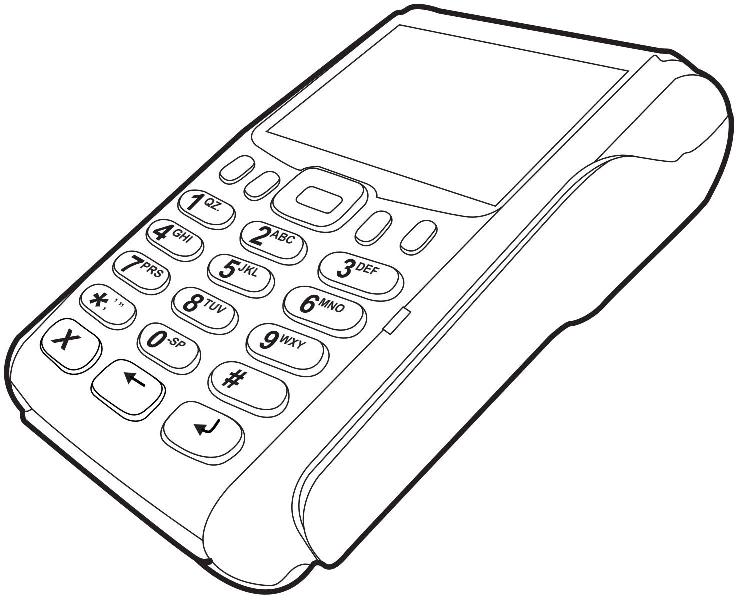
Verifone®

VX 675

Reference Guide



Verifone Part Number DOC265-004-EN-G, Revision G

VX 675 Reference Guide

The information contained in this document is subject to change without notice. Although Verifone has attempted to ensure the accuracy of the contents of this document, this document may include errors or omissions. The examples and sample programs are for illustration only and may not be suited for your purpose. You should verify the applicability of any example or sample program before placing the software into productive use. This document, including without limitation the examples and software programs, is supplied “As-Is.”

Comments? Please e-mail all comments on this document to your local Verifone Support Team.

Verifone, Inc.
2099 Gateway Place, Suite 600
San Jose, CA, 95110 USA
1-800-VERIFONE

www.verifone.com

Verifone Part Number DOC265-004-EN-G, Revision G

CONTENTS

CHAPTER 1 Terminal Overview

CHAPTER 2 Terminal Setup

CHAPTER 3
Using the Terminal Keys

CHAPTER 4
Verix Terminal Manager

CHAPTER 5
File Authentication

CHAPTER 6 Performing Downloads

CHAPTER 7 Specifications

Preface

This guide is your primary source of information for setting up and installing the VX 675 terminal.

Audience

This guide is useful for anyone installing and configuring a VX 675 terminal. Basic descriptions of the terminal features are also provided.

Organization

This guide is organized as follows:

Chapter 1, Terminal Overview. Provides an overview of the VX 675 terminal.

Chapter 2, Terminal Setup. Explains how to set up and install the VX 675 terminal. Provides information on how to select a location, establish power, and how to configure optional peripheral devices.

Chapter 3, Using the Terminal Keys. Explains how to set up and install the VX 675 terminal. It tells you how to select a location, establish power, and how to configure optional peripheral devices.

Chapter 4, Verix Terminal Manager. Describes password-controlled, Verix Terminal Manager operations, as well as how to use it to perform a variety of test and configuration procedures.

Chapter 5, File Authentication.Describes the file authentication module of the VeriShield security architecture and describes how to use the file signing utility, VeriShield File Signing Tool, to generate signature files.

Chapter 6, Performing Downloads. Documents procedures for downloading applications and files to VX 675 units.

Chapter 7, Specifications. Explains how to maintain your VX 675 terminal.

Chapter 8, Maintenance. Discusses the power requirements and dimensions of the VX 675 terminal.

Chapter 9, Verifone Service and Support. Provides information on contacting your local Verifone representative or service provider, and information on how to order accessories or documentation from Verifone.

Appendix A, System Messages. Provides description about error and information messages, which are grouped into two categories.

Appendix B, Troubleshooting Guidelines. Provides information to help you install and configure your VX 675 terminal successfully.

Appendix C, Port Pinouts. Provides list of pinouts for the VX 675 terminal, dongles, and cable connectors.

Appendix D, ASCII Table. Provides an ASCII table.

Appendix E, VX 675 Battery Information. Provides information about the VX 675 Smart Battery.

Related Documentation

To learn more about the VX 675 terminal, refer to the following set of documents:

VX 675 Certifications and Regulations Sheet	VPN DOC265-001-EN
VX 675 Quick Installation Guide	VPN DOC265-002-EN
VX 675 Installation Guide	VPN DOC265-003-EN
VX 675 Base Certifications and Regulations Sheet	VPN DOC265-005-EN
VX 675 Full-Featured Base Quick Installation Guide	VPN DOC265-026-EN
VX 675 USB Base Quick Installation Guide	VPN DOC265-025-EN
VX 675 ECR Certifications and Regulations Sheet	VPN DOC265-027-EN
VX 675 ECR Quick Installation Guide	VPN DOC265-028-EN
Verix eVo Volume I: Operating System Programmers Manual	VPN DOC00301
Verix eVo Volume II: Operating System and Communications Programmers Guide	VPN DOC00302

Conventions and Acronyms

This section describes conventions and acronyms used in this manual.

Document Conventions

Various conventions are used to help you quickly identify special formatting. Table 1 describes these conventions and provides examples of their use.

Table 1 Document Conventions

Convention	Meaning	Example
Blue	Text in blue indicates terms that are cross referenced.	See Conventions and Acronyms.
Italics	Italic typeface indicates book titles or emphasis.	You *must* install a roll of thermal-sensitive paper in the printer.
`Courier`	The courier typeface is used while specifying onscreen text, such as text that you would enter at a command prompt, or to provide an URL.	`RetrieveClearCardData` retrieves the previous swipe's clear track data and places it into the `pstSwipeOut` argument.

Table 1 Document Conventions (continued)

Convention	Meaning	Example
NOTE	The pencil icon is used to highlight important information.	RS-232-type devices do not work with the PINpad port.
CAUTION	The caution symbol indicates possible hardware or software failure, or loss of data.	The terminal is not waterproof or dustproof, and is intended for indoor use only.
WARNING	The lightning symbol is used as a warning when bodily injury might occur.	Due to risk of shock do not use the terminal near water.

Acronym Definitions

Various acronyms are used in place of the full definition. Table 2 presents acronyms and their definitions.

Table 2 Acronym Definitions

Acronym	Definitions
AC	Alternating Current
A-GPS	Assisted GPS
ECR	Electronic Cash Registers
EMV	Europay MasterCard and VISA
GPRS	General Packet Radio Service
GPS	Global Positioning System
GSM	Global System for Mobile Communication
HSPA	High Speed Packet Access
ITP	Internal Thermal Printer
LCD	Liquid Crystal Display
LED	Light Emitting Diode
MRA	Merchandise Return Authorization
MSAM	Micromodule-Size Security Access Module
PED	PIN Entry Device
PIN	Personal Identification Number
QVGA	Quarter Video Graphics Array
RJ45	Registered Jack 45
RS-232	Recommended Standard 232
R-UIM	Removable User Identity Module
SAM	Security Access Module
SD	Secure Digital
SIM	Subscriber Identity Module
TFT	Thin Film Transistor
UART	Universal Asynchronous Transmitter/Receiver
UMTS	Universal Mobile Telecommunications System
USB	Universal Serial Bus
VPN	Verifone Part Number

CHAPTER 1

Terminal Overview

This chapter provides a brief description of the VX 675 terminal. This terminal features a color screen display, fast processor, abundant memory, and PCI 3.0 security.

The VX 675 terminal is a portable, battery-powered device designed to fit comfortably during handheld consumer-facing applications. It features a 2.8” TFT LCD display and a backlit spill-resistant keypad. It supports 3G Universal Mobile Telecommunications System (UMTS), 802.11 b/g/n/ Wireless Fidelity (Wi-Fi), Bluetooth Wireless Technology (BT), Global Positioning System (GPS)/Assisted GPS (A-GPS), and GPRS communications technology.

NOTE

Verifone ships variants of the VX 675 terminal for different markets. Your terminal may have a different configuration—VX 675 3G supports dual SIM slots and optional SD flash memory, VX 675 with ECR functionality is specific only to Turkey market.

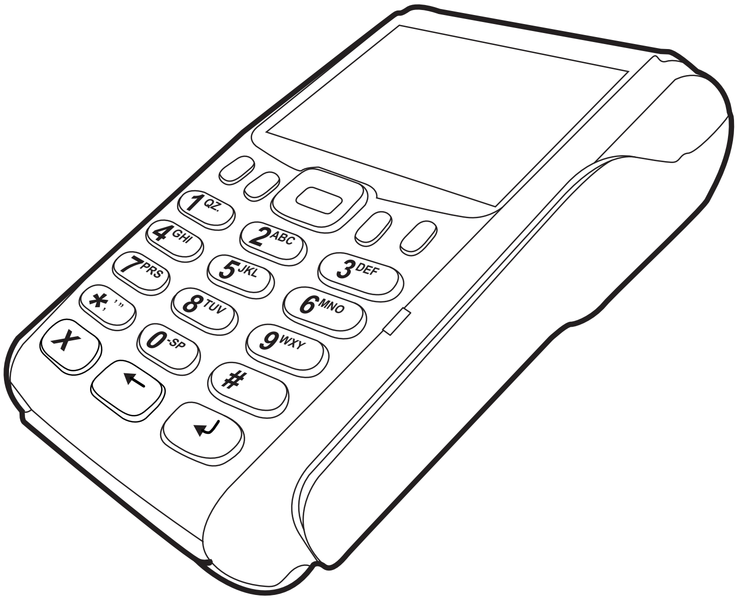


Figure 1 VX 675 Terminal

Features at a Glance

The following are the features of VX 675:

- 400 MHz ARM11 RISC processor delivers power and usability in a convenient “hand-over” design.
- Multi-application operating environment.
- Advanced memory architecture to meet tomorrow’s needs with support for 192 MB.
- Backward compatibility with Verifone solutions help reduces development costs.
- Drop-resistant design minimizes breakage.
- 32-bit processing and multi-tasking capabilities.
- Security architecture exceeds specifications for PCI-PED and sophisticated file authentication.
- Securely supports and runs payment and value-added applications along with signature capture.
- Offers unsurpassed performance on EMV smart card transactions
- Max UI design provides large 2.8” color LCD display, and large blue backlit keys for easier viewing.
- Adds vibrant color screen to the smallest purpose-built wireless payment device.
- Multiple connectivity options.
- Spill-resistant design forces liquid down and off the front of the terminal.

Features and Benefits

VX 675 terminals provide the right combination of features and functions including a triple-track magnetic stripe card reader, supports the “mini-format” cards, Hi/Low coercivity cards, micro SD cards, smart card reader, one or two SAMs, integrated PIN pad, color screen display, and a quiet yet fast internal thermal printer (ITP).

Exceptional Ease of Use

- Lightweight, tapered design, compact, stylish, and the ergonomic balance allows convenient terminal hand-off to the consumer for PIN entry or other input.
- 2.8” TFT LCD display for boundless application possibilities and easy readability under various lighting conditions.
- Large, blue backlit keys provide tactile response to simplify usage and minimize finger slips.
- 25 mm (VX 675 GPRS) and 40 mm diameter paper roll support with a trouble-free, drop-in, “clam shell” loading and dual tear bar that allow receipts to be torn in any direction.
- Quiet and fast integrated thermal printer (25 LPS with a fully charged battery) with Out-of-Paper sensor.
- Vertical magnetic stripe card reader with an extended blade for optimal card reading.

Performance and Durability

- Fast transactions due to powerful 400 MHz ARM11 processor.
- High-capacity 3.6 V 2200 mAh Li-ion battery. VX 675 3G and VX 675 WiFi-BT supports 3.7 V 2450 mAh Li-ion battery pack.
- Base for drop-and-go charging.

- Rounded corners and drop resistant to three feet on concrete floor to minimize breakage.
- 192 MB of memory.

Security

- PCI PED 3.0 approved for debit and other PIN-based transactions.
- EMV Level 1 and 2 Type Approval.
- Tamper-resistant construction, SSL protocols, and VeriShield file authentication.

Communication Technology

- VX 675 GPRS and VX 675 3G: Long-range wireless payment for retailers that have no physical location limitations.
- VX 675 WiFi-BT: Ideal for retailers that need multiple wireless devices and have existing IP infrastructure. It also offers simple, plug-and-play installation for locations that need short-range wireless capability.

CHAPTER 2

Terminal Setup

This chapter describes terminal setup procedures. You will learn about:

- Selecting Terminal Location
- Unpacking the Shipping Carton
- Examining Terminal Features
- Examining Connection Ports
- Installing the Paper Roll
- Installing the SIM Card
- Installing the SD Card
- Using the Battery
- Battery Behavior (No Power Pack)
- Charging the Battery
- Connecting the Terminal Power Pack
- Using the VX 675 Base Stations
- Docking the Terminal on the Base
- Undocking the Terminal from the Base
- Conducting Smart Card Transactions
- Using the Magnetic Card Reader
- Connecting to USB Host
- VX 675 ECR (Fiscal Module) Support
- VX 675 3G and GPS Support
- VX 675 WiFi-BT Support
- Establishing Bluetooth Connections
- Conducting Bluetooth Transactions
- Conducting Wireless Transactions

Selecting Terminal Location

Use the following guidelines when selecting a location for your VX 675 terminal.

Environmental Factors

- The VX 675 unit is a portable terminal. Select a flat support surface, such as a countertop or table, to keep the terminal safe in between uses.
- 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 motor.
- Do not use the terminal outdoors.

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.

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.

Bluetooth Base Considerations

The BT base requires the following:

- A power source within two meters.
- A telephone socket within three meters (for PSTN version)
- A location with minimal obstruction for communication with terminals.
- Install the BT base two meters from the ground to allow LEDs to be seen, and the state of connection be easily confirmed.

Unpacking the Shipping Carton

Open the shipping carton and carefully inspect its contents for possible tampering or shipping damage. The VX 675 device is a secure product and any tampering may cause it to cease functioning properly.

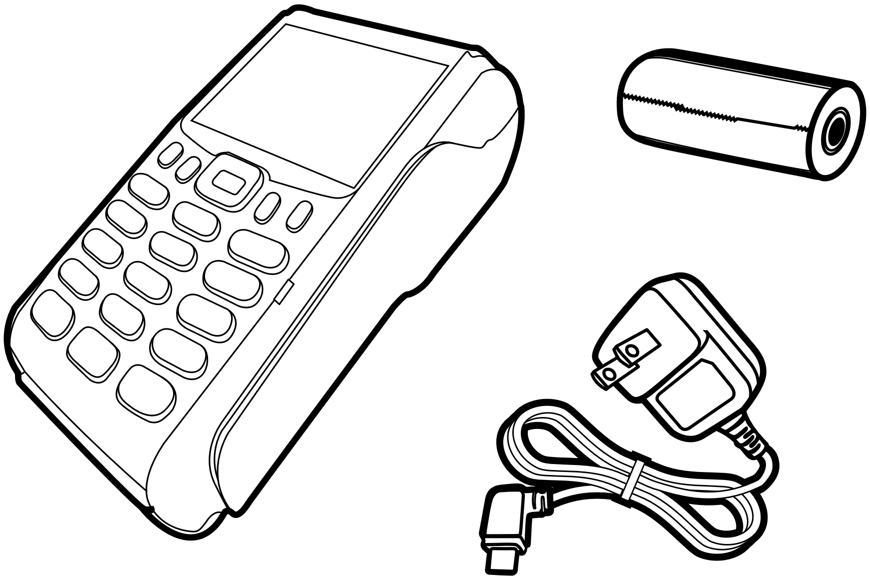


Figure 2 VX 675 Shipping Carton Contents

To unpack the Shipping Carton

1 Remove and inspect the following items:

- Terminal
- Power pack
- Paper roll

2 Remove all plastic wrapping from the terminal and other components.

3 Remove the clear protective film from the LCD screen.

CAUTION Do not use a terminal that has been damaged or tampered with. The terminal comes equipped with tamper-evident labels. If a label or component appears damaged, please notify the shipping company and your Verifone representative or service provider immediately.

4 Save the shipping carton and packing material for future repacking or moving the terminal.

Examining Terminal Features

Before you continue the installation process, see the terminal features illustrated below.

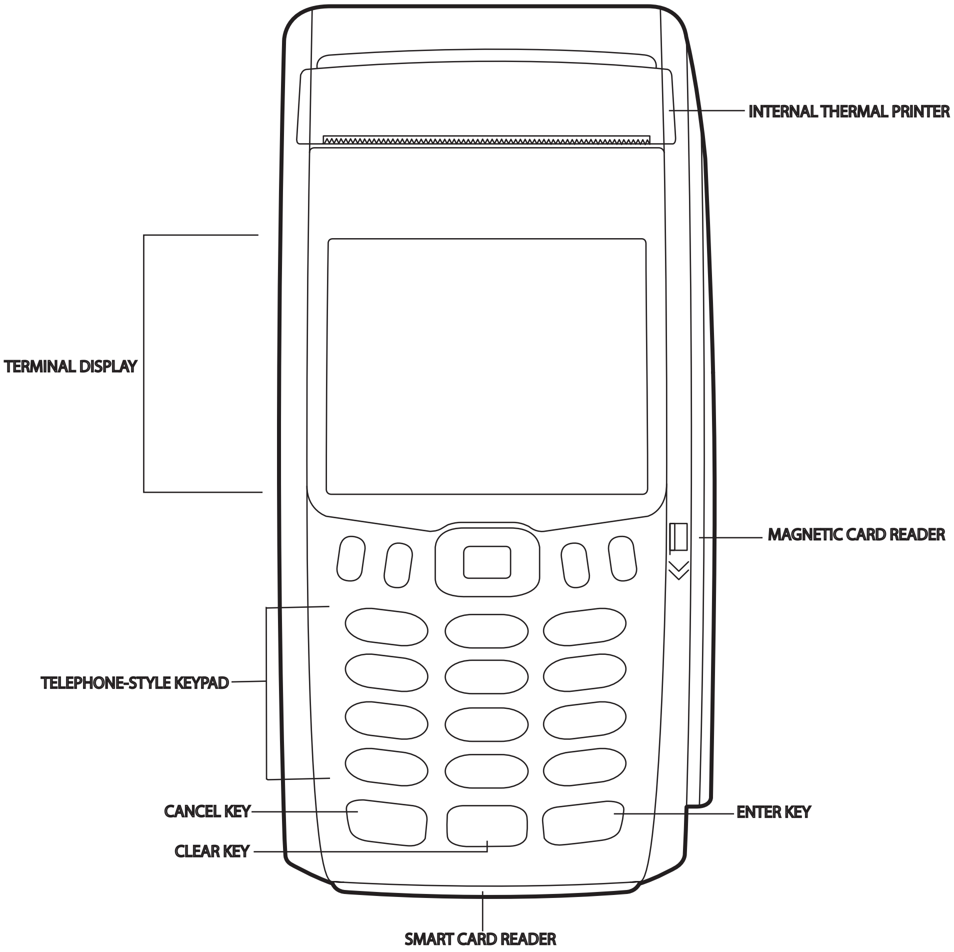


Figure 3 VX 675 Terminal Features (Front Panel)

Front Panel

The front panel includes the following features:

- A 2.8” TFT LCD display.
- A set of keys that include:
  - **a** A 12-key, telephone-style keypad (keypads may vary in style).
  - **b** Three color-coded function keys below the keypad (from left to right: CANCEL, CLEAR, ENTER).
  - **c** Four function keys below the display (PF1, PF2, PF3, PF4) and a five-way navigational key in the middle.
- A magnetic card reader, built into the right side. Swipe the card using the proper direction, with the magnetic stripe down and facing inward, toward the keypad.
- An internal thermal printer at the top front of the terminal.

- A smart card reader, built into the bottom of the terminal. For directions on how to use a smart card, see Conducting Smart Card Transactions.
- A Security Access Module (SAM) compartment, built into the bottom of the terminal inside the back compartment. The VX 675 terminal contains an MSAM cardholder to support stored-value card programs or other merchant card requirements.

NOTE Verifone ships variants of the VX 675 terminal for different markets. Your terminal may have a different configuration. However, the basic processes described in this guide remain the same, regardless of terminal configuration.

Examining Connection Ports

VX 675 has one primary micro-USB port used for power and download.
VX 675 3G and VX 675 WiFi-BT supports USB Host function via primary micro-USB port.

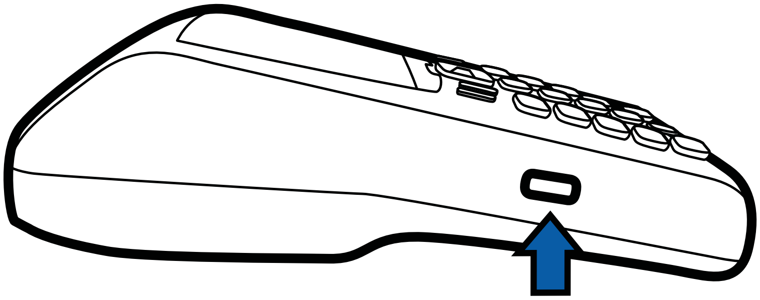


Figure 4 VX 675 Primary Micro-USB Port

Power Supply

Each VX 675 terminal comes with power supply (VPN PWR265-001-01-A) used to connect the terminal directly to a power outlet and to charge the battery.

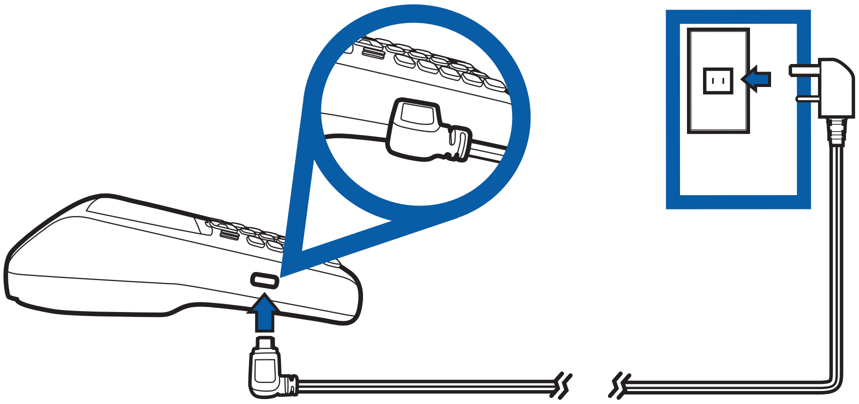


Figure 5 Power Supply Connection to a VX 675 Terminal

Installing the Paper Roll

A fast, quiet thermal printer is built into the VX 675 terminal. Before you can process transactions that require a receipt or record, you *must* install a roll of thermal-sensitive paper in the printer.

The ITP uses a roll of single-ply, thermal-sensitive paper: 25 mm and 40 mm. A pink *out-of-paper* indicator line appears on the edge of the paper approximately 18 inches before the end of the roll. After this line appears, there is enough paper remaining on the roll to conclude at least one transaction.

CAUTION

Poor-quality paper can jam the printer and create excessive paper dust. To order high-quality Verifone paper, refer to Accessories and Documentation.

Store thermal paper in a dry, dark area. Handle thermal paper carefully: impact, friction, temperature, humidity, and oils affect the color and storage characteristics of the paper.

Never load a roll of paper with folds, wrinkles, tears, or holes at the edges in the print area.

To Install a Paper Roll

1 Gently pull the latch located on the bottom of the terminal to unlock the paper roll cover.

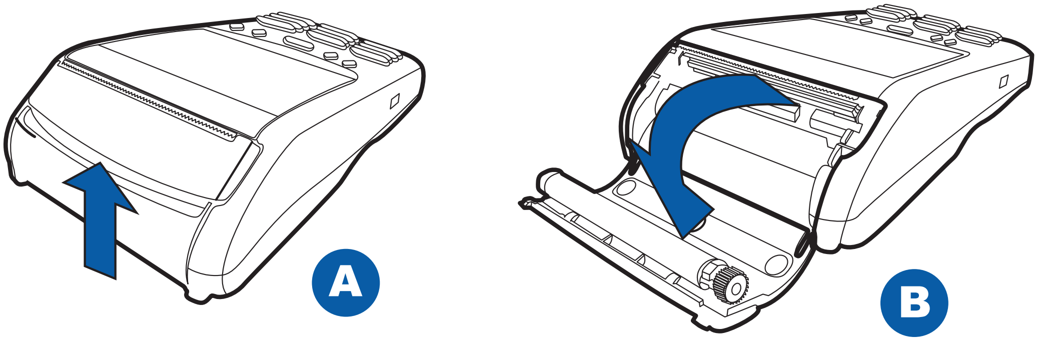


Figure 6 Unlocking the Printer Cover

2 Lift the printer cover up and back.

3 Remove any partial roll of paper in the printer tray.

4 Loosen the glued leading edge of the new roll of paper or remove the protective strip, if applicable. Unwind the paper roll past any glue residue.

5 Hold the roll so the paper feeds from the *bottom* of the roll when the terminal is inverted (see illustration below).

6 Drop the paper roll into the printer tray.

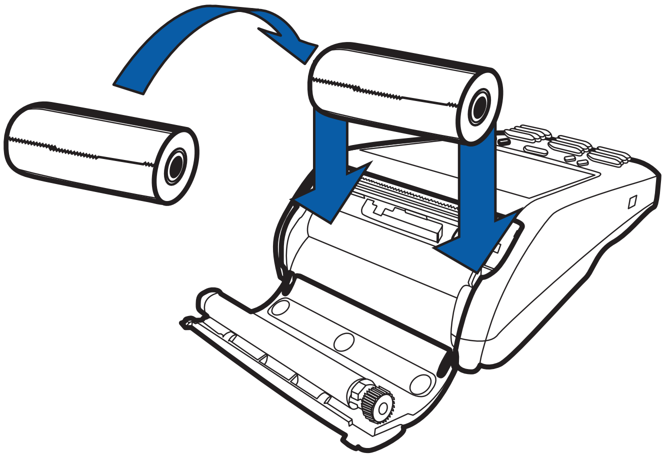


Figure 7 Loading Paper Roll

NOTE

VX 675 with ECR functionality uses 40 mm paper roll.

7 Pull paper up past the glue residue on the paper roll.

8 Close the paper roll cover by gently pressing directly on the cover until it clicks shut, allowing a small amount of paper past the glue residue to extend outside the printer door.

CAUTION

To prevent damaging the print roller, always gently press down on the paper roll cover to close it.

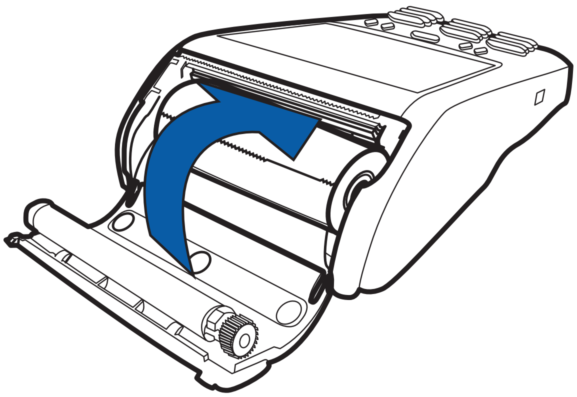


Figure 8 Closing Paper Roll Cover

9 Tear the paper off against the serrated plastic strip in the printer.

Installing the SIM Card

The VX 675 terminal for GPRS modems supports the installation of a GSM Subscriber Identity Module (SIM). Use the following procedure to install a SIM card.

To install or replace the card

1. Turn off the terminal.
2. Place the terminal upside down on a soft, clean surface to protect the lens from scratches.
3. Unscrew and remove the back compartment cover.
4. Lift the battery pack.

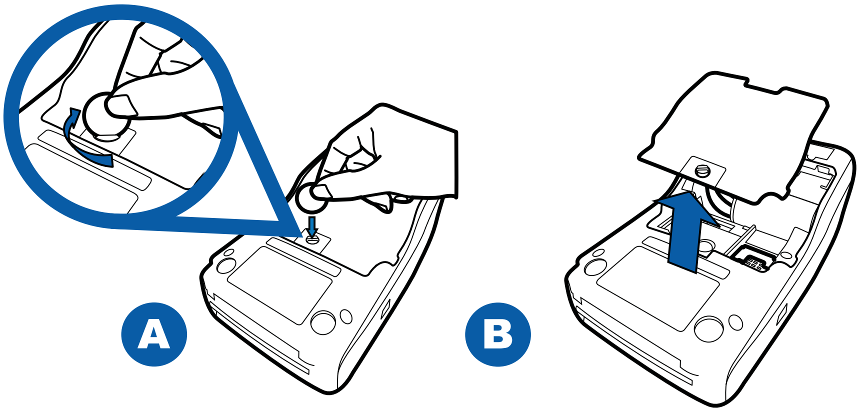


Figure 9 Removing the Back Compartment Cover

5. Insert the SIM card into the cardholder.

NOTE Ensure that the card's gold contacts facing the compartment. The cardholder connector base has a set of contacts and a notch to ensure the SIM card is positioned correctly. The SIM card has a notch on one corner to ensure that it fits into the connector base in only one way. VX 675 3G supports dual SIM and SIM detect behavior for SIM 2. SIM 1 is the primary default SIM and SIM 2 is the backup SIM.

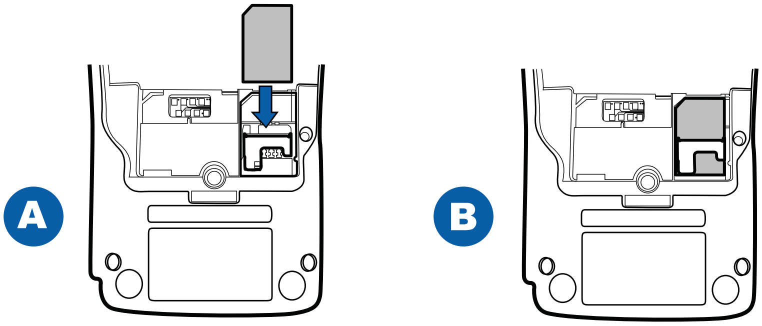


Figure 10 Inserting the SIM Card

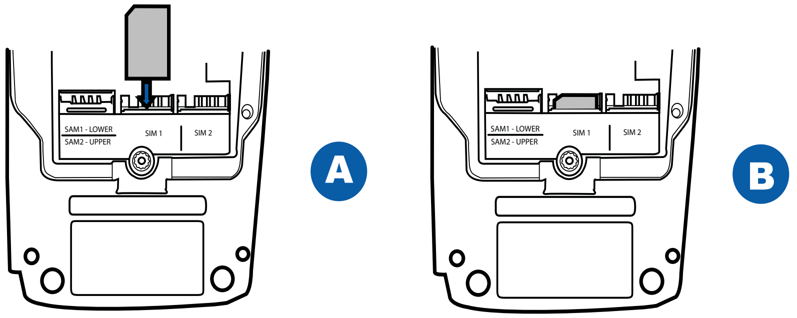


Figure 11 Inserting the SIM Card on VX 675 3G

6 Return the battery pack to its original position.

7 Close and screw the back compartment cover.

Installing the SD Card

VX 675 3G and VX 675 WiFi-BT supports an optional SD flash memory. Use the following procedures to replace or install an SD card.

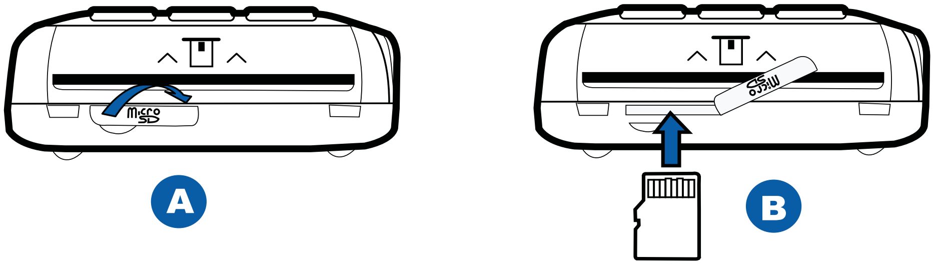
To install or replace the SD card:

1 Turn off the terminal.

2 Lift and turn the rubber flap cover.

3 Insert the micro SD card. The card should lock in place when inserted correctly.

4 Replace the rubber flap cover.



Using the Battery

VX 675 uses a single cell Li-ion battery (see Accessories and Documentation for ordering information). The internal logic of the battery prevents both overcharging and undercharging (a fault condition in which the battery level goes well below the minimum acceptable charge and the battery becomes unusable).

NOTE

VX 675 terminal will only operate when the battery is installed.

Battery Features

The following are features of the battery:

- One Li-ion cell.
- A safety circuit that:
  - Prevents cell damage from overcharge, over-discharge, or overheating.
  - Activates when the battery is left in an unused terminal for extended periods.

NOTE

- VX 675 battery pack is not customer changeable and therefore should not be disconnected and removed.
- Li-ion batteries are not affected by shallow charging. Furthermore, when the terminal has no external power source or battery, the coin cell battery provides power to the security circuit.
- Disconnecting and removing the battery, as well as unplugging the terminal power pack, reduce the life of the coin cell battery, which does not recharge and must be replaced if drained.
- Conserve battery power by turning the VX 675 terminal off when not in use. Keep the Li-ion battery inserted in the terminal and power up the terminal periodically to check the battery charge. Do not let the battery charge fall below 10% for extended periods of time as this may permanently diminish the battery capacity. Recharge the battery by attaching the micro-USB end of the power pack to the terminal and plugging the other end of the power pack into a wall outlet.

Battery Behavior (No Power Pack)

The terminal shifts to power pack mode and starts up automatically when the VX 675 is connected to a non-battery power source, regardless of the battery charge state.

Manual Startup

Hold the green key down for about four seconds until the terminal displays the startup screen.

NOTE

The four second power-up delay prevents terminal startup if the green key is accidentally held down. The time required to hold the green key down to power up the terminal is configurable.

The terminal lights up once the power is on.

NOTE

The Verifone copyright screen starts and displays a unique copyright screen once the terminal loads an application. However, **DOWNLOAD NEEDED** appears on screen after the initial Verifone copyright screen if there is no available application in the terminal.

Manual Shutdown

Hold the red key down for about four seconds until the terminal displays the shutdown verification screen. Keep holding the red key until the VX 675 terminal shuts down.

NOTE

- The four second shutdown delay that prevents terminal shutdown if the red key is accidentally held down. The time required to hold the red key down to shut down the terminal is configurable.
- The screen is blank when the terminal has no power.

Connecting the Terminal Power Pack

After installing the battery, connect the VX 675 terminal to the provided power source for initial charging.

CAUTION

Using an incorrectly rated power supply may damage the terminal or cause it not to work as specified. Before troubleshooting, ensure that the power supply being used to power the terminal matches the requirements specified on the bottom of the terminal. (See Specifications for detailed power supply specifications.) Obtain the appropriately rated power supply before continuing with troubleshooting.

WARNING

Do not plug the power pack into an outdoor outlet or operate the terminal outdoors.

During a transaction, disconnecting the power by removing the battery or unplugging the terminal from a wall power while at very low battery charge may cause transaction data files not yet stored in the terminal memory to be lost.

The VX 675 unit comes with a universal input power pack capable of operating from voltages of 100 V to 240 V AC.

To Connect the Terminal Power Supply

1 Insert the micro-USB plug into the micro-USB port of the VX 675, as shown in the figure below.

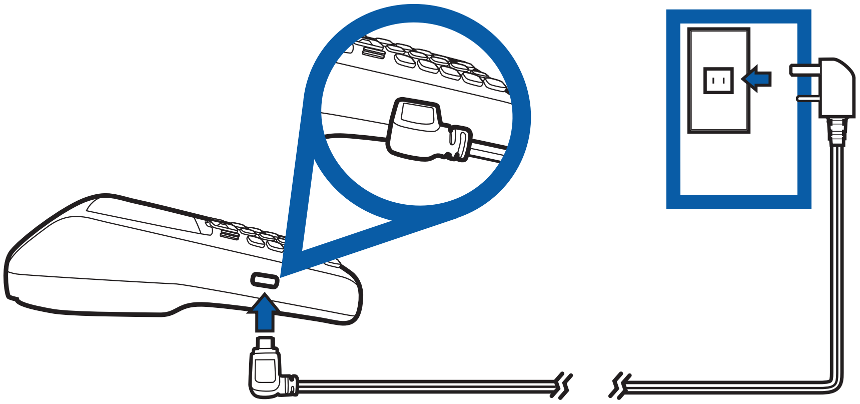


Figure 12 VX 675 Power Supply Connection

2 Plug the AC power pack into a wall outlet or powered surge protector.

NOTE To protect against possible damage caused by lightning strikes and electrical surges, consider installing a power surge protector.

Once it loads the application, the terminal starts the initial Verifone copyright screen and displays a unique copyright screen. If there is no available application in the terminal, **DOWNLOAD NEEDED** appears on screen after the initial Verifone copyright screen.

Charging the Battery

After unpacking your VX 675 terminal, connect the power pack to the unit for 4.65 hours or until fully charged.

NOTE The terminal charges the VX 675 battery when the terminal is in the base. For more information, see Docking the Terminal on the Base.

The battery has a safety circuit to protect the Li-ion cells from overcharging and over-discharging. If the battery is over-discharged, the safety circuit shuts down the battery. The battery must then be recharged to restore operation.

NOTE The VX 675 terminal automatically shuts off when the battery reaches the *critically low* charge state. If this occurs, the battery must be recharged for a minimum of 1/2 hour before it can power the terminal. *It may take several recharge attempts to reset the safety circuit* when charging a battery that has been discharged below this critical state.

Battery Life

Charging and discharging the VX 675 battery hundreds of times will wear out the battery. Significantly reduced operating times indicate the need for battery replacement (see Accessories and Documentation for ordering information).

WARNING Do not dispose of batteries in a fire. Li-ion batteries must be recycled or disposed of properly. Do not dispose of Li-ion batteries in municipal waste sites.

Using the VX 675 Base Stations

Like the terminal, Verifone ships variants of the VX 675 base for different markets. Your base may have a different configuration.

USB Base

A charging base to charge the terminal and provide a docking station when the terminal is not in use. It also has USB Host port for downloading applications and secure keys via USB flash drive. The base can be positioned on a countertop.

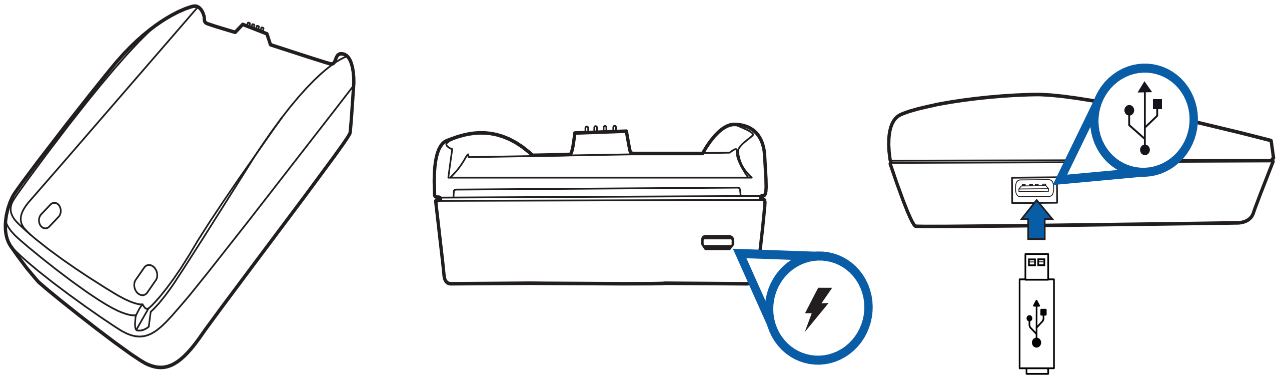


Figure 13 USB Base Showing Micro-USB and USB Host Ports

Full-Feature Base

A charging base with Dial, Ethernet, Serial (RS-232), and USB Host ports for full back-up connectivity options and support to some peripherals like ECR, check reader, and barcode reader, among others.

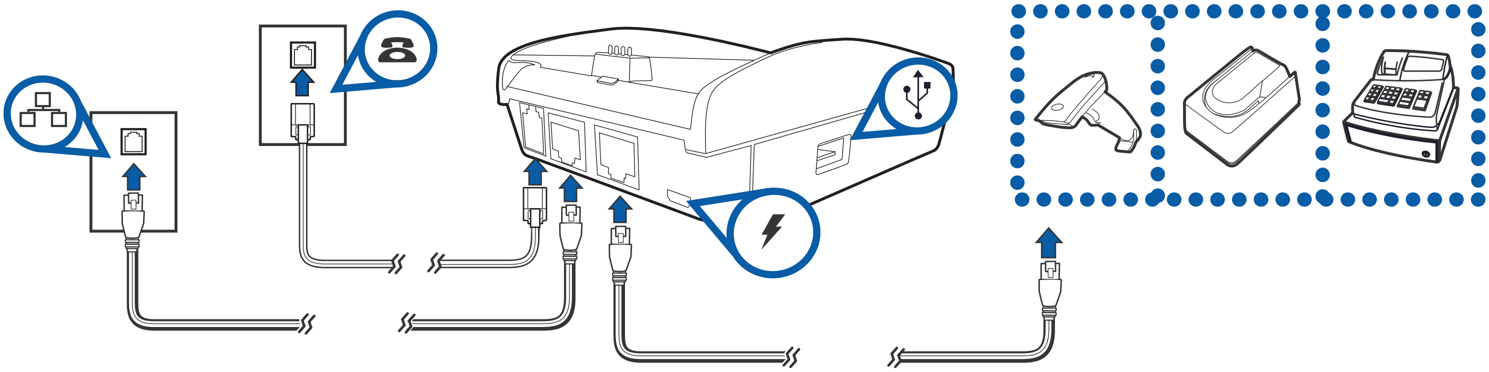


Figure 14 Full-Feature Base Showing Dial, Ethernet, Serial, Micro-USB and USB Host Ports

Bluetooth Base A base station that relays wireless data received from the terminal via modem and transmits back the response to the terminal, also with Dial, and Ethernet connectivity options.

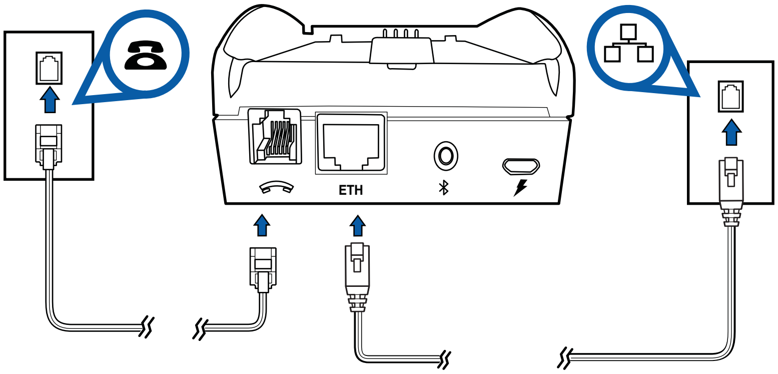


Figure 15 Bluetooth Base

Powering Up the Base

Use the procedure below to connect the VX 675 Base to a power source.

To power up the base

1 Insert the micro-USB plug into the micro-USB port of the base, as shown in the figure below.

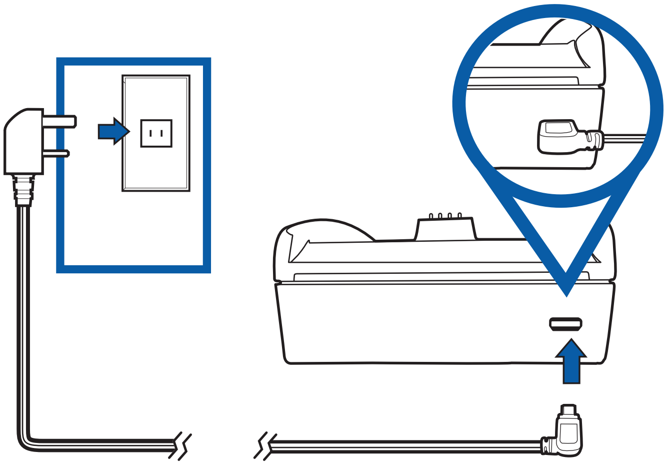


Figure 16 Connecting the Base to a Power Source

2 Plug the AC power pack into a wall outlet or power surge protector.

Docking the Terminal on the Base

The VX 675 terminal can be placed on the base when not in use for continuous charging of its battery.

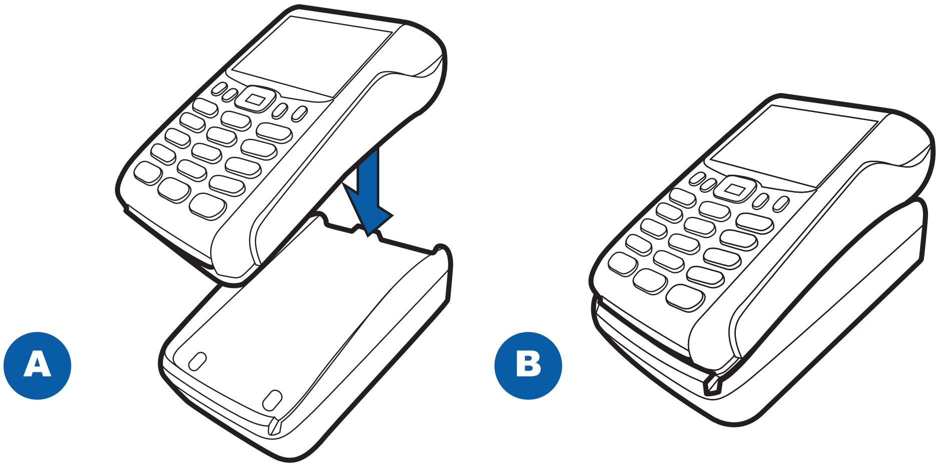


Figure 17 Docking the VX 675 Terminal on the Base

Undocking the Terminal from the Base

The VX 675 terminal can be taken from the base when in use.

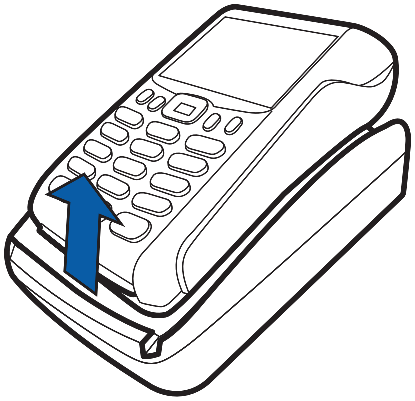


Figure 18 Undocking the VX 675 Terminal from the Base

NOTE To protect against possible damage caused by lightning strikes and electrical surges, consider installing a power surge protector.

WARNING Do not plug the power pack into an outdoor outlet or operate the terminal outdoors.

Disconnecting the power during a transaction may cause transaction data files not yet stored in terminal memory to be lost.

Conducting Smart Card Transactions

The smart card transaction procedure may vary from one application to another. Verify the procedure with your application provider before performing a smart card transaction.

To Conduct a Smart Card Transaction

1. Position a smart card with the contacts facing upward (see illustration below).
2. Insert the smart card into the smart card reader slot in a smooth, continuous motion until it seats firmly.
3. Remove the card only when the application indicates the transaction is complete.

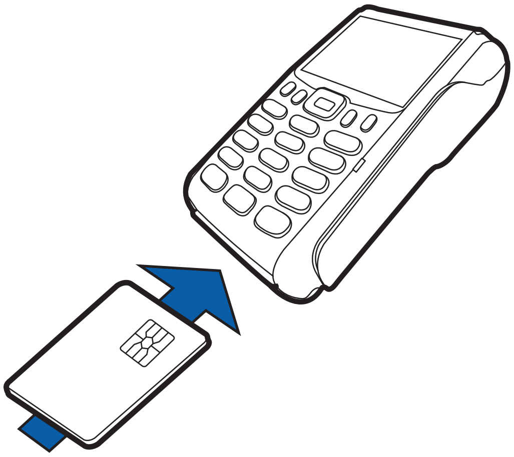


Figure 19 Inserting a Smart Card

CAUTION Do not remove the smart card in the card reader until the transaction is complete. Premature card removal will invalidate the transaction.

Using the Magnetic Card Reader

The VX 675 terminal supports credit/debit card transactions.

To Conduct a Credit or Debit Card Transaction

1. Position a magnetic card with the stripe in the card reader and facing inward, toward the keypad.
2. To ensure a proper read of the magnetic swipe card, the user should insert the magnetic card from the top of the unit, as shown in the following illustration.

3 Swipe the card through the magnetic card reader.

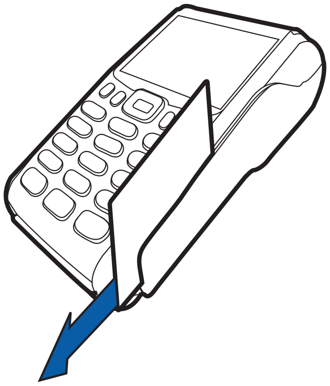


Figure 20 Using the Magnetic Card Reader

Connecting to USB Host

USB Host support, allows you to download applications and secure keys via USB flash drive.

To connect to the USB Host

1 Power up the base by inserting the micro-USB plug into the micro-USB port of the base as shown in Figure 16.

2 Make sure that the terminal is docked on the base.

3 Insert the USB plug into the USB Host port on the left side of the base.

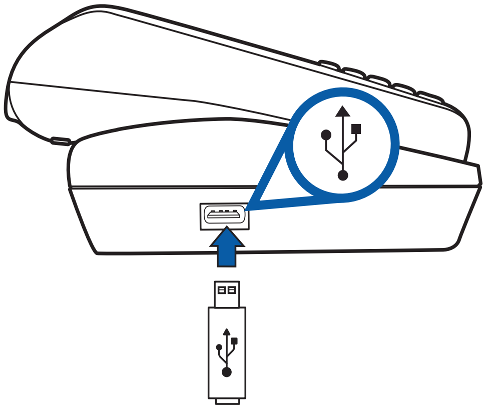


Figure 21 Connecting USB Flash Drive to the USB Host

VX 675 ECR (Fiscal Module) Support

The fiscal module allows ECRs to have direct connection to the Ministry of Finance servers. When a mobile transaction is made, the transaction data is sent over to the Ministry of Finance servers, and then goes to the banking host system. The fiscal module stores the transaction data (up to 2 MB). A metallic seal is placed on the right side, under the MSR to secure the fiscal module.

Customer Display

A 42mm single line customer-facing display (no backlight) that can display up to 8 characters including "," or "." between any character. It is located below the paper roll cover.

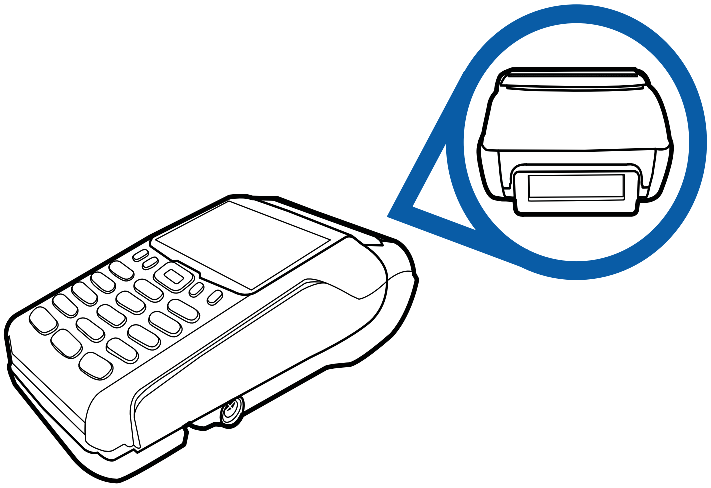


Figure 22 VX 675 ECR Customer Display

VX 675 3G and GPS Support

VX 675 3G uses the Cinterion PHS8-P radio module that incorporates 3G High-Speed Packet Access (HSPA+) connectivity. The PHS8-P radio module is optimized for high bandwidth and allows a downlink speed of 14.4 Mbps and an uplink speed of 5.7 Mbps.

GPS Receiver

The Cinterion PHS8-P radio module integrates a GPS receiver that offers the full performance of GPS/A-GPS technology.

Connecting by 3G

To connect to existing 3G operator-provided infrastructure, check that SIM has been inserted, see Installing the SIM Card.

VX 675 WiFi-BT Support

VX 675 WiFi-BT integrated module uses Broadcomm BCM4329 chip, which provides SDIO interface for Wi-Fi and UART interface for Bluetooth. The module includes an integrated WLAN RF transceiver optimized for use in Wireless LAN systems with advanced power management unit, and an integrated radio transceiver optimized for use in Bluetooth wireless systems.

Establishing Bluetooth Connections

Before the Bluetooth variant of the VX 675 Terminal can be used online to authorize transactions, it must be paired with a Bluetooth AP Charging Base Station. Both the VX 675 Terminal and Bluetooth AP Charging Base Station have roaming capabilities and must be within a five-meter of each other for initial pairing. The Bluetooth AP Charging Base Station must be installed but powered OFF and the VX 675 Terminal should be powered ON.

Bluetooth AccessPoint (AP) Charging Base (Bluetooth Interface)

The Bluetooth AP Base Station relays wireless data received from the VX 675 terminal via modem and then transmits back the response to the terminal. It pairs with the Bluetooth Base to go online for authorization. These are both Class 1 Bluetooth devices providing secure radio communication.

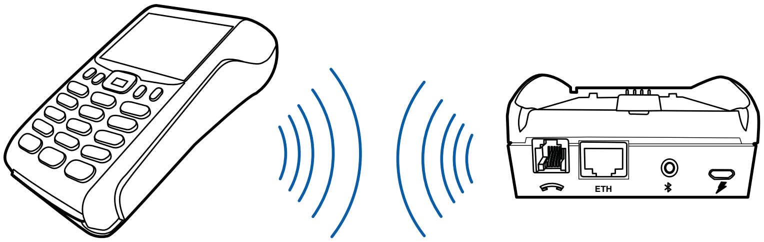


Figure 23 VX 675 Bluetooth Terminal Communicating with the Bluetooth Base

To improve the range performance of the VX 675 terminal, the Bluetooth AP Base Station should be placed in a position that will service all of the card payment areas in your premises. The ideal placement is to position the base station within line of sight of all areas of card acceptance.

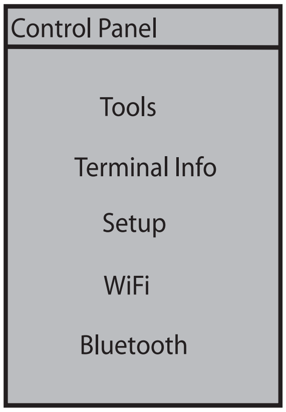
Searching for a Bluetooth AP Charging Base Station

The first step towards establishing a connection between the Bluetooth version of the VX 675 Terminal and a Bluetooth AP Charging Base Station is to search for the Bluetooth AP Charging Base Station using the VX 675 Terminal.

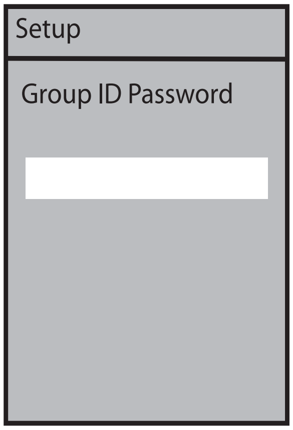
To search for a Bluetooth AP Charging Base Station using the VX 675 Terminal:

1 Power On the terminal. The Select Options menu is shown on the terminal display once the device is powered ON.

2 On the Network Control Panel, select Bluetooth. Click Bluetooth to access the Bluetooth menu.



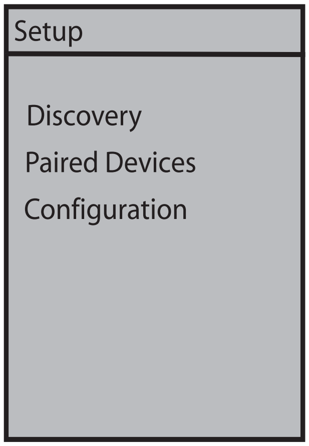
3 Before you can access the Setup menu, you will be asked to enter your password. Enter your password, then press the Enter key.



Setup

Group ID Password

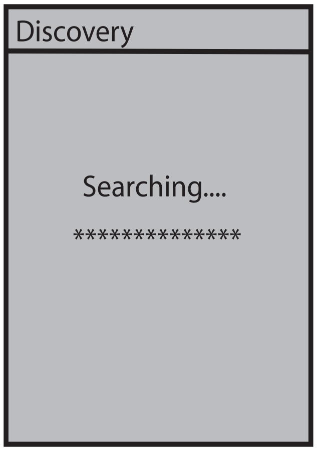
4 On the Setup menu, Discovery is selected by default. Press the Enter key to start searching for a base station.



Setup

Discovery
Paired Devices
Configuration

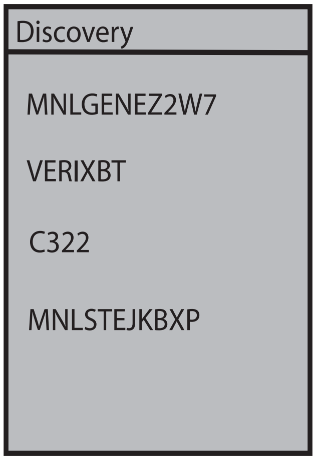
5 There is a short delay as the terminal searches for the base station. The message is shown on the terminal display.



Discovery

Searching....
****

6 Once the terminal discovers the Bluetooth AP Charging Base Station, the base station's friendly name is then displayed.



Discovery

MNLGENEZ2W7

VERIXBT

C322

MNLSTEJKBXP

NOTE If the devices are unable to find each other after two minutes, press the Bluetooth switch (blue button) found on the back of the VX 675 AP Charging Base. This switch is located between the power and Ethernet sockets. After pressing the switch, the two LEDs will blink (blue) indicating that the VX 675 AP Charging Base is discoverable.

WARNING Pressing the Bluetooth switch while there is an existing Bluetooth connection may result in loss of connection, loss of modem profile, and loss of all modem settings/configuration.

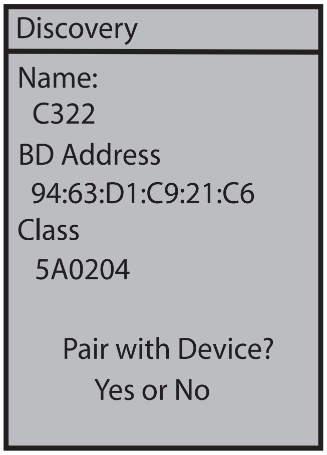
Pairing the Terminal with a Bluetooth AP Charging Base Station

Even after you have successfully searched for a Bluetooth AP Charging Base Station using the terminal, you will still not be able to conduct Bluetooth transactions until you have paired the terminal and the base station.

To pair the terminal with the base station:

1 Navigate to the BT Devices menu, select the base station's friendly name, then press the Enter key.

2 Select the base station's name, then press the Enter key.

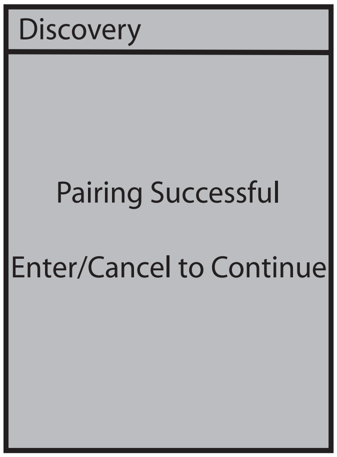


Discovery

Name:
C322
BD Address
94:63:D1:C9:21:C6
Class
5A0204

Pair with Device?
Yes or No

3 If pairing is successful, the BT Devices menu appears on the terminal screen. The friendly name of the Bluetooth AP Charging Base Station appears on the first line of the BT Devices menu.



Discovery

Pairing Successful

Enter/Cancel to Continue

If everything is connected properly and the terminal is unable to go online, refer to Troubleshooting Guidelines.

Setting the Connection Information for a Paired Device

To set the connection information for a paired device:

1 Select Paired Device.

2 Select a device from the list.

3 On the BT Device Port, select either Ethernet, Modem, or Serial (this is for XPS019).

Pairing with Another Bluetooth AP Charging Base Station

Once the terminal is paired with a Bluetooth AP Charging Base Station and initialized, it may be paired with additional Bluetooth AP Charging Base Station.

To pair a terminal with another Bluetooth AP Charging Base Station:

1. Select Discovery on the terminal's Setup menu, then press Enter.
2. Make sure the terminal is within 5 meters of the new Bluetooth AP Charging Base Station, which must be powered off.
3. When the terminal displays the base station, select it by pressing the appropriate name, and then press Enter.
4. On the Discover menu, select Yes when asked if Pair with Device screen appears.
5. The terminal and base station will then pair. The terminal will then make the new Bluetooth AP Charging Base Station the default pairing device.

If everything is connected properly and the terminal is unable to go online, refer to Troubleshooting Guidelines.

Removing a Paired Bluetooth AP Charging Base Station

To remove a Bluetooth AP Charging Base Station to which a terminal has been paired:

1. Navigate to the BT Devices menu.
2. Select the Bluetooth AP Charging Base Station you want to remove as a pair.
3. Select Remove All Pairs, then press the Enter key.
4. The Bluetooth AP Charging Base Station's friendly name will disappear from the display when the base station is removed.

Removing a Paired Device via Network Control Panel of EOS

To remove a paired device via Network Control Panel of EOS:

1. On the Menu, select Bluetooth.
2. On the Bluetooth menu, select Setup.
3. On the Setup menu, select a paired device, then, select Remove.

Conducting Bluetooth Transactions

To conduct a Bluetooth transaction:

- Ensure the terminal is paired with the Bluetooth AP Charging Base Station not more than 100 meters away.
- Follow the on-screen instructions provided with your application.

Conducting Wireless Transactions

To conduct a wireless transaction:

- Ensure the terminal is in an optimal position for transmitting.
- Follow the on-screen instructions provided with your application.

Using the Terminal Keys

Before proceeding to other tasks, familiarize yourself with the operational features of the VX 675 terminal keypad to enter data.

This section describes how to use the VX 675 keypad, which consists of four programmable function keys (PF1 to PF4), a 5-way navigation key, a 12-key telephone-style main keypad (0 to 9, *, and #), and three command keys (CANCEL, CLEAR, and ENTER).

Using these keys, you can perform all data-entry tasks described in this manual. The function keys allow you to navigate though the system mode menus and select specific operations.

For added convenience, the keypad is automatically back-lit when you power on the terminal.

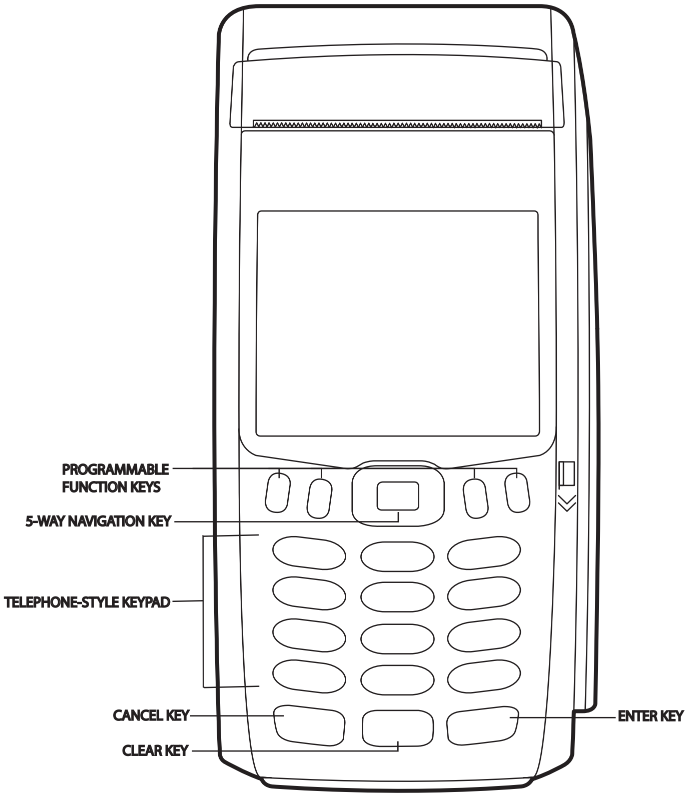


Figure 24 Front Panel Key Arrangement.

NOTE

Actual keypad may vary.

Data Entry Modes

Before you can use the keys on the front panel to enter ASCII characters, the VX 675 terminal must be in a mode that accepts keyed data entry. There are two terminal operating modes, each enabling 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 mDRAM and currently running.
- **Verix Terminal Manager (VTM) mode:** This is a special, password-controlled terminal operating mode for performing a variety configuration procedures that cannot be performed when an application is running.

NOTE

If you enter Verix Terminal Manager while a terminal application is running in normal mode, Verix Terminal Manager preempts the application and takes control of the display and keyboard. The only way to exit Verix Terminal Manager is to restart the terminal. For this reason, once you enter the Verix Terminal Manager, you cannot return to the application in the same session.

If you turn on a VX 675 terminal with an application stored in memory and `*GO` variable set to the application name, the application executes and the terminal automatically enters normal mode. The application then controls how terminal keys process transactions and when you can use specific keys to type characters or respond to prompts.

Main Keypad

The main keypad is a 12-key telephone-style main keypad.

NOTE

The VTM functions described in the Verix Terminal Manager section requires you to enter numbers, letters, or symbols using the keypad.

Using the keypad, you can enter up to 50 ASCII characters, including the letters A–Z, the numerals 0–9, and the following 20 special characters: (*), (,), (‘), (“), (-), (.), (#), (%), (:), (!), (+), (@), (=), (&), (space), (;), ($), (_), (\), and (/).

Alphabetic characters are entered by pressing its corresponding number in the keypad multiple times within a given time.

Characters found in the * and # keys may vary in some units (for example, VX 675 with ECR fiscal module functionality).

Command Key Descriptions

The following are the command keys of the terminal's keypad.

NOTE

The terminal's operating mode and context determine the specific action performed when you press one of the function keys. The following descriptions are provided solely to acquaint you with some general characteristics of these function keys before presenting more detailed Verix Terminal Manager procedure descriptions.

Cancel Key

Pressing the **Cancel** key in normal mode — when the terminal's application is loaded and running. It terminates the current function or operation.

In Verix Terminal Manager, use **Cancel** to perform a variety of functions. The most common use of **Cancel** in Verix Terminal Manager is to exit a Verix Terminal Manager submenu and return to the main Verix Terminal Manager menu. The specific effect of pressing the Cancel key depends on the currently active Verix Terminal Manager menu.

In VX 675 ECR units, the red key may display a string of letters.

Clear Key

In normal mode, the **Clear** key is commonly used to delete a number, letter, or symbol on the terminal's display screen. Press **Clear** one time to delete the last character typed on a line. To delete additional characters, moving from right-to-left, press **Clear** once for each character or hold down **Clear** to delete all characters in a line.

In Verix Terminal Manager, the specific effect of pressing the **Clear** key depends on the currently active Verix Terminal Manager menu.

Enter Key

In normal mode, the **Enter** key is generally used in the same way 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 Verix Terminal Manager, press the **Enter** key to begin a selected procedure, step forward or backward in a procedure, and confirm data entries. The specific effect of the **Enter** key depends on the currently active Verix Terminal Manager menu.

In VX 675 ECR units, the green key may display a new currency symbol.

CHAPTER 4

Verix Terminal Manager

This chapter describes a category of terminal functions called *terminal manager operations*.

- Press **ENTER** and **7** keys at the same time and enter the password to open the Verix Terminal Manager (VTM). See Entering Verix Terminal Manager.
- Since files are loaded into specific groups, VTM users can view files, delete files, and manage configuration variables. See File Groups.
- Use the system and file group passwords to secure applications and information on the terminal. See Passwords.
- Use the terminal manager menus and submenus to configure terminals; download and debug applications; perform diagnostics such changing console settings, managing keys and view terminal information; and perform routine tests and terminal maintenance. See Verix Terminal Manager Menus.

Verix Terminal Manager is used exclusively by those responsible for configuring, deploying, and managing on-site VX 675 terminal installations.

When to Use Verix Terminal Manager

Use the Verix Terminal Manager functions to perform different subsets of related tasks:

- **Application programmers** configure a development terminal, download development versions of the VX 675 application program, then test and debug the application until it is validated and ready to be downloaded to other terminals.
- **Deployers of VX 675 terminals to end-user sites** perform the specific tasks required to deploy a new VX 675 terminal on-site, including configuring the terminal, downloading application software, and testing the terminal prior to deployment.
- **Terminal administrators or site managers** change passwords, perform routine tests and terminal maintenance, and configure terminals for remote diagnostics.

To perform the subset of tasks that corresponds to a job, select the appropriate Verix Terminal Manager menu(s) and execute the corresponding procedure(s).

Local and Remote Operations

The terminal manager operations available on a VX 675 terminal can be divided into the following two categories or types:

- **Local operations** address a stand-alone terminal and do not require communication or data transfers between the terminal and another terminal or computer. Perform local Verix Terminal Manager operations to configure, test, and display information about the terminal.
- **Remote operations** require communication between the terminal and a host computer (or another terminal) over a cable connection. Perform remote Verix Terminal Manager operations to download application software to the terminal, upload software from one terminal to another, or download using a service dongle from VeriCentre or from another download host.

This chapter contains descriptions on how to perform local Verix Terminal Manager operations. For information on performing remote operations, such as downloads, refer to the Performing Downloads section.

Verifying Terminal Status

The VX 675 terminal you are using may or may not have an application program running on it. After you have set up the terminal (refer to Terminal Setup) and the terminal is turned on, use the following guidelines to verify terminal status regarding software and current operating mode:

- If no application program is loaded into terminal memory, the message **DOWNLOAD NEEDED** appears on the display screen.

NOTE

From this point, press **ENTER** and **7** key simultaneously to access Verix Terminal Manager and perform the required download.

- If an application program is loaded and `*GO` is set in the configuration file in group 1 to the application's name into terminal memory, an application-specific prompt appears. The application is running and the terminal is in normal mode. If all installation steps are complete, the terminal can process transactions.

Entering Verix Terminal Manager

To prevent unauthorized use of the Verix Terminal Manager menus, the VX 675 terminal OS requires a system password each time you enter Verix Terminal Manager. To access the Verix Terminal Manager password entry screen, simultaneously press the **ENTER** and **7** keys.The default, factory-set system password is "**166831**." Use the following key sequence to enter this password:

1 6 6 8 3 1 ENTER

After entering the correct password, the terminal enters the terminal manager and displays the first terminal manager main menu. You can now cycle through all Verix Terminal Manager main menus.

File Groups

The VX 675 operating system implements a file system in memory. Files are assigned to one of 15 groups for access control. Groups are similar to directories on a computer in that different applications can be stored in separate file groups, just like different computer applications can be stored in separate directories. Groups are referred to as Group n or GIDn throughout this manual.

Each group is protected by a separate password, and each has a separate `CONFIG.SYS` file. The following rules apply to the VX 675 file group system:

- The primary application must be downloaded into Group 1.
- On terminal power up and after a restart, the terminal defaults to Group 1 as the controlling group.
- Group 1 applications have access to files stored in all groups. Other applications can reside in Groups 2 – 14.
- Applications in a group other than Group 1 have access only to themselves and files stored in Group 15.
- Group 15 is globally accessible, making it an ideal location for files shared by multiple applications, such as shared libraries.
- File Groups 1 – 15 are empty until they are filled through a download to the VX 675 terminal.

For more information on managing file groups, refer to the *Verix eVo Volume I: Operating System Programmers Manual* -VPN DOC00301.

Passwords

Handle passwords as you would PC passwords.

CAUTION

If you change a password but forgot it later on, there is no password recovery method. Without the password, you are unable to access Verix Terminal Manager operations and may be prevented from requesting a download, performing remote diagnostics, or changing any of the information already stored in memory. The terminal can, however, continue to process transactions in normal mode.

If you forget or lose the system password to your terminal, please contact your local Verifone representative for assistance.

NOTE

Passwords must be in numeric characters only and must be greater than five digits and less than 10 digits in length.

System Password

When you key in the system password to enter terminal manager, an asterisk (*) appears for each character you type. These asterisks prevent your password from being seen by an unauthorized person.

NOTE Some application program downloads automatically reset the system password. If your system password no longer works, check if a download has changed your password.

File Group Passwords

From manufacture, each file group uses the default password "166831," which is entered as follows:

1 6 6 8 3 1, and press **ENTER**

Verix Terminal Manager Menus

The two main terminal manager menus are listed in the following table.

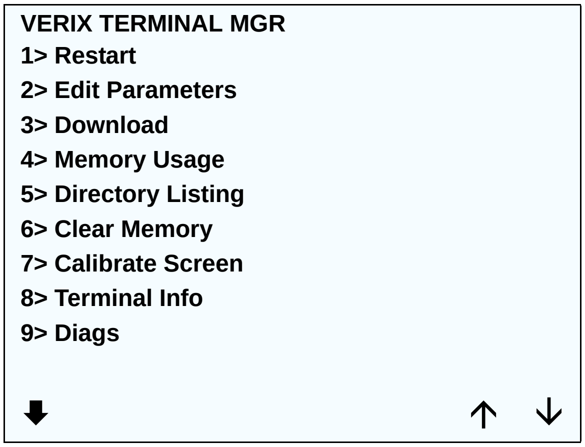


Figure 25 Menu 1

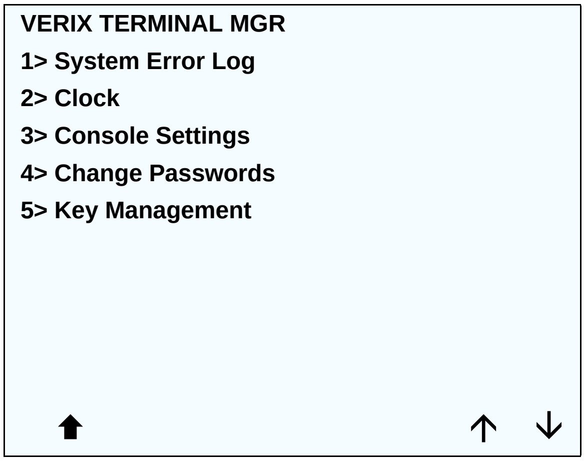


Figure 26 Menu 2

On successful entry of the system password, **VERIX TERMINAL MGR** menu appears.

to return to a previous menu, press the **UP** icon (⬆) on the left side of the screen. To go to the next menu, press the **DOWN** icon (⬇). The smaller arrows on the right side of the screen, **UP** (↑) and **DOWN** (↓), are used to select any submenu from the list. Pressing **ENTER** will choose the highlighted function. To return to the main Verix Terminal Manager menu and cancel any changes, press the **CANCEL** key. The user can also select the item from the menu by pressing the corresponding number key indicated at the left of the item selected.

Each menu has items to select; some items contain submenus or a series of prompts. When prompted to enter alphabetic or special characters, use the procedure described in Chapter 3.

When performing downloads or operations that change or clear files, the password for each file group is required. The password is only required once per session per file group.

Verix Terminal Manager Procedures

The procedures in this section explain how to use each of the Verix Terminal Manager menus. Each procedure description starts at a main Verix Terminal Manager menu. Each procedure takes you step-by-step through a complete Verix Terminal Manager operation in the following sequence:

1. When the main Verix Terminal Manager menu appears, scroll up or down using the **UP** (↑) and **DOWN** (↓) icons on the right side of the screen to select an operation.
2. Press **ENTER** to select the operation.
3. Complete the operation.
4. Return to the main Verix Terminal Manager menu.

Procedure descriptions are arranged in the following tabular format:

Table 3 Procedural Description Example

Display	Action
Screen displayed	Action required
Submenu Row	
Screens displayed on submenu selection	Action required

The Display column in Table 3 indicates what appears on the terminal display screen at each step of the procedure. Please note the following conventions used in this column:

- If a prompt or message appears on the screen exactly as it is described, it is shown in Arial bold font and in lower case with the first letter capitalized. For example, **Download Needed**.
- If text is enclosed in parentheses, the actual text or message may vary depending on the terminal version you have. For example, in (Application Prompt), the normal font is used and text appears in lower case with first letter capitalized.

The Action column provides a procedural description that:

- Describes the current step and context of the procedure.
- Indicates the entries to perform using the keypad in response to a prompt or message.
- Provides additional explanations or information about the steps of that particular Verix Terminal Manager menu.

A submenu row indicates a specific menu evoked from a main menu screen. A description of that screen and procedure immediately follows the submenu row.

The following keys have the same function on all submenus:

- Press the **ENTER** key to choose the function and display the submenu selected. When editing, pressing **ENTER** will save a newly entered variable.
- Press the **CANCEL** key to exit any submenu without saving changes.

Enter and Exit Verix Terminal Manager

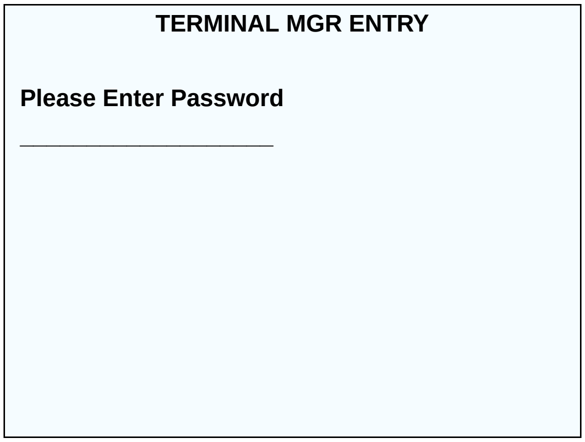
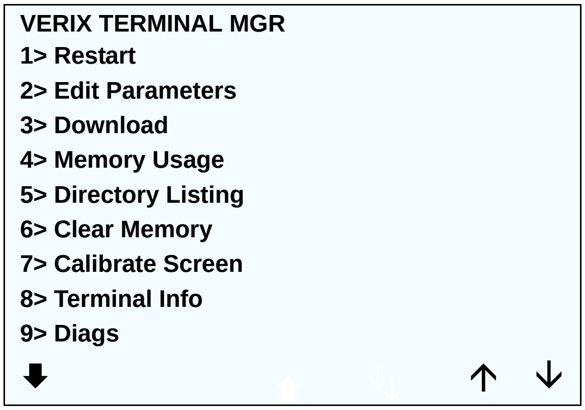
To enter terminal manager after you have turned on the VX 675 terminal, follow the procedure described below.

NOTE On successful completion, some operations automatically exit Verix Terminal Manager and restart the terminal. Other operations require that you exit Verix Terminal Manager and restart the terminal. To manually exit Verix Terminal Manager, select **1> RESTART** in **VERIX TERMINAL MGR**.

Table 4 Enter Verix Terminal Manager

Display	Action
VERIFONE VX675 **QT65010M** **03/09/2012 Verix** **COPYRIGHT 1997-2012** **VERIFONE** **ALL RIGHTS RESERVED** **BATTERY 100%** **FOR STATUS PRESS KEY 3**	At startup, the terminal displays a copyright notice screen that shows the terminal model number, the OS version of the VX 675 stored in the terminal's memory, the date the firmware was loaded into the terminal, and the copyright notice. This screen appears for three seconds, during which time you can enter Verix Terminal Manager by simultaneously pressing **ENTER** and **7** key. You can extend the display period of this screen by pressing any key during the initial three seconds. Each keypress extends the display period an additional three seconds. If the battery has not been initially charged, the screen displays **BATTERY NOT CALIBRATED** to inform the user to initialize and condition the battery. For more information about the battery, refer to VX 675 Battery Information.
VERIFONE VX675 **QT65010M** **03/09/2012 Verix** ****TAMPER**** **COPYRIGHT 1997-2012** **VERIFONE** **ALL RIGHTS RESERVED**	If an attempt to break into the terminal's system has been made, the message ****TAMPER**** is displayed in place of the certificate. The terminal will remain in this state until the condition has been remedied.
<application prompt>	If an application already resides on the terminal, an application-specific prompt is displayed. Otherwise, an error message is displayed. For more information on startup errors, see STARTUP ERRORS.

Table 4 Enter Verix Terminal Manager (continued)

Display	Action
 **TERMINAL MGR ENTRY** **Please Enter Password** ________________	If an application prompt appeared and you chose to enter the terminal manager, you are prompted to type the system password. Use the default password “166831.” This password is entered as: **1 6 6 8 3 1**, and press **ENTER.** Use **CLEAR** to delete the entry and correct any mistakes. If you enter an incorrect password, the terminal exits the **TERMINAL MGR ENTRY** screen. Verify your password and reenter it. To quit this operation and return to the application prompt or **DOWNLOAD NEEDED** screen, press **CANCEL**.
 **VERIX TERMINAL MGR** **1> Restart** **2> Edit Parameters** **3> Download** **4> Memory Usage** **5> Directory Listing** **6> Clear Memory** **7> Calibrate Screen** **8> Terminal Info** **9> Diags** ⬇ ↑ ↓	The first of the two **VERIX TERMINAL MGR** menus is displayed. To go to **VERIX TERMINAL MGR** menu 2, tap the **DOWN** icon (⬇) on the left of the screen. To toggle with the submenus, use the **UP** (↑) and **DOWN** (↓) until you reach the desired menu then press **ENTER**. You can also choose an option in the menu by pressing the corresponding number on the keypad.

Menu 1

In this menu you can restart the terminal, edit parameters, download terminal software updates, check memory usage and availability, as well as view the contents of I: drive and F: drive directories. You can also clear the memory and calibrate the touchscreen.

Table 5 Verix Terminal Manager Menu 1

Display	Action
VERIX TERMINAL MGR **1> Restart** **2> Edit Parameters** **3> Download** **4> Memory Usage** **5> Directory Listing** **6> Clear Memory** **7> Calibrate Screen** **8> Terminal Info** **9> Diags** ⬇ ↑ ↓	To restart the terminal, select **1> RESTART**. To edit the parameters, select **2> EDIT PARAMETERS.** (For more information, refer to the Edit Keyed Files section that follows this main menu description.) To download applications, select **3> DOWNLOAD**. To view memory usage, select **4> MEMORY USAGE .** To view directory listing, select **5> DIRECTORY LISTING**. To clear the memory, select **6> CLEAR MEMORY**. To test and calibrate the screen, select **7> CALIBRATE SCREEN**. To view terminal information, select **8> TERMINAL INFO**. To view diagnostics, select **9>DIAGS.** To toggle to **VERIX TERMINAL MANAGER** menu 2, press **DOWN** icon (⬇) or to quit any operation within this menu, press **CANCEL**.
2> EDIT PARAMETERS	
VTM SELECT GROUP **GROUP ID: nn** **APP: <*APNAME or application or EMPTY or NOT EMPTY>** ⬆ ⬇	The file group number is represented as **Gnn or GROUP nn**. Type the **Group ID** of the file group (1 for the primary application; between 1–15 for other applications) into which to perform the download. (Refer to Chapter 6 for detailed download instructions and information). To select the **Group ID,** use the **UP** (⬆) and **DOWN** icon (⬇). The application name will appear if *APNAME is set in the group and also if there are files in the group selected. After you select a file group number, press **ENTER**.

Table 5 Verix Terminal Manager Menu 1 (continued)

Display	Action
VERIX TERMINAL MGR **Please enter** **Password for GID n:** ________________	To continue, enter the required password. If you enter an incorrect password, the following message appears: **Change Passwords Gn** **Please Try Again** Press **ENTER**. Verify your password and reenter it.
3> DOWNLOAD	
VERIX TERMINAL MGR **Group ID: _1**	To continue, enter the **Group ID**. The value of 1 is for the primary application while value between 1-15 is for other applications. Then, press **ENTER**. To return immediately to **VERIX TERMINAL MGR MENU** or to quit any operation within this menu, press **CANCEL**.
VTM DOWNLOAD MGR Gn **1> Single-app** **2> Multi-app** ↑ ↓	For a single application download, select **Single-app**. For multiple application download, select **Multi-app**. **Note:** Multi-app is only available for group 1. (Refer to Chapter 6 for detailed download instructions and information). To select, use the **UP** (↑) and **DOWN** icon (↓) then press **ENTER**. You can also choose an option in the menu by pressing the corresponding number on the keypad. To return to **VERIX TERMINAL MGR**, press **CANCEL**.

Table 5 Verix Terminal Manager Menu 1 (continued)

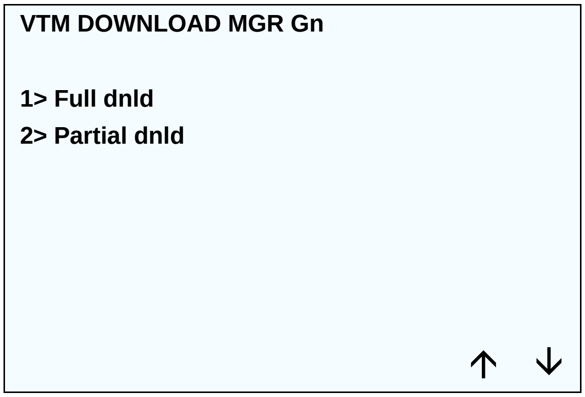
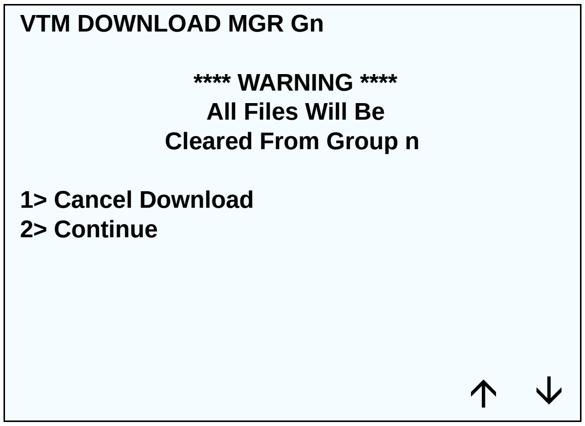
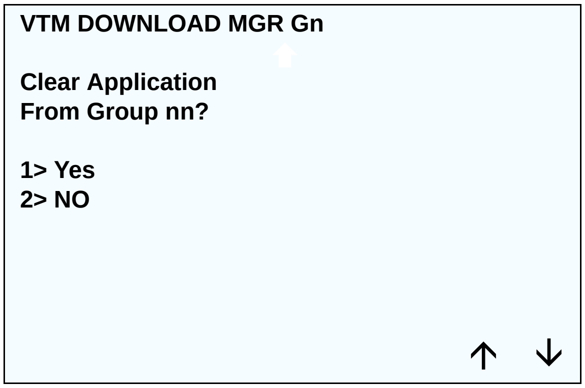
Display	Action
 **VTM DOWNLOAD MGR Gn** **1> Full dnld** **2> Partial dnld** ↑ ↓	Select the type of download mode: **Full dnld** or **Partial dnld.** A full download will delete all data on the group's memory. A partial download only adds new files to the group's memory. If a downloaded file is identical to an existing file in the memory, the existing file is replaced. To select**,** use the **UP** (↑) and **DOWN** icon (↓) then press **ENTER**. You can also choose an option in the menu by pressing the corresponding number on the keypad. To return to **VERIX TERMINAL MGR**, press **CANCEL**.
 **VTM DOWNLOAD MGR Gn** ****** WARNING ****** **All Files Will Be** **Cleared From Group n** **1> Cancel Download** **2> Continue** ↑ ↓	If you selected **FULL** on a single application download, a screen will appear warning you that all existing files in the selected group will be deleted. To return to **VERIX TERMINAL MGR**, press **CANCEL** or press **ENTER** to continue downloading an application.
 **VTM DOWNLOAD MGR Gn** **Clear Application** **From Group nn?** **1> Yes** **2> NO** ↑ ↓	If you selected **FULL** on a multiple application download, you will be prompted to clear the existing application on the currently selected group. Select **YES** to continue or **NO** to cancel downloading applications.

Table 5 **Verix Terminal Manager Menu 1** (continued)

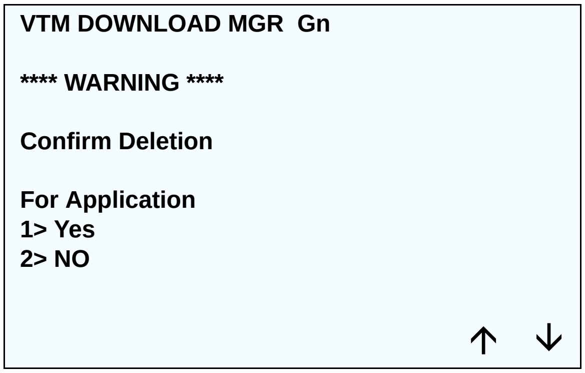
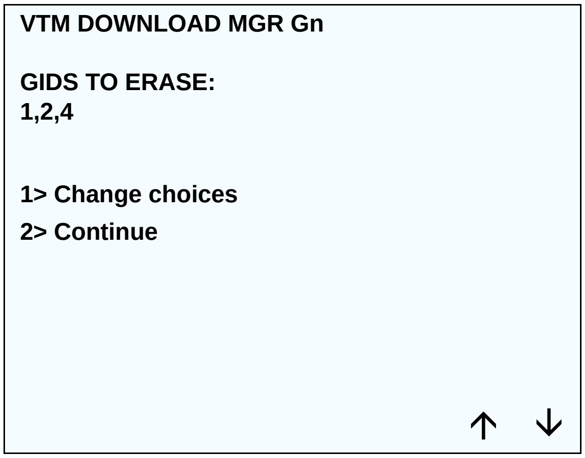
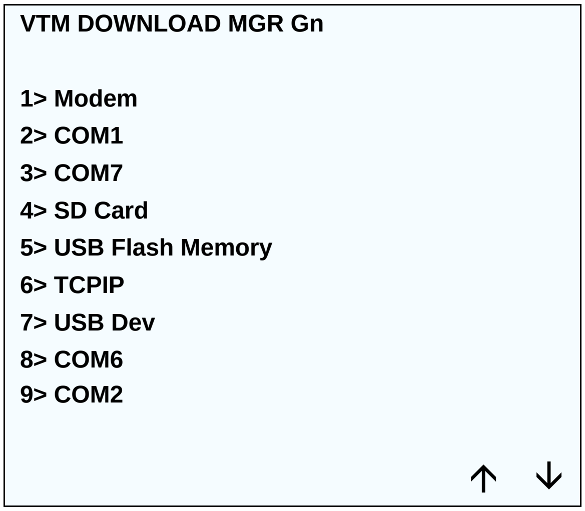
Display	Action
 **VTM DOWNLOAD MGR Gn** ****** WARNING ****** **Confirm Deletion** **For Application** **1> Yes** **2> NO** ↑ ↓	If you selected **YES** from the previous screen, a confirmation screen appears. Select **YES** to confirm or **NO** to cancel the deletion.
 **VTM DOWNLOAD MGR Gn** **GIDS TO ERASE:** **1,2,4** **1> Change choices** **2> Continue** ↑ ↓	If a FULL multiple download has been previously done, this screen appears instead of the previous two screens. This screen lists all the erased GIDs on the previous download. Select **CONTINUE** to erase all memory.
 **VTM DOWNLOAD MGR Gn** **1> Modem** **2> COM1** **3> COM7** **4> SD Card** **5> USB Flash Memory** **6> TCPIP** **7> USB Dev** **8> COM6** **9> COM2** ↑ ↓	If a Partial download has been selected, select the download mode in this screen. An application that supports the TCP stack is loaded with the OS to be able to use the **6> TCPIP** option. If no application can be found, an error message appears. **Note:** Not all listed options are available for all platforms. To return to the main menu without saving your selection, press **CANCEL**.

Table 5 **Verix Terminal Manager Menu 1** (continued)

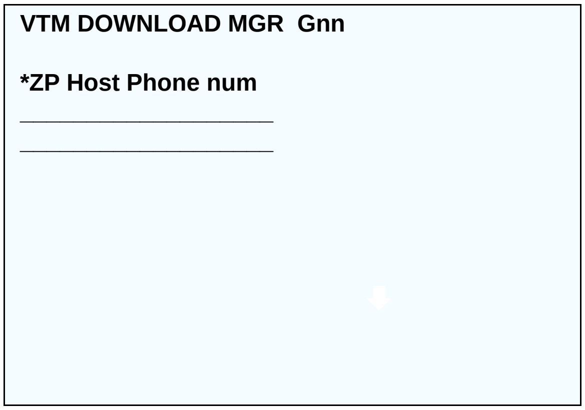
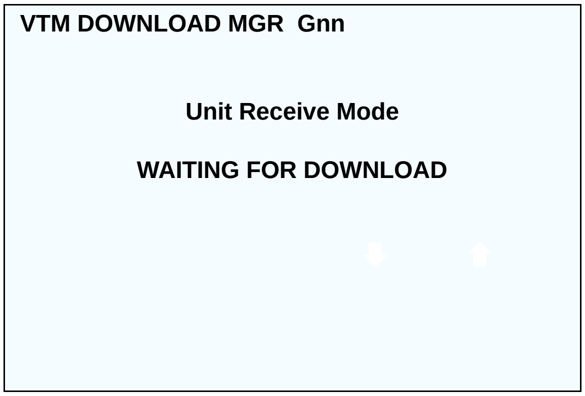
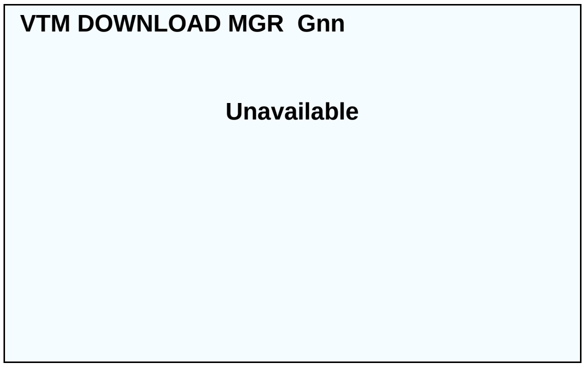
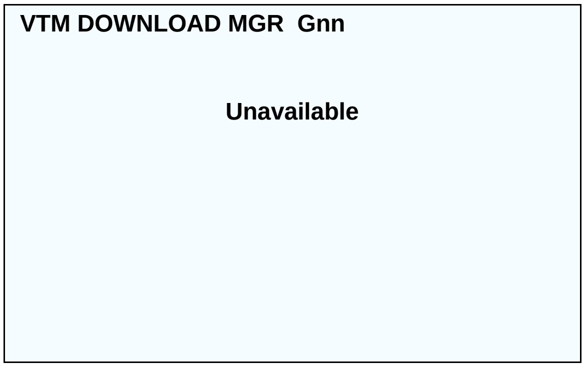
Display	Action
 **VTM DOWNLOAD MGR Gnn** ***ZP Host Phone num** ____________________ ____________________	If you selected **1> MODEM** and `*ZP` (host phone number) is not defined, you must enter valid phone number (up to 32 characters long) and press **ENTER**.
 **VTM DOWNLOAD MGR Gnn** **Unit Receive Mode** **WAITING FOR DOWNLOAD**	Select **2> COM1** to download via the COM 1 port. Select **3> COM7** to download via the COM 7 port. To return to the main menu without saving your selection, press **CANCEL**.
 **VTM DOWNLOAD MGR Gnn** **Unavailable**	Select **4> SD CARD** to download from a stored digital (SD) card. If no SD Card is inserted in the unit, the ‘Unavailable’ message is shown. To return to the main menu without saving your selection, press **CANCEL**.
 **VTM DOWNLOAD MGR Gnn** **Unavailable**	Select **5> USB FLASH MEMORY** to download from a memory stick. If no Memory Stick is inserted in the unit, the ‘Unavailable’ message is shown. To return to the main menu without saving your selection, press **CANCEL**.

Table 5 Verix Terminal Manager Menu 1 (continued)

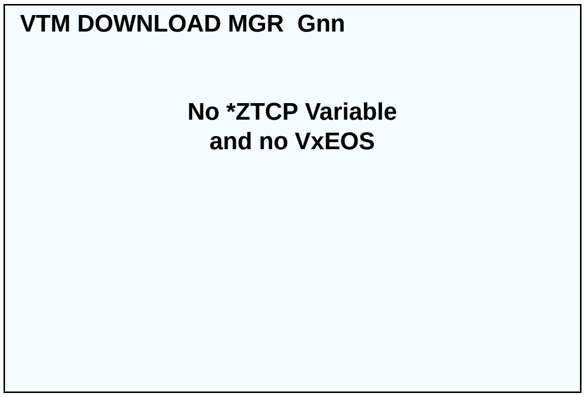
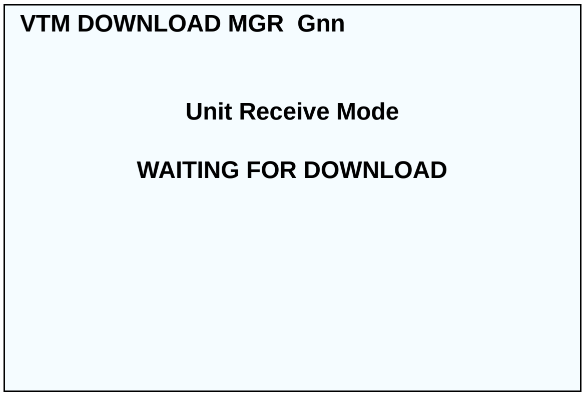
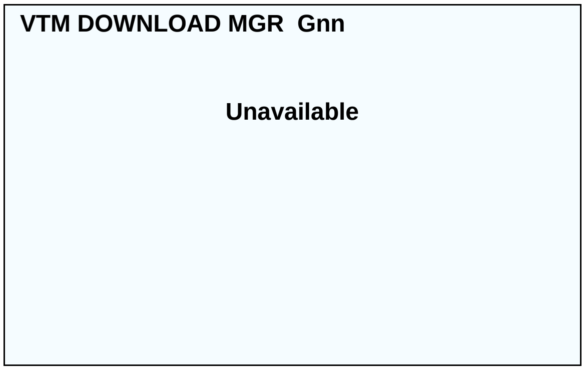
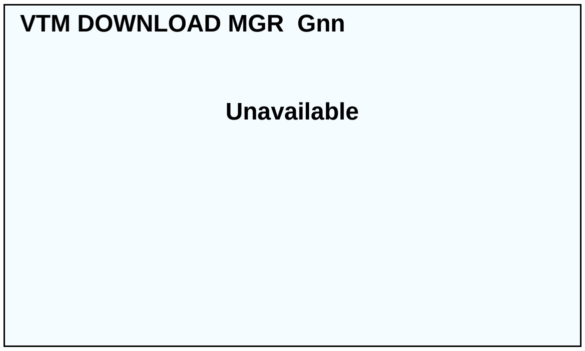
Display	Action
 **VTM DOWNLOAD MGR Gnn** **No *ZTCP Variable and no VxEOS**	Select **6> TCPIP** to download from your TCPIP connection. An application that supports the TCP stack is loaded with the OS to be able to use the **6> TCPIP** option. If no application can be found, an error message appears. Not all listed options are available for all platforms.
 **VTM DOWNLOAD MGR Gnn** **Unit Receive Mode** **WAITING FOR DOWNLOAD**	Select **7> USB DEV** to download using the USB connection. To return to the main menu without saving your selection, press **CANCEL.**
 **VTM DOWNLOAD MGR Gnn** **Unavailable**	Select **8> COM6** to download via the COM 6 port. To return to the main menu without saving your selection, press **CANCEL**.
 **VTM DOWNLOAD MGR Gnn** **Unavailable**	Select **9> COM2** to download via the COM 2 port. To return to the main menu without saving your selection, press **CANCEL**.

Table 5 **Verix Terminal Manager Menu 1** (continued)

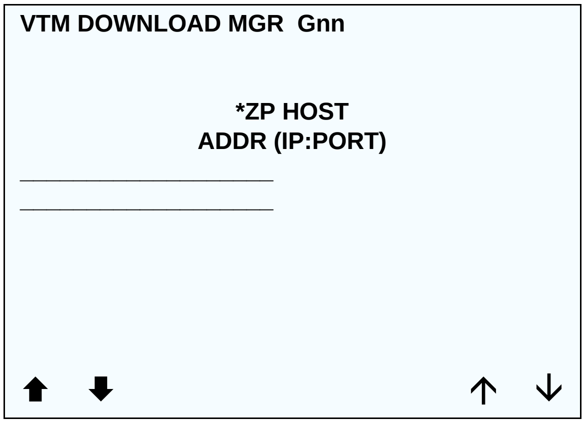
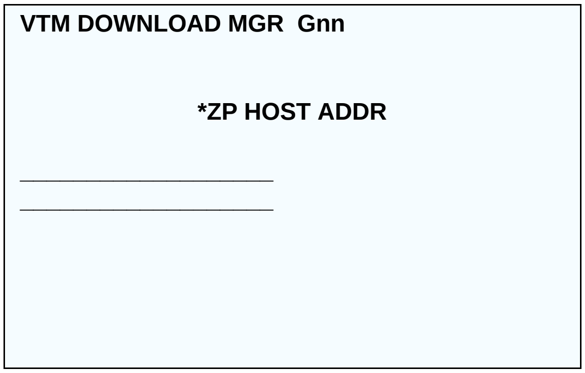
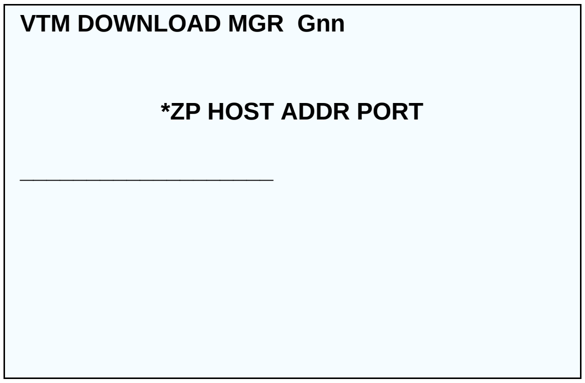
Display	Action
 VTM DOWNLOAD MGR Gnn *ZP HOST ADDR (IP:PORT) ____________________ ____________________ ⬆ ⬇ ↑ ↓	If you selected **6> TCPIP** and `*ZP` (TCP address) is not defined, you must enter a valid TCP address (up to 40 characters long including the colon and port number) and press **ENTER.**
 VTM DOWNLOAD MGR Gnn *ZP HOST ADDR ____________________ ____________________	
 VTM DOWNLOAD MGR Gnn *ZP HOST ADDR PORT ____________________	

Table 5 **Verix Terminal Manager Menu 1** (continued)

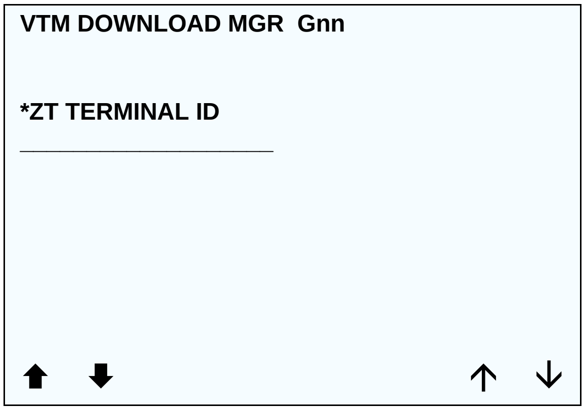
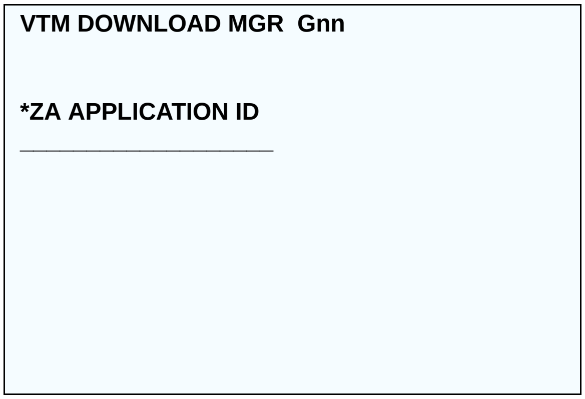
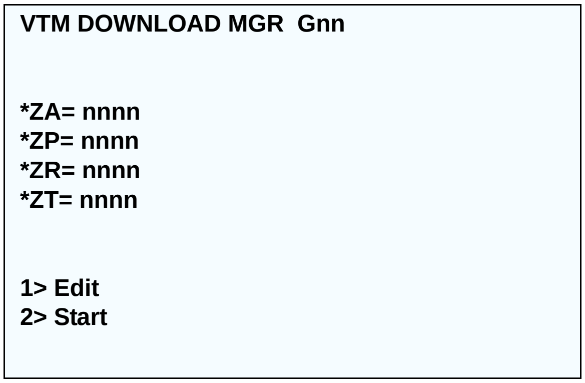
Display	Action
 **VTM DOWNLOAD MGR Gnn** ***ZT TERMINAL ID** ____________________ ⬆ ⬇ ↑ ↓	If *`ZT` (terminal ID used by VeriCentre) is not defined, you must enter a valid terminal ID (up to 15 characters long) and press **ENTER**.
 **VTM DOWNLOAD MGR Gnn** ***ZA APPLICATION ID** ____________________	If *`ZA` (application ID) is not defined, you must enter a valid application ID (up to 10 characters long) and press **ENTER.**
 **VTM DOWNLOAD MGR Gnn** ***ZA= nnnn** ***ZP= nnnn** ***ZR= nnnn** ***ZT= nnnn** **1> Edit** **2> Start**	You can view the specified values on the confirmation screen. Select **1> EDIT** to go back and modify the specifications or **2> START** to begin the download.

Table 5 Verix Terminal Manager Menu 1 (continued)

Display	Action
VTM DOWNLOAD MGR Gnn **UNIT RECEIVE MODE** ***________________	If you selected **2> COM1** or **3> COM7** , a line of asterisks appears that shows the percentage of completion. Each asterisk equals approximately 10% of the download. You can cancel a download in progress by pressing **CANCEL**. Doing so restarts the terminal.
VTM DOWNLOAD MGR **GROUP n PASSWORD** ____________________	**Note:** If you have not previously entered a group's password in this session, the terminal prompts for the group's password prior to downloading applications. To continue, enter the required password. If you enter an incorrect password, **PLEASE TRY AGAIN** appears. Press **ENTER**. Verify your password and reenter it.
4> MEMORY USAGE	
MEMORY USAGE **Drive I: Files 2** **Inuse 10 KB** **Drive F: Files 0** **Inuse 0** **RAM Avail 29168 KB** **FLASH Avail 124158 KB**	This screen displays how much mDRAM is used and how much is available. • **INUSE** - Closest estimate of used memory (in KB). • **AVAIL** - Lowest number of free memory (in KB). To return to the main menu, press **CANCEL**. **Note:** RAM memory is the terminal working memory. RAM memory is where the OS and applications execute. It is completely separate from the FLASH memory. FLASH memory is where code and data is stored when it is not executing. RAM and FLASH are physically different and are different sizes.

Table 5 Verix Terminal Manager Menu 1 (continued)

Display	Action
5> DIRECTORY LISTING	
NAVIGATION CONTROLS **2/8 Up/Down** **1/7 Page Up/Down** *** Send to Com Port** **# Send to Printer** **ENT Select** **CAN Return** **PRESS ENTER TO CONT**	To continue, enter the **Group ID**. The value of 1 is for the primary application while value between 1-15 is for other applications. Press **ENTER**. `CONFIG.SYS` protected records that begin with * or # are retained when you clear a mDRAM file group.
SELECT DRIVE **I :** **F:** **N:**	This screen shows the different **Directory.** To return to the main menu, press **CANCEL.** To return immediately to **VERIX TERMINAL MGR MENU 1** or to quit any operation within this menu, press **CANCEL**.

Table 5 Verix Terminal Manager Menu 1 (continued)

Display	Action
6> CLEAR MEMORY	
VERIX TERMINAL MGR **Group ID: _1**	To clear a file group's memory, enter the group ID. Press **ENTER**.
VERIX TERMINAL MGR **1> Clear CONFIG. SYS** **2> Clear Split Files** **3> Clear GID Files** **4> Clear All Groups** ↑ ↓	To choose an option in the menu, press the corresponding number on the keypad or scroll down to the option using the **DOWN** arrow then press **ENTER**. Use the **UP** key to scroll up the menu options. Select which files to delete: Select **1> CLEAR CONFIG.SYS** to delete only the `CONFIG.SYS` file. On the next screen, press 1 to completely delete the `CONFIG.SYS` file or 2 to retain protected records that begin with `*` or `#`. Select **2> Clear Split Files** delete only the split files. Select **3> CLEAR GID FILES** to delete all files in the currently selected file group from the memory. Select **4> CLEAR ALL GROUPS** to delete all files in all file groups. On the next screen, press 1 to cancel or 2 to confirm the deletion. This option is only available when file Group 1 is entered as the group ID. To go back to the second menu of the **VERIX TERMINAL MGR** without deleting files, press **CANCEL**.

Table 5 Verix Terminal Manager Menu 1 (continued)

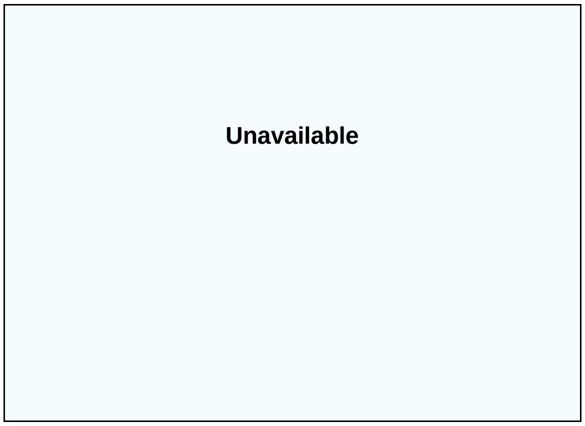
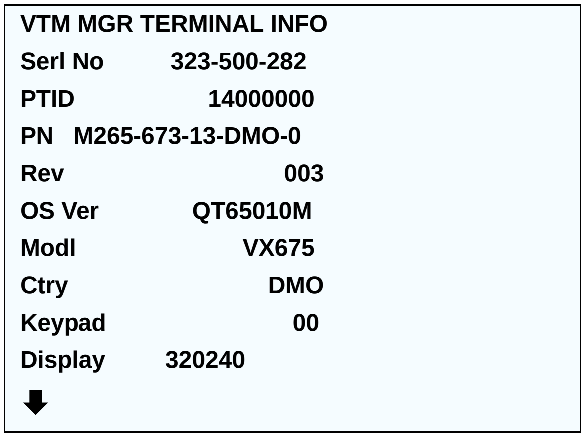
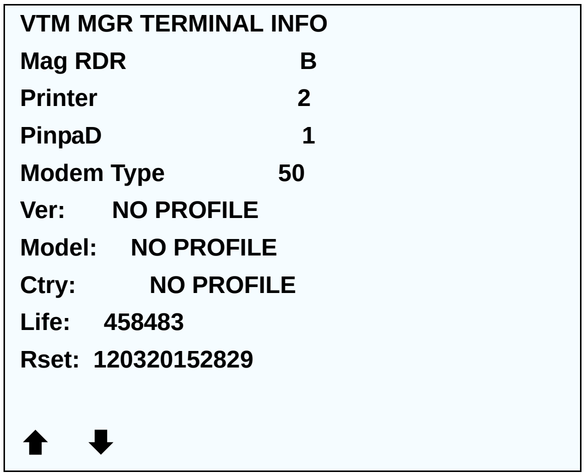
Display	Action
7> CALIBRATE SCREEN	
 **Unavailable**	This option is not available for this terminal.
8> TERMINAL INFO	
 **VTM MGR TERMINAL INFO** **Serl No 323-500-282** **PTID 14000000** **PN M265-673-13-DMO-0** **Rev 003** **OS Ver QT65010M** **Modl VX675** **Ctry DMO** **Keypad 00** **Display 320240** ⬇	This screen shows configuration information specific to your terminal: • Serial Number of the terminal • Permanent terminal identification number (**PTID**) • Terminal part number • Terminal hardware version number • Operating System version • Model Number of the terminal • Country of Manufacture • Display unit type • Keypad type (0 = Telco, 1 = Calculator, 2 = Singapore) • Magnetic stripe card reader type • Whether or not a PIN pad terminal is integrated into the terminal (where 0 = No, 1 = Yes) • Modem Type • Model Number of Modem
 **VTM MGR TERMINAL INFO** **Mag RDR B** **Printer 2** **PinpaD 1** **Modem Type 50** **Ver: NO PROFILE** **Model: NO PROFILE** **Ctry: NO PROFILE** **Life: 458483** **Rset: 120320152829** ⬆ ⬇	Your terminal's screen may vary depending on the model and operating system version installed. To return to the previous menu, press **CANCEL**.

Table 5 Verix Terminal Manager Menu 1 (continued)

Display	Action
VTM MGR TERMINAL INFO **Rcnt 2009** **Tamper Detected N** **Heap 1232** **Stack 2280** **CERT 531010** **1> Next Cert**	This screen shows additional configuration information specific to your terminal: • Number of seconds the terminal has run (**Life**) • Last reset date and time, in YYMMDDHHMMSS format (where YY = year, MM = month, DD = day, HH = hour, MM = minute, and SS = second). • Number of times the terminal has been reset (**Rcnt**) either through application control, a Verix Terminal Manager request, or a power cycle. • Notifies if a tamper event has occurred. • Shows the first certificate (**Cert**). • Displays the memory designation used by the OS (**Heap**). • Shows the memory set aside for the OS stack. This is where the terminal stores data for running tasks like all the parameters from the call (**Stack**). To return to the previous menu, press the **UP** key; to return main menu, press **CANCEL**.

Table 5 Verix Terminal Manager Menu 1 (continued)

Display	Action
9> DIAGS	
VERIX DIAGS MGR **1> Printer Diag** **2> IPP Diag** **3> ICC Diags** **4> Keyboard Diag** **5> Mag Card Diag** **6> Debugger** **7> Tamper Log** **8> RKL Log** **9> RKL Log export** ⬇ ↑ ↓	To choose an option in the menu, press the corresponding number on the keypad or scroll down to the option using the **DOWN** key and press **ENTER**. To run printer diagnostics and test the printer, select **1> PRINTER DIAG**. To test the internal PIN pad, select **2> IPP DIAG**. To test the ICC, select **3> ICC DIAGS**. To test the keyboard, choose **4> KEYBOARD DIAG**. To test the magnetic card, choose **5> MAG CARD DIAG**. To check the debugger, choose **6> DEBUGGER**. To view the Tamper logs, choose **7> Tamper Log** To view the RKL logs, choose **8> RKL Log** To view the RKL Log export, choose **9> RKL Log export**

Table 5 **Verix Terminal Manager Menu 1** (continued)

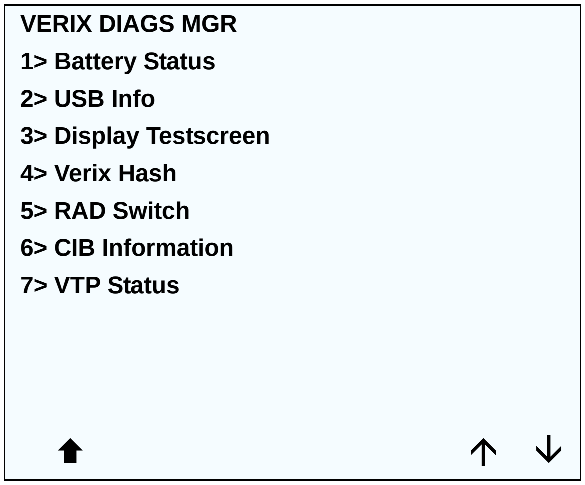
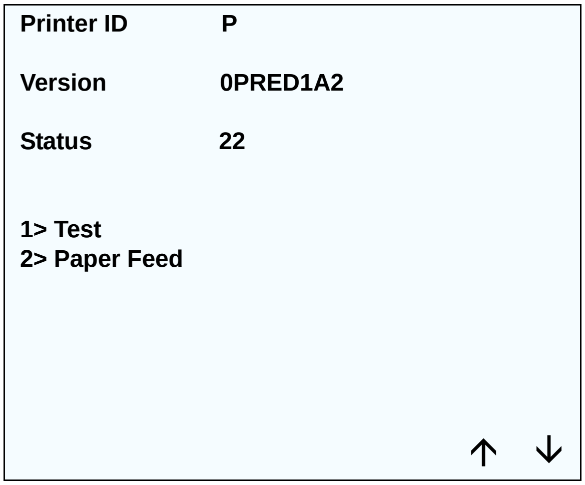
Display	Action
 **VERIX DIAGS MGR** **1> Battery Status** **2> USB Info** **3> Display Testscreen** **4> Verix Hash** **5> RAD Switch** **6> CIB Information** **7> VTP Status** ⬆ ↑ ↓	To choose an option in the menu, press the corresponding number on the keypad or scroll down to the option using the **DOWN** key and press **ENTER**. To view battery status, select **1> BATTERY STATUS** then press **ENTER**. To view USB info, select **2> USB INFO**. To run display screentest, choose **3> DISPLAY TESTSCREEN**, then press any three numbers from the keypad. To display Hash information, choose **4> VERIX HASH**. To run CDMA debugging, choose **5> RAD SWITCH**. (This option is not applicable to VX 675) To view CIB Information, choose **6> CIB Infromation** To view the VTP status, choose **7> VTP Status**
9> DIAGS 1> PRINTER DIAG	
 **Printer ID** **P** **Version** **0PRED1A2** **Status** **22** **1> Test** **2> Paper Feed** ↑ ↓	When you select **1> PRINTER DIAG**, the printer ID, firmware version, and the printer status appear. Press 1 to run the printer test. A print sample begins that uses approximately 30.5cm (12 in) of paper. This allows you to test the print quality and adjust your code for print optimization. Press 2 to run approximately 5cm (2 in) of paper through the printer without printing. To go back to the **VERIX DIAGS MGR** screen, press **CANCEL**.

Table 5 Verix Terminal Manager Menu 1 (continued)

Display	Action
9> DIAGS 2> IPP DIAG	
INTERNAL PIN PAD MEMORY TEST PASSED IPP8 EMUL02A 05/08 01 SN: 0000000000000000 BAUD: 1200 RESET 3 MODE: VISA EXIT 4	When you select 2, the **INTERNAL PIN PAD** screen appears and the diagnostic test begins. The firmware version and download date, IPP serial number, baud rate, and mode are displayed. To reset the IPP, press 1; to exit the test and return to the **VERIX DIAGS MGR** screen, press 2 or **CANCEL**.
9> DIAGS 3> ICC DIAGS	
VoyLib 03.09 0000 VxOS11 PSCR Build 10 SCRLIB 2.0 1/12 1> SMART CARD DIAG 2> LIST SYNC DRIVERS 3> EXIT	When you select 3, the software library version appears. Choose **1> SMART CARD DIAG** to run diagnostics on the Smart Card reader. Select **2> LIST SYNC DRIVERS** to view the drivers. Select **3> EXIT** to return to the **VERIX DIAGS MGR** screen.

Table 5 **Verix Terminal Manager Menu 1** (continued)

Display	Action
9> DIAGS 4> KEYBOARD DIAG	
TERMINAL MGR KBD TEST **KEYCODE nn**	This screen displays the hexadecimal ASCII keycode for each key you press. The value displayed corresponds to the actual key pressed. Other values assigned to keys are software dependent. To test the keyboard, press some keys and check that they match their keycodes (for example, the 1 key displays keycode 31). For more hexadecimal ASCII keycodes, refer to the ASCII table in Appendix D. To stop the test and return to the **VERIX DIAGS MGR** screen, press **CANCEL**.
9> DIAGS 5> MAG CARD DIAG	
VERIX TERMINAL MGR **TRK 1:VALID** **TRK 2:VALID** **TRK 3:VALID**	To test the magnetic-stripe card reader, swipe a magnetic-stripe card through it. A successful test displays **VALID DATA** for each track that reads valid data. An error generates one of the following error messages for each track with an error: • **NO DATA** • **NO START** • **NO END** • **LRC ERR** • **PARITY ERR** • **REVERSE END** For more information about magnetic card error messages, refer to the *Verix evo Volume I: Operating System Programmers Manual - VPN DOC00301*.

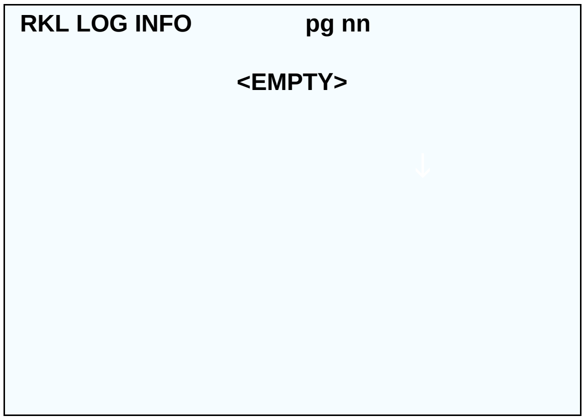
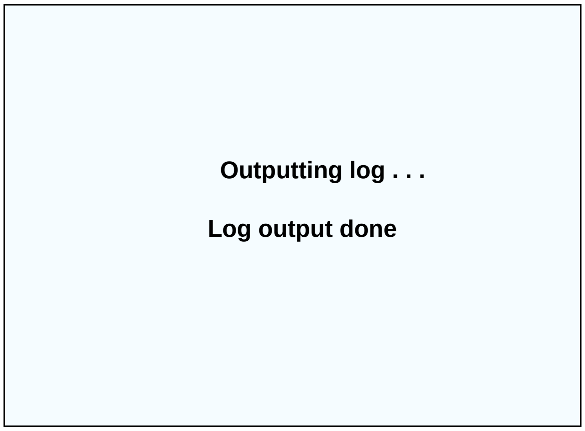
Table 5 Verix Terminal Manager Menu 1 (continued)

Display	Action
9> DIAGS 6> DEBUGGER	
VERIX TERMINAL MGR **Group ID: nn**	
VERIX TERMINAL MGR **Please enter** **Password for GID nn** ______________________	Enter the current password for the selected file group and press **ENTER**. If you enter an incorrect password, **PLEASE TRY AGAIN** appears. Press **ENTER**. Verify your password and reenter it. To return to the **VERIX DIAGS MGR** screen press **CANCEL**.

Table 5 Verix Terminal Manager Menu 1 (continued)

Display	Action
9> DIAGS 7> TAMPER LOGS	
TAMPER LOG **03/13/12 19:38 CLEAR** **03/13/12 19:36 020000** **01/01/00 17:07 CLEAR** **01/01/00 00:00 7FFFFF** **01/01/00 00:57 CLEAR** **01/01/00 00:00 7FFFFF**	The Tamper Log screen displays a list of possible tamper events. The list is sorted from the most current tamper event to the oldest event. The date is displayed in MM/DD/YY format, while the time is displayed as a 24-hour clock. Contact your Verifone representative for information about the events. Press any key to return to **VERIX TERMINAL MGR MENU 2**.
TAMPER LOG **<EMPTY>**	If the Tamper Log is empty, **<EMPTY>** is displayed on the screen. To go back to the **VERIX DIAGS MGR** screen, press **CANCEL**.

Table 5 Verix Terminal Manager Menu 1 (continued)

Display	Action
9> DIAGS 8> RKL LOG	
 **RKL LOG INFO pg nn** **<EMPTY>**	To go back to the **VERIX DIAGS MGR** screen, press **CANCEL**.
9> DIAGS 8> RKL LOG	
 **Outputting log . . .** **Log output done**	To go back to the **VERIX DIAGS MGR** screen, press **CANCEL**.

Menu 2

In this menu, you can view the terminal configuration information, change system passwords, perform remote diagnosis, view error and tamper logs, update time and date, load IPP key and adjust display contrast. Some application program downloads automatically reset the system password.

Edit Keyed Files

A keyed file is a collection of individual records that contain ASCII data and are identified by unique search keys. You can edit the ASCII data directly from the terminal keypad using the terminal's built-in keyed file editor by selecting option 2, **EDIT PARAMETERS**, on the first VTM menu. Each record has two parts: a key name and a key value. The search key is a variable-length string of up to 32 characters in length, or key name, that identifies the record. The information assigned to the search key is contained in a separate variable-length string from 1-128 characters in length, or key value.

For example, in `CONFIG.SYS`, the key name for the application serial ID number is *ZT. The value for the key is the actual application ID number. By entering *ZT using the editor, the terminal can quickly locate the application serial ID number. You can also use **ENTER** to scroll through the search keys instead of entering the characters *ZT through the keypad. The keys are displayed in the order in which it has been entered, not in alphabetic order.

NOTE

For a complete list of the ASCII characters supported by the VX 675 series, as well as their decimal and hexadecimal equivalents, please refer to ASCII Table.

CONFIG.SYS: Protected and Non-protected Records

The concept of protected and non-protected records applies only to the `CONFIG.SYS` files in your terminal. Protected records are those with search keys beginning with an asterisk (*) or a pound/hash symbol (#).

Protected records in the file Group 1 `CONFIG.SYS` file are retained in a full application download and when memory is cleared. Non-protected records are all other `CONFIG.SYS` files, and records of other files. These records are deleted when memory is cleared.

Editing CONFIG.SYS with an External Editor

You can create and edit the `CONFIG.SYS` files of VX 675 applications through an IBM PC-compatible computer when you download files to the terminal. For more information on editing an application's `CONFIG.SYS` file, refer to the VeriCentre Reference Manual and the *Verix eVo Volume I: Operating System Programmers Manual* (VPN DOC00301), or contact your local Verifone representative.

For more information about using VeriCentre Download Management Module in client/server installations, please contact your local Verifone representative.

Table 6 Verix Terminal Manager Menu 2

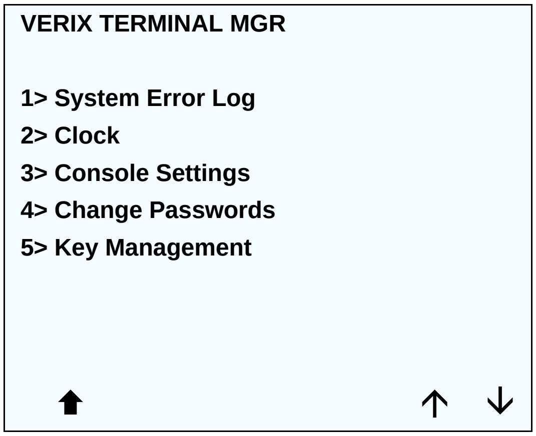
Display	Action
 **VERIX TERMINAL MGR** **1> System Error Log** **2> Clock** **3> Console Settings** **4> Change Passwords** **5> Key Management** ⬆ ↑ ↓	To view the error and tamper logs, select **1>SYSTEM ERROR LOG**. To set the date and time, select **2> CLOCK**. To adjust the display contrast, beeper and backlight, select **3> CONSOLE SETTINGS**. To change the Verix Terminal Manager and file group passwords, select **4> CHANGE PASSWORDS**. The file groups and Verix Terminal Manager all use a default password preset at the factory: 166831. It is entered as: **1 6 6 8 3 1** and press **ENTER**. To test the IPP and RKL key load, select **5> KEY MANAGEMENT**. To return to the Terminal Manager Menu 1, press the **UP** (⬆) icon on the left side of the screen. To quit any operation within this menu, press **CANCEL**.

Table 6 Verix Terminal Manager Menu 2 (continued)

Display	Action
1> SYSTEM ERROR LOG	
VERIX ERROR LOG **Type 2 OS QT65010M** **Task 3 GID 1** **Time 120314193309** **CPSR 60000010** **PC 00000024** **LR 7042018B** **Addr 00000000**	The error log screens display internal diagnostic information about the most recent unrecoverable software error. If you report a terminal problem, you may be asked to provide this information. This screen displays the following: • **TYPE** (error type), where the error type code is: • 1 = Data abort: attempt to access data at an invalid address • 2 = Program abort: attempt to execute code at an invalid address • 3 = Undefined abort: attempt to execute an illegal instruction • **TASK** (task number): indicates type of task that was currently executed: • 1 = Verix Terminal Manager • 2 = first user task • **TIME** (time of crash): clock time of the error in the format *YYMMDDhhmmss*, where *YY* = year, *MM* = month, *DD* = day, *hh* = hour, *mm* = minute, and *ss* = second • **CPSR** (Current Program Status Register): contains the processor and state condition code • **PC** (Program Counter): holds the execution address • **LR** (Link Register): holds the return address of the function call **Note:** LR may not always contain the current return address. • **ADDR** (fault address): contains the illegal address that the application was trying to access. Press any key to return to **VERIX TERMINAL MGR MENU 2**.

Table 6 Verix Terminal Manager Menu 2 (continued)

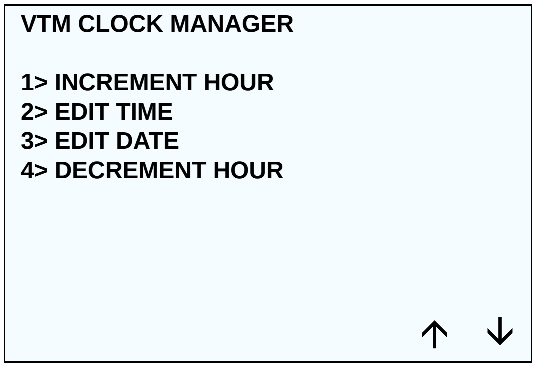
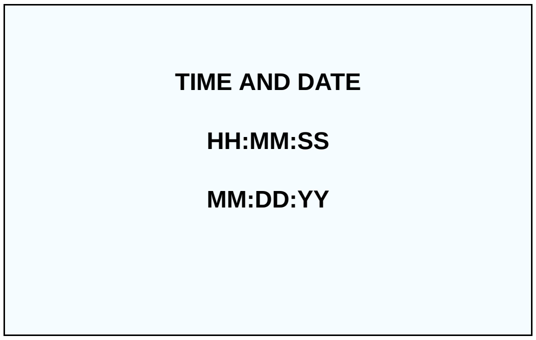
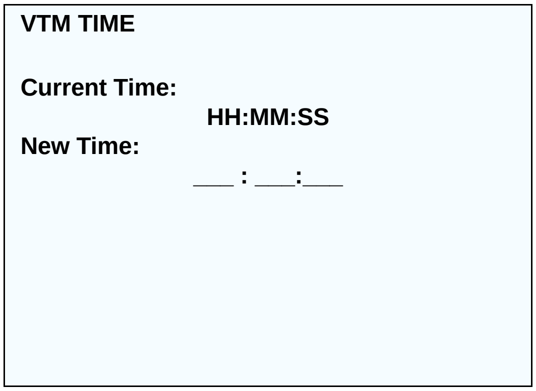
Display	Action
2> CLOCK	
 **VTM CLOCK MANAGER** **1> INCREMENT HOUR** **2> EDIT TIME** **3> EDIT DATE** **4> DECREMENT HOUR** ↑ ↓	To adjust the current time one hour forward, select **1> INCREMENT HOUR.** To see the time, select **2> EDIT TIME**. To set the date, select **3> EDIT DATE**. To adjust the current time one hour back, select **4> DECREMENT HOUR.** The terminal clock is battery-backed to retain date and time settings when the terminal is shut off. **Note:** The terminal clock is battery-backed to retain date and time settings when the terminal is shut off.
2> CLOCK 1> INCREMENT HOUR	
 **TIME AND DATE** **HH:MM:SS** **MM:DD:YY**	Select **1> INCREMENT HOUR** to add an hour to the current time setting.
2> CLOCK 2> EDIT TIME	
 **VTM TIME** **Current Time:** **HH:MM:SS** **New Time:** ___ : ___:___	Enter the new time in *HOURS:MINUTES:SECONDS* (HH:MM:SS) format. To correct a mistake, press **CLEAR** to delete and enter the correct number; press **ENTER** to set the new time. The current time and date is then displayed on the next screen. Press **CANCEL** to return to the third menu of the **VERIX TERMINAL MGR.**

Table 6 Verix Terminal Manager Menu 2 (continued)

Display	Action
2> CLOCK 3> EDIT DATE	
VTM DATE **Current Date:** **HH:MM:SS** **New Date:** **___ / ___ / ___**	Enter the new date in *MONTH/DAY/YEAR* (MM/DD/YY) format. To correct a mistake, press **CLEAR** to delete and enter the correct number; press **ENTER** to set the new date. The current time and date is then displayed on the next screen. Press **CANCEL** to return to the third menu of the **VERIX TERMINAL MGR**.
2> CLOCK 4> DECREMENT HOUR	
TIME AND DATE **HH:MM:SS** **MM:DD:YY**	Select **4> DECREMENT HOUR** to reduce an hour from the current time setting.
3> CONSOLE SETTINGS	
VTM CONSOLE MGR **1> Console Beeper OFF** **2> Console Beeper ON** **3> Backlight DOWN** **4> Backlight UP** **5> Keypad BL DOWN** **6> Keypad BL UP** **7> Contrast DOWN** **8> Contrast UP** ↑ ↓	Turn the terminal beeper sounds on or off by pressing the **1** or **2** key. Switch the backlight on or off by pressing the **3** or **4** key. Select **5> CONTRAST DOWN** or **6> CONTRAST UP** to increase or decrease display contrast respectively. To return to the main menu and save your changes, press **ENTER**. Otherwise, press **CANCEL** to go back to the second menu of the **VERIX TERMINAL MGR** without saving the changes.

Table 6 Verix Terminal Manager Menu 2 (continued)

Display	Action
4> CHANGE PASSWORDS	
VTM PASSWORD MGR **1> File Group** **2> TERMINAL MGR Entry** ↑ ↓	To change the password of file Group, select **FILE GROUP**. Then, go to the **GROUP nn PASSWORD** procedure below. See Passwords for more information. To change the password of another file group, select File Group, enter the appropriate file group number and press **ENTER**. Then, go to the **NEW PASSWORD** procedure below. To correct a mistake, press **CLEAR** to delete the number, and enter the new entry. To change the system password, select **TERMINAL MGR ENTRY**. Then, skip to **TERMINAL MGR PASSWORD NEW** below. **Note:** Some application program downloads automatically reset the Verix Terminal Manager password.
VERIX TERMINAL MGR **Please enter** **Password for GID n:** ____________________	Enter the current password for the selected file group and press **ENTER**. If you enter an incorrect password, the following message appears: **Change Passwords Gn** **Please Try Again** Press **ENTER**. Verify your password and reenter it.
TERMINAL MGR ENTRY **Please Enter Password** ____________________	Enter the current password for the terminal and press **ENTER**. If you enter an incorrect password, the following message appears: **Change Passwords** **Please Try Again** Press **ENTER**. Verify your password and reenter it.

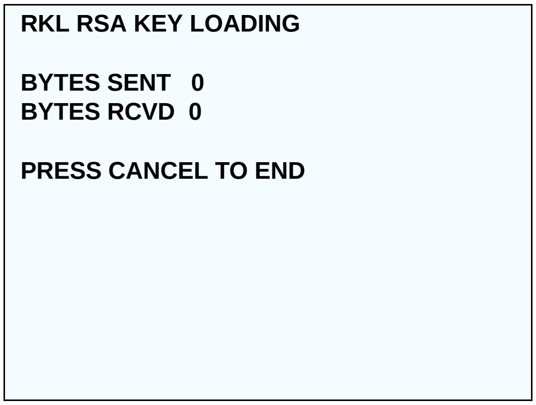
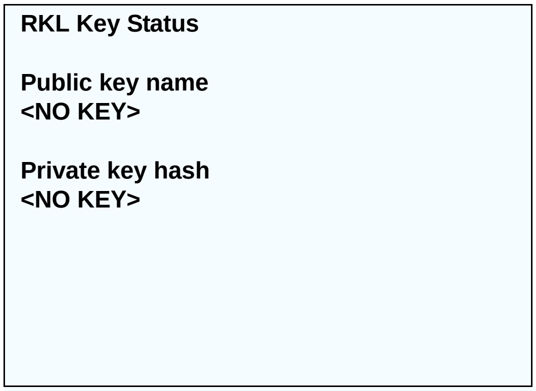
Table 6 Verix Terminal Manager Menu 2 (continued)

Display	Action
VTM PASSWORD MGR **New** ___________________	Type the new password and press **ENTER**. To correct a mistake, press **CLEAR** to delete the entry and then reenter the new password.
VTM PASSWORD MGR **Again** ___________________	The terminal requests that you verify the new password. Reenter the new password and press **ENTER**.
5> KEY MANAGEMENT	
Key Management **1> IPP Key Load** **2> RKL Key Load** **3> RKL Key Status** ↑ ↓	Select either **1> IPP Key Load** or **2> RKL Key Load** to download the appropriate keys. Select **3> RKL Key Status** to display the RKL public key and private key hash. To select**,** use the **UP** (↑) and **DOWN** icon (↓) then press **ENTER**. You can also choose an option in the menu by pressing the corresponding number on the keypad. To return to **VERIX TERMINAL MGR**, press **CANCEL**.

Table 6 **Verix Terminal Manager Menu 2** (continued)

Display	Action
5> KEY MANAGEMENT 1> IPP KEY LOAD	
VERIX TERMINAL MGR **Please enter** **Password for GID nn** ____________________	Enter the current password for the selected file group and press **ENTER**. **Note:** This requires group 1 privileges and the group 1 password. If you enter an incorrect password, **PLEASE TRY AGAIN** appears. Press **ENTER**. Verify your password and reenter it.
INTERNAL PIN PAD **KEY LOADING MODE** **BYTES SENT 0** **BYTES RCVD 0** **Press 1 to END**	Select this mode when you use the SecureKit or programming from your PC to inject keys into your terminal. In this mode, a pass-through connection is established between COM1 and COM5 (IPP port) to allow key loading. Press **CANCEL** to stop the key load session; Press 1 to **END** when finished with the key load. **Note:** The connection times out after a minute if the key loading does not start.
5> KEY MANAGEMENT 2> RKL KEY LOAD	
VERIX TERMINAL MGR **Please enter** **Password for GID nn** ____________________	Enter the current password for the selected file group and press **ENTER**. If you enter an incorrect password, **PLEASE TRY AGAIN** appears. Press **ENTER**. Verify your password and reenter it.

Table 6 Verix Terminal Manager Menu 2 (continued)

Display	Action
 **RKL RSA KEY LOADING** **BYTES SENT 0** **BYTES RCVD 0** **PRESS CANCEL TO END**	Press **CANCEL** to stop the key load session.
5> KEY MANAGEMENT 3> RKL KEY STATUS	
 **RKL Key Status** **Public key name** **<NO KEY>** **Private key hash** **<NO KEY>**	Press **ENTER** to view the Private Key Hash. Press **CANCEL** to return to the **KEY MANAGEMENT** screen.

NOTE

When entering any password, an asterisk (*) appears on the display screen for each character you type. These asterisks prevent your password from being seen by an unauthorized person. Pressing the **CLEAR** key changes the characters or symbols you enter, but does not cause additional asterisks to appear. Secure a copy of every password to ensure it is not forgotten or lost.

CHAPTER 5

File Authentication

This chapter discusses the following VeriShield Retain file authentication security architecture, VeriShield Retain file authentication module, and the organizational infrastructure that supports it (see Introduction to File Authentication).

This chapter also explains how the file authentication process may affect the tasks normally performed by application programmers, terminal deployers, site administrators, or entities authorized to download files to a VX 675 terminal (see File Authentication and the File System).

Lastly, this chapter explains how to generate the signature files required to perform downloads and authenticate files on the VX 675 terminal using the file signing utility (see VeriShield File Signing Tool).

In Chapter 6, the topic of file authentication is also discussed in the context of specific file download procedures.

Introduction to File Authentication

The VX 675 terminal uses the VeriShield Retain security architecture, which has both physical and logical components. The logical security component of the VeriShield Retain architecture, which is part of the terminal's operating system software, is called the file authentication module.

File authentication is a secured process for authenticating files using digital signatures, cryptographic keys, and digital certificates. This process makes it possible for the sponsor of a VX 675 terminal to logically secure access to the terminal by controlling who is authorized to download application files to that terminal. It verifies the file's origin, sender's identity, and integrity of the file's information.

The Verifone Certificate Authority

To manage the tools and processes related to the file authentication module of the VeriShield Retain security architecture, Verifone has established a centralized Verifone Certificate Authority, or Verifone CA. This agency is responsible for managing keys and certificates. The Verifone CA uses an integrated set of software tools to generate and distribute digital certificates and private cryptographic keys to customers who purchase VX 675 terminals.

Special Files Used in the File Authentication Process

The following specially formatted files support the file authentication process:

- A **digital certificate** is a digital public document used to verify the signature of a file.
- A **digital signature** is a piece of information based on both the file and the signer's private cryptographic key. The file sender digitally signs the file using a private key. The file receiver uses a digital certificate to verify the sender's digital signature.
- **Signer private keys** (`*.key` files) are securely conveyed to clients on smart cards. The secret passwords required by clients to generate signature files, using signer private keys, are sent as PINs over a separate channel such as registered mail or encrypted e-mail.

Some files, such as private key files, are encrypted and password protected for data security. Others, such as digital certificates and signature files, do not need to be kept secure to safeguard the overall security of VeriShield Retain.

Within the VeriShield File Signing Tool tool, you can recognize the special file types that support the file authentication process by the filename extensions listed in Table 7.

Table 7 VeriShield File Signing Tool Filename Extensions

File Type	Extension
Signature	`*.p7s`
Private key	`*.key`
Digital certificate	`*.crt`

All digital certificates are generated and managed by the Verifone CA, and are distributed on request to VX 675 clients—either internally within Verifone or externally to sponsors.

All certificates issued by the Verifone CA for the VX 675 platform, and for any Verifone platform with the VeriShield Retain security architecture, are hierarchically related. That is, a lower-level certificate can only be authenticated under the authority of a higher-level certificate.

The security of the highest-level certificate, called the platform root certificate, is tightly controlled by Verifone.

Certificates Contain Keys That Authenticate Signature Files

- Sponsor certificate: Certifies a client's sponsorship of the terminal. It does not, however, convey the right to sign and authenticate files. To add flexibility to the business relationships that are logically secured under the file authentication process, a second type of certificate is usually required to sign files.

A sponsor certificate is authenticated under a higher-level system certificate, called the application partition certificate.

NOTE Only one sponsor certificate is permitted per terminal. An application cannot be loaded without both a Sponsor and signer certificate.

- Signer certificate: Certifies the right to sign and authenticate files for terminals belonging to the sponsor.

  A signer certificate is authenticated under the authority of a higher-level client certificate (the sponsor certificate).

The required sponsor and signer certificates must either have been previously downloaded and authenticated on the terminal, or they must be downloaded together with the new signature and target files to authenticate.

Signer Private Keys Are Issued to Secure the File Signing Process

Signer private keys are loaded onto a smart card. This smart card is securely delivered to the business entity that the terminal sponsor has authorized to sign, download, and authenticate applications to run on the sponsor's terminal.

NOTE The signer private keys loaded onto the smart card is the only copy of the private key.

The Verifone CA can also issue additional sets of sponsor and signer certificates, signer private keys to support multiple sponsors, and multiple signers for a specific platform.

To establish the logical security of applications to download to a VX 675 terminal, the designated signer uses the signer private key issued by the Verifone CA as this is a required input to the VeriShield File Signing Tool.

A signature file is generated using a signer private key. Successful authentication depends on whether the signer private key used to sign the target file matches the signer certificate stored in the terminal's certificate tree.

How File Authentication Works

File authentication consists of three basic processes:

1. **Development:** The VeriShield File Signing Tool creates a signature file for each application file to authenticate.
2. **Pre-deployment:** An optimal certificate structure is determined, and the necessary certificates and keys are created.
3. **Deployment:** The development and pre-deployment processes, once complete, are used in combination to prepare a terminal for deployment.

Development Process

In this process:

1 The application developer creates an application file.

2 The application developer applies for Sponsor and Signer certificates. The absence of a “default” signer certificate compels developers to apply for a dedicated Signer certificate.

3 The developer assigns a name to the application file.

4 The application file becomes a required input for the VeriShield File Signing Tool.

5 Using the application file, Signer certificate, and Signer password, the VeriShield File Signing Tool creates a signature file (`*.p7s`).

6 The signature file and the original application file are loaded into a development terminal, where the following actions occur:

   a The terminal’s operating system searches for signature files.

   b When a signature file is found, the operating system then searches for a matching application file.

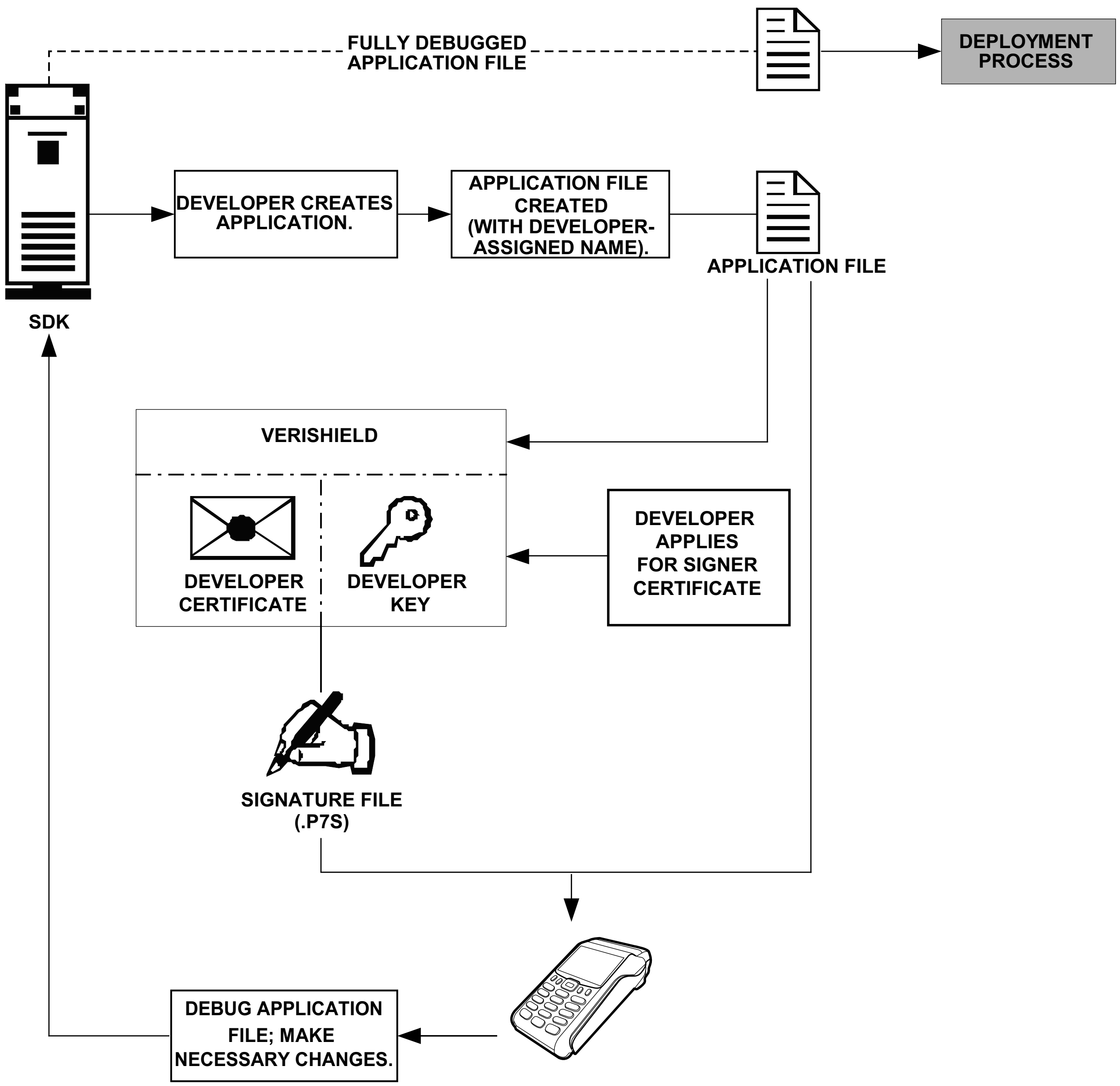
   c When a matching application file is found, the operating system compares the signature file’s signature against the values stored in the application file’s calculated signature.

   d If these values match, the operating system marks the application file “authenticated” and allows it to run.

7 The application file is tested and debugged.

8 After the application file is fully debugged, it becomes an input for the deployment process.

The following diagram describes the development process.


FULLY DEBUGGED APPLICATION FILE
DEPLOYMENT PROCESS
DEVELOPER CREATES APPLICATION.
APPLICATION FILE CREATED (WITH DEVELOPER-ASSIGNED NAME).
APPLICATION FILE
SDK
VERISHIELD
DEVELOPER CERTIFICATE
DEVELOPER KEY
DEVELOPER APPLIES FOR SIGNER CERTIFICATE
SIGNATURE FILE (.P7S)
DEBUG APPLICATION FILE; MAKE NECESSARY CHANGES.

1) DEVELOPMENT OS SEARCHES FOR A .P7S FILE.
2) IF A .P7S FILE IS FOUND, OS THEN SEARCHES FOR A MATCHING APPLICATION FILE.
3) IF A MATCHING APPLICATION FILE IS FOUND, OS COMPARES .P7S FILE'S SIGNATURE AGAINST VALUES IN THE APPLICATION FILE'S CALCULATED SIGNATURE.
4) IF THE VALUES MATCH, THE TWO FILES ARE AUTHENTICATED, AND THE ATTR_NOT_AUTH BIT IS SET TO 0.

Figure 27 The Development Process

Pre-Deployment Process

In this process:

1. A sponsor goes to the Verifone CA Web site and requests certificates for deployment terminals.
2. Based on information provided by the sponsor through the Verifone CA Web site, the Verifone CA determines the required certificate structure.
3. The Verifone CA generates the following items for the sponsor:
   a. Smart card containing a set of certificates and private key.
   b. Smart card PIN.
4. The Verifone CA sends the smart card and smart card PIN to the sponsor.
5. The sponsor uses the smart card and smart card PIN as inputs for the deployment process.

Figure 28 illustrates the pre-deployment process.

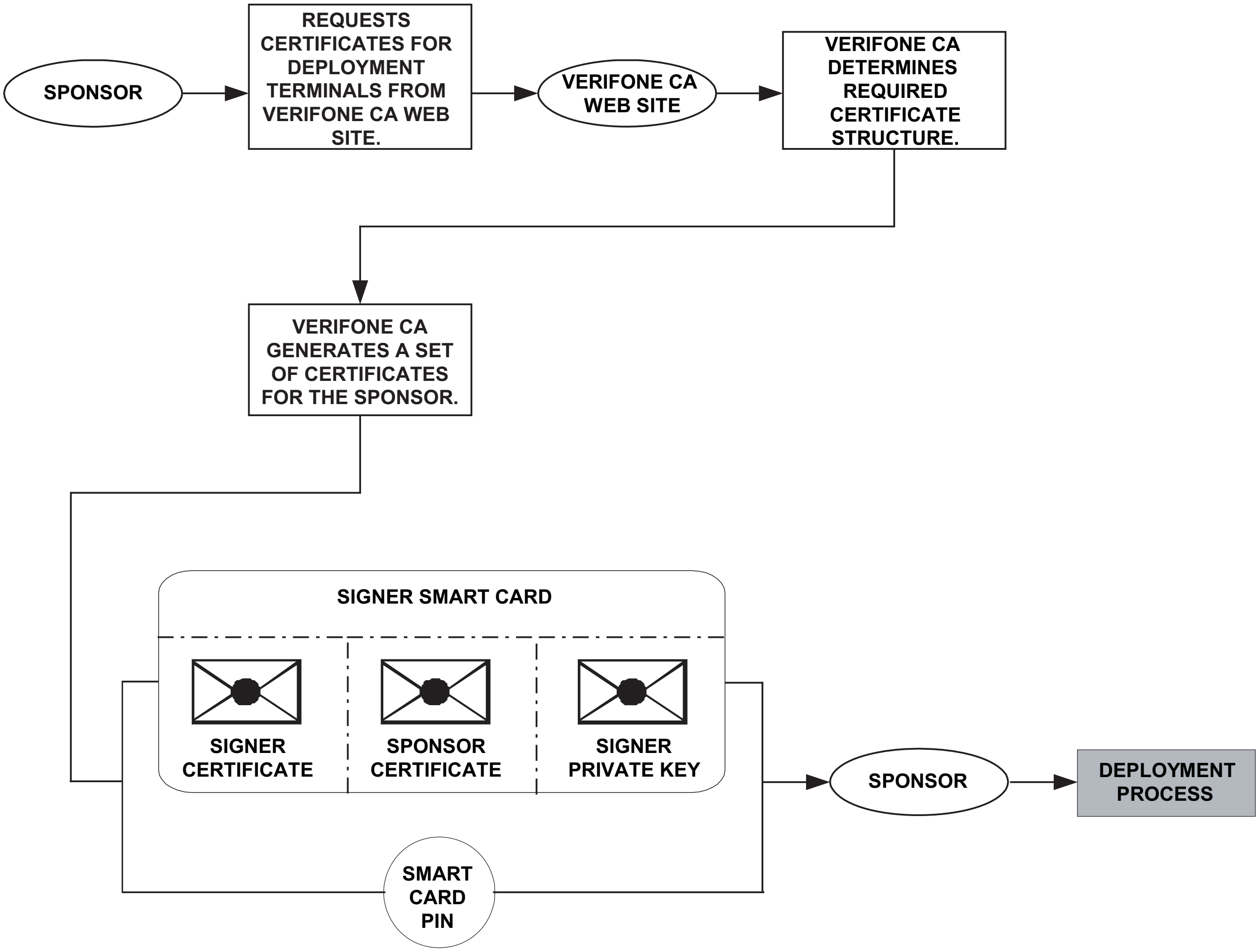

SPONSOR
REQUESTS CERTIFICATES FOR DEPLOYMENT TERMINALS FROM VERIFONE CA WEB SITE.
VERIFONE CA WEB SITE
VERIFONE CA DETERMINES REQUIRED CERTIFICATE STRUCTURE.
VERIFONE CA GENERATES A SET OF CERTIFICATES FOR THE SPONSOR.
SIGNER SMART CARD
SIGNER CERTIFICATE
SPONSOR CERTIFICATE
SIGNER PRIVATE KEY
SMART CARD PIN
SPONSOR
DEPLOYMENT PROCESS

Figure 28 The Pre-Deployment Process

Deployment Process (see Figure 29)

In this process:

1. The sponsor provides the application file (from the development process), the smart card, and smart card PIN (from the pre-deployment process) as inputs to VeriShield Retain.
2. VeriShield Retain extracts the signer key, signer certificate, and sponsor certificate from the smart card.
3. VeriShield Retain uses the extracted data, along with the application file, to create a signature file (`*.p7s`).
4. VeriShield Retain creates files suitable for downloading from the extracted smart card data.
5. The signature file, application file, and extracted signer and sponsor certificates are downloaded into a deployment terminal, where the following actions occur:
   - a The terminal's operating system searches for signature files.
   - b If a signature file is found, the operating system then searches for a matching application file.
   - c If a matching application file is found, the operating system compares the signature file's signature against the values stored in the application file's calculated signature.
   - d If these values match, the operating system marks the application file "authenticated" and allows it to run.
6. Each successfully authenticated executable application file is allowed to run on the terminal (otherwise, the executable remains stored in the terminal memory but is not allowed to run).

Figure 29 illustrates the deployment process.

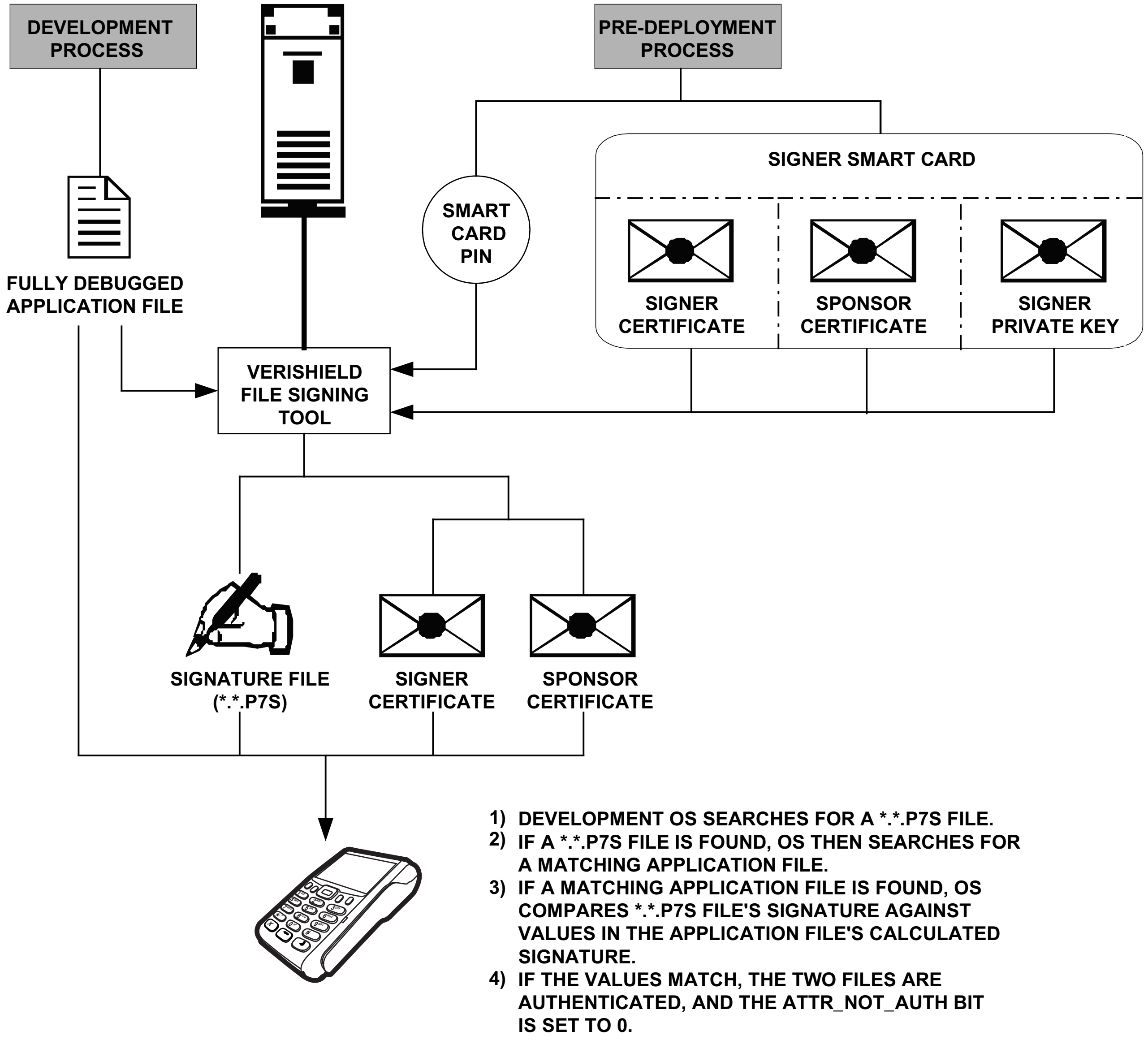

DEVELOPMENT PROCESS
PRE-DEPLOYMENT PROCESS
SIGNER SMART CARD
SMART CARD PIN
SIGNER CERTIFICATE
SPONSOR CERTIFICATE
SIGNER PRIVATE KEY
FULLY DEBUGGED APPLICATION FILE
VERISHIELD FILE SIGNING TOOL
SIGNATURE FILE (*.*.P7S)
SIGNER CERTIFICATE
SPONSOR CERTIFICATE
1) DEVELOPMENT OS SEARCHES FOR A *.*.P7S FILE.
2) IF A *.*.P7S FILE IS FOUND, OS THEN SEARCHES FOR A MATCHING APPLICATION FILE.
3) IF A MATCHING APPLICATION FILE IS FOUND, OS COMPARES *.*.P7S FILE'S SIGNATURE AGAINST VALUES IN THE APPLICATION FILE'S CALCULATED SIGNATURE.
4) IF THE VALUES MATCH, THE TWO FILES ARE AUTHENTICATED, AND THE ATTR_NOT_AUTH BIT IS SET TO 0.

Figure 29 The Deployment Process

Planning for File Authentication

File authentication is an integral part of every VX 675 terminal. To safeguard the terminal’s logical security, the file authentication module requires that any executable code file must be successfully authenticated before the operating system allows it to execute on the terminal.

Authentication Requirements for Specific File Types

For the purposes of file authentication, executable code files include two file types that can be recognized by the filename extensions listed in Table 8.

Table 8 Executable File Extensions

File Type	Extension
Compiled and linked application files	`*.out`
Global function libraries	`*.lib`

Depending on the logical security requirements of specific applications, other types of files used by an application (that is, non-executable files) must also be authenticated.

- Data files (`*.dat`) that contain sensitive customer information or other data that must be secure
- Font files (`*.vft` or `*.fon`) may need to be secure to prevent unauthorized text or messages from being displayed on the terminal screen.
- Any other type of file used by an application in which the application designer would like to logically secure using file authentication requirements

Decide Which Files to Authenticate in a Specific Application

The first step in the file authentication process is to determine which files must be authenticated for an application to meet its design specifications for logical security under the VeriShield Retain security architecture.

In most cases, application designers make these decisions based on specifications provided by the terminal sponsor. Determining which files to authenticate can be completely transparent to the person or business entity responsible for signing, downloading, and authenticating an application prior to deployment.

How (and When) Signature Files Authenticate Their Target Files

Signature files are usually downloaded together with their target application files in the same data transfer operation. This recommended practice lets you specify and confirm the logical security status of the VX 675 terminal each time you perform an application download.

When the file authentication module detects a new signature file after a terminal restart, it locates and attempts to authenticate the target file that corresponds to the new signature file.

It is not mandatory to always download a signature file and its target application file at the same time. For example, you can download the corresponding signature file in a separate operation. A non-authenticated application can reside in the terminal memory, but is not authenticated or allowed to run on the terminal until the signature files for the application executable files are processed by the file authentication module after a subsequent download procedure and terminal restart.

Determine Successful Authentication

To ensure the VX 675 terminal's logical security, never assume that a target file was authenticated simply because it was downloaded to the VX 675 terminal together with its signature file.

There are several ways to ensure a target file is successfully authenticated after a download:

- **Confirm if all downloaded executable files run.** If an executable code file is not successfully authenticated, the operating system does not allow it to execute and run, either following the initial download or on subsequent terminal restarts. The effect of this rule depends on whether or not all executable files are successfully authenticated.
  - If the executable file that failed to authenticate is the main application (`*.out`) specified in the `CONFIG.SYS *GO` variable, the main application is not allowed to run.
  - If the executable that failed to authenticate is a secondary executable (`*.out`) or shared library (`*.lib`) used by the main application, the `CONFIG.SYS *GO` application executes and runs until it issues a function call to that library. When the main application attempts to access a non-authenticated executable, the main application may crash.
- **Visually (and audibly) confirm file authentication during the process.** When the file authentication module is invoked at terminal restart and detects a new signature file, it displays status information on the screen indicating success or failure of the authentication of each target file based on its corresponding signature file. (A similar status display also appears on the screen when you download digital certificates.)

  You can watch the screen display following the download to see if a specific target file fails authentication. If this happens, **FAILED** is displayed for five seconds on the screen below the filenames of the target and signature files, and the terminal beeps as an alert.

  An application program can issue a function call to read the `ATTR_NOT_AUTH` bit's current value for all relevant files to verify they were successfully authenticated. If the `ATTR_NOT_AUTH` bit's binary value is 1, the file did not authenticate; if 0, the file did authenticate.

For non-executable files, it is the application's responsibility to confirm that all of the files it uses successfully authenticated on download completion, and when the application executes the first time following a restart.

NOTE Because the application is responsible for verifying data files and prompt files, it is recommended that each application check the `ATTR_NOT_AUTH` bit of all relevant files on restart.

NOTE Each successfully authenticated file is also write-protected. That is, the file's read-only attribute is set. If the read-only file is removed or if the file is modified in any way while stored in the terminal, the `ATTR_NOT_AUTH` bit is automatically set to `1`. If the modified file is an executable, it is no longer allowed to run.

Digital Certificates and the File Authentication Process

The file authentication module always processes certificates before it processes signature files. Digital certificates (`*.crt` files) generated by the Verifone CA have two important functions in the file authentication process:

- They define the rules for file location and usage (for example, the valid file group, `replaceable *.crt` files, `parent  *.crt` files, whether `child *.crt` files can exist, and so on).
- They convey the public cryptographic keys generated for terminal sponsors and signers that are the required inputs to the VeriShield File Signing Tool to verify file signatures.

Hierarchical Relationships Between Certificates

All digital certificates are hierarchically related to one another. Under the rules of the certificate hierarchy managed by the Verifone CA, a lower-level certificate must always be authenticated under the authority of a higher-level certificate. This rule ensures the overall security of VeriShield Retain.

To manage hierarchical relationships between certificates, certificate data is stored in terminal memory in a special structure called a certificate tree. New certificates are authenticated based on data stored in the current certificate tree. The data from up to 21 individual related certificates (including root, OS, and other Verifone-owned certificates) can be stored concurrently in a certificate tree.

This means that a new certificate can only be authenticated under a higher-level certificate already resident in the terminal's certificate tree. This requirement can be met in two ways:

- The higher-level certificate may have already been downloaded to the terminal in a previous or separate operation.
- The higher-level certificate can be downloaded together with the new certificate as part of the same data transfer operation.

A development set of higher-level certificates is downloaded into each VX 680 terminal upon manufacture. When you take a new VX 680 terminal out of its shipping carton, certificate data is already stored in the terminal's certificate tree. In this just-out-of-the-box condition, the VX 675 terminal is called a development terminal.

A sponsor requests a set of digital certificates from the Verifone CA to establish sponsor and signer privileges. This set of certificates is then downloaded onto the VX 680 when the device is being prepared for deployment. When this procedure is complete, the VX 675 is called a deployment terminal.

Adding New Certificates

When you add a new certificate file to a VX 675 terminal, the file authentication module detects it by filename extension (`*.crt`). On restart, the terminal then attempts to authenticate the certificate under the authority of the resident higher-level certificate stored in the terminal's certificate tree or one being downloaded with the new certificate.

In a batch download containing multiple certificates, each lower-level certificate must be authenticated under an already-authenticated, higher-level certificate. Whether or not the data a new certificate contains is added to the terminal's certificate tree depends on whether it is successfully authenticated. The following points explain how certificates are processed:

- If a new certificate is successfully authenticated, the information it contains is automatically stored in the terminal's certificate tree. The corresponding certificate file (`*.crt)` is then deleted from that file group's memory.
- If the relationship between the new certificate and an existing higher-level certificate cannot be verified, the authentication procedure for the new certificate fails. In this case, the certificate information is not added to the certificate tree and the failed certificate file (usually ~400 bytes) is retained in the application memory.

Development Terminals

A development terminal is a VX 675 with a Sponsor and Signer certificate issued to someone who intends to use the terminal for application development. An application developer must apply for a Sponsor/Signer certificate to allow loading an application. See Figure 30.

In the development device, the level of logical security provided by the file authentication module is the same as a deployment application.

NOTE With the factory set of certificates stored in the terminal memory, anyone who has the VX 675 SDK and VeriShield File Signing Tool can generate valid signature files for downloading and authenticating files on the VX 675 platform.

Deployment Terminals

While the application development process is being completed and while the new application is being tested on a development terminal, a sponsor can order specific sponsor and signer certificates from the Verifone CA to use to logically secure sponsor and signer privileges when the VX 675 terminal is prepared for deployment.

Customer-specific sponsor and signer certificates are usually downloaded to a VX 675 terminal as part of the standard application download procedure performed by a deployment service. In this operation, the new sponsor and signer certificates replace the development sponsor certificate that is part of the factory set of certificates, as shown in Figure 30.

When the sponsor and signer certificates are downloaded and successfully authenticated, the terminal is ready to deploy.

Ultimately, it is the sponsor’s decision how to implement the logical security provided by file authentication on a field-deployed terminal. Additional certificates can be obtained from the Verifone CA anytime to implement new sponsor and signer relationships in deployment terminals. VeriShield Retain allows for multiple sponsors and signing certificates in a terminal. This allows the flexibility of unique signatures for each executable or data files.

Figure 30 illustrates the certificate trees in development and deployment terminals.

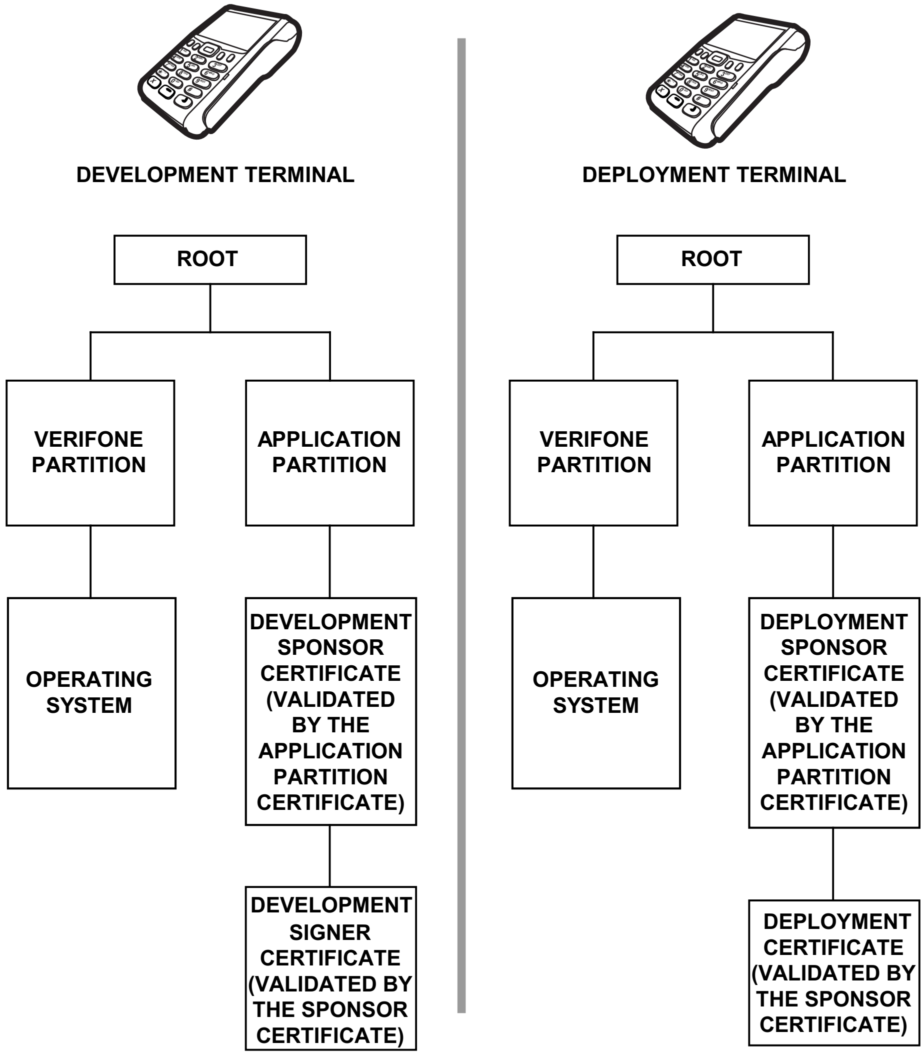

DEVELOPMENT TERMINAL
ROOT
VERIFONE PARTITION
APPLICATION PARTITION
OPERATING SYSTEM
DEVELOPMENT SPONSOR CERTIFICATE (VALIDATED BY THE APPLICATION PARTITION CERTIFICATE)
DEVELOPMENT SIGNER CERTIFICATE (VALIDATED BY THE SPONSOR CERTIFICATE)
DEPLOYMENT TERMINAL
ROOT
VERIFONE PARTITION
APPLICATION PARTITION
OPERATING SYSTEM
DEPLOYMENT SPONSOR CERTIFICATE (VALIDATED BY THE APPLICATION PARTITION CERTIFICATE)
DEPLOYMENT CERTIFICATE (VALIDATED BY THE SPONSOR CERTIFICATE)

Figure 30 Certificate Trees in Development and Deployment Terminals

Permanency of the Certificate Tree

The data contained in a digital certificate is stored in the terminal's certificate tree when the certificate is authenticated, and the certificate file itself is erased from memory.

The certificate tree file is stored in a reserved area of non-volatile memory and is therefore permanent. New certificate data can be added to the existing certificate tree (up to a maximum of 21 certificates).

Required Inputs to the File Signing Process

The required inputs to the file signing process are somewhat different for development terminals than deployment terminals. The significant differences are shown in Table 9.

Table 9 Differences Between Required Inputs

Development Terminals	Deployment Terminals
Manufacturing inputs to the file signing process are included, together with the VeriShield File Signing Tool in the VX 675 SDK. These inputs make it possible for anyone who has the VX 675 SDK to sign and authenticate files.	The required inputs to VeriShield File Signing Tool must be obtained from the Verifone CA to logically secure the sponsor and signer privileges for the terminal.
The following three unique inputs, which are issued at customer request by the Verifone CA, are required for the file signing process, as well as the application files you want to sign and authenticate: • **Developer signer certificate:** This unique certificate is a required input for VeriShield File Signing Tool and must be downloaded to the terminal along with the signature files and target application files to authenticate, unless already downloaded to the terminal in a previous operation. • **Developer signer private key:** The Verifone CA issues this unique, encrypted private key file (`*.key`) to an authorized signer at the sponsor's request. The signer private key is a required input to VeriShield File Signing Tool, but does not have to be downloaded to the terminal. • **Developer signer PIN:** The Verifone CA issues this unique password to an authorized signer at the sponsor's request. The customer signer password is a required input to VeriShield File Signing Tool, but it does not have to be downloaded to the terminal.	**Note:** The customer sponsor certificate, which authenticates the customer signer certificate, is usually downloaded to the terminal with the customer signer certificate, but it is not a required VeriShield File Signing Tool input when signing files.

Replace a Sponsor Certificate

A sponsor may need to clear the current sponsor certificate from a terminal so that a new sponsor can load certificates and applications. To do this, the original sponsor must order a “clear” smart card from the Verifone CA. The clear smart card is specific to the requesting sponsor. It restores a deployment terminal to the development state (refer to Figure 31) by:

- Deleting the current sponsor and signer certificates from the terminal’s application partition.

NOTE The process for replacing a signer certificate is the same as replacing a sponsor certificate.

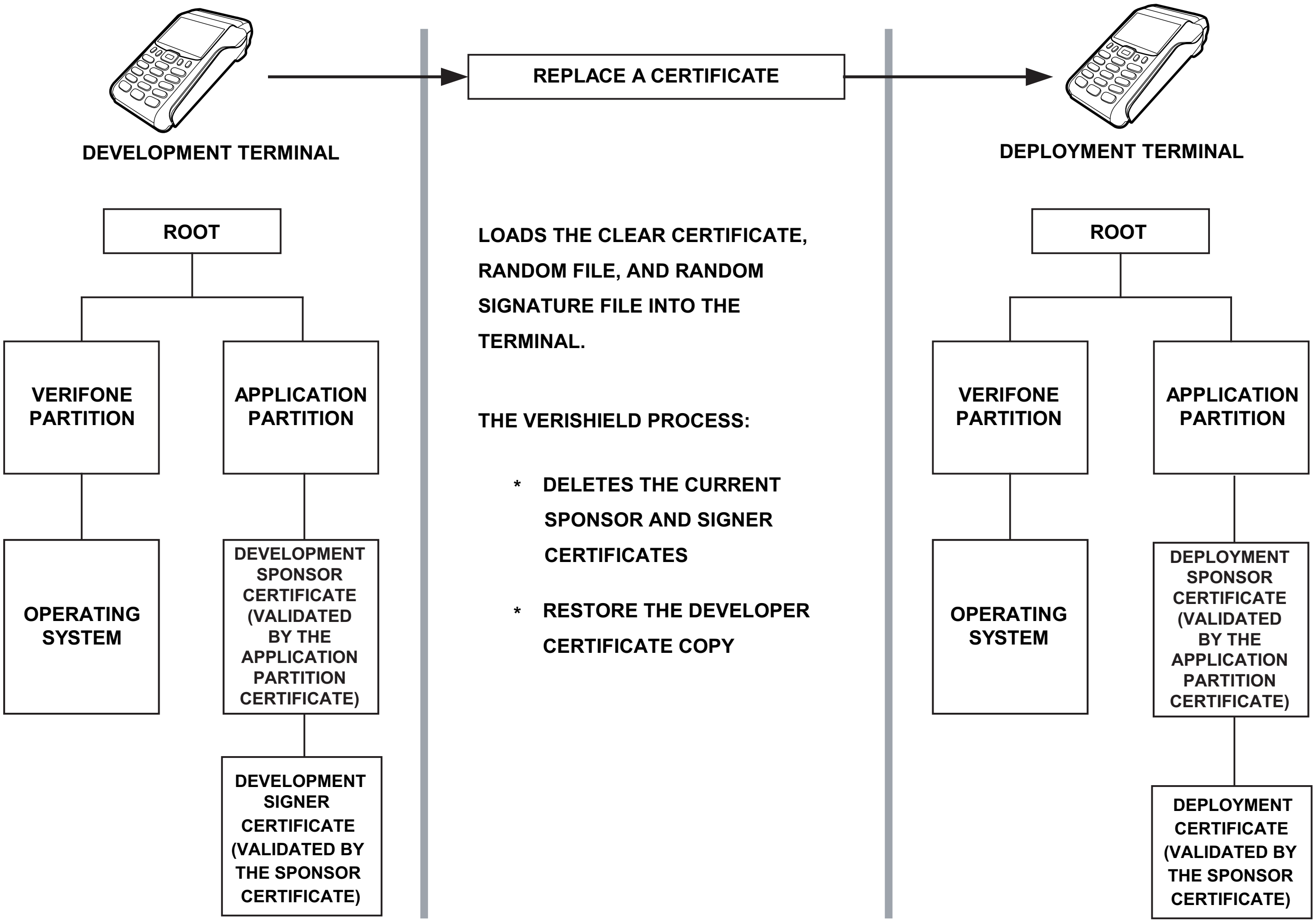

DEVELOPMENT TERMINAL
REPLACE A CERTIFICATE
DEPLOYMENT TERMINAL
ROOT
VERIFONE PARTITION
APPLICATION PARTITION
OPERATING SYSTEM
DEVELOPMENT SPONSOR CERTIFICATE (VALIDATED BY THE APPLICATION PARTITION CERTIFICATE)
DEVELOPMENT SIGNER CERTIFICATE (VALIDATED BY THE SPONSOR CERTIFICATE)
LOADS THE CLEAR CERTIFICATE, RANDOM FILE, AND RANDOM SIGNATURE FILE INTO THE TERMINAL.
THE VERISHIELD PROCESS:
* DELETES THE CURRENT SPONSOR AND SIGNER CERTIFICATES
* RESTORE THE DEVELOPER CERTIFICATE COPY
ROOT
VERIFONE PARTITION
APPLICATION PARTITION
OPERATING SYSTEM
DEPLOYMENT SPONSOR CERTIFICATE (VALIDATED BY THE APPLICATION PARTITION CERTIFICATE)
DEPLOYMENT CERTIFICATE (VALIDATED BY THE SPONSOR CERTIFICATE)

Figure 31 Certificate Replacement Process

File Authentication and the File System

Application Memory Logically Divided Into File Groups

The memory of a VX 675 terminal is logically divided into two main areas, or partitions:

- operating system
- applications

The application partition is further divided into sub-partitions. These sub-partitions are called file groups or GIDs.

This system of partitions and sub-partitions makes it possible to store multiple applications in terminal memory and prevent these applications from overlapping or otherwise interfering with each other's operation.

There are a total of 16 file groups (Figure 32). Group 0 is the name of the operating system partition. Group 1 is reserved for the main application. Groups 2–14 are available for related executable files or secondary applications. Group 15 is open, and used for shared files such as shared libraries.

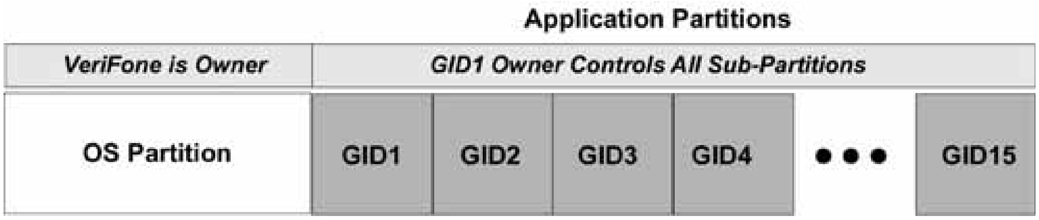


Figure 32 VX 675 Application Memory Partitions

NOTE

The VX 675 operating system only enforces the rule that the main application be always stored in GID1. You can, for example, store a shared library in any file group. Rules for Storing Applications in Specific File Groups states reasons to follow the guidelines previously described for storing applications and libraries in specific file groups.

Rules for Storing Applications in Specific File Groups

Here are some important VX 675 file system features, as they relate to storing application files in specific file groups, and how these features affect the file authentication process:

- Most applications consist of more than one executable. For each executable to run on the terminal, it must be signed and authenticated.
- Although not enforced by the operating system, it is recommended that only one application be stored per file group in the application partition. Any number of executable files can, however, be stored in a single file group.
- Using the `CONFIG.SYS *GO` variable, you can specify only one application to automatically execute following a download and terminal restart. The defined application is usually the main application stored in Group 1 and called from the `*GO` variable in the `CONFIG.SYS` file in GID1.

- The main application stored in GID1 can access files, secondary applications, or function libraries stored in any other file group.
- The application downloaded into GID1 is always the primary application for the terminal. This application is owned by the primary terminal sponsor (sponsor A) in cases where there are multiple sponsors.
- The Group 1 application controls any and all secondary applications stored in terminal memory. That is, a secondary application can only be invoked by a RUN command issued by the Group 1 application.
- An application stored in Groups 2–15 can only access files stored in its own file group and in Group 15. For example, an application authorized by the sponsor to be authenticated in Group 4 can only access files and libraries stored in Group 4 and Group 15.
- If multiple applications (main and secondary) are to run on the same terminal, each `.OUT` and/or shared library file must have its own matching signature file.

  Because each application is responsible for verifying its own data and prompt files, the other application files should have their own matching signature files. The master `.OUT` file should validate that these additional signature files are authenticated before they are used.
- If two or more applications will run on the same terminal, the signature files for the respective applications must be downloaded, together with the corresponding target files, into the specific file group(s) for which the applications are authorized. If an application is downloaded into a group for which is it not authorized, file authentication for that application fails.

  If, for example, Application B is downloaded into GID4, where it is authorized to run, but the signature files for all Application B executable files are downloaded into GID7, file authentication for Application B fails and it is not allowed to run.
- Each certificate contains an attribute to verify if an application is valid for a particular group.

Authenticate Files Stored in the Memory of a File Group

All `*.p7s` files are identified as I: drive or F: drive files and contain flags that indicate if the file to verify is identified as an I: drive or an F: drive file. A signature file must know if its matching application file is identified as an I: drive or an F: drive file. If a signature file cannot locate its matching application file, the application file is not authenticated.

If the signature file authenticates its target file, and if the *FA variable is present in the CONFIG.SYS file of the target file group and is set to 1, the signature file is retained in memory and is automatically moved, if necessary, into the same logical file system (I: or F:) as the target file it authenticates. That is, if the target file is identified as an F: drive file, the signature file is also identified as an F: drive file; if the target file is identified as an I: drive file, the signature file is also is identified as an I: drive file.

NOTE

Normally signature files are retained in the terminal even after being used to authenticate executable (code) or data files. This is to facilitate back-to-back downloads, as described in Chapter 6. Users who do not intend to perform back-to-back downloads can remove signature files after use, gaining space for other files. Automatic removal is performed if the user sets *FA=0 in the CONFIG.SYS file of Group 1. The main reason for using *FA is to force automatic removal. If the user desires the default behavior (retain signature files, to allow for back-to-back downloads), the user does not need to set *FA.

If the signature file authenticates its target file and the *FA variable is present in the CONFIG.SYS file of the target file group and is set to 0, the signature file is erased when its target file is authenticated.

If you intend to perform back-to-back downloads, as described in Chapter 6, all signature files must be retained in the VX 680 terminal's application memory, together with the target application files they authenticate.

NOTE

To control if signature files are retained or deleted when they are processed by the file authentication module, you must use the protected CONFIG.SYS variable *FA as documented in the *Verix eVo Volume I: Operating System Programmers Manual* (VPN DOC00301).

Restrictions on Downloading Different File Types

A typical application download includes a variety of different file types. The following restrictions in Table 10 describe how you can download different kinds of files to the VX 680 terminal and how files are stored in the file system:

Table 10 Download File Extensions

File Type	Restriction
Certificate (*.crt)	*Must* be downloaded into the I: drive of the target file group (GID1 – GID15) selected in Verix Terminal Manager.
Signature (*.p7s)	*Must* be downloaded into the I: drive of the target file group (GID1 – GID15) selected in Verix Terminal Manager.
Operating system	*Must* be downloaded into Group 1 I: drive. When the OS files, related certificates and signature files are authenticated, they are automatically moved from Group 1 I: drive into the Group 0 sub-partition reserved for the operating system.

The normal size of a signature file is approximately 400 bytes. Depending on the application's size and on how memory space is allocated, the area available for storing multiple signature files must be carefully managed. The memory space required by a certificate file is also approximately 400 bytes, but certificate files are temporary. When a certificate is authenticated, the data it contains is copied to the certificate tree, and the certificate file is erased from the target file group's I: drive.

VeriShield File Signing Tool

To generate the signature files required for file authentication, you must sign all executable files and other files to be logically protected using the file signing (VeriShield File Signing Tool) software tool. This section discusses the use of this tool, which is included in the VX 675 Verix eVo DTK.

The VeriShield File Signing Tool generates a formatted file called a signature file, recognized by the filename extension `*.p7s`.

You can run VeriShield File Signing Tool on a host computer (PC) in DOS command-line mode, or invoke the program under Windows 2000 or Windows XP and then use the dialog box shown on Figure 33 to make the required entries.

NOTE The file signing process for operating system files is done for VX 675 customers by the Verifone CA. For operating system updates, Verifone provides customers with a complete download package that includes all certificates and signature files required for authentication.

VeriShield File Signing Tool System Requirements

The file signing tool requires one of the following computing environments:

- Windows NT, Version 4.0, SP5
- Windows 95, with Internet Explorer Version 5.0

The SP5 and Internet Explorer Version 5.0 software can be downloaded from the Microsoft Web site located at www.microsoft.com.

Operating Modes for the VeriShield File Signing Tool

The VeriShield File Signing Tool can run on the host computer in two user modes:

- **Command-line mode** (Windows PC DOS shell): Command-line mode is useful for application developers who perform batch file downloads and is convenient when using file download tools provided by Verifone, such as the VeriCentre Download Management Module (DMM) and the `DDL.EXE` direct download utility. In command-line mode, you can sign a batch of files in a single operation.
- **Graphical interface mode** (Windows NT or Windows 95): Use the FileSign dialog box (Figure 33) to select the file to sign, and assign a name and destination location for the generated signature file on the host computer. When you run the file signing tool under Windows, you can sign only one file at a time.

You can also specify to store the target file in the target file group's I: drive (default location) or in the target file group's F: drive. If required, you can navigate through the file system on your PC to select the signer certificate file (`*.crt`) and signer private key file (`*.key`) to use as inputs to the file signing process.

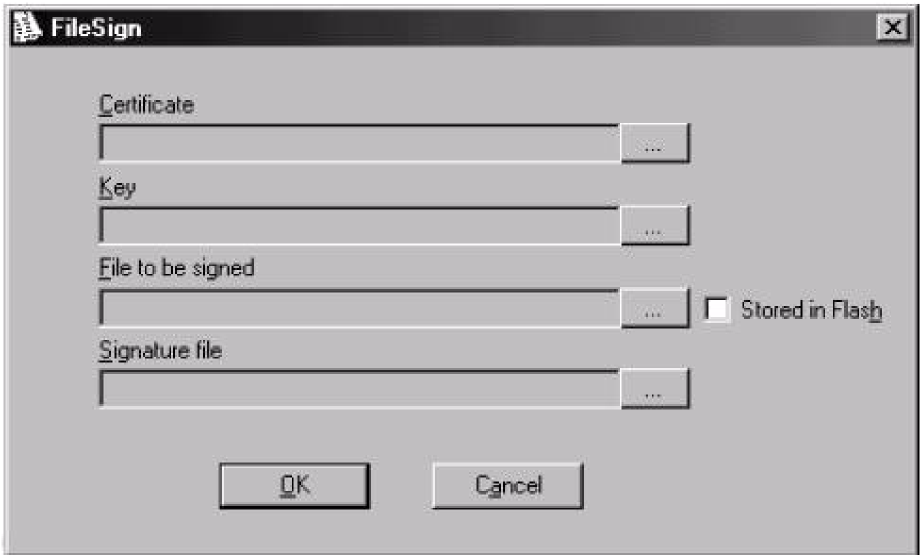


Figure 33 FileSign Dialog Box

NOTE If the entry of a signer password is a required input, a secondary dialog box is displayed to enter and confirm the password. Please also note that a signer password is required for a deployment terminal, but not for a development terminal.

Command-Line Entries for the File Signing Tool

Table 11 lists the switches that make up the command-line mode syntax for the file signing tool (VeriShield File Signing Tool).

Table 11 Command-Line Mode Switches for VeriShield File Signing Tool[a]

Switch	Description	Requirements
-C, -c	Signer certificate file name (`*.crt`).	Required input for development terminals and deployment terminals. Use the VxSIGN.CRT developer signer certificate for development terminals. Use the signer certificate issued by the Verifone CA for deployment terminals.
-K, -k	Signer private key filename (`*.key`).	Required input for development terminals and deployment terminals. Use the VxSIGN.KEY developer signer private key for development terminals. Use the signer private key provided by the Verifone CA for deployment terminals.
-P, -p	Signer password for decrypting the signer private key.	Required input for development terminals and deployment terminals. The Verifone CA issues and securely conveys this password to an authorized signer.
-F, -f	Name of the application file to sign (`*.out`, `*.lib`, or other file type).	Required for development terminals and for deployment terminals.

Table 11 Command-Line Mode Switches for VeriShield File Signing Tool[a]

Switch	Description	Requirements
-S, -s	Name of the signature file (`*.p7s`) for VeriShield File Signing Tool to generate for the target application file.	Required for development terminals and for deployment terminals.
-L, -l	Specifies to store the target application file to sign and authenticate in the drive F: file system. If you do not use this switch to specify F: drive as the target file destination, it is stored by default in the I: drive.	Optional entry. This switch assigns an F: prefix to the name of the `*.out` or `*.lib` file to download, and also stores this information in the signature file as part of the special filetype attribute. **Note:** Signature files must be downloaded into the target file group's I: drive. If the target file is authenticated, the corresponding `*.p7s` file is moved to the same memory area as the target file it authenticates. For example, if the target file is stored in F: drive, its `*.p7s` file is moved into the F: drive system. If, however, you set the `*FA` variable in the file group's `CONFIG.SYS` file to 0, all signature files are deleted from memory when file authentication is complete. Removing `*.p7s` files will prevent application files from executing after a back-to-back download.

[a] The switches described are not case-sensitive and can be entered on the command line in any order.

Please note also how the command-line mode switches described in Table 11 are used in this example:

```
filesign -L -f file.out -s file.p7s -c vxsign.crt -k vxsign.key
```

- The `-L` switch indicates to store the application file in the flash file system instead of the target group's (default) I: drive file system. (The target group for the download must be selected from Verix Terminal Manager when the download is performed.)
- The `-f` switch indicates that the application file "`file.out`" must be signed by the file signing tool.

  Executable files, such as `*.out` and `*.lib` files, must always be signed if they are to run on the terminal following a download. Depending on the application's logical security requirements, other types of files, such as data files and font files, may also need to be signed and authenticated on download.

- The `-s` switch is followed by the name of the signature file to be generated, `file.p7s`.
- The `-c` switch is followed by the name of the signer certificate to be used for file authentication with the development terminal, "`vxsign.crt`."
- The `-k` switch is followed by the name of the signer private key file, `vxsign.key`. A signer private key is a required input to the file signing process for development terminals and for deployment terminals.

Graphical Interface Mode for the VeriShield File Signing Tool

When you execute the VeriShield File Signing Tool file, the FileSign dialog box is displayed (see Figure 33).

The FileSign dialog box has four entry fields, each of which is followed by a "next" **[...]** selection button. There is one check box, and the OK and Cancel buttons.

- Press ALT+C or click the **[...]** button to the right of the Certificate field to locate and select the certificate file (`*.crt`) to be used to sign the file.
- Press ALT+K or click the **[...]** button to the right of the Key field to locate and select the signer private key file (`*.key`).
- Press ALT+F or click the **[...]** button to the right of the File to be signed field to locate and select the application file (`*.out`, `*.lib`, or other) to sign. If necessary, the filename can also be modified.

  To store the file in F: drive upon download to the terminal, check the Stored in Flash check box. This adds the F: prefix to the target file name.
- Press ALT+S or click the **[...]** button to the right of the Signature file field to enter a filename for the signature file to be generated. The filename extension must always be `*.p7s`. You can also choose another directory on the host PC to store the generated signature file.
- When all entries are complete, press ALT+O or click the OK button to execute the VeriShield File Signing Tool and generate the signature file, otherwise, press ALT+A or click Cancel to exit the VeriShield File Signing Tool utility.

When the necessary signature files are generated to authenticate the application or applications on the VX 680 terminal, perform the application download procedure.

For more information about file authentication within the context of specific download procedures, refer to Chapter 6.

CHAPTER 6

Performing Downloads

This chapter contains information and procedures to allow you to perform the various types of data transfers required to:

- Develop applications for the VX 675 terminal.
- Prepare VX 675 terminals for deployment.
- Maintain VX 675 terminal installations in the field.
- Transfer data to/from terminals.

In this chapter, information pertaining to file authentication is only discussed in the context of procedures while performing file downloads. See Chapter 5 for further file authentication discussion.

The VX 675 terminal contains ports that allow connection to a network or other terminals (for back-to-back downloads). See Download Methods.

Downloads and Uploads

Data can be transferred from a sending system to a receiving system while performing downloads. The term download also refers to a terminal receiving data. The term upload describes the process of a terminal sending data.

Use any of the following two operations to program, deploy, transfer data files from, and support VX 675 terminals:

- Host computer downloads: Applications, operating systems or OS updates, and associated files transfer from a host PC to a VX 675 terminal. A service dongle (SUB265-001-01-A) is used to connect the RS-232 serial ports between two systems. Please refer to Table 15 for the direct download procedure.
- Back-to-back downloads: Applications and associated files transfer from one VX 675 terminal to another VX 675 terminal.

Download Methods

The following methods are available for file and data downloads through the VX 675 download and upload procedures:

- **Direct downloads**: Files and/or data transfer directly from the sending system (a host computer) to the receiving system (a VX 675 terminal). A special cable called service dongle (SUB265-001-01-A) connects the RS-232 serial ports of the two systems.

- **Back-to-back downloads:** Files and data transfer from a sending VX 675 terminal to a receiving VX 675 terminal are sent over using the service dongle, it connects the RS-232 serial ports of the two systems.

NOTE

An external UART Dongle on both the sending and receiving terminal is required to attach the special cable.

Download Tools

Three software tools are available from Verifone for performing downloads: **VeriCentre Download Management Module (DMM), VeriCentre, and DDL.EXE (Direct Download Utility)**.

NOTE

Because of the large size of some download files, Verifone recommends only using download tools provided by Verifone. CRC and other error checking is not supported on the GSM system. Verifone download tools provide these error checking mechanisms.

The following tools perform direct downloads from a host computer to a VX 675 terminal:

- **VeriCentre DMM:** Multi-user environment for software downloads. DMM supports Windows NT clients and has a sophisticated database to manage up to 100,000 terminals. The VX 675 operating system supports file decompression for archives created using DMM.
- **VeriCentre:** PC-based software tool to manage applications and data for Verifone. In addition to being a database and communications management tool, VeriCentre automates application downloads and updates to terminal records.
- **DDL.EXE:** Downloads files and data from a development system or another host computer, directly to a VX 675 terminal over a serial cable connection. `DDL.EXE` is a Windows program included in the Verix eVo DTK (Verix eVo Developer’s Toolkit).

NOTE

No special software tool or utility is required to perform back-to-back application downloads. Only a serial cable connected between two terminals is required. This data transfer procedure, invoked from within Verix Terminal Manager, is handled by the OS software and firmware of the sending and receiving VX 675 terminals.

Download Content

In general, you can download files and data to a VX 675 terminal. The types of files and data can be grouped into the following functional categories:

- **Operating system files:** A set of related programs and data files provided by Verifone to control the terminal’s basic processes and functions. Files that belong to the OS are stored in a reserved area of the terminal memory.

A complete OS is downloaded to each VX 675 terminal during the manufacture. If necessary, download newer versions during application development, or when preparing for deployment to on-site terminals.

- **Applications and related files:** An application is a computer program consisting 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.

  VX 675 applications can be developed by Verifone, customers, or third parties on customer request. One or more applications must be downloaded to the VX 675 terminal before it can be deployed at a customer site and used to process transactions.

- **Files related to file authentication:** The logical component of the VeriShield security architecture in the VX 675 terminal is file authentication. For an executable to run on a VX 675 terminal, it must be authenticated by the VeriShield file authentication module.

NOTE

For details on file authentication, see Chapter 5.

Two special types of files are required for the file authentication process: digital certificates (`*.crt`) and signature files (`*.p7s`). These file types must be downloaded to the terminal together with the application files to authenticate.

- **Terminal configuration settings:** Files or records that contain various types of data can also be downloaded to a VX 675 terminal, including `CONFIG.SYS` variables, passwords for accessing protected Verix Terminal Manager functions, the current date and time, and the modem country code setting (refer to Chapter 4).

Full and Partial Downloads

When preparing to initiate a download procedure, choose either a full or partial download and the COM 1 port, through the Verix Terminal Manager menu options (refer to Chapter 4). Depending on the type of files you are downloading and the download method you are using, there are some restrictions on whether a full or partial download is permitted. Full download means all files in group 1-14 will be deleted. The common group, 15, is not affected. While partial download means no files currently on the system will be deleted.

The various types of full and partial download procedures are listed and described in Table 12.

Table 12 Types of Full and Partial Downloads

Download Type	Description and Effects	Download Methods Supported
Full application download	An entire application, including all executables and data files, transfers from one system to another in a single operation. Files related to the file authentication process and terminal configuration settings can be included in a full application download. During this process, memory is cleared. Following a full application download, the terminal restarts and the file authentication module is invoked. If application files are authenticated and `CONFIG.SYS *GO` variable is set, then the application executes.	• Direct downloads • Back-to-back downloads
Partial application download	A subset of application executables, font files, and/or data files transfer from one system to another to modify or update an existing application. Files related to file authentication and terminal configuration settings can be included in a partial application download. During this process, memory is *not* cleared. Following a partial application download, the terminal does not restart and returns control to Verix Terminal Manager or the issuing application. The file authentication module is not invoked, nor are any applications allowed to execute, until the terminal is manually restarted from within Verix Terminal Manager.	• Direct downloads **Note:** Partial back-to-back downloads are *not* supported.

Table 12 Types of Full and Partial Downloads

Download Type	Description and Effects	Download Methods Supported
Full operating system download	An *entire* OS version transfers from a host PC to the VX 675 terminal. Files related to file authentication and terminal configuration settings can be included in a full OS download. During this process, memory is cleared. Following a full OS download, the terminal restarts and the file authentication module is invoked. If the OS files are authenticated, the new OS updates (replaces) the existing OS. Application files stored in the memory area where the OS downloads (Group 1) are erased.	• Direct downloads **Note:** Full back-to-back OS downloads are *not* supported.
Partial operating system download	Either an *entire* or a *partial* OS version transfers from a host PC to the VX 675 terminal. Files related to file authentication and terminal configuration settings can be included in a partial OS download. Following a partial OS download, the terminal does not restart and returns control to Verix Terminal Manager or the issuing application. The file authentication module is not invoked, and the new OS is not processed until you manually restart the terminal from within Verix Terminal Manager. If the new OS is authenticated, it then updates (replaces) the existing OS. Application files stored in the memory area where the OS downloads into (Group 1) are retained.	• Direct downloads **Note:** Partial back-to-back operating system downloads are *not* supported.

Here are a few more points on the topic of full and partial downloads:

- The most common download procedure is a full (complete) application download.
- Partial application downloads are useful when developing and testing new applications, but are seldom performed by those who deploy terminals on-site.
- Full OS downloads are usually performed by Verifone at the factory and, on occasion, by those who deploy terminals on-site to upgrade older terminals to a newer OS version.
- Partial OS downloads are performed mainly by Verifone for development purposes and are rarely performed in the field.

- Partial downloads are routinely performed by many applications. This procedure, which can be automated by an application running on a remote host computer, permits the host application to update data files and terminal configuration settings in a VX 675 terminal and then return control to the main application.
- Full downloads restart the terminal; partial downloads return control to Verix Terminal Manager or the issuing application. OS and application downloads can be combined. The file authentication module is not invoked until the terminal is restarted following the download procedure.

Support for Multiple Applications

The VX 675 terminal architecture supports multiple applications. This means that more than one application can reside in terminal memory, and that more than one application can run (execute) on the terminal.

The application memory of the VX 675 terminal uses a system of file groups to store and manage multiple applications, as well as operating system files. This system of file groups are used in such a way that the data integrity of each application is ensured and applications do not interfere with each other (see File Groups).

How the File System Supports Multiple Applications

The application memory partition of the VX 675 terminal is divided into 15 logically-defined sub-partitions called file groups or GIDs (for example, Group 1, Group 2, and so on through GID15).

Another partition of the terminal memory area, called Group 0, is reserved for the operating system and is logically separated from the application memory area. So, including Group 0, there is a total of 16 file groups.

An application must be downloaded into a specific file group, along with any related files. Select the target file group for the download using Verix Terminal Manager menu options and by entering a file group password.

Usually, one application is stored in one file group. An application can, however, consist of more than one executable program file, and any number of executables (`*.out` or `*.lib`) can be stored in a given group. In most implementations, there is a main application, one or more related programs or secondary applications, and one or more libraries.

The main application, or the application to execute set in the `*GO CONFIG.SYS` variable, must always be stored in the Group 1 sub-partition. Related programs or secondary applications can be stored in GIDs 2–14. GID15 is available to all other groups.

The Main Application is Always Stored in GID1

The main application stored in GID1 is the controlling application for the terminal. Any function call that invokes a related program or a secondary application stored in GIDs 2–14 must be initiated by the GID1 application.

An application stored in a file group other than GID1 is limited in that it can only access executables and files stored in its own file group and in GID15.

Physical and Logical Access to File Groups

The VX 675 operating system controls physical access to GIDs 1–15 using password-protected Verix Terminal Manager functions.

To download data into a specific file group, first enter Verix Terminal Manager and choose the target group by making the appropriate menu selections, then, enter the correct password for that file group.

Each file group has its own `CONFIG.SYS` file. The `CONFIG.SYS` settings of the selected target group are used as the system parameters for the download operation.

The system of file groups also imposes some logical restrictions on which files can download into specific file groups:

- If GID1 is selected as the target group in Verix Terminal Manager, you can download files into GID1 and redirect files into any of the other file groups, as required, in the same download operation.
- If another file group is selected as the target file group, you can download files only into that group and redirect files only to GID15. For example, if you select GID5 as the target group for the download, files can only download into GID5 and be redirected to GID15.

Use of I: drive and F: drive

The VX 675 application memory partition has two separate logical file systems:

- Partition designator I:
- Partition designator F:

Having two different file systems has the following important implications for data transfer procedures:

- Depending on the requirements of a specific application, some files must download into the I: drive and others into the F: drive.
- There are also rules that restrict which types of files you can download and store in a file system (I: or F:).

With application files, the application designer or programmer usually decides which file types to download into which file system. Other file types, such as operating system files, digital certificates, and signature files, must download into I: drive.

In a typical download procedure, all files are loaded into the I: drive file system of the target group selected in Verix Terminal Manager. Specific files included in the download package must be redirected, as necessary, to the F: drive file system of the target group or to the I: drive or the F: drive file system of another file group.

To redirect files during a download procedure, see the following sections.

Redirection of Files During Application Downloads

You can download application files into I: drive or F: drive memory. By default, files downloaded to a specific file group are stored in the I: drive of that group. To store a file in the F: drive memory of that file group, provide instructions to redirect the file to F: drive as part of the procedure (see Manually Redirecting Files).

There are two methods used to redirect files during an application download, depending on the download tool:

- If you are using DMM, you must manually create and include special zero-length files called `SETDRIVE.x` and `SETGROUP.n` on the download computer, and add these files to the batch download list to direct files to a specific file system (drive) or file group.
- If you are using `DDL.EXE` to perform direct downloads, you can use a special command-line option that automatically redirects files to the drive and file group you specify.

Both of these methods are described in the following sections.

Manually Redirecting Files

To manually redirect files for DMM application downloads, create one or more files on the download computer with the special filename, `SETDRIVE.x`, where, x is the name of the partition to download files to.

- Partition designator `I:` This is the Verix Terminal Manager default for downloads.
- Partition designator `F:`

To create a zero-length SETDRIVE file on the download computer, use the DOS command, REM, as in the following example:

```
REM >SETDRIVE.F
```

To redirect a file from the I: drive of the target group to the F: drive memory of the same file group, insert the zero-length `SETDRIVE.F` file into the batch of application files to download. All files that follow the SETDRIVE.F file in the download list automatically load into the F: drive of the target group.

If you do not insert a `SETDRIVE.F` special file in the download list, all files download by default into the I: drive of the target file group. You can also insert a zero-length file with the name `SETDRIVE.I` into the download list at any point to indicate that all following files will download into I: drive.

For example, the following batch download list loads the executable code file `FOO.OUT` into the I: drive of the selected file group (default Group 1). Because the signature file, `FOO.P7S` is included, `FOO.OUT` is also authenticated when the terminal restarts after the download.

The *GO variable in this example indicates that the FOO.OUT application executes on restart, after successful authentication. The two data files that follow the zero-length SETDRIVE.F file, FOO.DAT and FOO.VFT, are redirected into GID1 F: drive. Because it follows the inserted zero-length SETDRIVE.I file, GOO.DAT downloads into Group 1 I: drive.

```
FOO.OUT
FOO.P7S
*GO=FOO.OUT
SETDRIVE.F
FOO.DAT
FOO.VFT
SETDRIVE.I
GOO.DAT
```

You can also insert zero-length SETGROUP.n files into a batch download list to redirect files from the target file group to other file groups (see Redirecting Files to Other File Groups). Together, the zero-length SETDRIVE.x and SETGROUP.n files allow you flexibility to store files as required in the F: drive or I: drive file systems, and in specific file groups in a single batch download operation.

NOTE

You can only use zero-length SETDRIVE.x files for batch application downloads, by direct or by only using the DMM download tool (and not DDL.EXE).

You cannot use this special file convention for operating system downloads or for back-to-back application downloads.

Redirecting Files to Other File Groups

GID1 is the default Verix Terminal Manager setting for performing downloads. Using the Verix Terminal Manager menu options, you can select another file group (GID 2–15) as the target group for the application download. If you select another group, files download directly into the I: drive of that file group.

To redirect files from the selected target file group to another file group as part of the download operation, insert a zero-length SETGROUP.n file in the batch download list (the same as SETDRIVE.x). The syntax of this convention is SETGROUP.n, where n = 1–15 for GIDs 1–15.

To create a zero-length SETGROUP file on the download computer, use the DOS command REM as in the following example:

```
REM >SETGROUP.2
```

If you do not insert SETGROUP.n special files into the download list, all files download into the target group selected in Verix Terminal Manager. If no number is added to the SETGROUP filename, SETGROUP.1 (GID1) is assumed.

Restrictions on File Redirection

The VX 675 file system restricts how you can redirect files to other file groups. Here are the important points to remember:

- The main application must always be downloaded into GID1.
- Because of the way file groups are managed in the VX 675 file system, only two schemes are available for redirecting files during a batch application download:
  - If using Verix Terminal Manager menu options, select Group 1 (default) as the target group for the download; files can be redirected to any other file group, including GID15.
  - If using Verix Terminal Manager menu options, select a file group other than Group 1 (GIDs 2–14) as the target group for the download; files can be redirected only into the selected file group or into GID15.

In the following example, GID1 is selected as the target group for the download. The download list loads `FOO.OUT` into Group 1 I: drive, `GOO.OUT` into GID2, and `COMN.LIB` shared library into GID15. When the terminal restarts after the download, the file authentication module is invoked for all three files, based on the certificate data that authorizes them to be stored in their respective file groups.

If `FOO.OUT` is authenticated, the GID1 application, `FOO.OUT`, executes as specified by the `*GO` variable when the terminal restarts following successful file authentication. The function library stored in GID15 can be shared by both applications, as both Group 1 and Group 2 applications can access Group 15.

```
FOO.OUT
FOO.P7S
*GO=FOO.OUT
SETGROUP.2
GOO.OUT
GOO.P7S
SETGROUP.15
COMN.LIB
COMN.P7S
```

NOTE

You can only use zero-length `SETGROUP.x` files for batch application downloads, by direct or only using the Download Manager or ZonTalk 2000 download tools (not `DDL.EXE`). You cannot use this special file convention for operating system downloads or back-to-back application downloads.

Using DDL.EXE to Automatically Redirect Files

The version of `DDL.EXE` included in the VX 675 SDK allows you to change the default drive and file group for a direct download by preceding the filename(s) on the DDL command line with a special filename. The syntax is as follows:

```
SETDRIVE.<drive letter>
```

where, `drive letter` is `I:` (default) or `F:`, and/or

```
SETGROUP.<group number>
```

where, `group number` is 1–15.

For example, the command-line entry

```
DDL SETDRIVE.F cardco.lib SETDRIVE.I SETGROUP.15 card.dat
```

downloads the executable file `cardco.lib` into the F: drive of the selected target group and the data file `card.dat` into Group 15 I: drive. (Because drive or group settings apply to all files that follow in the list, it is necessary to use SETDRIVE.x to reset the drive from F: back to I:.)

If you are using this `DDL.EXE` method, zero-length `SETDRIVE.x` and `SETGROUP.n` files do not need to exist as files on the download computer.

File Redirection in Operating System Downloads

When performing an operating system download, you must download the OS files into Group 1 I: drive and not into F: drive memory or into another file group.

OS files are downloaded into Group 1 I: drive because it is not possible to download these files directly into Group 0. OS files are redirected to Group 0 depending on if you perform a full or partial download (see Table 12).

- For full OS downloads, the redirection of OS files into Group 0 is performed automatically, after the terminal restart, and as part of the download procedure.
- For partial OS downloads, OS files are redirected from the I: drive of Group 1 into Group 0 on manual terminal restart by selecting the appropriate Verix Terminal Manager menu option.

A downloaded OS is processed and authenticated while stored in Group 1 I: drive. As the files are authenticated under the authority of the certificates and signature files included in the OS download package, they move automatically into Group 0. This process, which usually takes a few moments, is completely transparent during the download procedure.

File Redirection in Back-to-Back Application Downloads

In a back-to-back application download, all application files stored on the sending terminal—in both file systems and in all file groups—transfer to the receiving terminal in a single operation.

For this type of download, you must select Group 1 as the target group on the sending and receiving terminals. When you initiate the download on the receiving terminal, all application files, as well as all special files required for file authentication and terminal configuration settings on the sending terminal, download to the receiving terminal.

In this type of data transfer operation, some file redirection does occur automatically as a result of the file authentication procedure that occurs on the receiving terminal. This redirection process is transparent during the download.

Briefly, all files initially download into I: drive, and are then redirected based on the directory and subdirectory names of the sending terminal's file system. Signature files must always be authenticated in I: drive. If the target file that the signature file authenticates is stored in F: drive, the signature file is moved to F: drive only after the target file successfully authenticates.

To successfully perform a back-to-back download, all signature files that are required to authenticate application executables must reside in the memory of the sending terminal. If the `*FA` variable is present in the Group 1 `CONFIG.SYS` file of the sending terminal, it must be set to 1 to retain all previously downloaded signature files.

If a signature file is missing on the sending terminal, the target application file that it authenticates is not authenticated on the receiving terminal and, if the target file is an executable, it is not allowed to run on the receiving terminal.

File Authentication Requirements

Chapter 5 provided a general introduction to the file authentication process. Now we become more task-oriented and see how the file authentication process affects how to perform the various download procedures.

Required Certificates and Signature Files

The following are some important points to remember about how certificates and signature files relate to application download procedures:

- Before an executable file can be downloaded to and allowed to run on a VX 675 terminal, the file must be digitally signed on the download computer using the `FILESIGN.EXE` file signing tool. The result of this procedure is a signature file recognized by its `*.p7s` filename extension.
- A signature file must be downloaded with each executable that makes up an application. An executable can be a compiled and linked object file (`*.out`) or a shared function library (`*.lib`).

  In most cases, an application consists of multiple executables and requires a number of corresponding signature files.
- In a typical batch application download, all files, including executables, signature files, and any required certificates, download in the same operation.
- After the download is complete and the terminal restarts, the file authentication module is invoked if a new signature file (or certificate) is detected. If the application (executable) is authenticated, it is allowed to run on the terminal. Otherwise, it does not execute.
- If one executable file required by an application with multiple executables fails to authenticate, the main application may crash when it attempts to access the non-authenticated executable.

- Application files other than executables (for example, font and data files) may also require logical security under file authentication. In these cases, each protected non-executable file also requires a corresponding signature file.
- Digital certificates (`*.crt`) and signature files (`*.p7s`) are required to authenticate both application files and operating system files, which must be downloaded into the I: drive of the target file group.
- Certificate files are deleted from application memory after they are authenticated. If a certificate is not authenticated, it is retained in terminal memory.
- If the `*FA` variable in the `CONFIG.SYS` file of the target group is set to 1, signature files are redirected to the same location where the application file it authenticates is stored. If `*FA` is 0, signature files are deleted from I: drive when the file authentication process is complete.

The File Authentication Process During an Application Download

In the following example of a typical file authentication process, it is assumed that:

- an application is being downloaded to prepare a VX 675 deployment terminal for deployment. That is, a sponsor certificate and a signer certificate download in batch mode to GID1 I: drive of the receiving terminal, together with the application to authenticate.
- a signature file is generated for each executable that comprises the application on the download computer using `FILESIGN.EXE`, with the signer certificate, signer private key, and signer password as required inputs. These signature files are also downloaded to the receiving terminal.

In a typical batch application download, file authentication proceeds as follows:

1. All certificate files (`*.crt`), signature files (`*.p7s`), and application files (`*.out`, `*.lib`, `*.fon`, `*.vft`, `*.dat`, and so on) download to the VX 675 deployment terminal in batch mode.
2. When the terminal restarts after the download, the file authentication module searches the I: drive file system for the following two file types:

   - Authenticated certificate files (`*.crt`) to add to the permanent certificate tree.
   - Signature files (`*.p7s`) that authenticate corresponding target application files.

   Certificate files and signature files can download into the I: drive of any file group. For this reason, the file authentication module searches through the entire file system (all file groups) for new files with these filename extensions each time the terminal restarts.
3. The file authentication module builds a list of all newly detected certificates and signature files. If no new certificates or signature files are located, the module just returns. If one or more new files of this kind are detected, the file authentication module starts processing them based on the list.

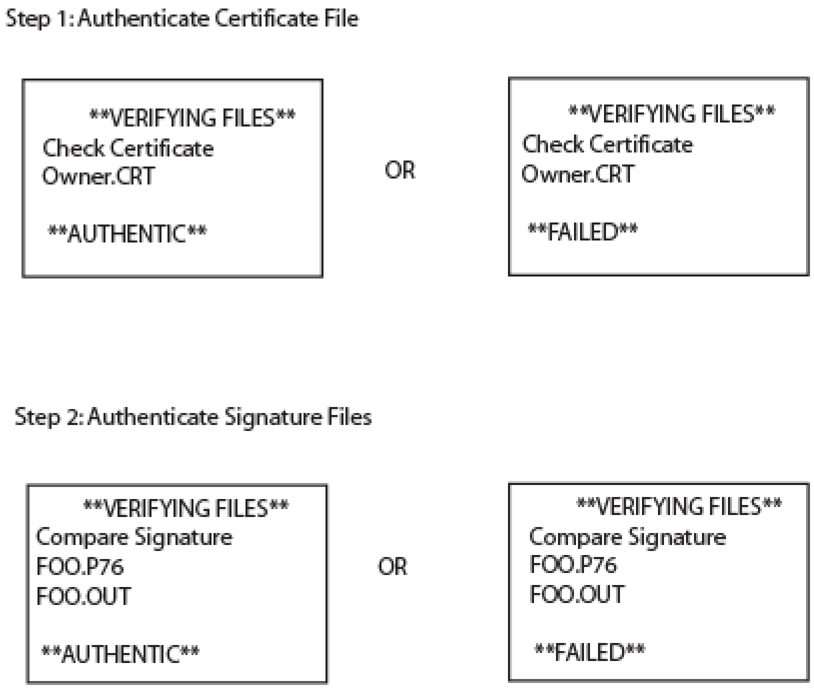
4 Certificates are always processed first (before signature files). The processing routine is called one time for each certificate in the list. If a certificate is authentic, it is noted, and the next certificate is processed. This process continues in random order until all certificates are authenticated.

When a certificate file in the processing list is authenticated, the "Authentic" message is displayed below the corresponding filename. If it fails to be authenticated, the "Failed" message is displayed for five seconds and the terminal beeps three times (see Figure 34). The routine then resumes processing and continues until all certificates are successfully processed.

The processing routine gives both visible and audible indications if a specific certificate authenticates successfully. The file authentication module does not halt the process if a certificate fails to authenticate, but continues to the next step, which is authenticating signature files.

If one or more certificates fail to authenticate, the ensuing file authentication process based on signature files probably also fails, resulting to an application not authenticated and not allowed to execute on the terminal.

When a certificate file is authenticated, the data it contains is added to the certificate tree and the certificate file is deleted from the I: drive. When all required certificates are authenticated and stored in the certificate tree, the file authentication process for signature files can proceed.



Step 1: Authenticate Certificate File

```
**VERIFYING FILES**
Check Certificate
Owner.CRT

**AUTHENTIC**
```

OR

```
**VERIFYING FILES**
Check Certificate
Owner.CRT

**FAILED**
```

Step 2: Authenticate Signature Files

```
**VERIFYING FILES**
Compare Signature
FOO.P76
FOO.OUT

**AUTHENTIC**
```

OR

```
**VERIFYING FILES**
Compare Signature
FOO.P76
FOO.OUT

**FAILED**
```

Figure 34 Display Prompts During the File Authentication Process

5 Signature files are now processed (after certificate files). The file authentication module calls the signature checking routine once for each new signature file it detects. Each `*.p7s` file is checked as it is detected; a list is not built and multiple processing passes are not required.

- If a signature file is authenticated, "**AUTHENTIC**" is displayed and the target file is flagged authentic.
- If the authentication process fails, "**FAILED**" is displayed for five seconds and the terminal beeps three times (see Figure 34). The routine then continues processing the next signature file until all newly detected signature files are checked.
- If a signature file fails to authenticate and its target file is an executable code file, such as `*.out` or `*.lib`, the executable is not allowed to run on the terminal on terminal restart.

For data files, font files, and any other files that require authentication to meet the application's design specification, the application must ensure that these files successfully authenticate.

While a signature file is being processed, it remains stored in the I: drive file system of the target file group. The target application file may be redirected immediately on download to the I: drive or the F: drive.

When the signature file successfully authenticates its target file, it is automatically moved to the same file system and file group as the target file it authenticates (that is, if `*FA` = 1).

The processing routine gives visible and audible indications when a specific signature file authenticates successfully. The file authentication module does not halt the process if a signature file fails to authenticate, but continues to the next step, storing the downloaded files in their final locations in the terminal file system.

6 Certificate files and signature files are retained in the I: drive file system until the file authentication process is complete. These special files are then either deleted or automatically redirected to another file system or file group, as previously described.

When an application file is authenticated, the operating system sets the file's read-only attribute to protect it from being modified while stored in terminal memory. This is also true for a signature file retained in terminal memory. When a signature file is assigned the read-only attribute, it is no longer detected as a new signature file by the file authentication module on terminal restart.

7 When all certificates and signature files are processed and special files are deleted or redirected as required, the terminal restarts and the `*GO` application executes.

File Group Permissions

This section discusses how file authentication controls who (which business entity) can store application files in which file groups in the VX 675 file system.

By inserting zero-length SETDRIVE.x and SETGROUP.n files into a download list, you can specify which drive (x = I: or F:) and in which group (n = 1–15) to store an application file. In addition to this file redirection protocol, the file authentication module controls which files are allowed, under the authority of the signer certificate used to sign them, to be stored in which file groups in the VX 675 file system.

For example, if the terminal owner specifies storing a loyalty application in GID2, the information is encoded in the sponsor and signer certificates and issued by the Verifone CA for that terminal.

Chapter 5 discussed how signer certificates are required inputs to FILESIGN.EXE when preparing a deployment terminal. Each signature file generated under that signer certificate contains a logical link that allows the application to authenticate and run on the terminal only if the signature files and corresponding target files are downloaded into the target GID.

Although you can store files in any file group simply by selecting the target group in Verix Terminal Manager, the files downloaded are not authenticated for the selected target group unless they are properly signed under the authority of the sponsor and signer certificates issued for that terminal.

Download an Operating System Update Provided by Verifone

Because the operating system software for the VX 675 is developed and controlled by Verifone for its customers, Verifone provides the necessary certificates and signature files to ensure the authenticity and integrity of the operating system update as part of the download package.

NOTE Operating system files can only be transferred to a VX 675 terminal using a PC-to-terminal download procedure, by direct download. OS files cannot be downloaded to a VX 675 terminal in a back-to-back operation.

The file authentication procedure for OS downloads is much the same as application downloads, with the following exceptions:

- Verifone provides all files required for the OS download, including
  - The operating system files (such as Q.out, 1.out, and 2.out)
  - An encrypted list of the new files, called VFI.PED
  - A signature file generated by the Verifone CA under the authority of a higher-level OS partition sponsor certificate, called VFI.crt. The file authentication logic on the receiving terminal uses this signature file to confirm the origin and authenticity of the encrypted list of files, VFI.PED.
- The entire OS package must download into Group 1 I: drive. If you select a target group other than Group 1, the operation fails.
- If a full OS download was selected in Verix Terminal Manager, the terminal automatically restarts and the new OS is processed and replaces the existing

OS. In this download operation, all application files stored in Group 1 are automatically erased.

- If a partial OS download was selected in the Verix Terminal Manager, the operating system returns control to Verix Terminal Manager after the download completes. To process the new OS, you must manually restart the terminal by selecting the appropriate Verix Terminal Manager menu option. In a partial OS download operation, application files stored in Group 1 are not erased.
- When the OS download is initiated, the OS file authentication progress is displayed on the screen as new certificates are authenticated and added to the terminal's certificate tree, and as signature files for corresponding OS files are detected and authenticated, as shown in Figure 34.
- While the new OS is being processed, there is no visible indication on the terminal display of the progress of processing. When the new OS is processed (this usually takes a few moments), the terminal restarts automatically and the OS download procedure is complete.

CAUTION If the power supply to the receiving terminal is accidentally cycled during an operating system download procedure, the terminal may permanently lock up. In that case, return the terminal to Verifone for service.

File Authentication for Back-to-Back Application Downloads

When performing a back-to-back application download between two VX 675 terminals, the file authentication process on the receiving terminal is similar to an application download from a host computer to a standalone VX 675 terminal. There are, however, some important differences to take into account:

- Only a full application download is supported for back-to-back data transfers. You cannot perform partial back-to-back application downloads.
- Before you can initiate the back-to-back download, you must enter Verix Terminal Manager in both terminals, select Group 1 as the target group for both terminals, and enter all required passwords.
- All signature files required to authenticate the download application(s) must reside in the memory of the sending terminal. They must not be deleted through the `*FA` variable being cleared to 0 on previous downloads.
- Any sponsor and signer certificates downloaded to and authenticated on the sending terminal are stored in the certificate tree of that terminal. When you perform a back-to-back download, certificate files are reconstructed from the data present in the sending unit's certificate tree.
- All certificates transfer to Group 1 I: drive on the receiving terminal, except for the highest-level platform root certificate, which can never be transferred to another terminal.
- When certificates are detected by the file authentication module of the receiving terminal, they are processed exactly as in a direct download: All

certificates are checked one by one and, on authentication, are added to the certificate tree of the receiving terminal. Then, all signature files are checked.

- Downloaded certificates (receiving terminal) must synchronize with the certificate data present in the certificate tree.

  "Synchronized" means that the certificate tree of the receiving terminal can be no more than one revision out-of-sync with the certificate tree on the sending terminal or the files on the receiving terminal do not successfully authenticate. In this case, the term revision refers to any generic change to the current sponsor and signer certificates stored in the certificate tree of a deployment terminal.
- When the back-to-back download completes and all certificates and signature files authenticate, the receiving terminal restarts. If the name of the *GO application is specified in the Group 1 `CONFIG.SYS` file of the receiving terminal, the application executes and the application prompt or logo is displayed on the terminal.

Timing Considerations Due to the Authentication Process

The file authentication process takes some time. The total amount of time required depends on a number of factors:

- The number and size of application files.
- The number of certificates and signature files.
- Whether the file compression feature of Download Manager is being used to perform the download.

Here are a few additional considerations that may affect the total elapsed time required to complete the download operation:

- Because additional processing steps are required, an operating system download takes longer to complete than an application download (several minutes as opposed to a few seconds).
- The download order of a batch of certificate files may affect total processing time. Digital certificates are validated in a looping process where the validation process cycles as many times as necessary to establish the proper relationship and position of a given certificate in the certificate tree that exists in the terminal.

  To optimize the authentication process, download certificates in a higher-level-certificates-first order. This way, they process faster than a random order download.

Support for File Compression

For information regarding file compression, refer to the *Verix eVo Volume I: Operating System Programmers Manual* (VPN DOC00301).

Effect of Downloads on Existing Files and Data

When downloading application files and data to a VX 675 terminal, an important consideration is the effect of download procedure on existing application files, files used in the file authentication process, and terminal configuration settings stored in `CONFIG.SYS` files in the receiving terminal. Here are some important points:

- If a file already exists in the target file group, the existing file is replaced with the new file of the same name. (Files in separate file groups can have identical names.)
- Always download executable files (and any other files to logically protect under VeriShield file authentication) with the certificates and signature files required to authenticate them.
- In full or partial application downloads, all `CONFIG.SYS` records on the receiving terminal, both protected and non-protected (that is, beginning with * or #), are retained. New `CONFIG.SYS` variables included in the download package, including the `*GO` variable, selectively replace existing variables with the same key name in the `CONFIG.SYS` file of the target group.
- All current passwords are retained on the receiving terminal during an application or operating system download (direct and back-to-back). This includes the Verix Terminal Manager password and file group passwords. If required, you can replace existing file group passwords with new values as part of the data transfer operation.

NOTE

Always modify the Verix Terminal Manager password in a separate, securely-controlled operation. Ensure that this password is retained in a secure place.

- For back-to-back application downloads, it is recommended to clear the memory of the receiving terminal before initiating the download. All application files stored on the receiving terminal, including `CONFIG.SYS` settings, are replaced by those of the sending terminal. Verix Terminal Manager and file group passwords are retained on the receiving terminal.
- For full operating system downloads, Group 1 I: drive is cleared as part of the operation and any application files stored in GID1 are erased. In this case, previously downloaded and authenticated applications must be downloaded in a subsequent operation, together with the certificates and signature files required to authenticate them.

Direct Application Downloads

This section provides the hardware and software checklist needed for direct application downloads. The procedure for direct application downloads is also discussed.

Hardware Checklist

- ❑ The correct cable connects the download computer serial port (COM1 or COM2) to the RS-232 serial port (COM1) of the VX 675 terminal.

Software Checklist

- ❑ Download Manager, VeriCentre, or `DDL.EXE` running on the host computer.
- ❑ The application file to download (full or partial) is located on the host computer.
- ❑ The correct keyed record variables exist in the `CONFIG.SYS` file(s) of the file group(s) to store the application files.
- ❑ Certificate files (`*.crt`) required for file authentication on the receiving terminal are stored in memory or they are located on the host computer, and must download with the application files.
- ❑ All required signature files (`*.p7s`) generated using `FILESIGN.EXE` are located on the host computer. One signature file downloads for each executable (`*.out` or `*.lib`) to run on the terminal.
- ❑ The filenames in the batch download list on the host computer indicate which application files to redirect to F: drive and file groups other than the target group.
- ❑ Ensure that filenames and `CONFIG.SYS` variables to download are correct in relation to those stored in the memory of the receiving terminal to avoid accidental overwrites.
- ❑ The required Verix Terminal Manager and file group passwords are available to make the required Verix Terminal Manager menu selections and to prepare the receiving terminal to receive the application download.

Checklist for Effects on Files and Settings in the Receiving Terminal

- ❑ Protected records in the `CONFIG.SYS` file(s) of the receiving terminal — keyed records that begin with * or # — are not erased.
- ❑ The bootloader, OS, and other firmware on the receiving terminal are not modified as a result of the application download.
- ❑ The certificate tree that exists on the receiving terminal is not modified unless one or more new certificate files are downloading to the terminal. When new certificates are authenticated on the receiving terminal, the data they contain is stored in the certificate tree and the certificate files are deleted from the I: drive of the target group.

Direct Application Download Procedure

The procedure in Table 14 describes how to perform a direct application download from a host download computer into the Group 1 application memory area of a VX 675 deployment terminal.

Steps described in the Action column are performed directly on the VX 675 terminal. Notes provided in this column indicate and explain actions you must perform on the host computer.

NOTE The steps listed in Table 13 are required for all download and upload procedures. In each of the following procedural tables, step numbering starts at 1 to indicate the unique steps of the specific download method. In subsequent procedures, only the method-specific steps are documented; the five steps in Table 13 are assumed to be complete.

Table 13 Common Steps to Start a Download

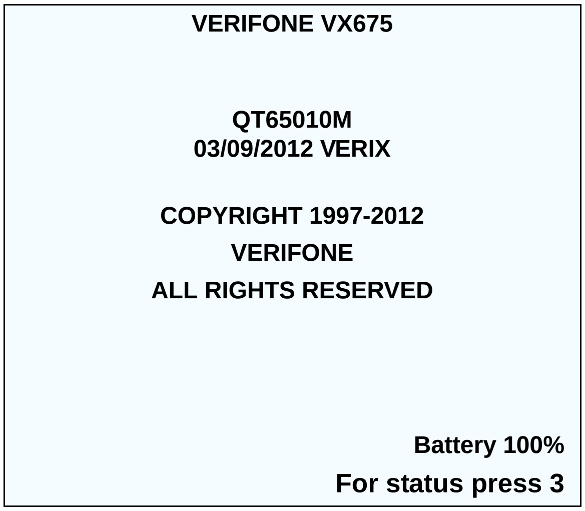
Step	Display	Action
1	 **VERIFONE VX675** **QT65010M** **03/09/2012 VERIX** **COPYRIGHT 1997-2012** **VERIFONE** **ALL RIGHTS RESERVED** **Battery 100%** **For status press 3**	When the terminal restarts, the copyright screen displays the version of VX 675 system firmware stored in the terminal's EPROM, the date the firmware was developed, and the copyright. This screen is displayed for three seconds, during which time you can enter Verix Terminal Manager by simultaneously pressing the **ENTER** and **7** keys. To extend the display period of this screen, press any key during the initial three seconds. Each key press extends the display period an additional three seconds.

Table 13 Common Steps to Start a Download (continued)

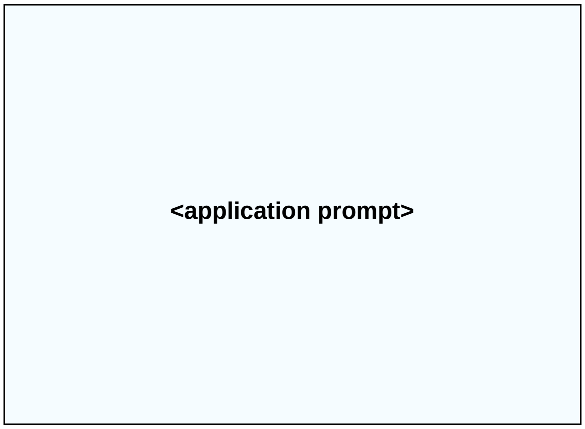
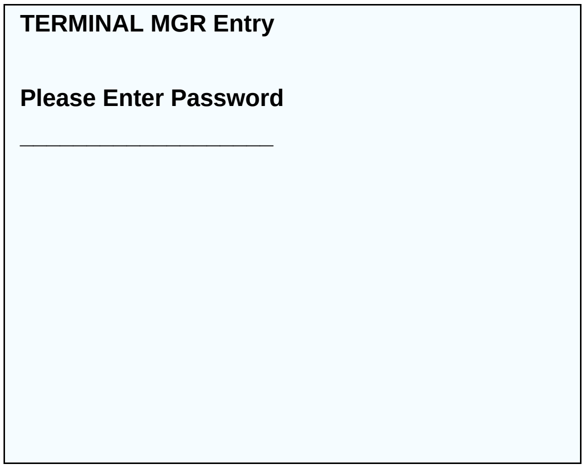
Step	Display	Action
2	 **<application prompt>**	If an application already resides on the terminal, an application-specific prompt is displayed. Otherwise, an error message is displayed. For more information on startup errors, see STARTUP ERRORS.
3	 **TERMINAL MGR Entry** **Please Enter Password** ____________________	Enter the Verix Terminal Manager password. If an application already resides on the terminal, a unique Verix Terminal Manager password may already exist. In this case, type that password and press enter to confirm your entry. If **DOWNLOAD NEEDED** is displayed in step 2, enter the default password, “166831”. To type this password on the keypad, enter: **1 6 6 8 3 1**, and then press **ENTER**. If you enter an incorrect password, the message, **PLEASE TRY AGAIN** is displayed. Reenter the password. To correct a typing mistake, press **CLEAR** to delete the entry, and retype your entry. To end the password entry session and return to the display shown in Step 2, press **CANCEL**.

Table 13 Common Steps to Start a Download (continued)

Step	Display	Action
4	**VERIX TERMINAL MGR** **1> Restart** **2> Edit Parameters** **3> Download** **4> Memory Usage** **5> I: drive Directory** **6> F: drive Directory** **7> EOS Directory** **8> Clear Memory** **9> Calibrate Screen** ↑ ↓	The first of the two **VERIX TERMINAL MGR** menus is displayed. To toggle through other menu, tap the **UP** (⬆) and **DOWN** icon (⬇). To choose an option in the menu, use the **UP** (↑) and **DOWN** (↓) on the left of the screen to scroll on the menu then press **ENTER** until you reach the desired menu. You can also choose an option in the menu by pressing the corresponding number on the keypad. To perform any type of download operation, press **3** to select the **DOWNLOAD** menu option. To cancel the download procedure, press **CANCEL**.

Table 14 Direct Application Download Procedure

Step	Display	Action
1	**VERIX TERMINAL MGR** **Group ID: _1**	Enter the target file group for the download. **FILE GROUP _1** (Group 1) is displayed as the default selection. To select Group 1 as the target file group, press **ENTER**; to select a file group other than Group 1, type the one or two-digit number of the desired file group (2–15) for the download.

Table 14 Direct Application Download Procedure (continued)

Step	Display	Action
2	**VERIX TERMINAL MGR** **Please enter** **Password for GID 1:** ____________________	Enter the password of the selected file group. For example, if Group 1 is the target group, the **GROUP _1 PASSWORD** message shown at left is displayed. To continue, enter the required file group password and press **ENTER** to confirm entry.
3	**VTM DOWNLOAD MGR Gn** **1> Single-app** **2> Multi-app**	For a single application download, select **Single-app.** For multiple application download, select **Multi-app.** (Refer to Chapter 6 for detailed download instructions and information.) To return to **VERIX TERMINAL MGR**, press **CANCEL**.

Table 14 Direct Application Download Procedure (continued)

Step	Display	Action
4	**VTM DOWNLOAD MGR Gn** **1> Full dnld** **2> Partial dnld**	Select the type of download mode: **Full dnld** or **Partial dnld**. To return to **VERIX TERMINAL MGR**, press **CANCEL**.
5	**VTM DOWNLOAD MGR Gn** **1> Modem** **2> COM1** **3> COM7** **4> SD Card** **5> USB Flash Memory** **6> TCPIP** **7> USB Dev** **8> COM6** **9> COM2**	Select the download mode: **Modem, COM1, COM2 , SD Card, Memory Stick, TCPIP, USB Dev, COM6** (If there are any additional menu options press the **DOWN** key).
6	**VTM DOWNLOAD MGR Gn** ****** WARNING ****** **All Files Will Be** **Cleared From Group 1** **1> Cancel Download** **2> Continue**	A warning message will first appear once a download mode is selected. To return to the main menu without saving your selection, press **CANCEL**.

Table 14 Direct Application Download Procedure (continued)

Step	Display	Action
7	VTM DOWNLOAD MGR Gn Unit Receive Mode WAITING FOR DOWNLOAD	Initiate the download by executing the proper command(s) in the download tool running on the host computer. The data transfer operation starts, and the status messages are displayed on the terminal screen. The progress of the download is indicated by a series of ten asterisks (each asterisk indicates that 10% of the download is complete). When the last asterisk is displayed, the download is complete. To stop the download operation, press the **CANCEL** key. The terminal restarts automatically.
8	**VERIFYING FILES** CHECK CERTIFICATE (FILENAME.CRT) **AUTHENTIC** or --- FAILED ---	When the download is complete, the terminal restarts automatically. The file authentication module on the receiving terminal begins to check for new certificate (`*.crt`) and signature (`*.p7s`) files included in the download. These special files then process one at a time; certificates process first, then signature files. When the file authentication module is invoked, the status display informs you of the progress of the file authentication process. If file authentication succeeds for a specific certificate, the "**AUTHENTIC**" message is displayed directly below the certificate filename. If file authentication fails for a specific certificate, the "**FAILED**" message is displayed for five seconds below the filename and the terminal beeps three times, allowing you to note which certificate failed to authenticate. The authentication process then continues to the next certificate until all new certificates are authenticated.

Table 14 Direct Application Download Procedure (continued)

Step	Display	Action
9	****VERIFYING FILES**** **CHECK CERTIFICATE** **(FILENAME.CRT)** ****AUTHENTIC**** or **--- FAILED ---**	The file authentication module continues to authenticate any new signature files downloaded with the OS files. When the signature file authentication routine starts, the status display informs you of the progress of the authentication process. If file authentication succeeds for a specific signature file, the "**AUTHENTIC**" message is displayed directly below the filename of the signature file. If file authentication fails for a specific signature file, the "**FAILED**" message is displayed for five seconds below the filename and the terminal beeps three times, allowing you to note which signature file failed to authenticate. The authentication process then proceeds to the next signature file until all signature files are validated. When all new signature files are authenticated, the terminal restarts, and the application specified in the `*GO` variable or the default application in Group 1 executes and starts running on the terminal.
10	(Application Prompt) or **DOWNLOAD NEEDED**	If the downloaded application successfully authenticates, the corresponding application prompt or logo is displayed upon restart. The terminal can now process transactions. **Note:** The message **DOWNLOAD NEEDED** appears if: • The `*GO` variable is not set. • `*GO` does not specify that an application is present. • The application did not authenticate (invalid or missing `*.p7s` file). • The application uses shared libraries that are missing or were not authenticated (invalid or missing `*.p7s` files). If one or more executables in the application fail to successfully authenticate, the application may not run. If the application attempts to access an unauthenticated executable or library, it may crash. Repeat the Direct Operating System Download Procedure using the correct certificates and/or signature files.

Direct Operating System Downloads

This section provides the hardware and software checklist needed for direct operating system downloads. The procedure for direct operating system downloads is also discussed.

Hardware Checklist

❑ The correct cable connects the download computer serial port (COM1 or COM2) to the RS-232 serial port (COM1) of the VX 675 terminal.

Software Checklist

❑ Download Manager, VeriCentre, or `DDL.EXE` running on the host computer.

❑ The complete OS version to download is located on the host computer.

❑ Select full or partial download of the OS. In a full OS download, the terminal restarts automatically and the new OS is processed, replacing the existing OS. In a partial OS download, the terminal returns to Verix Terminal Manager and the new OS does not process until you manually initiate a terminal restart from Verix Terminal Manager.

❑ The correct keyed record variables for the download exist in the `CONFIG.SYS` files of Group 1. (OS files must always download into GID1 I: drive). The required variables can also be written into the `CONFIG.SYS` file as part of the download operation.

❑ The following files provided by Verifone CA for full OS downloads must reside on the host computer:

- The new OS version or OS update (`Q*.out`, `1*.out`, `2*.out`, `3*.out`, `4*.out`, `5*.out`, `6*.out`).
- A signature file called `VFI.p7s` for the OS update. This signature file is generated by the Verifone CA using the high-level OS certificates for the VX 675 platform.
- A file called `VFI.PED`. This file is an encrypted list of the new OS files.

❑ The required Verix Terminal Manager and file group passwords are available to make the required Verix Terminal Manager menu selections to prepare the receiving terminal to receive the application download.

Checklist for Effects on Files and Settings in the Receiving Terminal

❑ A full OS download replaces the existing OS and erases all application files from the Group 1 I: drive.

❑ A partial OS download returns control of the terminal to Verix Terminal Manager and does not erase application files from the Group 1 I: drive.

❑ Protected records in the `CONFIG.SYS` file(s) of the receiving terminal — keyed records that begin with * or # — are not erased.

❑ An OS download does not overwrite terminal configuration settings, including the current date and time, passwords, and modem country code. If required, you can download new terminal configuration settings together with the OS files.

- The certificate tree that exists on the receiving terminal is not modified unless one or more new certificate files required to authenticate the new OS are being downloaded to the terminal. When new certificates authenticate on the receiving terminal, the data they contain is stored in the certificate tree and the certificate files are deleted from the Group 1 I: drive.
- The certificates and signature files required to authenticate the new OS are processed by the file authentication module of the receiving terminal the same as application files.
- When the terminal restarts and the new OS files process, they are moved out of the Group 1 I: drive into the Group 0 area of the VX 675 file system.

Direct Operating System Download Procedure

The procedure in Table 15 describes how to perform a direct operating system download from a host computer into the Group 1 I: drive of a VX 675 terminal.

Steps described in the Action column are performed directly on the VX 675 terminal. Notes provided in this column indicate and explain actions you must perform on the host computer.

NOTE In Table 15 and in the following procedures, only method-specific steps are included. For a description of the steps required to enter Verix Terminal Manager and display **VERIX TERMINAL MGR MENU 2**, refer to Table 13.

Table 15 Direct Operating System Download Procedure

Step	Display	Action
1	**VERIX TERMINAL MGR** **Group ID: _1**	Enter the target file group for the download. **FILE GROUP _1** (Group 1) is displayed as the default selection. To select Group 1 as the target file group, press **ENTER**; to select a file group other than Group 1, type the one or two-digit number of the desired file group (2 – 15) for the download.

Table 15 Direct Operating System Download Procedure (continued)

Step	Display	Action
2	**VERIX TERMINAL MGR** **Please enter** **Password for GID 1:** ____________________	Enter the password of the selected file group (Group 1) and press **ENTER** to confirm the entry.
3	**VTM DOWNLOAD MGR Gn** **1> Single-app** **2> Multi-app**	For a single application download, select **Single-app**. For multiple application download, select **Multi-app.** (Refer to Chapter 6 for detailed download instructions and information.) To return to **VERIX TERMINAL MGR MENU 1**, press **CANCEL**.
4	**VTM DOWNLOAD MGR Gn** **1> Full dnld** **2> Partial dnld**	Select **Full dld** for a full OS download or select **Partial dnld** for a partial OS download operation. To return to **VERIX TERMINAL MGR MENU 1**, press **CANCEL**.

Table 15 Direct Operating System Download Procedure (continued)

Step	Display	Action
5	**VTM DOWNLOAD MGR Gn** **1> Modem** **2> COM1** **3> COM7** **4> SD Card** **5> Memory stick** **6> TCPIP** **7> USB Dev** **8> COM6** **9> COM2**	Select the terminal port to use for the data transfer from the host computer to the receiving terminal. (If there are any additional menu options, press the **DOWN** key.) For a direct OS download using a modem, select the **Modem** menu option by pressing the **1** key For a direct OS download using COM1 of a multiport adapter, select the **COM1** menu option by pressing the **2** key. For a direct OS download using COM7 of a multiport adapter, select the **COM7** menu option by pressing the **3** key. For a direct OS download using an SD card, select the **SD Card** menu option by pressing the **4** key. For a direct OS download using an external memory stick, select the **Memory stick** menu option by pressing the **5** key. For a direct OS download using TCP/IP, select the **TCPIP** menu option by pressing the **6** key. For a direct OS download using USB device, select the **USB Dev** menu option by pressing the **7** key. For a direct OS download using the external dongle, select the **COM6** menu option by pressing the **8** key. For a direct OS download using the external dongle, select the **COM2** menu option by pressing the **8** key. In either case, when you press **ENTER**, the terminal is ready to receive the OS download from the host computer.
6	**VTM DOWNLOAD MGR Gn** **Unit Receive Mode** **WAITING FOR DOWNLOAD**	Initiate the download by executing the proper command(s) in the download tool running on the host computer (when the receiving terminal is ready to receive the direct OS download). The data transfer operation starts, and the status messages are displayed on the terminal screen. The progress of the download is indicated by a series of ten asterisks (each asterisk indicates that 10% of the download is complete). When the last asterisk is displayed, the download is complete. To stop the download operation, press the **CANCEL** key. The terminal restarts automatically.

Table 15 Direct Operating System Download Procedure (continued)

Step	Display	Action
7	****VERIFYING FILES**** **CHECK CERTIFICATE** **(FILENAME.CRT)** ****AUTHENTIC**** or **--- FAILED ---**	When the OS download is complete, the terminal restarts automatically. The file authentication module on the receiving terminal begins to check for new certificate (`*.crt`) and signature (`*.p7s`) files included in the download. These special files then process one at a time; certificates process first, then signature files. When the file authentication module is invoked, the status display informs you of the progress of the file authentication process. If file authentication succeeds for a specific certificate, the "**AUTHENTIC**" message is displayed directly below the certificate filename. If file authentication fails for a specific certificate, the "**FAILED**" message is displayed for five seconds below the filename and the terminal beeps three times, allowing you to note which certificate failed to authenticate. The authentication process then continues to the next certificate until all new certificates are checked.
8	****VERIFYING FILES**** **CHECK CERTIFICATE** **(FILENAME.CRT)** ****AUTHENTIC**** or **--- FAILED ---**	The file authentication module continues to authenticate new signature files downloaded with the OS files. When the signature file authentication routine starts, the status display informs you of the progress of the authentication process. If file authentication succeeds for a specific signature file, the "**AUTHENTIC**" message is displayed directly below the filename of the signature file. If file authentication fails for a specific signature file, the "**FAILED**" message is displayed for five seconds below the filename and the terminal beeps three times, allowing you to note which signature file failed to authenticate. The authentication process then proceeds to the next signature file until all signature files are validated. When all new signature files are authenticated, the terminal restarts and begins processing the new OS (full download) or it returns control to Verix Terminal Manager (partial download). If you are performing a partial download, the terminal does not restart until you manually press the **4** key in **VERIX TERMINAL MGR MENU 1**. If an application resides on the terminal following the OS download, it executes on restart. **Note:** Because a full OS download clears the I: drive, all terminal applications, related certificates, and signature files must download to the terminal when performing this type of download.

Table 15 Direct Operating System Download Procedure (continued)

Step	Display	Action
9	(Application Prompt) or **DOWNLOAD NEEDED**	If you performed a full OS download, the **DOWNLOAD NEEDED** prompt is displayed. A direct application download on the receiving terminal can be performed. If you performed a partial OS download and manually restarted the terminal, the application residing in the terminal (if any) executes. The application prompt is displayed on terminal restart, after OS processing, and the application starts.

Back-to-Back Application Downloads

This section provides the hardware and software checklist needed for back-to-back application downloads. The procedure for back-to-back terminal downloads is also discussed.

Hardware Checklist

□ The correct cable connects the RS-232 ports of the sending and receiving VX 675 terminals.

Software Checklist

□ The firmware versions of the sending and receiving terminals must be identical or very similar.

□ One or more complete and authenticated application programs are stored in the GIDs 1–15, I: drive or F: drive of the sending terminal. In this type of operation, *all* files stored in application memory of the sending terminal download to the receiving terminal.

□ Before initiating the download procedure, remember to select Group 1 as the target file group on both the sending and receiving terminals. The required Verix Terminal Manager and file group passwords must also be available to make the required Verix Terminal Manager menu selections on both terminals.

□ The current `CONFIG.SYS` variables, date and time, and other terminal configuration settings on the sending terminal are those downloaded to the receiving terminal. Ensure that the desired settings are correct.

□ All signature files required to authenticate the application files being downloaded to the receiving terminal are present in the I: drive or F: drive file system of the sending terminal.

□ The certificate tree of the sending and receiving terminal must be synchronized. That is, there can be no more than one revision difference between the certificate data currently stored in the memory of the sending and receiving terminals.

Checklist for Effects on Files and Settings in the Receiving Terminal

❏ A back-to-back application download overwrites existing applications, libraries, or any other files stored in the I: drive of the receiving terminal.

❏ All `CONFIG.SYS` records and settings on the receiving terminal—protected and non-protected—are replaced by those of the sending terminal. Ensure that these records and settings on the sending terminal are correct before initiating the download.

❏ Passwords on the receiving terminal are retained.

❏ Certificates and signature files downloaded to the receiving terminal, together with application files, must be processed by the file authentication module on the receiving terminal on terminal restart after the back-to-back download completes.

❏ The OS software on the receiving terminal is not affected by a back-to-back application download.

Note: OS files cannot be downloaded in a back-to-back operation.

❏ An application upload does not overwrite the existing certificate tree on the receiving terminal. Any downloaded certificate files are authenticated and then added to the tree.

Back-to-Back Application Download Procedure

The back-to-back application download process consists of two main phases:

1 Preparing a Gold VX 675 terminal (transfers application files to the Target VX 675 terminal).

2 Downloading application files from the Gold terminal to a properly configured Target terminal.

Prepare Gold Terminal (PC-to-Terminal)

1 Configure the host PC for an application download operation to the Gold terminal:

- Set the `*FA` variable (if present in the application) to 1.
- Ensure that all certificates, `*p7s` files, applications, and other required files are present.
- Ensure that the download is exactly what you want your Target terminal to receive.

2 Configure the Gold terminal to receive an application download from a PC:

- From **VERIX TERMINAL MGR MENU 1**, set Group 1 and COM1 as the port to receive the download.

3 Connect a cable between the RS-232 serial ports of the PC and the Gold terminal.

4 Initiate the file transfer on the PC.

5 From **VERIX TERMINAL MGR MENU 1** on the Gold terminal, select either a full or a partial download using a UART Dongle connected to each terminal.

The PC transfers files to the Gold terminal.

Download Application Files to Target Terminal

1. Configure a Gold terminal for an application download operation to a deployment terminal:
   - If the `*FA` variable (if present in the application) is set to 0, you can reset it to 1. For more information on the `*FA` variable, refer to the *Verix eVo Volume I: Operating System Programmers Manual* (VPN DOC00301).
   - Ensure that the download is exactly what you want your Target terminals to receive.
   - Ensure that previously authenticated files are not changed prior to the file transfer operation.
2. Configure the Target terminal to receive an application download from the Gold terminal. From **VERIX TERMINAL MGR MENU 1**, set Group 1 and COM1 as the port to receive the file transfer.
3. Connect a cable (Verifone part number 05651-xx) between the RS-232 serial ports of the Gold and Target terminals using a UART Dongle connected to each terminal.
4. From any Verix Terminal Manager menu on the Gold terminal, press [*] and enter the GID1 password to initiate the file transfer.
5. From **VERIX TERMINAL MGR MENU 1** on the deployment terminal, select either a full or a partial download. The Gold terminal begins to transfer files to the Target terminal.

Figure 35 illustrates these two phases and how they relate to each other.

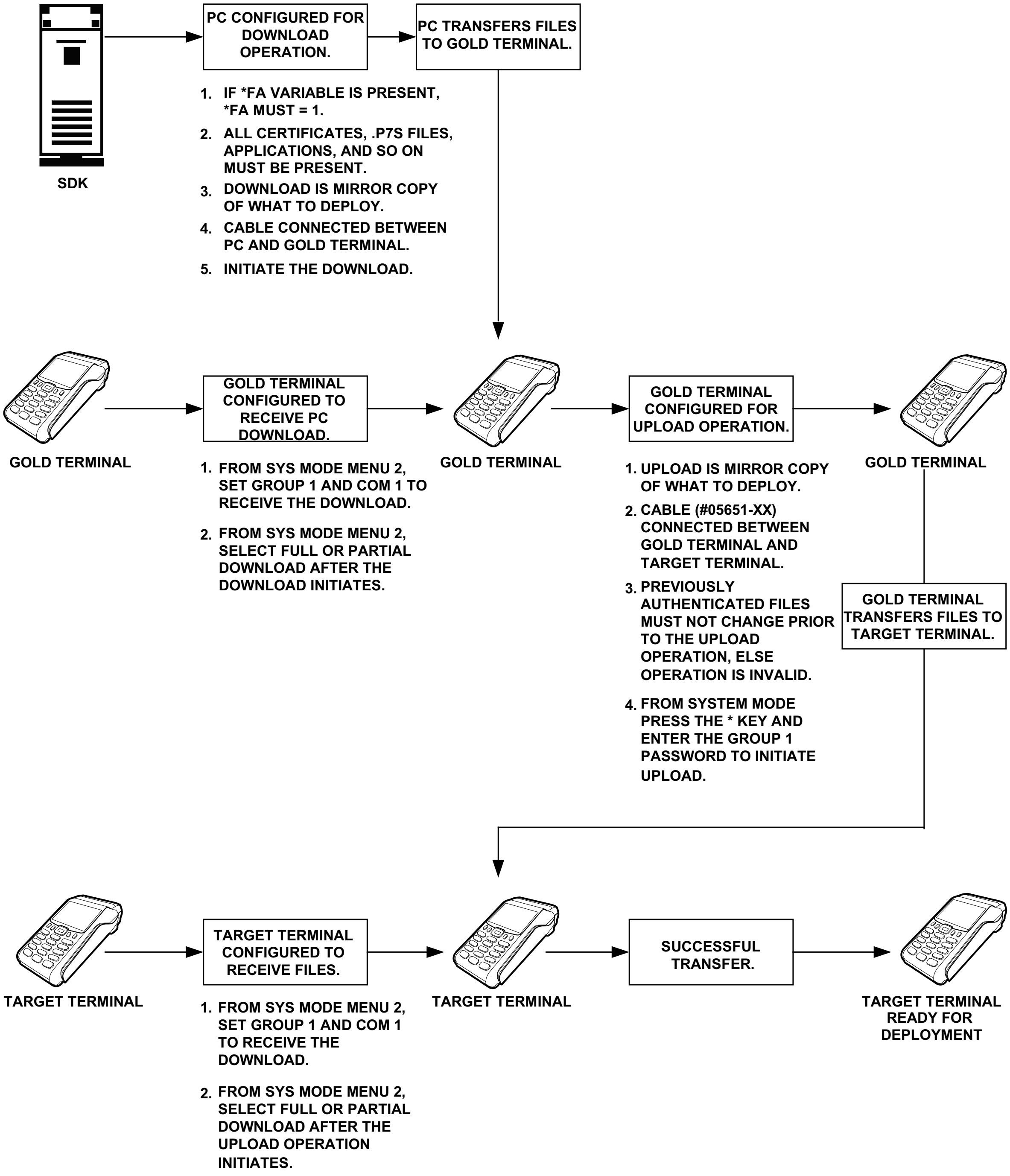

SDK
PC CONFIGURED FOR DOWNLOAD OPERATION.
PC TRANSFERS FILES TO GOLD TERMINAL.
1. IF *FA VARIABLE IS PRESENT, *FA MUST = 1.
2. ALL CERTIFICATES, .P7S FILES, APPLICATIONS, AND SO ON MUST BE PRESENT.
3. DOWNLOAD IS MIRROR COPY OF WHAT TO DEPLOY.
4. CABLE CONNECTED BETWEEN PC AND GOLD TERMINAL.
5. INITIATE THE DOWNLOAD.
GOLD TERMINAL
GOLD TERMINAL CONFIGURED TO RECEIVE PC DOWNLOAD.
1. FROM SYS MODE MENU 2, SET GROUP 1 AND COM 1 TO RECEIVE THE DOWNLOAD.
2. FROM SYS MODE MENU 2, SELECT FULL OR PARTIAL DOWNLOAD AFTER THE DOWNLOAD INITIATES.
GOLD TERMINAL
GOLD TERMINAL CONFIGURED FOR UPLOAD OPERATION.
1. UPLOAD IS MIRROR COPY OF WHAT TO DEPLOY.
2. CABLE (#05651-XX) CONNECTED BETWEEN GOLD TERMINAL AND TARGET TERMINAL.
3. PREVIOUSLY AUTHENTICATED FILES MUST NOT CHANGE PRIOR TO THE UPLOAD OPERATION, ELSE OPERATION IS INVALID.
4. FROM SYSTEM MODE PRESS THE * KEY AND ENTER THE GROUP 1 PASSWORD TO INITIATE UPLOAD.
GOLD TERMINAL
GOLD TERMINAL TRANSFERS FILES TO TARGET TERMINAL.
TARGET TERMINAL
TARGET TERMINAL CONFIGURED TO RECEIVE FILES.
1. FROM SYS MODE MENU 2, SET GROUP 1 AND COM 1 TO RECEIVE THE DOWNLOAD.
2. FROM SYS MODE MENU 2, SELECT FULL OR PARTIAL DOWNLOAD AFTER THE UPLOAD OPERATION INITIATES.
TARGET TERMINAL
SUCCESSFUL TRANSFER.
TARGET TERMINAL READY FOR DEPLOYMENT

Figure 35 Back-To-Back Download Process

The procedure in Table 16 walks you through a back-to-back application download from a sending VX 675 terminal (Gold) to a receiving VX 675 terminal (Target).

Back-to-back downloads require that one terminal, the Gold terminal, be loaded with the required applications. The receiving terminal is the Target terminal. The procedure in Table 16 assumes the following:

- The Target terminal has no applications loaded.
- There is enough memory in the Target terminal to complete the download.

NOTE The Target terminal does not display an error message if there is not enough memory to complete the download. However, the Gold terminal displays **DOWNLOAD INCOMPLETE** before returning to **SYS MODE MENU 2**.

- You are performing a full download.

Table 16 Back-to-Back Application Download Procedure

Step	Gold Terminal	Target Terminal
1	Connect a MOD10 cable (P/N 05651-XX) between the RS-232 ports of the terminals using a UART Dongle connected to each terminal. Allow each terminal to boot up. After boot up, the Target terminal displays **DOWNLOAD NEEDED**.	
2	Press **ENTER**+**7** to enter Verix Terminal Manager.	
3	Enter the Verix Terminal Manager password (factory default is **“1 6 6 8 3 1”** and press **ENTER**.	
4	Press the * (asterisk) key, then press **ENTER**. You are prompted to reenter the Verix Terminal Manager password. **UPLOADING NOW** is displayed.	Press **3**, **DOWNLOAD**, to enter download mode.
5		Press **ENTER** at the next **VERIX TERMINAL MGR DOWNLOAD** screen to select **FILE GROUP_1** (default displayed) as the target file group.
6		For a single application download, select **Single-app**. For multiple application download, select **Multi-app** in the next **VERIX TERMINAL MGR DOWNLOAD** screen.

Table 16 Back-to-Back Application Download Procedure

Step	Gold Terminal	Target Terminal
7		Select **2** (**COM1**) in the next **VERIX TERMINAL MGR DOWNLOAD** screen. **DOWNLOADING NOW** is displayed.
	Both terminals display a status indicator, where each dash represents a 10% increment of the download. Ensure that the Gold terminal displays **UPLOAD COMPLETE** before returning to **VERIX TERMINAL MGR MENU 1**. This is when the Gold terminal might display an error message if problems occurred during the download process. The Target terminal begins to validate all files. Allow the Target terminal to complete file authentication and reboot the terminal. The Gold terminal is ready to perform another download. An application-specific menu is displayed after the Target terminal completes the reboot.	

CHAPTER 7

Specifications

This chapter discusses power requirements, dimensions, and other specifications of the VX 675 terminal.

Power

5 V DC 1.0 A

Micro-USB Power Pack

UL, ITE listed, LPS power supply:

a Input rated: 100 - 240 V AC, 50/60 Hz

b Output rated: 5 V DC 1.0 A

Temperature

- Operating temperature: 0 °C to +50 °C (32 °F to 122 °F)
- Non-operating temperature: -30 °C to 60 °C (-22 °F to 140 °F)
- Relative humidity: 5% to 90%; non-condensing

External Dimensions

- Length: 148mm (5.8 in); 163 mm (6.41 in); 109.2 mm (4.3 in) for VX 675 ECR
- Width: 78 mm (3.1 in)
- Depth: 42 mm (1.6 in); 52 mm (2 in); 56.3 mm (2.2 in) for VX 675 ECR

CHAPTER 8

Maintenance

The VX 675 terminal and base have no user-serviceable parts.

Cleaning the Terminal

To clean the terminal and base, use a clean cloth slightly dampened with water and a drop or two of mild soap. For stubborn stains, use alcohol or an alcohol-based cleaner.

CAUTION Never use thinner, trichloroethylene, or ketone-based solvents – they may cause deterioration of plastic or rubber parts.

Do not spray cleaners or other solutions directly onto the keypad or terminal display.

Terminal Contacts

Gently swab the contacts with alcohol or contact cleaner to remove the dirt. It is important that the exposed contacts of the VX 675 battery stay clean and unbent.

CAUTION Avoid touching the contacts of the VX 675 battery and the recessed area on the terminal. Finger oils tarnish contacts, causing bad connections. When operating on battery power and experiencing a high occurrence of bad or incomplete data transfers, clean the contacts.

Smart Card Reader

Do not attempt to clean the smart card reader. Doing so may void any warranty. For smart card reader service, contact your Verifone distributor or service provider.

CHAPTER 9

Verifone Service and Support

For VX 675 terminal problems, contact your local Verifone representative or service provider.

For VX 675 product service and repair information:

- USA – Verifone Service and Support Group, 1-800-Verifone (837-4366), Monday - Friday, 8 A.M. - 8 P.M., Eastern time
- International – Contact your Verifone representative

Returning a Terminal for Service

Before returning a VX 675 terminal or base to Verifone, you must obtain an MRA number. The following procedure describes how to return one or more VX 675 terminals or bases for repair or replacement (U.S. customers only).

NOTE Customers outside the United States are advised to contact their local Verifone representative for assistance regarding service, return, or replacement of terminals or batteries.

To Return a Terminal for Service

1 Get the following information from the printed labels on the bottom of *each* VX 675 terminal or base to be returned:

- Product ID, including the model and part number. For example, “VX 675” and “M265-XXX-XX-XXX-2.”
- Serial number (S/N nnn-nnn-nnn)

2 Obtain the MRA number(s) by completing one of the following:

a Call Verifone toll-free within the United States at 1-800-Verifone and follow the automated menu options.

- Select the MRA option from the automated message. The MRA department is open Monday to Friday, 8 A.M.– 8 P.M., Eastern Time.
- Give the MRA representative the information you gathered in Step 1. If the list of serial numbers is long, you can fax the list, along with the information gathered in Step 1, to the MRA department at 727-953-4172 (U.S.).

b Address a fax to “Verifone MRA Dept.” with the model and part number(s)

- Include a telephone number where you can be reached and your fax number.

c Complete the Inquiry Contact Form at http://www.verifone.com/aboutus/contact/contact_form.cfm.

- Address the Subject box with to “Verifone MRA Dept.”
- Reference the model and part number in the Note box.

NOTE

One MRA number must be issued for each VX 675 terminal you return to Verifone, even if you are returning several of the same model.

3 Describe the problem(s).

4 Provide the shipping address where the repaired or replacement unit must be returned.

5 Keep a record of the following items:

- Assigned MRA number(s).
- Verifone serial number assigned to the VX 675 terminal or base you are returning for service or repair (terminal serial numbers are located on the bottom of the unit.
- Shipping documentation, such as air bill numbers used to trace the shipment.
- Model(s) returned (model numbers are located on the Verifone label on the bottom of the VX 675 terminal).

Accessories and Documentation

Verifone produces the following accessories and documentation for the VX 675 terminal. When ordering, please refer to the part number in the left column.

- Verifone online store at www.store.verifone.com
- USA – Verifone Customer Development Center, 800-Verifone (837-4366), Monday - Friday, 7 A.M. - 8 P.M., Eastern time
- International – Contact your Verifone representative

Power Pack

Contact your local Verifone distributor to determine which power pack fits your needs.

VPN PWR265-001-01-A	DC Power Pack (Universal)

Printer Paper

VPN PPR265-001-01-A	25 mm (0.98 in) diameter, 57 mm (2.24 in) wide
VPN PPR268-001-01-A	40 mm (1.57 in) diameter, 57 mm (2.24 in) wide

Verifone Cleaning Kit

VPN 02746-01	Cleaning Kit

Micro-USB Cable

VPN SUB265-001-01-A	Micro-USB service dongle

Documentation

VX 675 Certifications and Regulations Sheet	VPN DOC265-001-EN
VX 675 Quick Installation Guide	VPN DOC265-002-EN
VX 675 Installation Guide	VPN DOC265-003-EN
VX 675 Base Certifications and Regulations Sheet	VPN DOC265-005-EN
VX 675 Full-Featured Base Quick Installation Guide	VPN DOC265-026-EN
VX 675 USB Base Quick Installation Guide	VPN DOC265-025-EN
VX 675 ECR Certifications and Regulations Sheet	VPN DOC265-027-EN
VX 675 ECR Quick Installation Guide	VPN DOC265-028-EN
Verix eVo Volume I: Operating System Programmers Manual	VPN DOC00301
Verix eVo Volume II: Operating System and Communications Programmers Guide	VPN DOC00302

APPENDIX A

System Messages

This appendix describes error and information messages, which are grouped into two categories. For ease of use, these messages are grouped alphabetically in each of these two categories.

These messages include the following:

- Digital certificate displays and signature file downloaded to the terminal.
- File authentication module processes.
- File compression module use messages from the VeriCentre DMM terminal management and download tool.

Error Messages

The following error messages may appear when the VX 675 terminal is in Verix Terminal Manager.

Table 17 Error Messages

Display	Action
COMPRESSION MODULE ERROR	
**** UNZIP Error n** **xxxxxx** **yyyyyy**	If you are using the file compression module in DMM, information similar to what is shown above appears when an error occurs during file extraction from a downloaded ZIP archive. Note the error number and error codes (xxxxx and yyyyy) and try to download the archive again.

Table 17 Error Messages (continued)

Display	Action
DEBUGGER ERRORS	
ALREADY DEBUGGING	The debugger has already been invoked.
LOAD DBMON.OUT	The `DBMON.OUT` debugging monitor program is included in the SDK, but is not stored in the terminal memory of a factory unit. To use the debugging tool, you must sign, download, and authenticate the `DBMON.OUT` application.
DOWNLOADING ERRORS	
VTM DOWNLOAD MGR Gn **TCP/IP NOT PRESENT**	This error only occurs on a VX 675 terminal when downloading through TCP/IP. An application that supports the TCP stack does not exist.
VTM DOWNLOAD MGR Gn **NO *ZTCP VARIABLE**	This error only occurs on a VX 675 terminal when downloading through TCP/IP. An application that supports the TCP stack does not exist.

Table 17 Error Messages (continued)

Display	Action
VTM DOWNLOAD MGR Gn **GID: nn** **APP ID: nnnn** **STATUS: CONNECTING** **<error message>**	The following error message may occur while connecting to a host during wireless download: • **NO CARRIER** - The terminal could not establish a connection with the host. • **LOST CARRIER** - The carrier was lost during connection. • **BUSY** - The host is currently busy. • **NO ENQ FROM HOST** - The host did not send an ENQ (Enquiry).
VTM DOWNLOAD MGR Gn **GID: nn** **APP ID: nnnn** **STATUS: DOWNLOADING** **<error message>**	The following error message may occur while connecting to a host during a modem or wireless download: • **BAD RX COMM** - The terminal received too many bad packets. • **BAD TX COMM** - The host received too many bad packets. • **LOST CARRIER** - The carrier was lost during download. • **NO RESP FROM HOST** - The terminal timed out waiting for a packet from the host.
EDIT PARAMETERS ERROR	
TERMINAL MGR EDIT **GID nn: NOT EMPTY** **<parm name> NOT FOUND** **1> Cancel** **2> Add Variable**	You entered an invalid parameter name. Select **CANCEL** to go back to the parameter editor or **ADD VARIABLE** to add the entered parameter name as a new variable.

Table 17 Error Messages (continued)

Display	Action
PASSWORD ERRORS	
Change Passwords G1 **Please Try Again**	You entered an invalid GID password. Press **CANCEL** or **ENTER** and enter a valid password.
VERIX TERMINAL MGR **Please enter** **Password for GID n:** __________	This message is displayed when you initiate the procedure for modifying existing Verix Terminal Manager passwords through **Change Passwords** in **VERIX TERMINAL MGR MENU 2**. The menu option displayed allows you to change the password of a **File Group** (Press **1**) or the **TERMINAL MGR Entry** (Press **2**).
VTM PASSWORD MGR **New __________**	This message is displayed when you select **Change Passwords** in **VERIX TERMINAL MGR MENU 2** to modify the existing Verix Terminal Manager password. **NEW**: Make the appropriate menu selections to enter the new password. **AGAIN**: Repeat the entry to confirm the new password. **PASSWORD CHANGED**: Displayed when the new password is accepted.

Table 17 Error Messages (continued)

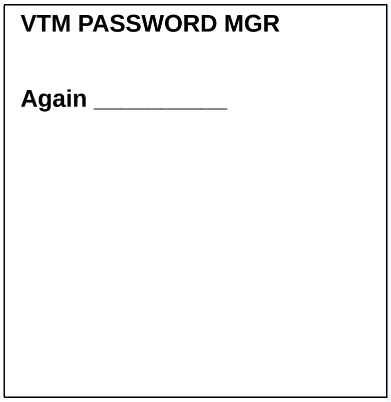
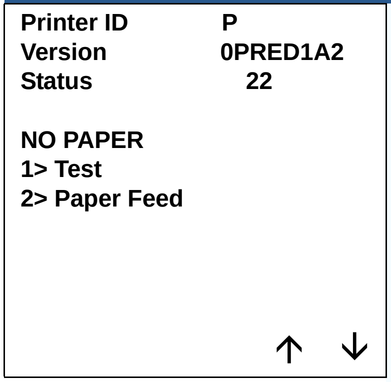
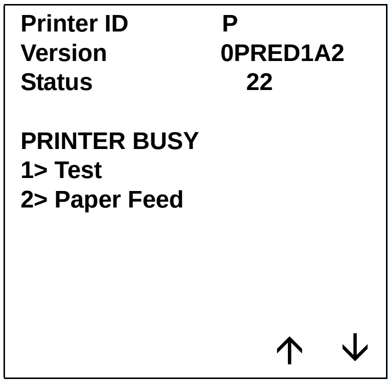
Display	Action
 VTM PASSWORD MGR Again __________	
PRINTER DIAGNOSTICS ERRORS	
 Printer ID P Version 0PRED1A2 Status 22 NO PAPER 1> Test 2> Paper Feed ↑ ↓	**NO PAPER** is displayed when you select **TEST** or **PAPER FEED** and there is no paper installed in the printer.
 Printer ID P Version 0PRED1A2 Status 22 PRINTER BUSY 1> Test 2> Paper Feed ↑ ↓	When you select **TEST** or **PAPER FEED** from the printer diagnostics screen, terminal manager first checks if the printer is currently active. If it is, **PRINTER BUSY** is displayed.

Table 17 Error Messages (continued)

Display	Action
REMOTE DIAGNOSTICS ERROR	
LOAD TERMINAL MANAGEMENT AGENT	The (optional) Terminal Management Agent (TMA) software is not resident in the VX 675 terminal. The TMA software is required to perform remote diagnostics. For more information about support for remote diagnostics, contact your Verifone service provider.
SMART CARD DIAGNOSTICS ERRORS	
TEST NOT SUPPORTED	This message appears if the terminal does not support ICC devices. Therefore, a SAM card diagnostics session cannot be performed. Press any key to go back to the main menu.
SAM nn **POWER UP: FAILED**	This screen is displayed when there is no SAM card inserted in the selected slot.
NO SYNC DRIVERS INSTALLED	This screen is displayed if sync drivers are not installed in the terminal. Therefore, a sync drivers test cannot be performed. Press any key to go back to the smart card diagnostics screen.

Table 17 Error Messages (continued)

Display	Action
STARTUP ERRORS	
DOWNLOAD NEEDED **<error message>**	The following error messages may occur if a defect is found on the *GO variable. *GO is a variable in the CONFIG.SYS file and is the first thing that runs on startup if available. • **NO *GO VARIABLE -** There is no *GO environment variable in the group one CONFIG.SYS file. • ***GO NOT FOUND -** The *GO variable is set but the executable file is missing. • ***GO NOT AUTHENTICATED -** The *GO variable is set but the executable file is not authenticated. • **NOT ENOUGH MEMORY** - The *GO variable is set but there is not enough memory to execute the file. • **INVALID *GO VARIABLE -** This is the defalut error condition. The system could not run the *GO variable eventhough it is set, authenticated, and enough memory is available to execute the file.
FLASH CHKSUM ERROR Gnn	A corrupt file is detected in the F: drive file system during terminal start up, after power on, or during restart. This message may indicate a hardware problem; the error condition may be resolved through another download of the file.
RAM CHKSUM ERROR Gnn	A corrupt file is detected in the I: drive file system at terminal start up, after power-on, or during restart. This message may indicate a hardware problem; the error condition may be resolved through another download of the file.

Table 17 Error Messages (continued)

Display	Action
****VERIFYING FILES**** **COMPARE SIGNATURE** **FILENAME.P7S** **FILENAME.OUT** ***FAILED***	This message appears on screen when the file authentication module fails to authenticate a new signature file. ***FAILED*** appears for five seconds and the terminal beeps three times to draw attention to the filename of the certificate that could not be authenticated. This message remains on screen until all new signature files are checked. New digital certificates are always checked first, followed by new signature files, in an uninterrupted process.
****VERIFYING FILES**** **CHECK CERTIFICATE** **FILENAME.CRT** ***FAILED***	This message appears on screen when the file authentication module fails to authenticate a new digital certificate. ***FAILED*** is displayed for five seconds and the terminal beeps three times to draw attention to the filename of the certificate that could not be authenticated. This message remains on screen until all new certificates are checked, one by one. In special cases where system certificates are being installed, **SYSTEM CERTIFICATE** is displayed instead of **CHECK CERTIFICATE**.

Information Messages

The following information messages may appear when the VX 675 terminal is in terminal manager.

Table 18 Information Messages

Display	Action
DOWNLOADING INFORMATION	
VERIX TERMINAL MGR **UPLOAD** **I:CONFIG.SYS** ******_______** **UPLOADING NOW**	During a back-to-back download session, this screen appears on the Gold terminal indicating that an application is being uploaded to the Target terminal.
VERIX TERMINAL MGR **DOWNLOAD Gnn** ******_______** **DOWNLOADING NOW**	During a back-to-back download session, this screen appears on the Target terminal indicating that an application is being downloaded from the Gold terminal.
VERIX TERMINAL MGR **DOWNLOAD Gnn** **GID: nn** **APP ID: nnnn** **STATUS: DOWNLOADING** *****________**	An application is being downloaded to a *receiving* VX 675 terminal from a host PC. The terminal displays a series of asterisks (*) to indicate the progress of the download (each asterisk represents 10% of the download). When ten asterisks appear, the data transfer is complete.

Table 18 Information Messages

Display	Action
VERIX TERMINAL MGR **DOWNLOAD Gnn** **UNIT RECEIVE MODE** *****________**	An application is being downloaded to a *receiving* VX 675 terminal from a host PC directly over a serial cable. The terminal displays a series of asterisks (*) to indicate the progress of the download (each asterisk represents 10% of the download). When ten asterisks appear, the data transfer is complete.
VERIX TERMINAL MGR **DOWNLOAD Gnn** **UNIT RECEIVE MODE** **WAITING FOR DOWNLOAD**	This screen indicates that the terminal is ready for download and is waiting for a response from the host.

Table 18 Information Messages

Display	Action
ERROR LOG	
VERIX ERROR LOG **TYPE 1** **TASK 2** **TIME 060302201212** **CPSR 40000010** **PC 00000004** **LR 70448B23** **ADDR 27FFFFEF9**	The following information helps developers interpret the cause of the most recent unrecoverable software error that occurred on the terminal: This first screen displays the following: • **TYPE** (error type), where the error type code is: • 1 = Data abort: attempt to access data at an invalid address. • 2 = Program abort: attempt to execute code at an invalid address. • 3 = Undefined abort: attempt to execute an illegal instruction. • **TASK** (task number): indicates type of task that was currently executed: • 1 = Verix Terminal Manager • 2 = First user task • **TIME** (time of crash): clock time of the error in the format *YYMMDDhhmmss*, where *YY* = year, *MM* = month, *DD* = day, *hh* = hour, *mm* = minute, and *ss* = second. • **CPSR** (Current Program Status Register): contains the processor and state condition code. • **PC** (Program Counter): holds the execution address. • **LR** (Link Register): holds the return address of the function call. **Note:** LR may not always contain the current return address. • **ADDR** (fault address): contains the illegal address that the application was trying to access. If you report a system error to Verifone, you may be asked to provide the information displayed on this screen. For detailed information about the error log function and the terms listed above, please refer to the *Verix eVo Volume I: Operating System Programmers Manual* (VPN DOC00301).

Table 18 Information Messages

Display	Action
INTERNAL PIN PAD DIAGNOSTICS INFORMATION	
INTERNAL PIN PAD **MEMORY TEST PASSED** **IPP8 EMUL02A 05/08 01** **SN: 0000000000000000** **BAUD: 1200 RESET 3** **MODE: VISA** **EXIT 4**	After an internal PIN pad diagnostic session, the firmware version and download date, IPP serial number, baud rate, and mode are displayed.
KEYBOARD DIAGNOSTICS INFORMATION	
TERMINAL MGR KBD TEST **KEYCODE nn**	This screen displays the hexadecimal ASCII keycode for each key you press during a keyboard diagnostics session. The value displayed corresponds to the actual key pressed. Other values assigned to keys are software dependent.
MAGNETIC CARD DIAGNOSTICS INFORMATION	
VERIX TERMINAL MGR **TRK 1:VALID** **TRK 2:VALID** **TRK 3:VALID**	When you invoke a local terminal manager diagnostic test of the magnetic stripe card reader, status information appears for the data tracks (TRK1, TRK2, and TRK3) on the card. A successful test displays **VALID DATA** for each track that reads valid data. An error generates one of the following error messages for each track with an error: • **NO DATA** • **NO START** • **NO END** • **LRC ERR** • **PARITY ERR** • **REVERSE END** For more information about magnetic card error messages, refer to the *Verix eVo Volume I: Operating System Programmers Manual* (VPN DOC00301).

Table 18 Information Messages

Display	Action
MEMORY INFORMATION	
MEMORY USAGE **Drive I: Files n** **Inuse nn KB** **Drive F: Files n** **Inuse n** **RAM Avail nnnn KB** **FLASH Avail nnnn KB**	This screen displays how much I: drive and F: drive memory is used and how much is available. - **INUSE -** Closest estimate of used memory (in KB). - **AVAIL -** Lowest number of free memory (in KB).
RAM drive Directory GNN **<filename>** **36 MM/DD/YY -** **<filename>** **36 MM/DD/YY -** **<filename>** **36 MM/DD/YY -** **PRINT**	The following screens display the contents of the I: and F: drives. If there are no files inside an I: drive or an F: drive, **<EMPTY>** is displayed.
FLASH drive Directory GNN **<filename>** **36 MM/DD/YY -** **<filename>** **36 MM/DD/YY -** **<filename>** **36 MM/DD/YY -** **PRINT**	

Table 18 Information Messages

Display	Action
ALL RAM AND FLASH CLEARED	This screen indicates that all I: and F: drive data within a GID is deleted.
ALL RAM AND FLASH CLEAR **COALESCING FLASH**	This screen indicates that all I: and F: drive data within all GIDs is deleted and the memory is being merged.
PASSWORD INFORMATION	
VERIX TERMINAL MGR **PASSWORD CHANGED**	This message confirms that you have successfully changed a GID password or the system password.

Table 18 Information Messages

Display	Action
PRINTER DIAGNOSTICS INFORMATION	
Printer ID P **Version 0PRED1A2** **Status 22** **1> Test** **2> Paper Feed** ↑ ↓	This screen displays the printer ID, firmware version, and the printer status appear. See the *Verix eVo Volume I: Operating System Programmers Manual* (VPN DOC00301). for specifics on application development and the internal thermal printer.
Printer ID P **Version 0PRED1A2** **Status 22** **1> Test** **2> Paper Feed** ↑ ↓	**NO PAPER** is displayed when you select **TEST** and **PAPER FEED** there is no paper installed in the printer.
SMART CARD DIAGNOSTICS INFORMATION	
VoyLib 03.09 0000 **VxOS11 PSCR Build 10** **SCRLIB 2.0 1/12** **1> SMART CARD DIAG** **2> LIST SYNC DRIVERS** **3> EXIT**	This screen displays system and driver information and the number of SAM card slots available.

Table 18 Information Messages

Display	Action
CUSTOMER CARD POWER UP: PASSED GET ATR: PASSED READ TEST: PASSED WRITE TEST: PASSED READ VERIFY TEST: PASS ALL TESTS: PASSED	When a SAM card is tested, the following information is displayed.
STARTUP INFORMATION	
VERIFONE VX675 QT65010M 03/09/2012 Verix COPYRIGHT 1997-2012 VERIFONE ALL RIGHTS RESERVED	At startup, the terminal displays a copyright notice screen that shows the terminal model number, the OS version of the VX 680 stored in the terminal's memory, the date the firmware was loaded into the terminal, and the copyright notice. This screen appears for three seconds, during which time you can enter Verix Terminal Manager by simultaneously pressing **ENTER** and **7**. You can extend the display period of this screen by pressing any key during the initial three seconds. Each keypress extends the display period an additional three seconds.
VERIFONE VX675 QT65010M 03/09/2012 Verix COPYRIGHT 1997-2012 VERIFONE ALL RIGHTS RESERVED	If some other certificate is loaded by a reseller (e.g., bank), the fourth line on the startup screen is left blank.

Table 18 Information Messages

Display	Action
VERIFONE VX675 QT65010M 03/09/2012 Verix **TAMPER** COPYRIGHT 1997-2012 VERIFONE ALL RIGHTS RESERVED	If an attempt to break into the terminal's system has been made, the message ****TAMPER**** is displayed in place of the certificate on the startup screen. The terminal will remain in this state until the condition has been remedied.
VERIFYING FILES COMPARE SIGNATURE FILENAME.P7S FILENAME.OUT *AUTHENTIC*	This message appears on screen when the file authentication module successfully authenticates a new signature file. ***AUTHENTIC*** appears for five seconds and the terminal beeps three times to draw attention to the filename of the certificate that could not be authenticated. This message remains on screen until all new signature files are checked. New digital certificates are always checked first, followed by new signature files, in an uninterrupted process.
VERIFYING FILES CHECK CERTIFICATE FILENAME.CRT *AUTHENTIC*	This message appears on screen when the file authentication module successfully authenticates a new digital certificate. ***AUTHENTIC*** is displayed for five seconds and the terminal beeps three times to draw attention to the filename of the certificate that could not be authenticated. This message remains on screen until all new certificates are checked, one by one. In special cases where system certificates are being installed, **SYSTEM CERTIFICATE** is displayed instead of **CHECK CERTIFICATE**.

Table 18 Information Messages

Display	Action
VTM MGR TERMINAL INFO **Serl No** **PTID 12000000** **Part** **Rev ■■** **OS Ver QT65010M** **Modl** **Ctry** **Keypad ■** **Display 240320** **Mag RDR ■** **Pinpad ■** **Modem Type 0** **Ver: <NO RESP>** **Modem Model: <NO RES**	The following screens show configuration information specific to your terminal: • **SERL NO** - serial number • **PTID** - permanent terminal identification number • **PART** - terminal part number • **REV** - terminal hardware version number • **OS VER** - operating system version • **MODL** - model number • **CTRY** - country of manufacture • **KEYPAD** - keypad type (0 = Telco, 1 = calculator, 2 = Singapore, 6 = EBS100) • **DISPLAY** - display unit type • **MAG RDR** - magnetic stripe card reader type • **PINPAD** - whether or not a PIN Pad device is integrated into the terminal (0 = No, 1 = Yes) • **MDM TYPE** - determines the modem type (0 = none, 4 = 14.4 modem, 22 = modem/ethernet combo) • **VER** - shows the modem firmware patch (B3 = Banshee modem, 05xx = firmware patch version, yy = country profile code, zz = country profile major version) • **MODEM MODEL** • **PRINTER** - shows if a thermal printer is integrated with the terminal (0 = No, 1 = Yes) •
Life -630433889 **Rset** **Rcnt -1485327014** **Tamper Detected N** **Cert** **Heap 0** **Stack 1936**	• **LIFE** - number of seconds the terminal has run • **RSET** - last reset date and time, in YYMMDDHHMMSS format (YY = year, MM = month, DD = day, HH = hour, MM = minute, and SS = second) • **RCNT** - number of times the terminal has been reset either through application control, a terminal manager request, or a power cycle • **TAMPER DETECTED** - indicates whether the terminal has been tampered (N = No, Y = Yes) • **CERT** - shows the first certificate • **HEAP** - displays the memory designation used by the OS • **STACK** - shows the memory set aside for the OS stack. This is where the terminal stores data for running tasks like all the parameters from the call

Troubleshooting Guidelines

The troubleshooting guidelines provided in the following section are included to help you install and configure your VX 675 terminal successfully. Typical examples of malfunction you may encounter while operating your VX 675 terminal and steps you can take to resolve them are listed in this chapter.

If the problem persists even after performing the outlined guidelines or if the problem is not described below, contact your local Verifone representative for assistance.

NOTE The VX 675 terminal comes equipped with tamper-evident labels. The VX 675 unit contains no user serviceable parts. Do not, under any circumstance, attempt to disassemble the terminal. Perform only those adjustments or repairs specified in this guide. For all other services, contact your local Verifone service provider. Service conducted by parties other than authorized Verifone representatives may void any warranty.

CAUTION Use only a Verifone-supplied power pack. Using an incorrectly rated power supply may damage the terminal or cause it not to work as specified. Before troubleshooting, ensure that the power supply being used to power the terminal matches the requirements specified on the bottom of the terminal. (See Specifications, for detailed power supply specifications.) Obtain the appropriately rated power supply before continuing with troubleshooting.

Terminal Does Not Start

- Ensure that the battery charge state is not below the critically low level.
- Recharge or replace the battery.
- Ensure that you pressed the green ENTER/ON key for approximately four seconds, until the unit lights up.

Terminal Display Does Not Show Correct/ Readable Info

- Recharge or replace the battery.
- Connect the VX 675 terminal into a known-good power supply (if you have one) to see if this clears the problem.
- If the problem persists, contact your local Verifone representative for assistance.

Battery Does Not Charge

The VX 675 battery must initially receive a full charge to ensure proper operation.

NOTE

- Allow the VX 675 terminal to remain connected to the power pack for 6 hours to ensure the battery receives a full charge.
- Li-ion batteries are not affected by shallow charging. Furthermore, when the terminal has no external power source or battery the coin cell battery provides power to the security circuit.
- Uninstalling the battery and unplugging the terminal power pack reduce the life of the coin cell battery, which does not recharge and must be replaced if drained.
- Conserve battery power by turning the VX 675 terminal off when not in use. Keep the Li-ion battery inserted in the terminal and power up the terminal periodically to check the battery charge. Do not let the battery charge fall below 10% for extended periods of time as this may permanently diminish the battery capacity. Recharge the battery by attaching USB end of the power pack to the terminal and plugging the other end of the power pack into a wall outlet.
- The VX 675 terminal automatically shuts off when the battery reaches the *critically low* charge state. If this occurs, the battery must recharge a minimum of 1/2 hour before it can power the terminal. *It may take several recharge attempts to reset the safety circuit* when charging a battery that has been discharged below this critical state.

Blank Display

When the VX 675 terminal display screen does not show correct or clearly readable information:

- The battery pack may not be connected properly. Remove and reinstall the battery pack.
- Check terminal power connection.
- Remove and reapply power to the terminal.
- If the problem persists, contact your local Verifone service provider.

Printer Does Not Print

If the printer does not work properly:

- Make sure the battery is properly installed in the terminal. The printer will not print if there is no battery in the terminal.
- Check battery status or terminal power connection. The printer will not print if there is an insufficient charge remaining in the battery to complete the print operation.
- Check if the printer is out of paper (slow red blinking light) and that the roll is properly installed. Open the paper roll cover and install a new roll of printer paper or ensure that the roll is feeding correctly. A solid red indicator light indicates a printer error.

- Verify that the printer door is properly latched.
- If the problem persists, contact your Verifone distributor or service provider.

Printer Paper Jam

If paper jams inside the printer:

- Press the button at the bottom of the terminal to unlatch the paper roll cover, then open the cover.
- Remove the damaged paper from the paper roll and clear the feed mechanism.
- Install a roll of printer paper, as described in Installing the Paper Roll.
- If the problem persists, it may be due to poor paper quality. Install a new roll of higher-quality paper.

WARNING

Poor-quality paper may jam the printer. To order high-quality Verifone paper, refer to Accessories and Documentation.

Keypad Does Not Respond

If the keypad does not respond properly:

- Check the terminal display. If it displays the wrong character or nothing at all when you press a key, follow the steps outlined in Transactions Fail to Process.
- If pressing a function key does not perform the expected action, refer to the user documentation for that application to ensure you are entering data correctly.
- If the problem persists, contact your local Verifone representative.

Transactions Fail to Process

There are several reasons why the terminal may not be processing transactions. Use the following steps to troubleshoot failures.

Check the Magnetic Card Reader

- Perform a test transaction using one or more different magnetic stripe cards to ensure the problem is not a defective card.
- Ensure that you are swiping cards properly. With the VX 675 card reader, the black magnetic stripe on the card should face down and inward, toward the keypad and must be inserted from the top of the terminal (see Figure 20).
- Process a transaction manually, using the keypad instead of the card reader. If the manual transaction works, the problem may be a defective card reader.
- Contact your Verifone distributor or service provider.
- If the manual transaction does not work, proceed to Check the Signal Strength.

Check the Smart Card Reader

- Perform a test transaction using several different smart cards to ensure the problem is not a defective card.
- Ensure that the card is inserted correctly and that the card is not removed prematurely.
- Contact your Verifone distributor or service provider.
- If the manual transaction does not work, proceed to Check the Signal Strength.

Check the Signal Strength

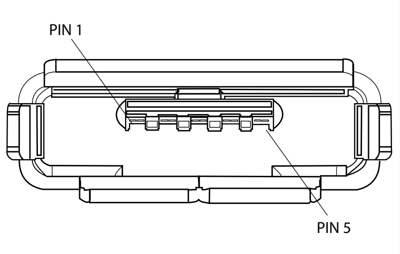
- On-screen signal-strength indicator displays at least one bar to indicate connectivity to radio network.
- Ensure that the radio has been activated by your service provider.

APPENDIX C

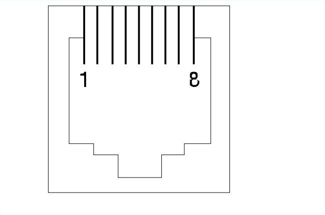
Port Pinouts

The following tables list the pinouts for VX 675 terminal's micro-USB port and VX 675 Full-Feature and USB base's Dial, Ethernet, Serial (RS-232), and USB Host ports.

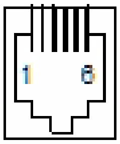
Micro-USB Port

Connector	Pin	Function	Description
	1	USB_PWR	5V DC External Power input for all VX 675 series. **Note:** Support 5V / 300 mAh outputs when VX 675 3G and VX 675 WiFi-BT are operating in USB Host mode.
	2	USB_DN	multi-port, USB Signal - / RS-232 TX
	3	USB_UP	multi-port, USB Signal + / RS-232 RX
	4	NC **Note:** USB_ID in VX 675 3G and VX 675 WiFi-BT.	No connection **Note:** USB_ID is used to signal USB controller for the port function in VX 675 3G and VX 675 WiFi-BT.
	5	EXTGND	External Ground

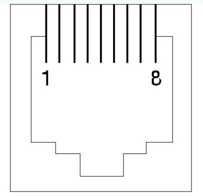
RS-232 Port (FFB only)

Connector	PIN	Function	Description
	1	Power	5V power 300 mAh Max.
	2	NC	No connection
	3	NC	No connection
	4	GND	Power ground
	5	/RXD	Receive data
	6	/TXD	Transmit data
	7	CTS	Clear to send
	8	RTS	Request to send

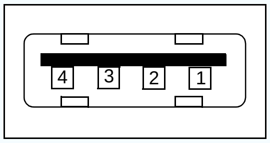
Telco Port (FFB only)

Connector	PIN	Function	Description
 LOOKING INTO MOD 6P4C	1	NC	No connection
	2	NC	No connection
	3	Tip	Telephone line
	4	Ring	Telephone line
	5	NC	No connection
	6	NC	No connection

Ethernet Port (FFB only)

Connector	PIN	Function	Description
	1	TXD+	Transmit data +
	2	TXD-	Transmit data -
	3	RXD+	Receive data +
	4	TCT	Center tap for the transformer
	5	RCT	Center tap for the transformer
	6	RXD-	Receive data -
	7	NC	No connection
	8	NC	No connection

USB Host Port (FFB and USB base)

Connector	PIN	Function	Description
	1	USB_5V_EXT	5V USB Power (300 mAh)
	2	nUSB_DEVICE	USB Device Signal -
	3	pUSB_DEVICE	USB Device Signal +
	4	GND	USB Ground

APPENDIX D

ASCII Table

The ASCII Table

An ASCII table for the VX 675 display is presented in Table 19.

Table 19 VX 680 Display ASCII Table

Dec	Hex	ASCII	Dec	Hex	ASCII	Dec	Hex	ASCII	Dec	Hex	ASCII
0	00	NUL	32	20	SP	64	40	@	96	60	'
1	01	SOH	33	21	!	65	41	A	97	61	a
2	02	STX	34	22	"	66	42	B	98	62	b
3	03	ETX	35	23	#	67	43	C	99	63	c
4	04	EOT	36	24	$	68	44	D	100	64	d
5	05	ENQ	37	25	%	69	45	E	101	65	e
6	06	ACK	38	26	&	70	46	F	102	66	f
7	07	BEL	39	27	'	71	47	G	103	67	g
8	08	BS	40	28	(	72	48	H	104	68	h
9	09	HT	41	29	)	73	49	I	105	69	i
10	0A	LF	42	2A	*	74	4A	J	106	6A	j
11	0B	VT	43	2B	+	75	4B	K	107	6B	k
12	0C	FF	44	2C	,	76	4C	L	108	6C	l
13	0D	CR	45	2D	-	77	4D	M	109	6D	m
14	0E	SO	46	2E	.	78	4E	N	110	6E	n
15	0F	SI	47	2F	/	79	4F	O	111	6F	o
16	10	DLE	48	30	0	80	50	P	112	70	p
17	11	DC1	49	31	1	81	51	Q	113	71	q
18	12	DC2	50	32	2	82	52	R	114	72	r
19	13	DC3	51	33	3	83	53	S	115	73	s
20	14	DC4	52	34	4	84	54	T	116	74	t
21	15	NAK	53	35	5	85	55	U	117	75	u
22	16	SYN	54	36	6	86	56	V	118	76	v
23	17	ETB	55	37	7	87	57	W	119	77	w
24	18	CAN	56	38	8	88	58	X	120	78	x
25	19	EM	57	39	9	89	59	Y	121	79	y
26	1A	SUB	58	3A	:	90	5A	Z	122	7A	z
27	1B	ESC	59	3B	;	91	5B	[	123	7B	{
28	1C	FS	60	3C	<	92	5C	\	124	7C	|
29	1D	GS	61	3D	=	93	5D	]	125	7D	}
30	1E	RS	62	3E	>	94	5E	^	126	7E	~
31	1F	US	63	3F	?	95	5F	_	127	7F	DEL

APPENDIX E

VX 675 Battery Information

Battery

The VX 675 terminal uses a Lithium-ion battery. The internal logic of the battery prevents both overcharging and undercharging (a fault condition in which the battery level goes well below the minimum acceptable charge and the battery becomes unusable).

NOTE The VX 675 terminal will operate on battery power or on power pack power. The battery charger in the terminal will be active whenever the power pack is connected.

The VX 675 comes with a high-capacity battery pack.

Charging

The battery has a safety circuit to protect the Lithium-ion cells from overcharging and over-discharging. If the battery is over-discharged, the safety circuit shuts down the battery. The battery must then be recharged to restore operation.

NOTE The VX 675 terminal automatically shuts off when the battery reaches the critically low charge state. If this occurs, the battery must be recharged for a minimum of 1/2 hour before it can power the terminal. It may take several recharge attempts to reset the safety circuit that has been discharged below this critical state.

Battery Life

The VX 675 battery can be charged and discharged hundreds of times, but will eventually wear out. When operating times are noticeably shorter than usual, it is time to order a new battery.

WARNING Do not dispose of batteries in a fire. Lithium-ion batteries must be recycled or disposed of properly. Do not dispose of Lithium-ion batteries in municipal waste sites.

Advantages

Lithium-ion batteries have numerous advantages over other types of rechargeable batteries.

High energy density

Lithium-ion batteries typically have twice the energy density of standard nickel-cadmium batteries. This means that for their size or weight they can store more energy than other rechargeable batteries.

Light weight

Lithium is the lightest metal. Thus, lithium-ion batteries enable the manufacture of lightweight devices.

Long Life

Lithium-ion batteries require low maintenance. They do not exhibit memory effects, thereby eliminating the need for scheduled cycling to prolong the battery life.

Does Not Require Prolonged Initial Charging

Unlike their nickel-cadmium counterparts, lithium-ion batteries do not require prolonged initial charging. All that is needed is a regular charge.

Low Self-Discharge Rate

Lithium-ion batteries have a lower self-discharge rate compared to other types of battery (the self-discharge rate for a lithium-ion battery is less than one-half of that of a nickel-cadmium battery). This means that once they are charged, they will retain their charge for a longer time than other types of rechargeable batteries. Other battery types can lose anywhere from 1-5% of their charge per day, (depending on the storage temperature) even if they are not installed in a terminal. Lithium-ion batteries will retain most of their charge even after months of storage.

High Voltage Capacity

Lithium-ion batteries operate at higher voltages than other rechargeable batteries, typically about 3.6 V for lithium-ion versus 1.2 V for nickel-metal-hydride or nickel-cadmium batteries. This means a single cell can often be used rather than multiple metal-hydride or nickel-cadmium cells.

Precautions

Observe the following precautions when handling lithium-ion batteries.

Aging Effects

Battery packs are subject to aging, even when they are not used.

- Aging leads to deterioration in capacity or battery life.

TIP

Storing the battery in a cool environment (25 °C or less) at 40% charge reduces the effects of aging.

- Batteries typically fail after two or three years, or approximately 300 charge-discharge cycles.
- Other chemicals may also affect the aging properties of batteries.

Transportation Restrictions

- It is illegal to ship fully charge batteries by air because they may cause accidental explosions.
- Shipment of large quantities of lithium-ion batteries may be subject to regulatory control.

NOTE

These precautions do not apply to personal carry-on battery packs.

Storage Precautions

- Do not fully charge batteries before storage. Instead, keep the batteries partially charge before storing them, then charge them fully before actual usage.
- Do not store batteries when they are fully depleted. If a battery is empty, charge it for at least one hour before storage. When a depleted battery self discharges, it may become unusable.
- Do not stock pile batteries. Avoid buying dated battery stocks even at reduced prices. In addition, always check the date when the batteries were manufactured.

Notable VX 675 Battery Specifications

The battery is designed to offer optimum protection to the VX 675 terminals and their users.

Safety/Protection Circuit

The battery features a safety/protection circuit that provides the following benefits:

- Limits the peak voltage in each cell during charging – a field effect transistor (FET) opens if voltage level in any cell reaches 4.28 V.
- Prevents cell voltage from dropping too low during discharge – a field effect transistor (FET) opens if voltage in any cell reaches 2.3 V.
- Limits the current going in and coming out of the battery pack. A field effect transistor (FET) opens the current path when charge current exceeds 6.5 A or when the discharge current exceeds 7 A. This prevents damage caused by shorting the battery contacts.

Cell Temperature Monitoring

A discrete thermistor is built into the battery pack to prevent cell or terminal damage during charging. The terminal’s OS monitors the cell temperature using the thermistor and automatically shuts down the charger if the temperature exceeds 50 °C or falls below 0 °C.

ESD Protection

Electrostatic Discharge (ESD) protection: ±8 KV air discharge, ±4 KV contact discharge

Trip Recovery

The VX 675 battery features a trip recovery system, which resolves faulty or hazardous conditions that led to a safety trip. Application of current through the charger will reset the safety circuit.

Battery FAQs (for VX 675)

Should I allow the battery to discharge completely before charging?

No. It is better to recharge the battery often and avoid frequent full discharge. However, allow a full discharge once a month to enable reset.

Should I charge the battery partially or fully?

It does not matter whether you charge the battery fully or partially. Charging a full battery will not harm the battery.

Should I charge the battery before putting it into storage?

It is advisable to store the battery with a 40% charge. However, storing the battery in a cool place is more important than the state of charge. In addition, make sure that the battery is not fully depleted before putting it in storage. Otherwise, the safety/protection circuit may trip.

Will the battery heat up during charging?

It is normal for the battery to emit a small amount of heat during charging. The battery is equipped with a temperature sensor that will disrupt the flow of charge current when extreme temperature levels are detected.

NOTE

The recommended operating temperature for the VX 675 is from 0 °C to 50 °C (32 °F to 122 °F).

VX 675 Battery Specific Terms and Definitions

The following terms and definitions apply to the VX 675 terminal's battery.

Percent of Charge (%)

The ratio of the RC (remaining charge) value to the FC (full charge = 2250 mAh) value multiplied by 100%. The range is from 0 to 100.

The Percent of Change value is available to terminal applications via OS calls. It is updated every 20 seconds.

Remaining Charge (RC)

The amount of usable energy in the battery at a given time in mAh. The OS writes RC=FC at the end of charge. The range is from 0 to FC.

The RC value is available to terminal applications via OS calls. It is updated every 20 seconds.

Safety/Protection Circuit

The VX 675 terminal is equipped with a safety/protection circuit that protects the terminal from damage. For more information, see Safety/Protection Circuit.

Voltage

Under system load, the VX 675 terminal reports battery pack voltage. The range is from 3 V to 4.2 V. It is updated every 20 seconds.

General Battery Terms and Definitions

The following terms and definitions apply to most battery types, in general.

Ampere-hour, Amp-hour (Ah)

A unit of electrical energy. It is the specified current flowing for one hour. Two ampere-hour is two amps of current flowing for one hour.

Battery Cell

The battery cell is the basic electrochemical unit used to store energy. Each cell is typically rated 3.7 V (3.6 V for VX 675 GPRS). VX 675 terminal uses one lithium-ion rechargeable cell per battery pack.

Battery Pack

A battery pack is an assembly of battery cells, safety circuit, temperature sensor, terminal contacts, and plastic case.

Battery Status, State of Charge

This refers to the amount of electrical charge stored in the battery, expressed as a percentage of the difference between the fully-charged and fully-discharged states.

Capacity

This refers to the amount of available energy in a fully charged battery, expressed in ampere-hours (Ah) or milliampere hours (mAh).

TIP

The capacity of VX 675 terminal's high capacity battery pack is 2450 mAh typical (new).

Charge

The amount of usable electrical energy stored in the battery, expressed in coulombs.

Charge Rate

This refers to the amount of current applied to the battery during charging.

NOTE

Charge rate for the VX 675 terminal's battery: Initially 0.7 A tapering to zero at end of charge.

Charge Time

The amount of time required to charge a battery. Maximum charge time refers to the amount of time to fully charge a fully discharged battery.

NOTE

Typical charge time for the VX 675 terminal’s battery: 2450 mAh in approximately 4.33 hours.

Charging

Refers to the process of converting electrical energy, in the form of electric current, from an external source (charger) into chemical energy within a battery cell.

Current

The flow of electrons through a conductor, measured in amperes

Cycle Life

This refers to the number of charge/discharge cycles the battery can endure before it loses its ability to store useful charge.

NOTE

The VX 675 terminal’s battery pack will retain approximately 75% of its original charge after 300 cycles.

Dead Battery

A battery is considered “dead” when it deep discharges to the point that it can no longer accept a charge or when it has reached the end of its cycle life.

Deep Discharge

The state of a battery that has been discharged well below its useful charge level. When a battery is in this state, it may be difficult to recharge. This characteristic typically indicates a reduced cycle life.

Discharge Time, Run Time

This refers to the amount of time a battery can provide power to a system before it discharges fully. It is a function of the load that receives power from the battery.

Discharging

Refers to the process of converting the chemical energy of a battery into electrical energy, and the transfer of the electrical energy into a load.

Self-Discharge Rate

The amount by which the charge of the battery is reduced without providing any current to an external terminal or load.

Shelf-Life

The length of storage under specified conditions that a battery can endure while retaining the ability to give a satisfactory performance upon full charge.

NOTE

The shelf life of the VX 675 battery pack is six months at 30% initial charge.

Voltage

This is the unit of potential power or electric pressure, which is the force that causes current to flow through an electric conductor. It is measured in volts.

GLOSSARY

Application ID An alphanumeric code that identifies an application program downloaded to a terminal from a download computer. For ZonTalk 2000 application downloads, the application ID is stored in the `CONFIG.SYS` record which begins with the *ZA key. A VX 675 application ID can be up to 21 characters long. For VeriCentre Download Management Module, the application ID, as well as other `CONFIG.SYS` variables, may differ from those used for ZonTalk 2000.

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

Application prompt The information shown on the terminal's display panel when power is applied to the terminal, assuming that an application program has already been downloaded into the terminal's memory and authenticated by the file authentication module. The application prompt often contains a graphical logo, and date and time, but it can consist of anything the programmer chooses for that purpose.

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 contents of one terminal's application memory to another terminal's application memory. A terminal-to-terminal application upload require that the sending and receiving terminal be connected to each other by a serial cable. The same operation as a *terminal-to-terminal* application upload."

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 micro-USB port.

Bit Short for *binary digit*. Either of the two digits 0 and 1 in the binary number system. Also, a unit of information equal to one binary decision. The bit is the smallest unit of storage and hence of 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) that are stored in adjacent physical positions in memory or on a peripheral storage terminal. A block can therefore be 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 non-volatile memory, 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 memory area 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 VX 675 service dongle a byte consists of eight bits. See also Bit.

Calendar/clock chip A real-time clock inside the VX 675 terminal which keeps track of the current date and time.

Card reader Also called *magnetic stripe card reader*. The slot on the right side of the VX 675 terminal that automatically reads 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. A carrier signal transmits data from a host computer to a VX 675 terminal through a service dongle.

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 file A special keyed file that is stored in terminal memory and which contains system and application configuration parameters. Each record in a `CONFIG.SYS` file is identified by an alphanumeric search key. In the VX 675 file system, there is one password-protected `CONFIG.SYS` file per file group (Groups 1–15). You can modify `CONFIG.SYS` records using the keyed file editor. See Keyed file 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. Data is to be distinguished from applications or program instructions. In the VX 675 terminal, application files and data files can be stored in memory.

Data entry The process of using a keyboard, card reader, or other terminal 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.

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.

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 terminal.

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 remote, system environment.

Display The backlit LCD screen on the VX 675 terminal that shows numerals, letters, and punctuation symbols in selected fonts, graphics in various formats, information entered from the keypad, as well as system prompts and messages.

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

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 memory.

Fixed prompt A system prompt or message stored as part of system firmware in terminal memory. Fixed prompts appear on the terminal display to alert the user to specific system occurrences or malfunctions, and to prompt the user to enter specific information or select options.

Flash memory An area of non-volatile memory where files can be stored. Files can be stored in drive `I:` or in drive `F:` memory area of any file group (Groups 1–15).

Host computer Also called a *download* computer. The primary or controlling computer in a multiple computer operation. Also, a computer—usually a PC running Windows XP, Windows 2000, Windows NT or Windows 95 or 98—used to prepare programs for download to POS terminals. Host computers are also used to process transactions that originate from a distributed network of POS terminals.

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

Interface A common boundary between two systems, devices, or programs. Also, to interact with a terminal.

Keyed file character set A limited set of 96 ASCII characters, from 00h to 5Fh (or 0 to 95 decimal), that is used by the VX 675 keyed file editor. Although an application program can download all 95 characters in this set, you can only enter 50 of these characters from the terminal keypad: 0–9, A–Z, and 14 special characters.

Keyed file editor A keyed file editor lets you create new records or modify existing records stored in a keyed file such as `CONFIG.SYS`. See CONFIG.SYS file.

Keyed file record ASCII data, or variables, stored in the terminal's `CONFIG.SYS` file(s). A keyed file record consist 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 VX 675 terminal is used to enter data and perform operations.

Local functions Operations performed at the terminal only and not in interaction with a host computer. For the VX 675, local functions such as internal diagnostics are performed in Verix Terminal Manager. See Chapter 4.

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 terminal, such as a magnetic stripe card reader.

Memory A terminal 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 VX 675, files are stored 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.

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. For the VX 675, application files and data files are stored in non-volatile flash memory.

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 also Verix Terminal Manager.

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 the Verix Terminal Manager is called the *system mode password*. In the VX 675 file system, each file group (Groups 1–15) also has its own password.

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

Peripheral terminal In a computer system, any equipment that provides the processing unit with outside communication. Typical peripheral devices for a POS terminal include PINpads and check readers.

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 microprocessor.

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 input 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 Verifone terminal at the factory, upon customer request. The PTID is an eight digit number, consisting of a two digit manufacturer's ID (12 for Verifone), followed by a six digit terminal ID. If no PTID is assigned to the unit then, the default value 12000000 is used.

RAM *Random-access memory*. The type of memory in which storage locations are addressable and can therefore be accessed in any order. In the VX 675 terminal, the mDRAM is used to run applications.

Application files and data are stored in the non-volatile flash memory system. By default, files downloaded to the terminal are stored in the I: drive of the target file group(s). See Flash memory.

Remote host computer A host computer connected to a VX 675 service dongle to download files or data, or to process transactions. The opposite of remote is *local*.

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 VX 675, 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 VX 675, a short character string used by an application to identify a keyed file record stored in `CONFIG.SYS` file(s). For example, *ZA or *OT. A *keyed file record* consist of two parts: a search key to identify the record, and the variable data stored in the record. See also Keyed file record and CONFIG.SYS file.

Serial port A connection point through which digital information is transferred one digital bit at a time. Same as *serial interface*. The VX 675 terminal has one serial port, available at the multiport connector. The main serial port on a download computer is usually assigned the terminal ID, 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.

mDRAM See RAM.

Subroutine A software routine that can be part of another routine. When a main routine calls a subroutine, program control is transferred to the subroutine. 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 VX 675 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.

Verix Terminal Manager For the VX 675, Verix Terminal Manager 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 VX 675 system firmware stored in terminal memory, the date it was loaded into the terminal, and the copyright notice. This screen appears for three seconds. To enter Verix Terminal Manager, simultaneously press the ENTER and 7keys during this three-second period. Pressing any other key(s) during that period resets the copyright notice screen to display an additional three seconds.

Verix Terminal Manager password A unique set of characters entered by the user to access the Verix Terminal Manager local functions of the terminal. A default password is supplied with each terminal. For the VX 675 terminal, the default system password set at manufacture is: 166831.

To prevent unauthorized access, change the default password upon 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.

Terminal Any terminal capable of sending and receiving data over a data link, such as a RS-232 cable. Some terminals, such as the VX 675, 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. For ZonTalk 2000 downloads, the VX 675 terminal ID is stored in the *ZT record in the `CONFIG.SYS` file. This variable should not exceed 10 characters in length. Not the same as PTID

Terminal-to-terminal application upload The process of copying the application memory contents of one terminal to the application memory of another terminal. A terminal-to-terminal application upload requires that the terminals be connected to each other by a serial cable. See also Back-to-back application download.

Track 1, 2, or 3 data Information stored on tracks 1, 2, or 3 of a debit or credit card magnetic stripe, which can be read by a magnetic card reader terminal, such as the one that is integrated in the VX 675 terminal.

Transaction An exchange of data resulting in a transfer of goods, services, value, and/or information between two parties.

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. In the VX 675 applications run from volatile memory, mDRAM. Compare with Non-volatile memory.

INDEX

Verifone, Inc.
2099 Gateway Place, Suite 600
San Jose, CA, 95110 USA
1-800-VERIFONE
www.verifone.com

VX 675

Reference Guide

Verifone Part Number DOC265-004-EN-G, Revision G