reset date + time Number of resets Modem country code Modem type
[F3] – Edit **Note: Each GID has its own CONFIG.SYS file.**	1. Select the file group (GID). 2. Enter the file group's password (default = 1 [Alpha] [Alpha] 66831). 3. Press ↵ twice. The system displays SYS MODE EDIT and the first value in the file. 4. To scroll through the keys, press ↵ or ↓ to move forward or ↑ to move backward. 5. Once the parameter displays, press ↵ or [F3] to modify the value. 6. Enter the new value, then press ↵. 7. To select another parameter, press [F3] and enter its name (key) followed by ↵. To add a new parameter, you must press ↵ until you scroll past the last CONFIG.SYS parameter. 1. Select the file group (GID). 2. Enter the file group's password (default = 1 [Alpha] [Alpha] 66831). 3. Press ↵. The system displays SYS MODE EDIT and the first value in the file. 4. To scroll through the keys, press ↵ or ↓ until you scroll past the last parameter. 5. Enter the new key (parameter) and press ↵. 6. Enter the new value, then press ↵.

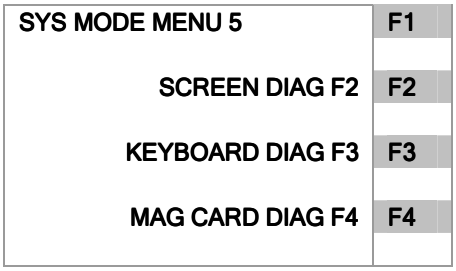
[F4] - Passwords	1. Press [F2] to change file group (GID). 2. Press [F3] to change System Mode. 3. Skip steps 1 + 2 to change the System Mode password. 4. Select the file group (GID). 5. Enter the GID's password. 6. Enter the new password. 7. Re-enter the new password to confirm. System displays PASSWORD CHANGED.

System Mode Menu 4



Function Key	Description
[F2] - Remote Diagnostics	Reserved for future use.
[F3] - Error Log	Displays the error type and stack frame. Used for advanced troubleshooting.
[F4] - Debugger	Places the terminal in debug mode. Only used by application developers.

System Mode Menu 5



Function Key	Description
[F2] - Screen Diag	Press [F2] to display dark screen. Press ↵ to display clear screen.
[F3] - Keyboard Diag	Displays ASCII code for each key pressed.
[F4] - Mag Card Diag	Displays one of the following messages:

	VALID DATA LRC ERR PARITY ERR REVERSE END	NO DATA NO START NO END

System Mode Menu 6

SYS MODE MENU 6	F1
IP DIAG F2	F2
IPP KEY LOAD F3	F3
PRINTER DIAG F4	F4

If an internal PIN pad is not installed, selecting any options on this menu causes the terminal to display "INTERNAL PIN PAD NOT INSTALLED".

Function Key	Description
[F2] – IPP Diag	Retrieves version information from the IPP, runs a one-pass RAM test and displays this information along with: the PROM version and checksum, serial number, baud rate, and mode (VISA or Spain). Press [F3] to reset the baud rate to 1200 (factory default). Press [F4] to exit this menu.
[F3] – IPP Key Load	Provides a pass-thru connection from the key loading tool (e.g., MKIXOR or SecureKit) to the IPP. The key load option does not interpret data, has no knowledge of key loading protocols, and performs no setup or monitoring. To begin the load process, enter the system password unless the default 1 [Alpha] [Alpha] 66831 is being used. If so, this step is not required. The *IPPMKI CONFIG.SYS variable (in GID 1) is used to set the data format and baud rate required by the key loading tool (if these values are not configurable). Valid values for *IPPMKI: 1200 (or another valid baud rate, factory default = 19200) E = even parity (A7E1) O = odd parity (A7O1) D = assert DTR R = assert RTS Values may be set in any order (e.g., 1200E or ER or R9600) and only apply to the terminal's COM1 port. The terminal's IPP is on COM2. As the key load progresses, the terminal displays the bytes sent and received. If there is an error, a message in the format **** dev ERROR n **** displays where **dev** is either COM1 or IPP and **n** is one of the following error numbers: -1 = can't open COM2 -2 = can't communicate with IPP -3 = COM2 read/write error -4 = timeout waiting for start of packet -5 = timeout waiting for next byte -6 = received too many NAKs -7 = received EOT before end of transaction
[F4] – Printer Diag	Displays the printer firmware ID, the printer firmware version, and a status byte. Press [F3] to perform a printer test (press [CLEAR] or remove power to terminate). Press [F4] to advance the paper 10 lines.

System Mode Menu 7

SYS MODE MENU 7	F1
	F2
RAM DIRECTORY F3	F3
FLASH DIRECTORY F4	F4

Function Key	Description
[F3] – RAM Directory	Displays a list of files stored in RAM for the selected GID, including the file date and size in bytes. If the file was authenticated by VeriShield, an 'A' displays to the right of the file date.
[F4] – Flash Directory	Displays a list of files stored in Flash for the selected GID, including the file date and size in bytes. If the file was authenticated by VeriShield, an 'A' displays to the right of the file date.

NOTE The quick and easy way to find out what files are stored in a particular GID is to print the VMAC Detail Report.

The CONFIG.SYS File

The CONFIG.SYS file is a special file that resides in every GID (except for GID 0). It contains parameters used by the operating system to control terminal functions and operations. It is also be used by application programs to store parameters that control how the application operates. For example, the *GO parameter indicates the name of the application file to execute upon start-up.

Note that the CONFIG.SYS parameters listed below all begin with an asterisk (*). CONFIG.SYS parameters that begin with an asterisk (*) or a pound sign (#) are retained after a download. If terminal memory is cleared in all GIDs, the CONFIG.SYS parameters in each GID are cleared. The only exception is that in GID 1, parameters that begin with * and # are retained.

Verix CONFIG.SYS Parameters

The following table lists CONFIG.SYS variables used by the Verix operating system. Some variables are set by the application and do not have to be set by the user.

Variable	GID(s)	Description
*ZA	1 - 14	Download application name. For multi-application downloads from VeriCentre, set *ZA = *MA (unless applications are bundled). This parameter is the same for telephone or Ethernet downloads.
*ZT	1 - 14	Download terminal ID. This parameter is the same for telephone or Ethernet downloads.

*ZP	1 - 14	For telephone downloads, the download system telephone number. For Ethernet downloads, the network address of the VeriCentre server. <network_address>:<port number> For example: vcindl.verifone.com:8013 or 208.237.46.19:8013
*ZR	1 - 14	For telephone downloads, the download baud rate (3 = 2400, 6 = 14.4). For Ethernet downloads, *ZR = 9.
*ZRESP	1 - 14	For telephone downloads, the external modem connection response (10 = 2400, 16 = 14.4 bps). For Ethernet downloads, *ZRESP=19.
*ZINIT	1 - 14	Not required unless specified by your VeriFone support representative.
*ZRESET	1 - 14	Not required unless specified by your VeriFone support representative.
*ZSWESC	1 - 14	Software termination of connection. For Ethernet downloads, *ZSWESC=1. NOT REQUIRED FOR DIAL.
*ZX	1	Automatically restart the application after a download (0 = remain on Download Done screen until a key press, 1 = restart application).
*MC	1	Modem country code (U.S. = 22). This parameter must be specified for both telephone and Ethernet downloads.
*DEFRAG	1	Defrag/coalesce Flash (blank or '0' enables this feature). Valid in operating system version Q50016A5 or higher.
*GO	1 - 14	Name of application program to execute (e.g., *GO = F:SP2000.OUT). If *GO is empty or the operating system cannot find the specified file, the terminal displays DOWNLOAD NEEDED.
*SMDL	1	Poll for direct download during the power-up sequence (before copyright screen displays).
*PW	1 - 15	GID password. The actual password is not stored in the CONFIG.SYS file.
*SMPW	1	System Mode password. The actual password is not stored in the CONFIG.SYS file.
*UNZIP	1 - 15	Automatically decompress specified ZIP file during start up (e.g., *UNZIP = F:SOFTPAY.ZIP, where F: = Flash). The terminal displays each file name as it is decompressed from the ZIP file. NOTE: Do not confuse *UNZIP with UNZIP. UNZIP is a CONFIG.SYS parameter set by the operating system after it attempts to unzip a file within a GID. 0 = unzip process was started, 1 = file was successfully unzipped, 2 = problem with the unzip process.

Performing Downloads

To help you plan downloads tasks and to explain how the download procedures for the Omni 3750 terminals may differ from those you may be accustomed to using for other POS terminals, you must consider the following:

- Support for multiple applications
- Use of RAM and Flash memory
- Redirection of files during application downloads
- File authentication requirements
- File compression (unzipping of application files after the download)

Where Can Files Be Downloaded?

The system of file groups imposes some logical restrictions on which files you can download into each file group.

- If you select GID 1 as the target group in System Mode during a single download, you can download files into GID 1 and then redirect these files into any other file groups as required.
- If you select a file group other than GID 1 as the target file group, you can download files only into that group and redirect files only to GID 15. For example, if you select GID 5 as the target group for the download, files can only be downloaded into GID 5 and redirected to GID 15 (as required).
- Depending upon the memory configuration of the terminal (i.e., the amount of RAM or Flash), files may be downloaded either into RAM or Flash. During a download, all files are loaded into the file system of the target file group you select in System Mode. Specific files that are included in the download package must then be redirected (if required) to the RAM or Flash file system of the target file group or to another file group.

What Can Be Downloaded?

In general, you can download files and data to an Omni 3750 terminal that can be grouped into the following functional categories:

- **Operating system files**

  The operating system (OS) is a set of related programs and data files that is provided by VeriFone to control the terminal's basic processes and functions. Files that belong to the operating system are stored in a reserved area of terminal memory.

  A complete operating system is downloaded into each Omni 3750 terminal during the manufacturing process. If necessary, a new version of the OS can be downloaded to the terminal during the application development process, when preparing the terminal for deployment, or in the field at customer sites. Operating system files are downloaded just like any other Omni application.

NOTE The operating system can be downloaded via a partial download without disturbing applications already existing in the terminal.

WARNING If the terminal part number begins with M197, it MUST be downloaded with operating system version Q50015A1 or later. If you load an older version of the operating system into a terminal with this part number, the terminal will become completely inoperative and must be sent in for repair; however, if the terminal part number begins with M097, it may be downloaded with operating system version Q50015A1 or earlier.

- **Applications and related files.** An application is a computer program that consists of one or more "executables", including compiled and linked object files (*.out) and one or more function libraries (*.lib). Most applications also include font files (*.vft, .fon), data files (*.dat), and other related file types.

  Omni 3750 applications may be developed by VeriFone, by customers, or by third parties at the customers' request. One or more applications must be downloaded into the Omni 3750 terminal before it can be deployed at a customer site and used to process transactions.

- **Terminal configuration settings.** Files or records containing various kinds of data can also be downloaded into the Omni 3750 terminal, including CONFIG.SYS variables, passwords for accessing protected System Mode functions, the current date + time, the modem country code setting, etc.

- **Files related to the file authentication process.** The logical component of the VeriShield security architecture in the Omni 3750 terminal is called file authentication. The VeriShield file authentication module must authenticate every executable that is to run on an Omni 3750 terminal.

  Two types of special files are required for the file authentication process: digital certificates (*.crt) that are loaded with the operating system and signature files (*.p7s) that are loaded with individual applications. These file types must be downloaded to the terminal along with the corresponding application files to be authenticated.

Application Compression

To reduce download time, the Verix operating system allows application files to be compressed into a "zip" file prior to downloading. The application is pre-compressed using a VeriFone file compression utility.

This function is performed by the application developer using the file compression utility. The compression process places a trailer record at the end of the zip file. The trailer record contains information used by the operating system when uncompressing (unzipping) the application.

NOTE Terminal operating system versions 14 and above do not check for the trailer record.

File compression reduces the application size approximately 40% depending upon the types of files being compressed. Downloading the SoftPay application into an Omni 3200 with a 2400 baud modem typically takes 30 – 35 minutes. Downloading the compressed SoftPay application into an Omni 3750 with a 14.4 baud modem can be accomplished in under 10 minutes. Not only does this reduce communications costs, it frees up the merchant's phone line a lot sooner.

NOTE File compression is only supported by operating system versions 3AO and above. Only operating system versions 12AO and above support decompression in individual GIDs. Operating system versions prior to 12AO require all compressed files to be downloaded into GID1. The operating system then decompresses the file and moves its contents into the specified GID.

After the download is complete, the operating system checks each GID (1 – 15) for the *UNZIP parameter. If this parameter is found, it then attempts to unzip the application specified in the *UNZIP parameter (e.g., *UNZIP = SOFTPAY.ZIP). If the specified application zip file is located in that GID, the terminal displays the application's files as they are unzipped.

Unzip F:SOFTPAY.ZIP	F1
F: SP2000.OUT	
F:IMM.INI	F2
F:DIALER.OUT	
F:ASC4X16.VFT	F3
F:ASC4X8.VFT	
F:ASC8X21.VFT	F4
F:ABOUT.TXT	

After the operating system reads the *UNZIP parameter, it deletes it from the GID's CONFIG.SYS file.

NOTE If the *UNZIP parameter is missing, contains an invalid zip file name, or does not point to the correct RAM/Flash directory, the application file is not unzipped; however, it remains in memory.

File Authentication

When the download completes, the operating system must authenticate each application's executable (.OUT) and library (.LIB) files before the application is allowed to run.

** VERIFYING FILES **	F1
Compare Signature	F2
G2	
SP2000.P7S	F3
F:sp2000.OUT	
** Authentic **	F4

If the file does not authentic, the operating system beeps and displays '** Failed **'. The authentication process does not terminate if this occurs; however, the terminal will not be in a usable state after the authentication process completes.

Full vs Partial Downloads

A full application download includes both the application program and any associated parameters. A partial download only includes the application parameters.

Performing Downloads

A quick review… in order to perform any type of download, the following parameters must be set:

*ZA	Download application name. For multi-application downloads from VeriCentre, set *ZA = *MA (unless applications are bundled). This parameter is the same for telephone or Ethernet downloads.
*ZT	Download terminal ID. This parameter is the same for telephone or Ethernet downloads.

*ZP	For telephone downloads, the download system telephone number. For Ethernet downloads, the network address of the VeriCentre server. <network_address>:<port number> For example: vcindl.verifone.com:8013 or 208.237.46.19:8013
*ZR	For telephone downloads, the download baud rate (3 = 2400, 6 = 14.4). For Ethernet downloads, *ZR = 9.
*ZRESP	For telephone downloads, the external modem connection response (10 = 2400, 16 = 14.4 bps). For Ethernet downloads, *ZRESP=19.

Performing a Full Download Into an Empty Terminal

VMAC must be loaded into the terminal at some point for other applications to successfully operate. Typically, VMAC is loaded into an empty terminal with one or more other applications.

1. Enter System Mode by pressing [F2] + [F4] at the same time.
2. Enter the System Mode password and press  .
3. Go to System Mode Menu 3 and select [F3] – Edit.
4. Press  to select GID 1.
5. Enter the password for GID 1 and press  .
6. Press  to select the CONFIG.SYS file.
7. Enter the Key and corresponding Value for each download parameter for GID 1 (e.g., *ZA, *ZP, *ZT, *ZR, *ZRESP).
8. Press  twice to return to System Mode Menu 3.
9. Press ↑ to return to System Mode Menu 2.
10. Press [F2] – Download.
11. Press  to select GID 1.
12. Press [F3] – Full.
13. Press [F2] – Modem, [F3] – COM1 (for direct downloads), or [F4] – TCPIP for TCP/IP downloads.

As the download is progressing, the terminal displays SYS MODE DOWNLOAD – DOWNLOADING NOW and a series of 10 asterisks (one asterisk for each 10% completed) **----------. When all ten asterisks display, the download is complete and the terminal begins unzipping the application files (if the application was compressed) and initializing the application.

NOTE Do not disturb the terminal while it is initializing. Wait until the main menu screen displays before proceeding.

NOTE For more detailed instructions on performing downloads that include screen examples, refer to Appendix A.

Adding a New Application To the Terminal (Full Download)

The steps for adding a new application assume that VMAC and one ore more applications are already loaded in the terminal and that you want to download an additional application into an empty GID.

1. Enter System Mode by pressing [F2] + [F4] at the same time.
2. Enter the System Mode password and press ↵.
3. Go to System Mode Menu 3 and select [F3] – Edit.
4. Enter the GID you want to download and press ↵.
5. Enter the password for the selected GID and press ↵.
6. Press ↵ to select the CONFIG.SYS file.
7. Enter the Key and corresponding Value for each download parameter for the selected GID (e.g., *ZA, *ZP, *ZT, *ZR, *ZRESP).
8. Press X twice to return to System Mode Menu 3.
9. Press ↑ to return to System Mode Menu 2.
10. Press [F2] – Download.
11. Enter the GID you want to download and press ↵.
12. Press [F3] – Full.
13. Press [F2] – Modem, [F3] – COM1 (for direct downloads), or [F4] – TCPIP for TCP/IP downloads.

As the download is progressing, the terminal displays SYS MODE DOWNLOAD – DOWNLOADING NOW and a series of 10 asterisks (one asterisk for each 10% completed) **----------. When all ten asterisks display, the download is complete and the terminal begins unzipping the application files (if the application was compressed) and initializing the application.

> **NOTE** Do not disturb the terminal while it is initializing. Wait until the main menu screen displays before proceeding.
>
> **NOTE** For more detailed instructions on performing downloads that include screen examples, refer to Appendix A.

Updating an Existing Application (Full Download)

The steps for updating an existing application require that you clear RAM and Flash memory for the GID you want to update.

1. Enter System Mode by pressing [F2] + [F4] at the same time.
2. Enter the System Mode password and press ↵.
3. Go to System Mode Menu 2 and select [F3] – RAM Files.
4. Enter the GID you want to clear and press [F2].
5. Enter the password for the selected GID and press ↵.
6. Press [F3] to cancel or press [F4] to confirm.
   After clearing RAM, the operating system redisplays System Mode Menu 2.
7. Select [F4] – Flash Files.
8. Press [F2] to clear the selected GID.
9. Press [F3] to cancel or press [F4] to confirm.
   After clearing Flash, the operating system redisplays System Mode Menu 2.
10. Select [F4] – Flash Files.
11. Select [F4] – Defrag.
12. Enter the password for GID 1 and press ↵.
13. Go to System Mode Menu 3 and select [F3] – Edit.
14. Press [F3] to cancel or press [F4] to confirm.
    The terminal displays SYS MODE DEFRAG RECLAIMING FLASH PLEASE WAIT
    After defragging Flash memory, the terminal exits System Mode and restarts.
15. Enter System Mode by pressing [F2] + [F4] at the same time.
16. Enter the System Mode password and press ↵.
17. Go to System Mode Menu 3 and select [F3] – Edit.
18. Enter the GID you want to download and press ↵.
19. Enter the password for the selected GID and press ↵.
20. Press ↵ to select the CONFIG.SYS file.
21. Enter the Key and corresponding Value for each download parameter for the selected GID (e.g., *ZA, *ZP, *ZT, *ZR, *ZRESP).
22. Press X twice to return to System Mode Menu 3.
23. Press ↑ to return to System Mode Menu 2.
24. Press [F2] – Download.

25. Enter the GID you want to download and press  .

26. Press [F3] – Full.

27. Press [F2] – Modem, [F3] – COM1 (for direct downloads), or [F4] – TCPIP for TCP/IP downloads.

As the download is progressing, the terminal displays SYS MODE DOWNLOAD – DOWNLOADING NOW and a series of 10 asterisks (one asterisk for each 10% completed) **----------. When all ten asterisks display, the download is complete and the terminal begins unzipping the application files (if the application was compressed) and initializing the application.

NOTE Do not disturb the terminal while it is initializing. Wait until the main menu screen displays before proceeding.

NOTE For more detailed instructions on performing downloads that include screen examples, refer to Appendix A.

Updating the Parameters For an Existing Application (Partial Download)

The following steps assume an application is already loaded in the GID you want to update.

1. Enter System Mode by pressing [F2] + [F4] at the same time.
2. Enter the System Mode password and press  .
3. Go to System Mode Menu 3 and select [F3] – Edit.
4. Enter the GID you want to download and press  .
5. Enter the password for the selected GID and press  .
6. Press  to select the CONFIG.SYS file.
7. Enter the Key and corresponding Value for each download parameter for the selected GID (e.g., *ZA, *ZP, *ZT, *ZR, *ZRESP).
8. Press  twice to return to System Mode Menu 3.
9. Press ↑ to return to System Mode Menu 2.
10. Press [F2] – Download.
11. Enter the GID you want to download and press  .
12. Press [F4] – Partial.
13. Press [F2] – Modem, [F3] – COM1 (for direct downloads), or [F4] – TCPIP for TCP/IP downloads.

As the download is progressing, the terminal displays SYS MODE DOWNLOAD – DOWNLOADING NOW and a series of 10 asterisks (one asterisk for each 10% completed) **----------. When all ten asterisks display, the download is complete and the terminal begins unzipping the application files (if the application was compressed) and initializing the application.

NOTE Do not disturb the terminal while it is initializing. Wait until the main menu screen displays before proceeding.

NOTE For more detailed instructions on performing downloads that include screen examples, refer to Appendix A.

Performing a Full Secure SSL Download

Secure downloads are encrypted using SSL technology in order to ensure the privacy of the data being transmitted. Secure downloads are initiated from the Comm Server menu instead of from System Mode Menu 2.

IMPORTANT Because SSL downloads are performed using the Comm Server application that resides in GID 1, you cannot perform a FULL multi-application download from GID 1 that includes the Comm Server application.

If you need to download the Comm Server application, VMAC, or any other application that resides in GID 1, you must download these applications from System Mode or perform a partial download from the Comm Server.

When performing a full download from GID 1, memory is not cleared (either manually by the user or automatically by the Comm Server application).

Secure SSL Downloads are only supported in Comm Server version 2.10 and above.

1. Select the Comm Server application from the VMAC menu.
2. Select Download from the Comm Server menu.
3. Enter the GID you want to download and press  .
4. If GID 1 selected, continue with Step 5; otherwise, skip to Step 6.
5. Press [F3] for a single application download or press [F4] for a multi-application download.

   The multi-application download cannot include Comm Server.
6. Press [F3] – Full.
7. Press [F3] – SSL to perform a secure SSL download.
8. If GID 1 selected, skip to step 10; otherwise, continue with the next step.
9. Press [F3] – Yes to clear the target GID or press [F4] – No to retain the application in the target GID.

   GID 1 is never cleared before a full download; therefore, this prompt will not display if GID 1 was selected in Step 3.
10. Verify the download parameters: *ZP, *ZA, and *ZT.
11. If one or more of these parameters is incorrect, press [F3] – Edit. Otherwise, press [F4] – Start.

    To edit a parameter, press  to delete the current parameter value, then enter the correct parameter value.
12. When all parameters have been verified and/or updated, press [F4] – Start.

NOTE Once the download has started, you will not be able to press the  key to abort the download.

Performing a Partial Secure SSL Download

Secure downloads are encrypted using SSL technology in order to ensure the privacy of the data being transmitted. Secure downloads are initiated from the Comm Server menu instead of from System Mode Menu 2.

NOTE Secure SSL Downloads are only supported in Comm Server version 2.10 and above.

1. Select the Comm Server application from the VMAC menu.
2. Select Download from the Comm Server menu.
3. Enter the GID you want to download and press  .
4. If GID 1 selected, continue with Step 5; otherwise, skip to Step 6.
5. Press [F3] for a single application download or press [F4] for a multi-application download.
6. Press [F4] – Partial.
7. Press [F3] – SSL to perform a secure SSL download.
8. Verify the download parameters: *ZP, *ZA, and *ZT.
9. If one or more of these parameters is incorrect, press [F3] – Edit. Otherwise, press [F4] – Start.

   To edit a parameter, press  to delete the current parameter value, then enter the correct parameter value.
10. When all parameters have been verified and/or updated, press [F4] – Start.

NOTE Once the download has started, you will not be able to press the  key to abort the download.

Troubleshooting Tips

How do I know how much memory the terminal has?

System Mode > Menu 3 > Config Info > Press Down Arrow > RAM + Flash size

512 = .5 Mb

1024 = 1 Mb

2048 = 2 Mb

Add the memory size for both RAM and Flash to determine the total amount of memory.

NOTE Before performing a full download, be sure to ask the merchant the amount of memory in the terminal AND the version of VMAC currently running in the terminal.

If the merchant changes the system mode password and forgets, what can be done?

Nothing, the terminal must be returned to VeriFone for repair to have the password reset to the default value.

Can a merchant plug a DSL line into the terminal?

Yes. If the merchant wants to utilize the high-speed DSL data channel for transaction authorization and settlement, two things must be in place:

- The merchant must have the Comm Server application installed on the terminal.
- Applications that the merchant intends to utilize must be modified to support IP/Ethernet and SSL (secure sockets layer). Using the DSL dial channel requires no application modifications or the Comm Server application.

The merchant has the IP module installed and is using their DSL line. They are unable to authorize transactions; however, if they plug the terminal into a straight analog line, it works.

Does the merchant have a filter installed on the jack where the terminal is plugged in? DSL filters block the DSL signal from reaching the phone, fax, terminal, etc. Except for the DSL modem, every device sharing the DSL phone number needs a filter

The download completes and is successful, but the terminal displays DOWNLOAD NEEDED, INVALID *GO PARAMETER.

Steps to resolve:

1. Determine if the VMAC application has been successfully downloaded into the terminal.

   System Mode > Menu 7 > RAM Directory > GID 1
   System Mode > Menu 7 > Flash Directory > GID 1

   If multiple application files are present in both the RAM and Flash directory for GID 1, proceed to Step 2.

   If multiple application files are not present in either RAM or Flash for GID 1, you must download the VMAC application into GID 1.

If you find a file called VMACN131.ZIP (or something similar) in either RAM or Flash for GID 1, this means that the VMAC application was downloaded correctly, but did not unzip because the *UNZIP parameter was either not included in the download or does not have the correct value.

System Mode > Menu 3 > Edit > GID 1

Set *UNZIP to the correct value (e.g., *UNZIP = F:VMACN131.ZIP).

Note: If the zip file for VMAC was loaded into Flash, the name of the zip file must be preceded by the drive designator (e.g., F:VMACN131.ZIP).

2. Verify that the *GO parameter is set correctly.

   System Mode > Menu 3 > Edit > GID 1 > *GO = F:IMM.OUT.

The download completes and is successful, but the terminal displays NO APPLICATIONS PRESENT.

This message indicates that VMAC has been downloaded and is running in GID 1, but no other applications exist in the terminal.

Steps to resolve:

1. Download an application into a GID (other than GID 1).
2. If a compressed application was downloaded into a GID, determine if the ZIP file is still present by reviewing the contents of RAM and Flash for this GID (e.g., GID 2 for SoftPay). If so, be sure the *UNZIP parameter is correctly set for this application ZIP file.

I'm helping a merchant download the terminal, but the download is taking a long time (e.g., 40 minutes or more).

Steps to resolve:

Using an Omni 3750 with a 14.4 modem and performing a compressed application download, the download time for VMAC and SoftPay should be under 10 minutes. If the download is taking much longer than this, the most likely cause is that the *ZR and *ZRESP parameters are not set to download at 14.4. Confirm the merchant is using the following values:

System Mode > Menu 3 > Edit > GID 1 > *ZR = 6
System Mode > Menu 3 > Edit > GID 1 > *ZRESP = 16

Note: If the merchant is downloading a value-added application into a different GID, edit the *ZR and *ZRESP values in that GID.

The download completed successfully, all applications files unzipped and authenticated, and yet the terminal display is blank.

Steps to resolve:

Verify there is at least one parameter in GID 15. You can enter any parameter name and value.

System Mode > Menu 3 > Edit > GID 15 > FAKEPARM = 1

The terminal displays DOWNLOADING NOW, but nothing is happening.

A few seconds may elapse until a series of 10 dashes appears on the display to indicate the download has started. If the dashes do not display in 15 – 20 seconds, then perform the following steps.

Steps to resolve:

1. Check to be sure a phone line is attached.
2. Does the merchant require a 9 in front of the phone number?
3. Verify the merchant has the correct download phone number in *ZP. Have the merchant attempt to dial the download phone number from a regular phone and see if the download host answers.

The terminal displays WRITE COMM FAIL immediately after a download is initiated.

Steps to resolve:

1. Make sure that the *ZR parameter is set to a valid value.
2. For a 14.4 modem, be sure that the *ZINIT or *ZRESET does not include E or E0 which disables command echo.

How do I tell if the terminal has a high-speed 14.4 modem?

Steps to resolve:

Look at the telco port on the rear of the terminal. If there is an H.S. (high-speed) above the telco port, the terminal has a 14.4 modem.

After unzipping an application after a download, the terminal screen goes blank for an extended period. Is something wrong?

No. The blank screen appears during the defrag (coalesce) of Flash memory that occurs automatically after all applications have been unzipped. Operating system versions 15 and above display “Reclaiming Flash, please wait…” instead of a blank screen.

An Omni 3750 with a 2400 baud modem takes a long time to connect to the download host – why?

The 2400 baud TDK modem does not set Tone dial as default; therefore, you need to place a T at the beginning of the phone number.

After a download, the terminal displays UNZIP ERROR 19.

UNZIP ERROR 19 means that the terminal is out of Flash memory. There is not enough memory left to store data.

Steps to resolve:

1. Confirm that the merchant cleared RAM and Flash memory (either all or for a selected GID), prior to starting the download.

   System Mode > Menu 2 > RAM Files > Clear Group # (for one GID)
   System Mode > Menu 2 > RAM Files > Clear All Files (for all GIDs)

   System Mode > Menu 2 > Flash Files > Clear Group # (for one GID)
   System Mode > Menu 2 > Flash Files > Clear All Files (for all GIDs)

2. If the merchant is attempting to download a value-added application into a GID and cleared Flash for that GID, did the merchant also defrag Flash?

   System Mode > Menu 2 > Flash Files > Defrag

3. Is the merchant attempting to download more applications than can fit into the terminal's memory? Contact your product group and provide a list of applications the merchant is attempting to store in the terminal.

The terminal completes the download, but displays DOWNLOAD DONE without doing anything else.

Steps to resolve:

Press the [Enter] key or [Clear] key after the download to begin the application initialization process.

After a download, the terminal displays UNZIP ERROR 2

UNZIP ERROR 2 means that there is a problem with the trailer record included at the end of the zip file.

Steps to resolve:

1. Contact your VeriCentre system administrator and confirm that the application zip file's date/time stamp has not been accidentally modified.

2. Have the merchant upgrade to operating system version 14 or above. These versions of the operating system do not check the trailer record.

The operating system needs to be upgraded without disturbing the existing applications. How can this be done?

The operating system can be setup as a partial download in VeriCentre and then downloaded as a partial download from System Mode.

Download Messages

App Not Configured	The application name entered for the *ZA parameter has not been found on the VeriCentre system. Confirm the *ZA value is correct and retry the download.
BAD RX COMMUN	The terminal has sent too many NAKs to the VeriCentre system indicating that VeriCentre has not been able to correctly send information to the terminal. This may be a result of a communications problem. Retry the download.
BAD TX COMMUN	The terminal has received too many NAKs from the VeriCentre system indicating that VeriCentre has not been able to correctly receive information from the terminal. This may be a result of a communications problem. Retry the download.
BUSY	1. You may need a PBX code in front of the download phone number. 2. The download system phone number entered for the *ZP parameter is incorrect and has dialed a phone number that is actually busy. Confirm the *ZP value is correct and retry the download. 3. If you are still having problems, use a phone to dial the VeriCentre system to confirm the system is really busy.
NO CARRIER	The terminal has dialed the VeriCentre download system, but VeriCentre has not responded with carrier tone. Retry the download.
NO DIAL TONE	The terminal cannot detect dial tone on the phone line. Confirm the phone line is plugged into the terminal, then retry the download.
NO ENQ FROM HOST	The terminal has dialed the VeriCentre system. VeriCentre has answered the call, raised carrier, but has not responded with an ENQ to prompt the terminal to transmit the download request packet. Retry the download.
NO LINE	The terminal cannot detect the required line voltage level that indicates a phone line is plugged in. Ensure a phone line is securely plugged into the terminal, then retry the download.
NO RESP FR HOST	The terminal has not received a response from the VeriCentre system within the specified timeout period. 1. You may need a PBX code in front of the download phone number. 2. The download system phone number entered for the *ZP parameter is incorrect and has dialed a phone number that is actually busy. Confirm the *ZP value is correct and retry the download.
Term Not Available	The terminal ID entered for the *ZT parameter has not been found on the VeriCentre system. Confirm the *ZT value is correct and retry the download. Another reason this message may display is that someone else is downloading this terminal ID. Not as likely, but still a possibility.

Lesson 4: Review

- Every GID has a CONFIG.SYS file (except for GID 0) that contains parameters used by both the operating system and application programs. Parameters for each GID are edited using the CONFIG.SYS Editor located in System Modem Menu 3.
- Prior to performing a full download into a GID with an existing application, it is necessary to clear RAM and Flash memory for that GID. If you only clear a single GID, it is also necessary to defrag Flash memory for that GID. If you clear all GIDs, this step is not required.
- The Omni 3750 allows full and partial telephone downloads. A full download includes the application program and associated parameters. A partial download includes only application parameters. Downloads are initiated from System Mode Menu 2.
- File compression reduces download time approximately 40% for a given application. This results in lower communications costs and frees up the merchant's phone line.
- Depending upon the download system used (e.g., VeriCentre), it may be possible to download multiple application programs during a single download. In order to perform a download, the following parameters must be set:

  ***ZP** For telephone downloads, the phone number of download system. For Ethernet downloads, the network address of the download system (<network_address>:<port>).

  ***ZA** Application name to download. Enter *MA for a multi-application download (only valid for GID1) unless the applications are bundled into a single ZIP file.

  ***ZT** Terminal ID to download.

  ***ZR** Baud rate (6 = 14.4 bps). Must be set to '9' for Ethernet downloads.

  ***ZRESP** External modem connection response (16 = 14.4 bps). Must be set to '19' for Ethernet downloads.

- In addition to the CONFIG.SYS parameters required for downloading (listed above), two other CONFIG.SYS parameters you need to remember are:

  ***GO** Name of application program to execute (e.g., *GO = F:SP2000.OUT). If *GO is empty or the operating system cannot find the specified file, the terminal displays DOWNLOAD NEEDED.

  ***UNZIP** Automatically decompress specified ZIP file during start up (e.g., *UNZIP = F:SOFTPAY.ZIP, where F: = Flash). The terminal displays each file name as it is decompressed from the ZIP file.

- The different types of files that may be downloaded are: operating system, application, terminal configuration settings, and files related to the file authentication process.
- The Comm Server application (version 2.10 and higher) is used to perform full and partial SSL secure downloads.

Lesson 4: Test Your Knowledge

1. Why does each GID have a CONFIG.SYS file?

2. What CONFIG.SYS parameter contains the name of the application program to execute?

3. What CONFIG.SYS parameter must be set correctly to uncompress a zipped application file?

4. What is the significance of an '*' (asterisk) or '#' (pound sign) at the beginning of a CONFIG.SYS parameter name?

5. There are two additional steps that must be performed prior to performing a full download into a GID, what are they and why are they important?

6. If you are not sure what files exist in a GID's RAM or Flash memory, how can you find out?

7. Name two benefits of file compression.

8. What is the purpose of file authentication?

9. List the four types of files that may be downloaded.

Appendices

- Appendix A: Performing Downloads
- Appendix B: Terminal Keys
- Appendix C: Installing Peripherals
- Appendix D: Hardware Features
- Appendix E: Glossary
- Appendix F: Terminal Specifications
- Appendix G: Accessories and Documentation

Performing Downloads

Performing a Full Download Into an Empty Terminal

VMAC must be loaded into the terminal at some point for other applications to successfully operate. Typically, VMAC is loaded into an empty terminal with one or more other applications.

1	VERIFONE O3750 Q50014A0 11/26/2002 Verix COPYRIGHT 1997 - 2002 VERIFONE ALL RIGHTS RESERVED	F1 F2 F3 F4	When the Operating System splash screen displays, press [F2] + [F4] simultaneously.
2	SYSTEM MODE ENTRY PASSWORD _____	F1 F2 F3 F4	Enter the System Mode password 1 [Alpha] [Alpha] 66831 and press  .
3	SYS MODE MENU 1 CONTRAST F2 CLOCK F3 RESTART F4 ↓	F1 F2 F3 F4	Press the purple key below ↓ to advance to Sys Mode Menu 3.
4	SYS MODE MENU 3 CONFIG INFO F2 EDIT F3 PASSWORDS F4 ↑ ↓	F1 F2 F3 F4	Press [F3] to edit the CONFIG.SYS file.
5	SYS MODE FILE FILE GROUP _1	F1 F2 F3 F4	If you want to download into GID1, press  . To select a different GID, press  , enter the GID number you want to download, and press  .

6	SYSTEM MODE FILE GROUP 1 PASSWORD _____	F1 F2 F3 F4	Enter the password for the selected GID and press  . Typically, the default GID password is 1 [Alpha] [Alpha] 66831. The terminal displays FILE CONFIG.SYS.
7	SYS MODE EDIT G 1 FILE CONFIG.SYS_ _____	F1 F2 F3 F4	Press  to begin editing the file. **NOTE** In the upper right-hand corner of the display, the letter 'G' displays followed by the GID selected.
8	SYS MODE EDIT G 1 KEY _____ _____	F1 F2 F3 F4	The terminal displays KEY. The following parameters (keys) and their associated values must be entered to perform the download. ***ZP** Phone number or IP address of download system. ***ZA** Application name to download. Enter *MA for a multi-application download - valid for GID1. ***ZT** Terminal ID to download. ***ZR** Baud rate (6 = 14.4 bps, 9 = TCPIP) ***ZRESP** External modem connection response (16 = 14.4 bps, 19 = TCPIP). The following two parameters may be required depending upon the download system. Not required for TCPIP. ***ZINIT** Modem initialization string (ATV0\N0&D2). ***ZRESET** Modem reset string (AT&F0).
9	SYS MODE EDIT G 1 KEY *ZP_____ _____	F1 F2 F3 F4	Enter the key and press  .
10	SYS MODE EDIT G 1 VALUE 18005551212____ _____	F1 F2 F3 F4	Enter the associated value and press  . **NOTE** For TCPIP downloads, enter the VeriCentre IP address.

11	SYS MODE EDIT G 1 KEY *ZP KEY F2 18005551212 VALUE F3 ↑ ↓ ← →	F1 F2 F3 F4	Press the purple key below ↓ until an empty key displays. Repeat steps 8 - 10 until all parameters (keys) are entered. Press X twice to return to Sys Mode Menu 3. Press the purple key below ↑ to return to Sys Mode Menu 2.
12	SYS MODE MENU 2 DOWNLOAD F2 RAM FILES F3 FLASH FILES F4	F1 F2 F3 F4	From Sys Mode Menu 2, press [F2] to DOWNLOAD.
13	SYS MODE FILE FILE GROUP _1	F1 F2 F3 F4	Enter the GID number you want to download and press ↵. If prompted, enter the GID password.
14	SYS MODE DOWNLOAD G 1 FULL F3 PARTIAL F4	F1 F2 F3 F4	Press [F3] for a FULL download.
15	SYS MODE DOWNLOAD G 1 MODEM F2 COM1 F3 TCPIP F4	F1 F2 F3 F4	Press [F2] for a MODEM (telephone) download or press [F4] for a TCPIP (Ethernet) download. NOTE TCPIP will not appear as a download option unless the comm. module being used has a 10BaseT port. NOTE TCPIP downloads initiated from System Mode are not SSL secure.
16	SYS MODE DOWNLOAD G 1 **_____ DOWNLOADING NOW	F1 F2 F3 F4	As the download is progressing, the terminal displays SYS MODE DOWNLOAD - DOWNLOADING NOW and a series of 10 asterisks (one asterisk for each 10% completed) **----------. When all ten asterisks display, the download is complete and the terminal begins unzipping the application files (if the application was compressed) and initializing the application. NOTE Do not disturb the terminal while it is initializing. Wait until the main menu screen displays before proceeding.

Adding a New Application To the Terminal (Full Download)

The steps for adding a new application assume that VMAC and one or more applications are already loaded in the terminal and that you want to download an additional application into an empty GID.

1	VERIFONE O3750 Q50014A0 11/26/2002 Verix COPYRIGHT 1997 - 2002 VERIFONE ALL RIGHTS RESERVED	F1 F2 F3 F4	When the Operating System splash screen displays, press [F2] + [F4] simultaneously.
2	SYSTEM MODE ENTRY PASSWORD _____	F1 F2 F3 F4	Enter the System Mode password 1 [Alpha] [Alpha] 66831 and press  .
3	SYS MODE MENU 1 CONTRAST F2 CLOCK F3 RESTART F4 ↓	F1 F2 F3 F4	Press the purple key below ↓ to advance to Sys Mode Menu 3.
4	SYS MODE MENU 3 CONFIG INFO F2 EDIT F3 PASSWORDS F4 ↑ ↓	F1 F2 F3 F4	Press [F3] to edit the CONFIG.SYS file.
5	SYS MODE FILE FILE GROUP _4	F1 F2 F3 F4	To select a different GID, press  , enter the GID number you want to download, and press  .

6	SYSTEM MODE FILE GROUP 4 PASSWORD _____	F1 F2 F3 F4	Enter the password for the selected GID and press  . Typically, the default GID password is 1 [Alpha] [Alpha] 66831. The terminal displays FILE CONFIG.SYS.
7	SYS MODE EDIT G 4 FILE CONFIG.SYS_ _____	F1 F2 F3 F4	Press  to begin editing the file. **NOTE** In the upper right-hand corner of the display, the letter 'G' displays followed by the GID selected.
8	SYS MODE EDIT G 4 KEY _____ _____	F1 F2 F3 F4	The terminal displays KEY. The following parameters (keys) and their associated values must be entered to perform the download. ***ZP** Phone number or IP address of download system. ***ZA** Application name to download. Enter *MA for a multi-application download - valid for GID1. ***ZT** Terminal ID to download. ***ZR** Baud rate (6 = 14.4 bps, 9 = TCPIP) ***ZRESP** External modem connection response (16 = 14.4 bps, 19 = TCPIP). The following two parameters may be required depending upon the download system. Not required for TCPIP. ***ZINIT** Modem initialization string (ATV0\N0&D2). ***ZRESET** Modem reset string (AT&F0).
9	SYS MODE EDIT G 4 KEY *ZP_____ _____	F1 F2 F3 F4	Enter the key and press  .
10	SYS MODE EDIT G 4 VALUE 18005551212____ _____	F1 F2 F3 F4	Enter the associated value and press  . **NOTE** For TCPIP downloads, enter the VeriCentre IP address.

11	SYS MODE EDIT G 4 KEY *ZP KEY F2 18005551212 VALUE F3 ↑ ↓ ← →	F1 F2 F3 F4	Press the purple key below ↓ until an empty key displays. Repeat steps 8 - 10 until all parameters (keys) are entered. Press X twice to return to Sys Mode Menu 3. Press the purple key below ↑ to return to Sys Mode Menu 2.
12	SYS MODE MENU 2 DOWNLOAD F2 RAM FILES F3 FLASH FILES F4	F1 F2 F3 F4	From Sys Mode Menu 2, press [F2] to DOWNLOAD.
13	SYS MODE FILE FILE GROUP _4	F1 F2 F3 F4	Enter the GID number you want to download and press ↵. If prompted, enter the GID password.
14	SYS MODE DOWNLOAD G 4 FULL F3 PARTIAL F4	F1 F2 F3 F4	Press [F3] for a FULL download.
15	SYS MODE DOWNLOAD G 4 MODEM F2 COM1 F3 TCPIP F4	F1 F2 F3 F4	Press [F2] for a MODEM (telephone) download or press [F4] for a TCPIP (Ethernet) download. NOTE TCPIP will not appear as a download option unless the comm. module being used has a 10BaseT port. NOTE TCPIP downloads initiated from System Mode are not SSL secure.
16	SYS MODE DOWNLOAD G 4 **_____ DOWNLOADING NOW	F1 F2 F3 F4	As the download is progressing, the terminal displays SYS MODE DOWNLOAD - DOWNLOADING NOW and a series of 10 asterisks (one asterisk for each 10% completed) **----------. When all ten asterisks display, the download is complete and the terminal begins unzipping the application files (if the application was compressed) and initializing the application. NOTE Do not disturb the terminal while it is initializing. Wait until the main menu screen displays before proceeding.

Updating an Existing Application (Full Download)

The steps for updating an existing application require that you clear RAM and Flash memory for the GID you want to update.

1	VERIFONE O3750 Q50014A0 11/26/2002 Verix COPYRIGHT 1997 - 2002 VERIFONE ALL RIGHTS RESERVED	F1 F2 F3 F4	When the Operating System splash screen displays, press [F2] + [F4] simultaneously.
2	SYSTEM MODE ENTRY PASSWORD _____	F1 F2 F3 F4	Enter the System Mode password 1 [Alpha] [Alpha] 66831 and press  .
3	SYS MODE MENU 1 CONTRAST F2 CLOCK F3 RESTART F4 ↓	F1 F2 F3 F4	Press the purple key below ↓ to advance to Sys Mode Menu 2.
4	SYS MODE MENU 2 DOWNLOAD F2 RAM FILES F3 FLASH FILES F4 ↑ ↓	F1 F2 F3 F4	Press [F3] to clear RAM FILES.
5	SYS MODE RAM CLEAR GROUP _4 F2 CLEAR ALL FILES F3	F1 F2 F3 F4	Press [F2] to clear GID 1. **or** Enter the GID you want to clear, then press [F2]. **or** Press [F3] to clear all groups.

6	SYSTEM MODE FILE GROUP 4 PASSWORD _____	F1 F2 F3 F4	Enter the selected GID's password and press  . NOTE To clear all GIDs, you must enter the password for GID 1.
7	SYS MODE CONFIRM G 4 CANCEL F3 CONFIRM F4	F1 F2 F3 F4	Press [F3] to cancel or [F4] to confirm. Once the RAM files have been cleared, the terminal returns to Sys Mode Menu 2.
8	SYS MODE MENU 2 DOWNLOAD F2 RAM FILES F3 FLASH FILES F4 ↑ ↓	F1 F2 F3 F4	From Sys Mode Menu 2, press [F4] to clear FLASH FILES.
9	SYS MODE FLASH CLEAR GROUP _4 F2 CLEAR ALL FILES F3 DEFRAG 0 F4	F1 F2 F3 F4	Press [F2] to clear GID 1. **or** Enter the GID you want to clear, then press [F2]. **or** Press [F3] to clear all groups.
10	SYSTEM MODE FILE GROUP 4 PASSWORD _____	F1 F2 F3 F4	Enter the selected GID's password and press  . NOTE To clear all GIDs, you must enter the password for GID 1.
11	SYS MODE CONFIRM G 4 CANCEL F3 CONFIRM F4	F1 F2 F3 F4	Press [F3] to cancel or [F4] to confirm. As the Flash files are being cleared, the terminal displays: SYS MODE CLEAR CLEARING FLASH PLEASE WAIT This process may take a few seconds. After it is complete, the terminal returns to Sys Mode Menu 2.

12	SYS MODE MENU 2 DOWNLOAD F2 RAM FILES F3 FLASH FILES F4 ↑ ↓	F1 F2 F3 F4	From Sys Mode Menu 2, press [F4] to clear FLASH FILES. This step is not necessary if the Defrag value is 0.
13	SYS MODE FLASH CLEAR GROUP _1 F2 CLEAR ALL FILES F3 DEFRAG 43297 F4	F1 F2 F3 F4	Press [F4] to defragment Flash memory.
14	SYS MODE CONFIRM G 1 CANCEL F3 CONFIRM F4	F1 F2 F3 F4	Press [F3] to cancel or [F4] to confirm. As Flash memory is being defragmented, the terminal displays: SYS MODE CLEAR RECLAIMING FLASH PLEASE WAIT This process may take a few seconds. After it is complete, the terminal returns to Sys Mode Menu 2. Press the purple key below ↓ to advance to Sys Mode Menu 3.
15	SYS MODE MENU 3 CONFIG INFO F2 EDIT F3 PASSWORDS F4 ↑ ↓	F1 F2 F3 F4	Press [F3] to edit the CONFIG.SYS file.
16	SYS MODE FILE FILE GROUP _1	F1 F2 F3 F4	Press ↵ to edit GID 1. **or** Press ← and enter the GID you want to edit, then press ↵.

17	SYSTEM MODE FILE GROUP 4 PASSWORD _____	F1 F2 F3 F4	Enter the password for the selected GID and press ↵. The terminal displays FILE CONFIG.SYS.
18	SYS MODE EDIT G 4 FILE CONFIG.SYS_ _____	F1 F2 F3 F4	Press ↵ to begin editing the file. The first parameter displays.
19	SYS MODE EDIT G 4 KEY *ZA KEY F2 UEFT230 VALUE F3	F1 F2 F3 F4	Press ↵ to display the first parameter (key) and value. Verify each of the following parameters has the correct value. ***ZP** Phone number or IP address of download system. ***ZA** Application name to download. Enter *MA for a multi-application download - valid for GID1. ***ZT** Terminal ID to download. ***ZR** Baud rate (6 = 14.4 bps, 9 = TCPIP) ***ZRESP** External modem connection response (16 = 14.4 bps, 19 = TCPIP). The following two parameters may be required depending upon the download system. Not required for TCPIP. ***ZINIT** Modem initialization string (ATV0\N0&D2). ***ZRESET** Modem reset string (AT&F0). To modify a parameter value, perform steps 20 – 22.
20	SYS MODE EDIT G 4 KEY *ZA KEY F2 UEFT230 VALUE F3 ↑ ↓ ← →	F1 F2 F3 F4	Press the purple key below ↓ to advance to the download parameter. Review the value. If it is correct, press the down arrow until the next download parameter displays. If it is not correct, press [F3] to edit the CONFIG.SYS parameter.

21	SYS MODE EDIT G 4 VALUE UEFT230_____ _____	F1 F2 F3 F4	Press ← to clear the current value.
22	SYS MODE EDIT G 4 VALUE UEFT321_____ _____ ↑ ↓ ← →	F1 F2 F3 F4	Enter the correct parameter value and press ↵ Repeat steps 20 – 22 until all download parameters have been entered. Press X twice to return to Sys Mode Menu 3. Press the purple key below ↑ to return to Sys Mode Menu 2.
23	SYS MODE MENU 2 DOWNLOAD F2 RAM FILES F3 FLASH FILES F4	F1 F2 F3 F4	From Sys Mode Menu 2, press [F2] to DOWNLOAD.
24	SYS MODE FILE FILE GROUP _1	F1 F2 F3 F4	Enter the GID number you want to download and press ↵. If prompted, enter the GID password.
25	SYS MODE DOWNLOAD G 4 FILE GROUP _4 FULL F3 PARTIAL F4	F1 F2 F3 F4	Press [F3] for a FULL download.
26	SYS MODE DOWNLOAD G 4 MODEM F2 COM1 F3 TCPIP F4	F1 F2 F3 F4	Press [F2] for a MODEM (telephone) download or press [F4] for a TCPIP (Ethernet) download. NOTE TCPIP will not appear as a download option unless the comm. module being used has a 10BaseT port. NOTE TCPIP downloads initiated from System Mode are not SSL secure.

27	SYS MODE DOWNLOAD G 4 **_____ DOWNLOADING NOW	F1 F2 F3 F4	As the download is progressing, the terminal displays SYS MODE DOWNLOAD – DOWNLOADING NOW and a series of 10 asterisks (one asterisk for each 10% completed) **----------. When all ten asterisks display, the download is complete and the terminal begins unzipping the application files (if the application was compressed) and initializing the application. NOTE Do not disturb the terminal while it is initializing. Wait until the main menu screen displays before proceeding.

Updating the Parameters For an Existing Application (Partial Download)

Because the terminal is likely to be running multiple applications, it is critical to ensure the download is performed in the correct GID.

1	VERIFONE O3750 Q50014A0 11/26/2002 Verix COPYRIGHT 1997 - 2002 VERIFONE ALL RIGHTS RESERVED	F1 F2 F3 F4	When the Operating System splash screen displays, press [F2] + [F4] simultaneously.
2	SYSTEM MODE ENTRY PASSWORD _____	F1 F2 F3 F4	Enter the System Mode password 1 [Alpha] [Alpha] 66831and press  .
3	SYS MODE MENU 1 CONTRAST F2 CLOCK F3 RESTART F4 ↓	F1 F2 F3 F4	Press the purple key below ↓ to advance to Sys Mode Menu 3.
4	SYS MODE MENU 3 CONFIG INFO F2 EDIT F3 PASSWORDS F4 ↑ ↓	F1 F2 F3 F4	Press [F3] to edit the CONFIG.SYS file.
5	SYS MODE FILE FILE GROUP _1	F1 F2 F3 F4	If you want to download into GID1, press  . To select a different GID, press  , enter the GID number you want to download, and press  .
6	SYSTEM MODE FILE GROUP 1 PASSWORD _____	F1 F2 F3 F4	Enter the password for the selected GID and press  Typically, the default GID password is 1 [Alpha] [Alpha] 66831. The terminal displays FILE CONFIG.SYS.

7	SYS MODE EDIT G 4 FILE CONFIG.SYS_ _____	F1 F2 F3 F4	Press ↵ to begin editing the file. The first parameter displays.
8	SYS MODE EDIT G 4 KEY *ZA KEY F2 UEFT230 VALUE F3 ↑ ↓ ← →	F1 F2 F3 F4	Press ↵ to display the first parameter (key) and value. Verify each of the following parameters has the correct value. ***ZP** Phone number or IP address of download system. ***ZA** Application name to download. Enter *MA for a multi-application download - valid for GID1. ***ZT** Terminal ID to download. ***ZR** Baud rate (6 = 14.4 bps, 9 = TCPIP) ***ZRESP** External modem connection response (16 = 14.4 bps, 19 = TCPIP). The following two parameters may be required depending upon the download system. Not required for TCPIP. ***ZINIT** Modem initialization string (ATV0\N0&D2). ***ZRESET** Modem reset string (AT&F0). To modify a parameter value, perform steps 9 - 11.
9	SYS MODE EDIT G 4 KEY *ZA KEY F2 UEFT230 VALUE F3 ↑ ↓ ← →	F1 F2 F3 F4	Press the purple key below ↓ to advance to the download parameter. Review the value. If it is correct, press the down arrow until the next download parameter displays. If it is not correct, press [F3] to edit the CONFIG.SYS parameter.
10	SYS MODE EDIT G 4 VALUE UEFT230_____ _____	F1 F2 F3 F4	Press ← to clear the current value.
11	SYS MODE EDIT G 4 VALUE UEFT321_____ _____ ↑ ↓ ← →	F1 F2 F3 F4	Enter the correct parameter value and press ↵ Repeat steps 9 - 11 until all download parameters have been entered. Press X twice to return to Sys Mode Menu 3. Press the purple key below ↑ to return to Sys Mode Menu 2.

12	SYS MODE MENU 2 DOWNLOAD F2 RAM FILES F3 FLASH FILES F4	F1 F2 F3 F4	From Sys Mode Menu 2, press [F2] to DOWNLOAD.
13	SYS MODE FILE FILE GROUP _4	F1 F2 F3 F4	Enter the GID number you want to download and press  . If prompted, enter the GID password.
14	SYS MODE DOWNLOAD G 1 FILE GROUP _4 FULL F3 PARTIAL F4	F1 F2 F3 F4	Press [F4] for a PARTIAL download.
15	SYS MODE DOWNLOAD G 1 MODEM F2 COM1 F3 TCPIP F4	F1 F2 F3 F4	Press [F2] for a MODEM (telephone) download or press [F4] for a TCPIP (Ethernet) download. NOTE TCPIP will not appear as a download option unless the comm. module being used has a 10BaseT port. NOTE TCPIP downloads initiated from System Mode are not SSL secure.
16	SYS MODE DOWNLOAD G 4 **_____ DOWNLOADING NOW	F1 F2 F3 F4	As the download is progressing, the terminal displays SYS MODE DOWNLOAD - DOWNLOADING NOW and a series of 10 asterisks (one asterisk for each 10% completed) **----------. When all ten asterisks display, the download is complete.

Performing a Full Secure SSL Download

Secure downloads are encrypted using SSL technology in order to ensure the privacy of the data being transmitted. Secure downloads are initiated from the Comm Server menu instead of from System Mode Menu 2.

IMPORTANT Because SSL downloads are performed using the Comm Server application that resides in GID 1, you cannot perform a FULL multi-application download from GID 1 that includes the Comm Server application.

If you need to download the Comm Server application, VMAC, or any other application that resides in GID 1, you must download these applications from System Mode or perform a partial download from the Comm Server.

When performing a full download from GID 1, memory is not cleared (either manually by the user or automatically by the Comm Server application).

Secure SSL Downloads are only supported in Comm Server version 2.10 and above.

1	08/17/04 16:37 COMM SERVER SOFTPAY AGE VERIFY	F1 F2 F3 F4	From the VMAC menu, select the Comm Server application.
2	Config IP Ping Show IP Download	F1 F2 F3 F4	Press [F4] – Download.
3	Comm. Server Download Group ID: 1	F1 F2 F3 F4	Enter the GID you want to download and press  . If GID 1 selected, continue with Step 4; otherwise, skip to Step 5.
4	Comm. Server Download Single-App F3 Multi-App F4	F1 F2 F3 F4	Press [F3] for a single application download or press [F4] for a multi-application download. The multi-application download cannot include Comm Server.

5	Comm. Server Download Full F3 Partial F4	F1 F2 F3 F4	Press [F3] – Full. If GID 1 selected, skip to step 7; otherwise, continue with the next step.
6	Comm. Server Download Clear Target Group? Yes F3 No F4	F1 F2 F3 F4	Press [F3] to clear the selected GID and coalesce Flash or press [F4] to retain the application in the selected GID. **NOTE** If performing a full download into GID 1, memory will not be cleared.
7	Comm. Server Download SSL F3 TCPIP F4	F1 F2 F3 F4	Press [F3] - SSL to perform a secure SSL download.
8	Comm. Server Download GID: 01 Sec: SSL *ZP=SSL.TEST.DOWNLOAD *ZA=*MA *ZT=12345678 Edit Start	F1 F2 F3 F4	Verify the download parameters: *ZP, *ZA, and *ZT. If one or more of these parameters is incorrect, press [F3] - Edit. Otherwise, press [F4] - Start. To edit a parameter, press ← to delete the current parameter value, then enter the correct parameter value. When all parameters have been verified and/or updated, press [F4] – Start.
9	Comm. Server Download ***_ _ _ _ _ _ _ File:SOTPAY.ZIP File Count: 1 Drive: F Group ID: 2	F1 F2 F3 F4	As the download is progressing, the terminal displays a series of 10 asterisks (one asterisk for each 10% completed), as well as, the name of the file being downloaded, the number of files being download, the drive and group ID into which the current file is being downloaded. **NOTE** Once the download has started, you will not be able to press the X key to abort the download. When the download is complete, the terminal restarts and coalesces Flash.

Performing a Partial Secure SSL Download

Secure downloads are encrypted using SSL technology in order to ensure the privacy of the data being transmitted. Secure downloads are initiated from the Comm Server menu instead of from System Mode Menu 2.

NOTE Secure SSL Downloads are only supported in Comm Server version 2.10 and above.

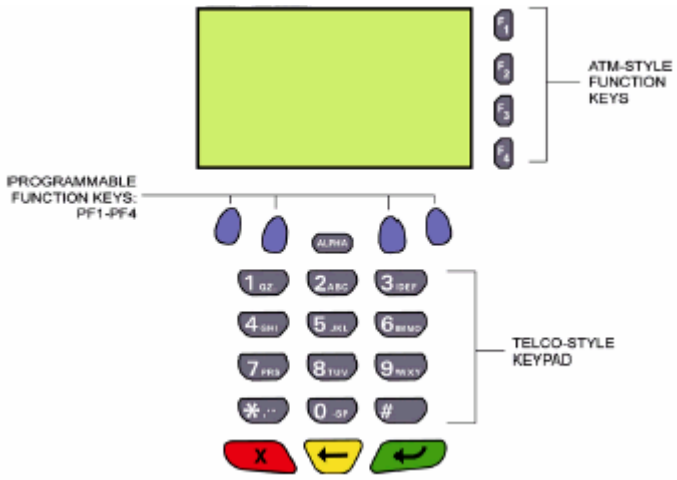
1	08/17/04 16:37 COMM SERVER SOFTPAY AGE VERIFY	F1 F2 F3 F4	From the VMAC menu, select the Comm Server application.
2	Config IP Ping Show IP Download	F1 F2 F3 F4	Press [F4] - Download.
3	Comm. Server Download Group ID: 1	F1 F2 F3 F4	Enter the GID you want to download and press  . If GID 1 selected, continue with Step 4; otherwise, skip to Step 5.
4	Comm. Server Download Single-App F3 Multi-App F4	F1 F2 F3 F4	Press [F3] for a single application download or press [F4] for a multi-application download.
5	Comm. Server Download Full F3 Partial F4	F1 F2 F3 F4	Press [F4] – Partial.

6	Comm. Server Download SSL F3 TCPIP F4	F1 F2 F3 F4	Press [F3] - SSL to perform a secure SSL download.
7	Comm. Server Download GID: 01 Sec: SSL *ZP=SSL.TEST.DOWNLOAD *ZA=*MA *ZT=12345678 Edit Start	F1 F2 F3 F4	Verify the download parameters: *ZP, *ZA, and *ZT. If one or more of these parameters is incorrect, press [F3] - Edit. Otherwise, press [F4] - Start. To edit a parameter, press ← to delete the current parameter value, then enter the correct parameter value. When all parameters have been verified and/or updated, press [F4] – Start.
8	Comm. Server Download ***_ _ _ _ _ _ _ File:SOTPAY.ZIP File Count: 1 Drive: F Group ID: 2	F1 F2 F3 F4	As the download is progressing, the terminal displays a series of 10 asterisks (one asterisk for each 10% completed), as well as, the name of the file being downloaded, the number of files being download, the drive and group ID into which the current file is being downloaded. **NOTE** Once the download has started, you will not be able to press the X key to abort the download. When the download is complete, the terminal restarts.

Terminal Keys

The Omni 3750 keypad consists of a 12-key telco-style keypad, three color-coded keys below the keypad, the [Alpha] key above the keypad, four ATM-style function keys (F1, F2, F3, and F4) to the right of the display, and four programmable function (PF) keys directly above the keypad.

Using these keys, you can perform all data-entry task. Where a specific key is mentioned, it appears within square brackets (for example, the [Alpha] key). The function keys allow you to navigate though system mode menus and select specific operations.



The Terminal Keypad

The keypad is a 13-key arrangement, consisting of a 12-key Telco-style keypad and the ALPHA key. Using the keypad, you can enter up to 50 ASCII characters, including 20 special characters.

Cancel Key

Pressing the [Cancel] key in normal mode—when the terminal's application is loaded and running—usually has the same effect as pressing the [Esc] (escape) key on a PC. That is, it terminates the current function or operation.

In system mode, use cancel to perform a variety of functions. The most common use of cancel in system mode is to exit a system mode submenu and return to the main system mode menu. The specific effect of pressing the [Cancel] key depends on the currently active system mode menu.

Backspace Key

In normal mode, the backspace key is commonly used to delete a number, letter, or symbol on the terminal's display screen. Press backspace one time to delete the last character typed on a line.

To delete additional characters, moving from right to left, press backspace once for each character or hold down backspace to delete all characters on a line. In system mode, the specific effect of pressing backspace depends the currently active system mode menu.

Enter Key

In normal mode, the enter key is generally used the same as the enter key on a PC, that is, to end a procedure, confirm a value or entry, answer “Yes” to a query, or select a displayed option.

In system mode, press the enter key to begin a selected procedure, step forwards or backwards in a procedure, and confirm data entries. The specific effect of the enter key depends on the currently active system mode menu.

[ALPHA] Alpha Key

In normal mode, the [Alpha] key enables you to enter one of the two or more characters or symbols assigned to individual keys on the 12-key telco-style keypad. Use the [Alpha] key to enter up to 50 different ASCII characters through the following procedure:

1. Press the key on the 12-key keypad that shows the letter or symbol you want (e.g., press 2 to type 2, A, B, or C). The number (1-9 or 0) or the symbol (* or #) you pressed now displays.
2. Press [Alpha] once to display the first letter (e.g., 2 [Alpha] displays the letter A).
3. Continue pressing [Alpha] as many times as required to display the desired character (e.g., press 2 to display the number 2; press [Alpha] once to display the letter A, twice to display B, or three times to display C.

Key To Press	Without Pressing [Alpha]	Press [Alpha] One Time	Press [Alpha] Two Times	Press [Alpha] Three Times
1 QZ.	1	Q	Z	.
2 ABC	2	A	B	C
3 DEF	3	D	E	F
4 GHI	4	G	H	I
5 JKL	5	J	K	L
6 MNI	6	M	N	O
7 PRS	7	P	R	S
8 TUV	8	T	U	V
9 WXY	9	W	X	Y
0 -SP	0	- [dash]	[space]	+ [plus sign]
*,’”	* [asterisk]	, [comma]	‘ [single quote}	“ [double quote]
#	#	! [exclamation]	: [colon]	; [semi-colon]
	The # key is used to display the following additional characters. Just continue to press the [Alpha] key until the desired character displays.			
	@ [At symbol]	= [equal sign]	& [ampersand]	/ [forward slash]
	\ [back slash]	% [percent sign]	$ [dollar sign]	_ [underscore]

Programmable Function Key Descriptions

The row of four PF keys directly above the keypad from left-to-right are referred to as PF1, PF2, PF3, and PF4. These keys can be assigned application-specific functions. Because such functions are often unique and can vary greatly between applications, they are not discussed in this manual.

The PF keys are also use to toggle through system mode menus. These keys are functioning when arrows appear in the display screen above the associated key, indicating the keys can be used as follows:

PF1 = Move to the previous menu or screen

PF2 = Move to the next menu or screen

PF3 = Scroll left

PF4 = Scroll right

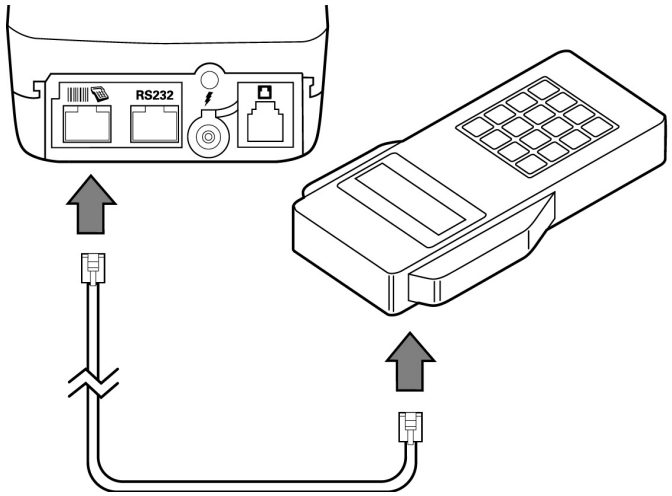
This page intentionally left blank.

Installing Peripherals

If necessary, insert the small modular plug on one end of the PIN pad cable into the PIN pad's modular jack. For a bar code wand, insert the RJ45-type connector into the PIN pad serial port on the back panel.

Connecting a PIN Pad

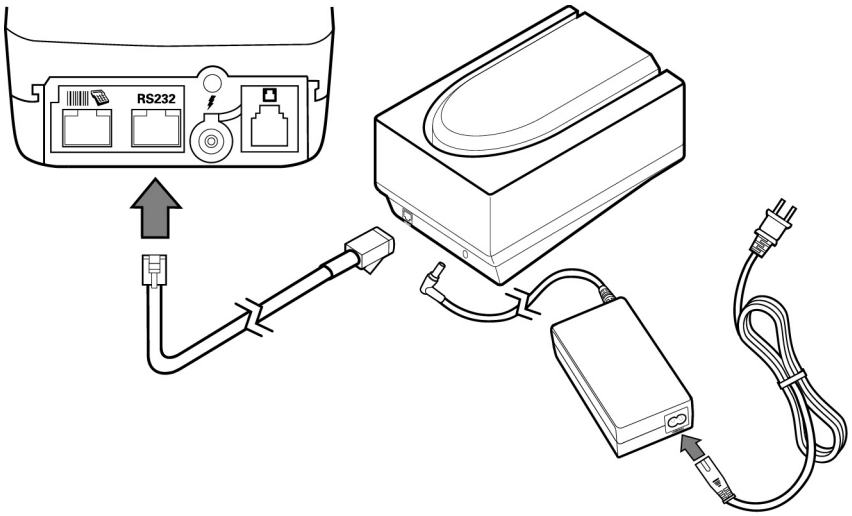
1. If installing a PIN pad 1000, position and insert the grommet to secure the cable connection.
2. Insert the larger RJ45-type connector on the other end of the PIN pad cable into the PIN pad serial port on the terminal's back panel.



Connecting a Check Reader

The Omni 3750 terminal supports the CR 600 and CR 1000i VeriFone check readers. Refer to the following diagram for an example of a peripheral connection to an RS232 port.

CAUTION Check readers require a separate power source. Before connecting a check reader or similar device, remove the power cord from the back of the terminal and be sure the LED is not lit.



This page intentionally left blank.

Hardware Features

Feature	Description
Microprocessor	Motorola 68000.
Memory	2 Mb RAM, 2 Mb Flash (standard configuration). Some older units may have 512K or 1Mb RAM, and 2 Mb Flash.
Display	128 x 64 pixel LCD with backlighting; supports 8 lines x 21 characters, including graphics.
Keypad	3 x 4 numeric, 8 soft function keys, 4 ATM-style keys.
Ports	One telco, two RS-232 ports.
Mag Stripe Reader	Bi-directional, triple-track (1, 2, and 3).
Modem	Bell 103/212a, CCITT V.21/V.22/V.22 bis, 300/1200/2400/14400 bps, synchronous and asynchronous. NOTE The 14.4 high-speed modem is indicated by the letters H S over the telco port. If these letters are not present, it is a 2400 baud modem. 
Ethernet Module	10BaseT Ethernet with standard RJ45 connection. Supports general Internet protocols such as, FTP. TCP/IP, UDP, DNS, SMTP, POP3, MIME, HTTP, and Telnet. Supports LAN Internet protocols, such as ARP, ICMP, and DHCP. Utilizes SSL.
Printer	Integrated thermal printer with graphics capabilities and clam shell design with drop-in paper loading, 12.5 lines per second, 32/42 columns; standard roll paper 58 mm (2.25 in.) x 25M, single ply.
Smart Card Reader	Primary Smart Card Reader EMV-compliant ISO 7816, 3V or 5V synchronous and asynchronous cards. SAM Card Reader (optional) 2 or 4 Security Access Modules (SAMs). NOTE The Omni 3740 is identical to the Omni 3750 except that it does not have a smart card reader.
Integrated PIN pad	Supports both master session and DUKPT key management schemes, 3DES encryption, PED certified.

This page intentionally left blank.

Glossary

10BaseT One of several adaptations of the Ethernet (IEEE 802.3) standard for Local Area Networks (LANs). The 10Base-T standard (also called *Twisted Pair Ethernet*) uses a twisted-pair cable with maximum lengths of 100 meters. Cables in the 10Base-T system connect with RJ-45 connectors. The 10Base-T system operates at 10 Mbps and uses baseband transmission methods.

Access code A code number dialed to gain access to a telephone line, such as dialing the number 9 to reach an outside line. Also known as a PBX code.

Application ID An alphanumeric name that uniquely identifies an application program to the VeriCentre download system. The application ID is stored in the *ZA parameter.

Application program The ordered set of programmed instructions by which a computer performs an intended task or series of tasks.

ARP Address Resolution Protocol is a protocol concerned with mapping nodes names to IP addresses. It equates logical and physical device addresses.

ASCII Abbreviation for American Standard Code for Information Interchange. A 7-bit code (with no parity bit) that provides a total of 128 bit patterns. ASCII codes are widely used for information interchange in data processing and communication systems.

Back-to-back application download The process of copying the entire memory image of one terminal (including batch records) to another terminal via an RS232 cable. Both the memory size and operating system versions must be identical on each terminal. Also referred to as unit-to-unit download.

Bar code Optical binary code imprinted on merchandise in retail stores. To support specific applications, an optional bar code reader can be attached to the Omni 3750 to read and process bar codes.

Bar code reader A pencil or wand-shaped optical scanner used to read bar codes. To read the code, you drag the tip of the bar code reader across the length of the bar code, in a left-to-right or right-to-left direction.

Baud The number of times per second that a system, especially a data transmission channel, changes state. The state of a system may represent a bit, digit, or symbol. For a POS terminal, the baud rate indicates the number of bits per second that are transmitted or received by the terminal's serial ports and modem.

Bit Short for binary digit. Either 0 or 1 in the binary number system. The bit is the smallest unit of storage/information in any binary system within a computer

Block A collection of data units such as words, characters, or records (generally more than a single word) stored in adjacent physical positions in memory or on a peripheral storage device.

A block is treated as a single unit for reading, writing, and, other data communication operations.

Boot loader Also called a bootloader or bootstrap loader. A short program, stored in flash EPROM, that allows the terminal to continue operating during an operating system download procedure, until the new operating system is downloaded into terminal memory.

Buffer A temporary storage area in memory for data. Normally used to accommodate the difference in the rate at which two devices can handle data during a transfer.

Byte A term developed to indicate a measurable number of consecutive binary digits that are usually operated on as a unit. For the Omni 3750, a byte consists of eight bits. See Bit.

Calendar/clock chip A microchip inside the Omni 3750 terminal that tracks the current date and time.

Card reader Also called magnetic stripe card reader. The slot on the right side of the Omni 3750 terminal that automatically reads the Track 1, 2, or 3 data stored in the magnetic stripe on the back of a specially-encoded card when you swipe the card through the slot.

Carrier Usually, an analog signal that is selected to match the characteristics of a particular transmission system. The carrier signal on a phone line is modulated with frequency or amplitude variations to allow a terminal to transmit or receive data using a modem. A carrier signal transmits data from a host computer to an Omni 3750 terminal over an analog telephone line.

Certificate Also called a digital certificate. A digital document or file that attests to the binding of a public key to an individual or entity, and that allows verification that a specific public key does in fact belong to a specific individual.

Character An element of a given character set. The smallest unit of information in a record. A letter, numeral, or other symbol to express information.

CONFIG.SYS editor A keyed file editor that allows you to create new records or modify existing records stored in a keyed file, such as CONFIG.SYS. See CONFIG.SYS file.

CONFIG.SYS file A special keyed file that is stored in terminal memory that contains system and application configuration parameters. Each record in a CONFIG.SYS file is identified by an alpha-numeric key.

In the Omni 3750 file system, there is one password-protected CONFIG.SYS file per file group (Groups 1-15). You can modify CONFIG.SYS records using the CONFIG.SYS editor.

CPU Abbreviation for central processing unit. The principal operating part of a computer system that controls the interpretation and execution of instructions stored in memory.

Data Information prepared, often in a particular format, for a specific purpose and used by an application program. In the Omni 3750 terminal, application files and data files can be stored in RAM or Flash memory.

Data entry The process of using a keyboard, card reader, or other device to input data directly into a system.

Data packet A group of bits of fixed maximum size and well-defined format that is switched and transmitted as a composite whole through a packet switching network. Any message that exceeds the maximum size is partitioned and carried as several packets. Data packets are formed by the controller in the sending data terminal and the data is extracted and reassembled by the controller at the receiving end.

Dedicated line A leased or private telephone line that is used for a particular communications purpose, such as to connect an Omni 3750 terminal to a host computer. See Leased line.

Default A value, parameter, option, or attribute that is assigned by the program or system when another has not been assigned by the user.

Delete To remove a record, field, or item of data.

DES Data Encryption Standard is an encryption standard defined by the U.S. government. DES encrypts data by breaking into 64-bit blocks of data and using a 56-bit key. DES is a symmetric algorithm since the keys used to encrypt and decrypt the data are identical. Single DES has a key space (largest number of different cipher texts that can be produced from one plain text) of $2^{56.}$ Triple DES provides much greater security since it has a key space of 2^{112}.

DHCP Dynamic Host Configuration Protocol enables enable individual computers on an IP network to extract their configurations from a server (the 'DHCP server') or servers, in particular, servers that have no exact information about the individual computers until they request the information. The overall purpose of this is to reduce the work necessary to administer a large IP network. The most significant piece of information distributed in this manner is the IP address.

Diagnostics Techniques employed for detection and isolation of malfunctions and errors in programs, systems, and devices. In a diagnostic test, a program or routine is run to detect failures or potential failures. These tests and routines help detect and isolate problems in a terminal or peripheral device.

Dial-up line A standard public telephone line. The switching equipment on a dial-up line requires that a party dial the other party before a connection can be made.

Direct download The process of transferring files and/or data from a download computer to a terminal over a serial cable connection and in a local, as opposed to a telephone download.

Display The small screen on the Omni 3750 terminal that shows numerals, characters, symbols, and graphics. Used to display system and application prompts and messages.

DNS Domain Name System is a distributed database system that provides name-to-address mapping to client applications. DNS servers maintain databases that contain hierarchical name structures of the various domains in order to use logical names for device identification. For example: www.verifone.com is translated to an IP address of 66.216.97.90.

Download To transfer files or data from a host computer or sending terminal over a communication link to a receiving terminal.

DSL Digital Subscriber Line is a technology for bringing high-bandwidth information to homes and small businesses over ordinary copper telephone lines. DSL provides data at rates up to 6.1 megabits (millions of bits) per second enabling continuous transmission of motion video, audio, and even 3-D effects. More typically, individual connections will provide from 1.544 Mbps to 512 Kbps downstream and about 128 Kbps upstream. A DSL line can carry both data and voice signals and the data part of the line is continuously connected.

DTMF Dual-tone multi-frequency. The ordinary dial tone on a telephone line.

EMV The Integrated Circuit Card (ICC) Specification for Payment Systems developed by EuroPay, MasterCard, and Visa that defines the minimum functionality required of credit and debit chip cards and terminals to ensure correct operation and inter-operability.

Ethernet A local-area network (LAN) architecture developed by Xerox Corporation in cooperation with DEC and Intel in 1976. Ethernet uses a bus or star topology and supports data transfer rates of 10 Mbps. The Ethernet specification served as the basis for the IEEE 802.3 standard, which specifies the physical and lower software layers. Ethernet uses the CSMA/CD access method to handle simultaneous demands. It is one of the most widely implemented LAN standards.

File authentication A process through which one proves and verifies the origin of a file, the identity of the sender, and the integrity of the information it contains.

Firmware System software, including the operating system, boot loader, default display font, and system messages, stored in terminal flash memory.

Flash memory An area of non-volatile memory where files can be stored. The Omni 3750 also has a RAM-based file system. Files can be stored in the RAM (drive I:) or in flash (drive F:) memory area of any file group (Groups 1–15).

FTP File Transfer Protocol is used to transfer files between network nodes, as well as, initiate processes on the remote host.

GID Numeric identifier (0 – 15) assigned to each file group.

Host computer 1) the primary or controlling computer in a multiple computer operation, 2) a computer running VeriCentre used to configure and download applications and parameters to a terminal, 3) a computer used to process transactions that originate from a distributed network of POS terminals.

HTTP Hypertext Transfer Protocol is the set of rules for transferring files (text, graphic images, sound, video, and other multimedia files) on the Internet. HTTP is an application protocol that runs on top of the TCP/IP suite of protocols (the foundation protocols for the Internet).

ICMP Internet Control Message Protocol is a protocol used with IP to augment error handling and control. It works at the network layer and is concerned with connection services.

Input The process of entering data into a processing system or a peripheral device such as a terminal, or the data that is entered.

Interface A common boundary between two systems, devices, or pro-grams.

Keyed file record ASCII data, or variables, stored in the terminal's CONFIG.SYS file(s). A keyed file record consists of two parts: a search key that identifies the record, and the data or variable stored in the record. See CONFIG.SYS file.

Keypad A small keyboard or section of a keyboard containing a smaller number of keys, generally those used in simple calculators. The 16-key core keypad of the Omni 3750 terminal is used to enter data and perform operations.

Leased line A private telephone line leased from the phone company. See Dedicated line.

Line cord A telephone-type cord with modular plugs on each end to connect the terminal to a dial-up telephone line.

Local functions Operations performed at the terminal only and not in interaction with a host computer. Local functions, such as internal diagnostics, are performed in system mode.

Manual transaction A transaction involving the manual entry of account information from the terminal keypad instead of automatic entry of the information from a reading device, such as a magnetic stripe card reader.

Memory A device or medium that can retain information for subsequent retrieval. The term is

most frequently used to refer to the internal storage of a computer (or a terminal) that can be directly addressed by operating instructions. In the Omni 3750, files can be stored in battery-backed RAM or in non-volatile Flash memory.

Messages Words and symbols appearing on the display screen which inform the user of the terminal of the result of a process, or if an error has occurred. The term “prompt” is used when the displayed message is requesting the user to enter information or to select an option.

Microprocessor A computer processor on a microchip. A microprocessor is designed to perform arithmetic and logic operations that make use of small number-holding areas called *registers*. Typical microprocessor operations include adding, subtracting, comparing two numbers, and fetching numbers from one area to another. These operations are the result of a set of instructions that are part of the microprocessor design. When the computer is turned on, the microprocessor is designed to get the first instruction from the basic input/output system (BIOS) that comes with the computer as part of its memory. After that, either the BIOS, or the operating system that BIOS loads into computer memory, or an application progam is "driving" the microprocessor, giving it instructions to perform.

MIME Multi-Purpose Internet Mail Extensions is an extension of the original Internet e-mail protocol that lets people use the protocol to exchange different kinds of data files on the Internet: audio, video, images, application programs, and other kinds, as well as the ASCII text handled in the original protocol, the Simple Mail Transport Protocol (SMTP).

Modem Modulator/demodulator. A device that converts a digital bit stream into an analog signal to transmit over an analog communication channel (modulation), and converts incoming analog signals into digital signals (de-modulation).

The Omni 3750 terminal’s internal modem allows communication with a host computer over a dial-up telephone line.

Non-volatile memory A memory or storage medium that retains data in the absence of power so that the data is available when power is restored. In the Omni 3750, application files and data files can be stored in battery-backed RAM or non-volatile Flash memory, according to the requirements of the application.

Normal mode The operating mode for normal transaction processing. The main application (downloaded and authenticated) starts and displays an application prompt, indicating that the terminal is in normal mode. In this mode, the terminal is ready to process transactions. See System mode.

Packet A group of bits of fixed maximum size and well-defined format that is switched and transmitted as a composite whole through a packet switching network. Any message that exceeds the maximum size is partitioned and carried as several packets.

Packet-switched networks Networks of computers or computing devices in which communication resources are allocated dynamically on a variety of levels to multiple communicating entities. Messages between entities are partitioned into segments, or packets, with a fixed maximum size.

Parameter A variable that is usually assigned a constant value for a specific subroutine, procedure, or function. Parameters stored in terminal memory or in the CONFIG.SYS file(s), enable a host or download computer to identify to terminal configuration.

Password A group of characters that identify a user to the system so that they can gain access to the system or part of that system. Passwords are used to ensure the security of computer systems by regulating the amount of access freedom. The password used to enter system mode is called the system mode password. In the Omni 3750 system, each file group (Groups 1–15) has its own password.

PED PIN Entry Device. Visa and MasterCard have specified a set of physical and logical security standards that PIN entry device manufacturers must meet in order to be considered PED-compliant.

PC Abbreviation for personal computer. Usually, PC refers to an IBM-compatible personal computer.

Peripheral device In a computer system, any equipment that provides the processing unit with outside communication. Typical peripheral devices for a POS terminal include PIN pads, bar code wands, and check readers.

PKI Public Key Infrastructure describes the total infrastructure used to deliver public key applications. These applications use RSA cryptography to protect confidential information over the Internet.

POP3 Post Office Protocol is a protocol used to download email from an SMTP email server to a network client. See SMTP.

Port An opening or connection that provides electrical or physical access to a system or circuit. Also, a connection point with associated control circuitry that allows I/O devices to be connected to the internal bus of a micro-processor.

POS terminal A terminal used at the point of sale, which is usually at a merchant site where a customer pays for goods or services received. Information concerning the sale can be entered into the terminal and transmitted to a remote host computer for verification and processing.

Power pack A unit for transforming and converting electrical power from one AC voltage level to another AC voltage level, or from AC to DC, for electronic devices.

Prompt A short message, sent from a process to a user, indicating that the process expects the user to present fresh data. For example, a prompt appears on the terminal display asking the user to enter specific information. See Messages.

Protocol An agreement that governs the procedures used to exchange information between cooperating entities. For example, protocols govern the format and timing of messages exchanged between devices in a communication system, such as between a terminal and a host computer.

PTID Permanent terminal ID. An optional identifier that can be permanently assigned to a terminal at the factory, upon customer request. The PTID has two parts: a 2-digit manufacturer ID (12 for VeriFone) and a unique 8-digit terminal ID. If no PTID is assigned, the default PTID value is 1200000000.

Pulse dialing A method of telephone dialing that specifies a phone number by the number of electrical pulses sent.

RAM Random-access memory. The type of memory in which storage locations are addressable and can therefore be accessed in any order. In the Omni 3750 terminal, the RAM (or SRAM) is commonly used to store applications and temporary data generated during a transaction.

The RAM is battery-backed, meaning that if power is turned off, data stored in this area of volatile memory is not lost. Application files and data can also be stored in the non-volatile flash memory system. By default, files downloaded to the terminal are stored in the RAM of the target file group(s). The RAM file system is called drive I:. See Flash memory.

Remote host computer A host computer connected to a Omni 3750 terminal over a dial-up telephone line to download files or data, or to process transactions. The opposite of remote is local.

RS232 Also RS-232C. A widely used standard interface that covers the electrical connection between data communication equipment, such as a modem, and data terminal equipment, such as a microcomputer or computer terminal.

The RS232 interface standard was developed by the EIA (Electronic Industries Association) and is essentially equivalent to the CCITT's V.24 inter-face.

Scroll To move all or part of the information displayed on a screen up or down, left or right, to allow new information to appear. For the Omni 3750 text that does not fit entirely within the display area can be scrolled to the left or right using the pound (#) and asterisk (*) keys.

Search key Also called key. In the Omni 3750, a short character string used by an application to identify a keyed file record stored in the CONFIG.SYS file(s).

Serial port A connection point through which digital information is transferred one digital bit at a time. Same as serial interface. The Omni 3750 terminal has one serial port, labeled RS232. The main serial port on a download computer is usually identified as COM1.

Signature file A digital file with the filename extension *.p7s generated in an industry-standard format by the file signing tool, FILESIGN.EXE. The output of the file signing tool is a signature file in an industry-standard format.

SMTP Simple Mail Transfer Protocol is a protocol for routing email messages. SMTP does not provide a user interface for sending and receiving messages, but many Internet email applications interface with it.

SSL. The Secure Sockets Layer (SSL) is a commonly-used protocol for managing the security of a message transmission on the Internet. SSL uses a program layer located between the

Internet's Hypertext Transfer Protocol (HTTP) and Transport Control Protocol (TCP) layers. The "sockets" part of the term refers to the sockets method of passing data back and forth between a client and a server program in a network or between program layers in the same computer. SSL uses the public-and-private key encryption system from RSA, which also includes the use of a digital certificate

Subroutine A software routine that can be part of another routine. When a main routine calls a subroutine, program control is transferred to the sub-routine. When the subroutine is completed, control reverts to the instruction in the main routine immediately following the subroutine call.

Swipe The action of sliding a magnetic stripe card through a terminal card reader. The Omni 3750 card reader has a bi-directional swipe direction. The user must hold the card so that the magnetic stripe is faces in and towards the keyboard.

System Mode For the Omni 3750, system mode temporarily disables normal mode operations, allowing you to perform local functions such as downloads, diagnostics, and other operations that cannot be performed while the application program is running.

At startup, the terminal displays a copyright notice screen that shows the version of Omni 3750 system firmware stored in terminal flash memory, the date it was loaded into the terminal, and the copyright notice. This screen appears for three seconds. To enter system mode, simultaneously press the [F2] and [F4] keys during this three-second period. See Local functions and Normal mode.

System mode password A unique set of characters entered by the user to access the system mode local functions of the terminal. A default password is supplied with each terminal. For the Omni 3750 terminal, the default system password is: 1 [Alpha] [Alpha] 66831.

To prevent unauthorized access, change the default password to a confidential password on terminal deployment. Store the new password in a safe place, as it is impossible to restore the terminal default password without sending the unit to VeriFone for service.

TCP/IP TCP/IP (Transmission Control Protocol/Internet Protocol) is the basic communication language or protocol of the Internet. TCP/IP is a two-layer program. The higher layer, Transmission Control Protocol, manages the assembling of a message or file into smaller packets that are transmitted over the Internet and received by a TCP layer that reassembles the packets into the original message. The lower layer, Internet Protocol, handles the address part of each packet so that it gets to the right destination. Each gateway computer on the network checks this address to see where to forward the message. Even though some packets from the same message are routed differently than others, they'll be reassembled at the destination.

Telephone download The process of transferring an application program and/or data from a remote host or download computer to a terminal over a telephone line.

Telephone jack Also, telephone line wall jack. Modular-type sockets for connecting telephone line cords. The Omni 3750 terminal has a TELCO RJ11-type telephone jack on the back panel used for a direct connection to a telephone line wall jack.

Telephone line The standard telephone wiring connecting your phone or terminal to a local or private telephone company.

Telnet A protocol used for terminal emulation. It enables users to access host-based applications by emulating one of the host's terminals.

Terminal Any device capable of sending and receiving data over a data link, such as a telephone line or a RS-232 cable. Some terminals, such as the Omni 3750, can print receipts and display information and graphics on a screen.

Terminal ID An alphanumeric code that identifies a terminal to a download computer. In this way, the download computer can determine what data or application programs to download to that terminal. The application ID is stored in the *ZT parameter.

Tone dialing Also called touch-tone dialing. A method of telephone dialing that uses different pitched tones to specify a phone number. See also DTMF.

Track 1, 2, or 3 data Information stored on tracks 1, 2, or 3 of a credit or debit card magnetic stripe, which can be read by a magnetic card reader device, such as the one that is integrated in the Omni 3750 terminal.

Transaction An exchange of data resulting in a transfer of goods, services, value, and/or

information between two parties.

UDP User Datagram Protocol is a connection-less protocol that transports datagrams but does not acknowledge their receipt. It is typically used as a broadcast protocol where message receipt acknowledgement is not required.

VAP Value-added Application Provider.

Variable A string of characters that denotes some value stored within the computer and that can be changed during execution. A variable may be internal to a program, in which case it is held in memory, or external if the program must perform an input operation to read its value. See Parameter.

Volatile memory A type of memory where the contents are destroyed if the power supply to the memory is interrupted.

When volatile memory, such as SRAM, is used for crucial applications, it is often back up by battery-supplied power. Compare with Non-volatile memory.

This page intentionally left blank.

Terminal Specifications

Power

24 V DC; 1.5 A

DC Power Pack

For non-switching power supplies:

- UL, ITE listed, Class 2 power supply
- Input rated: 110 - 127V AC, 60 Hz
- Output rated: 24V DC 1.5 A

For switching power supplies:

- UL, ITE listed, Class 2, switching power supply
- Input rated: 100 - 240 V AC, 50/60 Hz
- Output rated: 24 V DC, 1.5 A
- Barrel connector polarity:

Temperature

- Operating temperature: 0 °to 40 °C (32 °to 104 °F)
- Storage temperature: -18 °to + 66 °C (0 °to 150 °F)
- Relative humidity: 15% to 90%; no condensation

External Dimensions

- Length: 210 mm (8.3 in)
- Width: 104 mm (4.1 in)
- Depth: 83 mm (3.3 in)
- Weight: 760 gms (1.675 lb)

Weight

- Terminal unit weight: 1.28 kg (2.82 lb)
- Shipping weight: 3.26 kg (7.19 lb)

The shipping weight includes: shipping carton, terminal, power pack and cable, telephone line cable, one Omni 37xx Certifications and Regulations, and one Omni 37xx Quick Installation Guide.

This page intentionally left blank.

Accessories + Documentation

VeriFone produces accessories and documentation for the Omni 3750 as listed below. When ordering, refer to the part number to the left of the product description. Call 1-800-VERIFON or go to the VeriFone Online Store at http://www.store.verifone.com/products/supplies/index.html

Power Pack	CPS05791-3A	DC power pack (universal)
	21973-01	Power cable (US)
Thermal Printer Paper	CRM0039	High-grade thermal printer paper, 2.25-inch, 82-feet length; single roll
	CRM0039-01	CRM0039 in 30-roll bulk package
	CRM0040	High-grade thermal printer paper, 2.25-inch, 108 feet length; single roll
Paper Roll Spindle	02117-03	Plastic spindle for 58-mm (2.25-inch) rolls of thermal paper
VeriFone Cleaning Kit	02746-01	Cleaning kit
Download Cables	05651-xx	MOD10-MOD10 (terminal-to-terminal)
	26263-xx	MOD10-PC DB25F (terminal-to-PC)
	26264-xx	MOD10-PC DB9F (terminal-to-PC)
Cables for Optional Peripherals	07041-xx	MOD10-MDIN9 (CR 600/CR 1000i check readers; P250/P355/P900 external printers)
	26519-xx	MOD10-MD8M (P950 external printers)
	07042-xx	MOD10-4P4C (all VeriFone PIN pads)
Telephone Line Cord	00124-17	7-foot telephone line cord, black, with modular RJ11-type connectors
Wire Clip	07826	Wire clip
Swivel Stand	07326-01	Swivel stand
SAM Reader	07839-01	2 SAM reader
	07839-02	4 SAM reader
Comm Modules	22725-02	Ethernet only
	22669-01	14.4 modem only
	07943-01	Dual-comm (Ethernet + 14.4 modem)
Documentation	22398	Omni 3750 Quick Installation Guide
	19733	Verix Operating System Programmer's Manual
	22399	Omni 37xx Series Installation Guide
	22410	Omni 37xx Privacy Shield Quick Installation Guide
	22411	Omni 37xx Swivel Stand Quick Installation Guide
	19733	Verix Programmer's Manual

This page intentionally left blank.