

V^x810

Reference Guide



Vx810 Reference Guide
© 2008 VeriFone, Inc.

All rights reserved. No part of the contents of this document may be reproduced or transmitted in any form without the written permission of VeriFone, Inc.

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."

VeriFone, the VeriFone logo, Omni, VeriCentre, Verix, and ZonTalk are registered trademarks of VeriFone. Other brand names or trademarks associated with VeriFone's products and services are trademarks of VeriFone, Inc.

All other brand names and trademarks appearing in this manual are the property of their respective holders.

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

www.verifone.com

VeriFone Part Number 24964, Revision A



CONTENTS

	PREFACE	7
	Audience	7
	Organization	7
	Related Documentation	8
	Conventions and Acronyms	8
	Conventions	8
	Acronyms	9
CHAPTER 1		
V^x810 Overview	Features and Benefits	12
CHAPTER 2		
Using the V^x810 Keys	Data Entry Modes	16
	Entering Normal Mode	16
	Entering System Mode With No Application Loaded	16
	Entering System Mode While in Normal Mode	16
	Re-entering Normal Mode From System Mode	16
	Main Keypad	17
	ALPHA Key	17
	Command Keys	19
	Programmable Function (PF) Keys	19
	Sound	20
CHAPTER 3		
Setup	Selecting Location	21
	Ease of Use	21
	Environmental Factors	21
	Electrical Considerations	22
	Unpacking the Shipping Carton	22
	Examining the V ^x 810 Features	23
	Installing/Replacing MSAM Cards	24
	Options	26
	Privacy Shield	26
	Cable Connections	26
	Other VFI Devices	26
	RS-232 Connection with External Power Brick	27
	Standard USB Connection	27
	USB Download Support with External Power Brick	28
	Powered USB	28
	Ethernet Connection with External Power Brick	29
	Power Supply	29
	Using the Primary Smart Card Reader	30
	Using the Magnetic Stripe Card Reader	30

CHAPTER 4 System Mode

When to Use System Mode	31
Local and Remote Operations	32
Verifying Device Status	32
Entering System Mode	32
File Groups	33
Passwords	33
System Mode Password	34
File Group Passwords	34
Password Maintenance	34
System Mode Menus	37
System Mode Procedures	37
Entering System Mode	39
Menu 1	41
Menu 2	44
Menu 3	60

CHAPTER 5 File Authentication

Introduction to File Authentication	63
The VeriFone Certificate Authority	63
Special Files Used in the File Authentication Process	64
How File Authentication Works	66
Planning for File Authentication	70
Digital Certificates and the File Authentication Process	72
File Authentication and the File System	77
VeriShield File Signing Tool	81
System Requirements	81
Operating Modes	81
Command-Line Entries	82
Command-Line Mode Syntax Example	84
Graphical Interface Mode	84

CHAPTER 6 Performing Downloads

Downloads and Uploads	87
Download Methods	87
Download Tools	88
Download Content	89
Full and Partial Downloads	90
Support for Multiple Applications	92
How the File System Supports Multiple Applications	92
The Main Application is Always Stored in GID1	93
Physical and Logical Access to File Groups	93
Use of SRAM and Flash ROM Memory	93
Defragment Flash ROM for Application Downloads	94
Redirection of Files During Application Downloads	94
Manually Redirecting Files	94
Redirecting Files to Other File Groups	96
Restrictions on File Redirection	96
Using DDL.EXE to Automatically Redirect Files	97
File Redirection in Operating System Downloads	98
File Redirection in Back-to-Back Application Downloads	98

File Authentication Requirements	99
Required Certificates and Signature Files	99
The File Authentication Process During an Application Download	100
File Group Permissions	102
Download an Operating System Update Provided by VeriFone	103
File Authentication for Back-to-Back Application Downloads	104
Timing Considerations Due to the Authentication Process	105
Optimize Available Memory Space for Successful Downloads	106
Support for File Compression	106
Effect of Downloads on Existing Files and Data	106
Set Up the Download Environment	107
Cable Connection for Direct Downloads	108
Cable Connection for Back-to-Back Application Downloads	108
Direct Application Downloads	109
Hardware Checklist	109
Software Checklist	109
Checklist for Effects on Files and Settings in the Receiving Device	110
Direct Application Download Procedure	110
Direct Operating System Downloads	115
Hardware Checklist	115
Software Checklist	115
Checklist for Effects on Files and Settings in the Receiving Device	115
Direct Operating System Download Procedure	116
Back-to-Back Application Downloads	120
Hardware Checklist	120
Software Checklist	120
Checklist for Effects on Files and Settings in the Receiving Device	120
Back-to-Back Application Download Procedure	121
CHAPTER 7	
Specifications	
Product Specifications	127
Model	127
Processor	127
Flash ROM	127
SRAM	127
Operating System	127
Display	127
Magnetic Card Reader	127
Primary Smart Card Reader	127
SAM Card Reader	127
Input Device	127
Peripheral Ports	127
Supported Memory Media	128
Security	128
Audio Output	128
Physical	128
Voltage	128
Environmental, Regulatory and Performance Specifications	128
Temperature and Humidity	128
Compliance Certifications	128

CHAPTER 8	
Care and Maintenance	
	Additional Safety Information 132
	Power Adapter 132
	Potentially Explosive Environments 132
CHAPTER 9	
Service and Support	
	Product Returns 133
	Accessories and Documentation 135
	Power Pack 135
	Connectivity Cables 135
	Privacy Shield 135
	Integrated Base Station 135
	VeriFone Cleaning Kit 135
	Documentation 135
CHAPTER 10	
Troubleshooting Guidelines	
	Display Does Not Show Correct/Readable Info 137
	Blank Display 137
	Device Does Not Dial Out 138
	Keypad Does Not Respond 138
	Transactions Fail To Process 138
APPENDIX A	
System Messages	
	Error Messages 139
	Information Messages 140
APPENDIX B	
Port Pinouts	
	Multi-Port 145
	COM Port 145
APPENDIX C	
ASCII Table	
	GLOSSARY 149
	INDEX 155



This guide is your primary source of information for setting up and installing the Vx810.

Audience

This document has two primary audiences, but is useful for anyone installing and configuring the Vx810:

- **Deployment Administrators** who prepare multiple devices for deployment to customers, configuring the devices with applications, network configurations, phone numbers, and security. Deployment Administrators may work for a bank, credit card service company, or any company with a vertical application for the Vx810.
- **Local Administrators** integrate and maintain Vx810 devices into a single business site. Business owners or store managers generally perform this function.

Organization

This guide is organized as follows:

[Chapter 1, Vx810 Overview](#). Provides an overview of the Vx810.

[Chapter 2, Using the Vx810 Keys](#). Explains the operational features of the Vx810 and describes how to use the Vx810 keys to perform all the data entry or system mode tasks described in this manual.

[Chapter 3, Setup](#). Explains how to set up and install the Vx810. It tells you how to select a location, establish power and telephone line connections, and how to configure optional peripheral devices.

[Chapter 4, System Mode](#). Describes password-controlled, system-mode 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, the VeriShield File Signing Tool, to generate signature files.

[Chapter 6, Performing Downloads](#). Documents procedures for downloading applications and files to the Vx810.

[Chapter 7, Specifications](#). Discusses the power requirements and dimensions of the Vx810.

[Chapter 8, Care and Maintenance](#). Explains how to maintain the Vx810.

[Chapter 9, 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.

[Chapter 10, Troubleshooting Guidelines](#). Provides troubleshooting guidelines, should you encounter a problem in installation and configuration.

This guide also contains appendices for [System Messages](#), [Port Pinouts](#), [ASCII Table](#), and a [Glossary](#).

Related Documentation

To learn more about the V^x810, refer to the following set of documents:

V ^x 810 Certifications and Regulations Sheet	VPN 24960
V ^x 810 Quick Installation Guide	VPN 24961
V ^x 810 Installation Guide	VPN 24963
V ^x 810 Privacy Shield Quick Installation Guide	VPN 24965
Verix V Operating System Programmers Manual	VPN 23230
Verix V Tools Programmers Manual	VPN 23231




Conventions and Acronyms

This section describes conventions and acronyms used in this guide.

Conventions

The following table describes the conventions used in this guide to help you quickly identify special formatting.

Table 1 Document Conventions

Convention	Meaning	Example
Blue	Text in blue indicates terms that are cross references.	See Conventions and Acronyms .
<i>Italics</i>	Italic typeface indicates book titles or emphasis.	Operating system files <i>must</i> always be downloaded onto Group 1.
NOTE 	The pencil icon is used to highlight important information.	VeriFone ships variants of the this device for different markets. Your device may have a different configuration.
CAUTION 	The caution symbol indicates hardware or software failure, or loss of data.	The device 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 device near water.

Acronyms The following table lists various acronyms used throughout this guide in place of the full definition.

Table 2 Acronyms

Acronym	Definitions
3DES	Triple Data Encryption Standard
ARM	Advanced RISC Machines
CTS	Clear to Send
ECR	Electronic Cash Register
EMV	Joint Europay, MasterCard and Visa Standard
GID	Group Identifier
ICC	Integrated Chip Card (Smart Card)
LCD	Liquid Crystal Display
MSAM	Micromodule-size Security Access Module
MSR	Magnetic Stripe Reader
OS	Operating System
PED	PIN Entry Device
PIN	Personal Identification Number
POS	Point-of-Sale
PSCR	Primary Smart Card Reader
RFID	Radio Frequency Identification
RTS	Ready to Send
SAM	Security Access Module
SC	Smart Card (Integrated Chip Card)
SD	Secure Digital
SDK	Software Development Kit
SSL	Secure Sockets Layer
SRAM	Static Random Access Memory
USB	Universal Serial Bus

V^x810 Overview

This chapter provides a brief description of the V^x810. The V^x810 is a customer-facing premium PIN pad brought about by VeriFone's innovative Purpose Inspired Design program which focuses on real-world usage.

Apart from its sleek, compact, and functional design, the V^x810 features a triple-track, high coercivity magnetic stripe reader (MSR) and a Smart Card reader, both built and proven to perform consistently, even under the heaviest volumes. It also has a Secure Digital Input Output (SDIO) expansion port that allows you to upgrade the device to support contactless payments.

The V^x810 also offers an array of connectivity options all from a single port (including serial, USB, or optional Ethernet) so you can connect to almost any device or ECR. Plus, the V^x810 gives you the option to add a base unit with a printer and modem to create a fully-loaded payment solution with a hand-over PIN pad – all in one single device.



Figure 1 **The V^x810**



VeriFone ships variants of the V^x810 for different markets. Your device may have a different configuration. For example, the V^x810 may or may not have a PSCR; it may or may not have an MSR; it may have none or 3 SAMs; flash ROM size may be from 4MB, to 8MB or 16MB; and SRAM size may be from 2MB to 4MB. However, the basic processes described in this guide remain the same, regardless of configuration.

Features and Benefits

Acclaimed Vx Solutions Reliability and Security Guarantees Extra Protection

- Runs on Verix-based platform, proven in millions of VeriFone V^x Solutions installed worldwide.
- Has exceptionally reliable magnetic stripe and smart card readers to reduce read errors.
- Is PCI-PED approved for secure, reliable PIN entry on debit transactions.
- Has received EMV Level 1 and 2 Type Approval for smart card transactions.
- Provides end-to-end SSL security and supports the latest security options – including 3DES encryption, and Master/Session and DUKPT (Derived Unique Key Per Transaction) key management.
- Relies on VeriShield file authentication to help stop fraud and misuse, such as downloading rogue files or physical tampering.
- Hardware and software application separation minimizes or eliminates the need to re-certify existing payment applications every time an application is added or modified.

Flexibility and Future-Proofing Can Put You Years Ahead to Safeguard Your Investment

- Includes an SDIO expansion port to simplify upgrades to contactless or other emerging technologies – without replacing the PIN pad.
- Provides for a wide range of connectivity via a single connector – including RS-232, USB, and optional Ethernet – to accommodate nearly any ECR and fit most merchant needs.
- Offers the option of adding a base unit with a printer and modem that transforms the PIN pad into an all-in-one payment solution.
- Extensive memory (6 MB standard, 12 MB or 20 MB optional) to support multiple applications, including revenue-producing value-added solutions.
- Uses a 200 MHz, 32-bit, ARM 9 processor for trouble-free multitasking.

Ultra Sleek PIN Pad Puts Everything at Your Customer's Fingertips

- Ergonomic shape and silver casing holds high consumer appeal.
- Offers 128 x 128, high-resolution display with white backlighting for enhanced readability and branding opportunities.
- MAXui design provides a large keypad and screen without wasted space.
- Programmable function keys and on-screen prompts add to the V^x810's outstanding usability.
- Works well as either a handheld or a counter/poll-mounted device, offering flexibility in placement.

Using the V^x810 Keys

Before proceeding to other tasks, familiarize yourself with the operational features of the V^x810 keypad.

This section describes how to use the V^x810 keypad, which consists of four ATM-style function keys (F1 to F4), four programmable function keys (PF1 to PF4), an ALPHA key, a 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 through the system mode menus and select specific operations.

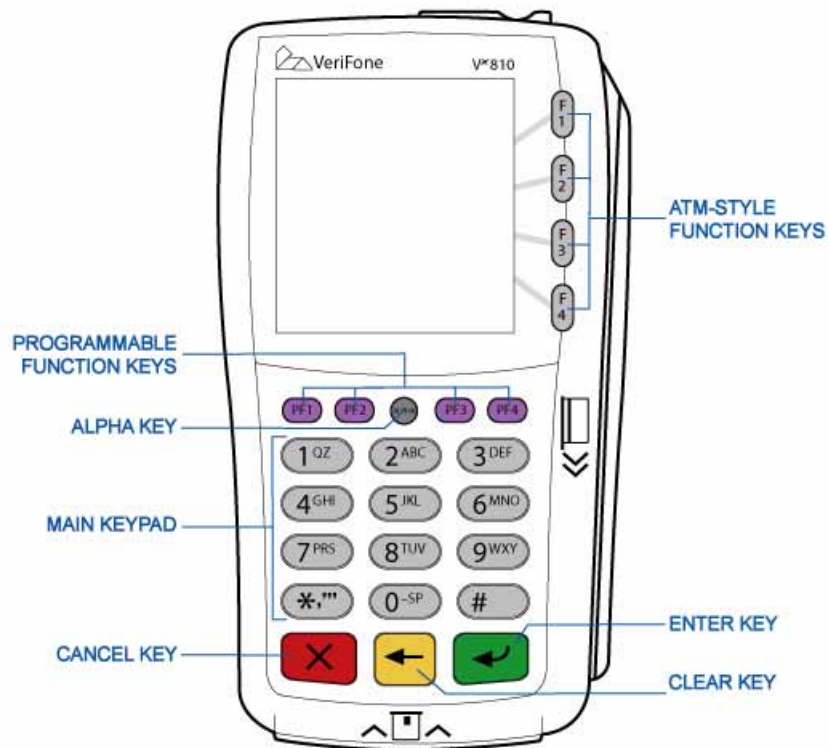


Figure 2 The V^x810 Keys.

Data Entry Modes

Before you can enter data in the form of ASCII characters, the V^x810 must be in a mode that accepts keyed data entry. There are two operating modes:

- **Normal mode:** This is the operating mode where an application is present and currently running.
- **System mode:** This is a special, password-controlled operating mode for performing a variety of test and configuration procedures that cannot be performed when an application is running.

Entering Normal Mode

If you turn on a V^x810 with an application stored in system memory, the application executes and the device automatically enters normal mode. The application controls how the keys process transactions and when you can use specific keys to type characters or respond to prompts.

Entering System Mode With No Application Loaded

If you turn on a V^x810 that does not have an application stored in system memory, the system prompt **DOWNLOAD NEEDED** appears. You can enter system mode by simultaneously pressing **F2** and **F4**, and entering the password. Once in system mode, you can configure the device as required or perform downloads.

NOTE

Alternatively, a second method for entering system mode is available – by simultaneously pressing the **7** and **ENTER** keys and then entering the password. But for simplification in this manual, only the first method, simultaneously pressing **F2** and **F4** and entering the password, is mentioned from this point on.

Some application downloads can automatically reset the system mode password. If your system mode password no longer works, check if an application download has changed your password.

To know more about system mode operations, see [System Mode](#).

Entering System Mode While in Normal Mode

If you enter system mode while in normal mode, the active application is preempted and system mode takes control of the display and keypad.

Re-entering Normal Mode From System Mode

The only way to re-enter normal mode from system mode is to restart the device. For this reason, once you enter system mode, you cannot return to the previously active application in the same session.

Main Keypad The main keypad consists of the keys 0 to 9, *, and #. You can enter up to 50 ASCII characters, including the letters A–Z, the numerals 0–9, and special characters such as: (*), (,), ('), ("), (-), (.), (#), (%), (:), (!), (+), (@), (=), (&), (space), (;), (\$), (_, \), and (/). For more information, see [ASCII Table](#).

ALPHA Key In normal mode, the ALPHA key enables you to enter one of the two or more characters or symbols assigned to individual keys on the main keypad (note that this is in normal mode and is application-specific).



Use the ALPHA key to enter up to 50 different ASCII characters through the following procedure:

- 1 Press the key on the keypad that shows the desired letter or symbol (for example, pressing the 2 key displays 2).
- 2 Press ALPHA once to display the first letter. Continuing our example, press the 2 key, then ALPHA to display the letter A.
- 3 Press ALPHA as many times as required to display the desired character. For example, press 2 to display the number 2; press ALPHA once to display the letter A, twice to display B, or three times to display C.

NOTE



If you firmly press and hold down one of the keys on the main keypad without using ALPHA, the same character repeats until you stop pressing the key. For example, if you press 2 and hold it down, “222222...” appears on the display.

If two or more characters display on the V^x810 screen, pressing ALPHA changes the last character on the line to the next letter, number, or symbol in the key sequence.

The following table provides additional examples of how to use the ALPHA key to select ASCII characters from the Telco-style keypad.

Table 3 Example ALPHA Key Entries

Desired Character	Press Keys
2	2
A	2 ALPHA
S	7 ALPHA ALPHA ALPHA
!	# ALPHA
Space	0 ALPHA ALPHA
Comma (,)	* ALPHA
Plus sign (+)	0 ALPHA ALPHA ALPHA

The following table lists all the ASCII characters you can type using the ALPHA key and the main keypad.

Table 4 Using the Keypad

Key to Press	Without Pressing ALPHA	Press ALPHA One Time	Press ALPHA Two Times	Press ALPHA Three Times
1 QZ.	1	Q	Z	.
2 ABC	2	A	B	C
3 DEF	3	D	E	F
4 GHI	4	G	H	I
5 JKL	5	J	K	L
6 MNO	6	M	N	O
7 PRS	7	P	R	S
8 TUV	8	T	U	V
9 WXY	9	W	X	Y
0 -SP	0	-	[space]	+
*,',"	*	,	'	"
# ^a	#	!	:	;

- a. The # key also supports eight additional characters: (@), (=), (&), (/), (\), (%), (\$), and (_). To enter @, press # once, then ALPHA four times. To enter =, press # once, then ALPHA five times. To enter &, press # once, then ALPHA six times. To enter /, press # once, then ALPHA seven times. To enter \, press # once, then ALPHA eight times. To enter %, press # once, then ALPHA nine times. To enter \$, press # once, then ALPHA ten times. To enter _, press # once, then ALPHA eleven times.



Actual keypad layout may vary. The Verix V OS in the V^x810 supports the following keyboard layouts: Calculator, Singapore Calculator, Telco, and EBS100.

Command Keys The following are the command keys of the V^X810:



CANCEL Key

Pressing the CANCEL key in normal mode – when an application is loaded and running – terminates the current function or operation.

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



CLEAR Key

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

In system mode, the specific effect of pressing the CLEAR key depends on the currently active system mode menu.



ENTER Key

In normal mode, the ENTER key is used to end a procedure, confirm a value or entry, answer “Yes” to a query, or select a displayed option.

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

Programmable Function (PF) Keys

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

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

- PF1 ⬆ Move to the previous menu or screen
- PF2 ⬇ Move to the next menu or screen
- PF3 ⬅ Scroll left
- PF4 ➡ Scroll right

Sound The V^x810 supports only monophonic sound capabilities. The keys produce a beeping sound when pressed.

NOTE



The OS does not contain any pre-defined tunes. This feature is handled entirely by an application. The OS merely provides an API.

Setup

This chapter describes the setup procedure for V^x810, in the following sections:

- Selecting Location
- Unpacking the Shipping Carton
- Examining the V^x810 Features
- Cable Connections
- Using the Primary Smart Card Reader
- Using the Magnetic Stripe Card Reader

Selecting Location

Use the following guidelines to select a location for the V^x810.

Ease of Use

- Select a location convenient for both merchant and cardholder.
- Select a flat support surface, such as a countertop or table.
- Select a location near a power outlet and the other VFI device, ECR, or computer connected to the V^x810. For safety, do not string cables or cords across a walkway.

Environmental Factors

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



The device is not waterproof or dustproof, and is intended for indoor use only. Any damage to the device from exposure to rain or dust can void 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 device near water or in moist conditions.

Unpacking the Shipping Carton

Open the shipping carton and carefully inspect its contents for possible tampering or shipping damage. The Vx810 is a secure product and any tampering can cause it to cease to function or to operate in an insecure manner.

- 1 Remove and inspect the contents of the shipping carton. Since the Vx810 ships in multiple configurations, the carton can include:
 - Vx810 device
 - Data cable
 - Power adapter
 - Power adapter patch cable
 - Power pack
 - Power cord
 - ECR cable
 - Privacy shield
- 2 Remove all plastic wrapping from the device and components.
- 3 Remove the clear protective film from the display.
- 4 Save the shipping carton and packing material for future repacking or moving of the device.

WARNING

Do not use a device that has been tampered with or damaged.

The device 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.

Examining the V^x810 Features

Before you continue the installation process, examine the features of the V^x810.

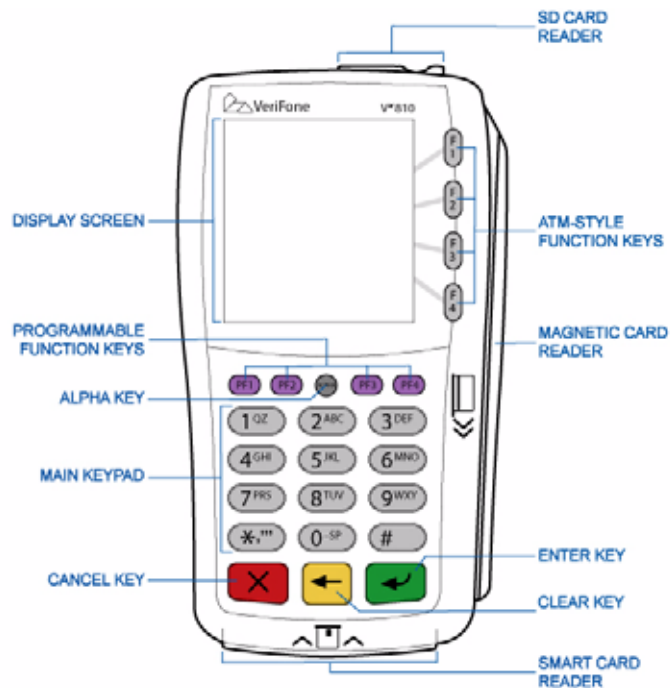


Figure 3 V^x810 Features

The V^x810 has the following features:

- A **display**.
- Five types of keys:
 - Four **ATM-style function keys** (F1 to F4).
 - Four **programmable function keys** (PF1 to PF4).
 - **ALPHA key** used for entering text.
 - **Main keypad** (0 to 9, *, and #).
 - Three color-coded **command keys** (CANCEL = Red; CLEAR = Yellow; and ENTER = Green).
- A **magnetic stripe card reader**, built onto the top side. An icon on the V^x810 surface shows the proper card swipe direction, with the stripe located near the bottom edge of the card when the card is slotted in, and the stripe faces the side where the icon is printed.
- A **primary smart card reader**, built onto the front side. An icon indicates the proper card position and insertion direction, with the IC chip contacts facing upwards when the card is inserted.

- A **SAM (Security Access Module) compartment**, built into the back side of the device. The Vx810 can have up to 3 Micromodule-size SAM (MSAM) cardholders to support multiple stored-value card programs or other merchant card requirements.

NOTE



VeriFone ships variants of the Vx810 for different markets. Your device may have a different configuration. For example, the Vx810 may or may not have a PSCR; it may or may not have an MSR; it may have none or 3 SAMs; flash ROM size may be from 4MB, to 8MB or 16MB; and SRAM size may be from 2MB to 4MB. However, the basic processes described in this guide remain the same, regardless of configuration.

Installing/ Replacing MSAM Cards

You may need to install one or more MSAM cards or replace old cards.

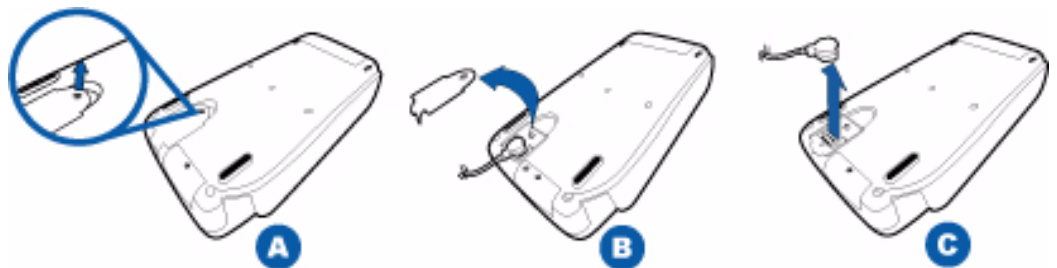
CAUTION



Observe standard precautions for handling electrostatically sensitive devices. Electrostatic discharges can damage this equipment. VeriFone recommends using a grounded anti-static wrist strap.

To change or install MSAMs

- 1 Place the device facedown on a soft, clean surface to protect the lens from scratches.
- 2 Remove the locking screw from the data cable compartment door, open the data cable compartment door, and then unplug the data cable.



NOTE



Removal of the cable ensures that no power is applied to the Vx810.

- 3 Remove the locking screw from the MSAM card compartment door, and then open the MSAM card compartment door.

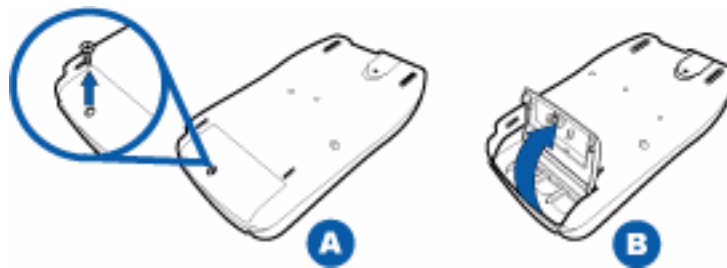


Figure 4 Removing the MSAM Compartment Door

- 4 Remove any previously installed MSAM card by sliding the card out.
- 5 Install an MSAM card by sliding it into the numbered slots. The MSAM card has a notch on one corner to ensure correct positioning of the MSAM card when inserted. The correct card position is also indicated on the MSAM card slot.

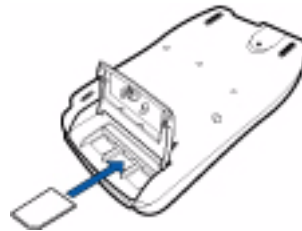


Figure 5 MSAM Insertion

- 6 Replace the MSAM compartment door and reinstall the locking screws.

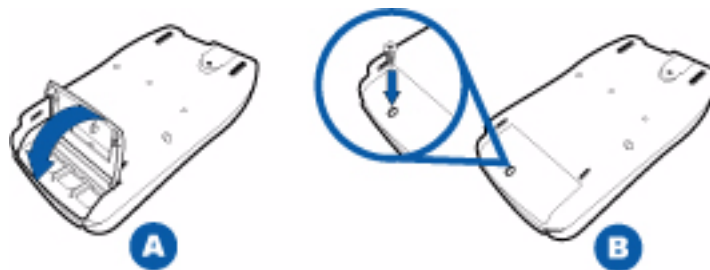


Figure 6 Replacing the MSAM Compartment

Options

VeriFone ships variants of the Vx810 for different markets. Your device may have a different configuration. Additionally, these variants can be ordered with different options.

Privacy Shield Example of an installed privacy shield.

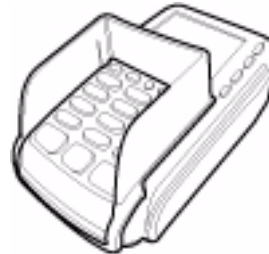


Figure 7 Installed Privacy Shield

Cable Connections

The Vx810 has six general cabling scenarios, depending on what the device connects to:

- Other VFI Devices
- RS-232 Connection with External Power Brick
- Standard USB Connection
- USB Download Support with External Power Brick
- Powered USB
- Ethernet Connection with External Power Brick

Other VFI Devices

Vx810 will connect to another VFI device via a straight cable. There is a minimum power requirement for the Vx810, currently specified as 3.5W. In cases where the other device is only able to provide a 7V DC output to power the Vx810, the other device must be able to source at least 0.5A of current. Otherwise, proper functioning of the Vx810 is not guaranteed.



Figure 8 Connection with Another VFI Device

RS-232 Connection with External Power Brick

A special dongle cable is used, where one end of the cable plugs into the Vx810 while the other end terminates to a female DB-9 connector housing (which is used to connect to an RS-232 serial port). On the housing, a DC jack is provided to connect to an external power brick. This is the generic cable for all RS-232-based hosts.



Figure 9 RS-232 Connection with External Power Brick

Standard USB Connection

For standard USB environments, this cable option has the host end terminating in a Type-A USB plug. Power (5V 500mA) for the Vx810 is provided via this connector.



Figure 10 Standard USB Connection

USB Download Support with External Power Brick

This cable option comes with a junction box that provides a mini-style Type B USB socket for connecting to the USB-based host and a DC jack for external power connection.

In addition, a Type A USB socket is provided on the junction box to support application download via a USB flash drive.

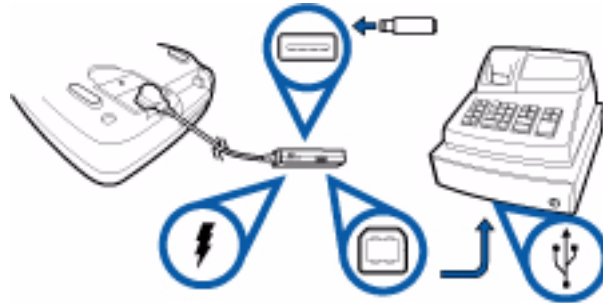


Figure 11 USB with Download Support

NOTE



The V^x810 only supports download functions from a USB flash drive. There is no API for applications or libraries to access the USB flash drive as an extension of internal RAM or flash.

Powered USB

For a USB-based host with PoweredUSB feature, a straight cable is all that is required. The V^x810 supports the 12V DC option.



Figure 12 PoweredUSB

Ethernet Connection with External Power Brick

This cable option has a junction box that provides a standard RJ-45 LAN socket and a DC jack. However, since most hosts do not support peer-to-peer LAN connection to a PIN pad, an additional RJ-45 socket is provided on the junction box to allow a direct connection between V^x810 and the host.

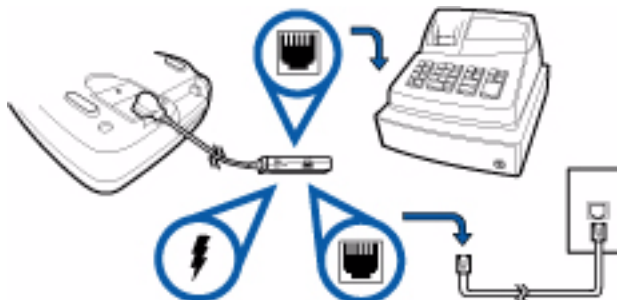


Figure 13 Ethernet Connection with External Power Brick

Power Supply

Not all V^x810 configurations and device contexts require use of a power supply. However, VeriFone ships power supplies with those that require them.

If you have changed the context in which the V^x810 must work or have questions about whether a power supply should be used, contact your VeriFone representative.



Using an incorrectly rated power supply can damage the device or cause it not to work properly.

Before connecting a power supply, disconnect the power pack cord from the power outlet.

Make all V^x810 and device ECR or PC connections before connecting the power pack cord into a wall outlet or surge protector.



Do not plug the power pack into an outdoor outlet or operate the device outdoors. Also, disconnecting power during a transaction can cause transaction data files not yet stored in memory to be lost.



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

When the V^x810 has power and an application is loaded, the application starts after the initial VeriFone copyright screen and displays a unique copyright screen. If no application is loaded, **DOWNLOAD NEEDED** appears on the display after the initial VeriFone copyright screen.

Using the Primary Smart Card Reader

The smart card transaction procedure can vary depending on the application. Verify the proper procedure with your application provider before performing a smart card transaction.

To conduct a smart card transaction:

- 1 Position a smart card with the gold contacts facing upward.
- 2 Insert it into the smart card reader slot in a smooth, continuous motion until it seats firmly.
- 3 Remove the card when the display indicates the transaction is completed.



Figure 14 Smart Card Reader Use



Leave the smart card in the card reader until the transaction is completed. Premature removal can void the transaction.

Using the Magnetic Stripe Card Reader

To conduct a credit/debit card transaction:

- 1 Position a magnetic stripe card with the stripe facing the keypad.
- 2 Swipe it through the magnetic stripe card reader.



Figure 15 Magnetic Stripe Card Reader Use



System Mode

This chapter describes a category of VFI device functions called system mode operations.

- Press F2 and F4 at the same time and enter the password to invoke system mode. See [Entering System Mode](#).
- Assign files and applications to groups for access control. See [File Groups](#).
- Use the system and file group passwords to secure applications and information on the V^x810. See [Passwords](#).
- Use the system mode menus and submenus to configure the V^x810; download, test, and debug applications; and perform routine tests and device maintenance. See [System Mode Menus](#).

The V^x810 System Mode menus are designed to reference four ATM-style function keys (F1 to F4). System mode is used exclusively by those responsible for configuring, deploying, and managing on-site V^x810 installations.

When to Use System Mode

Use the system mode functions to perform different subsets of related tasks:

- **Application programmers** configure a development device, download development versions of applications, then test and debug these applications until they are validated and ready to be downloaded to other devices.
- **Deployers** perform the specific tasks required to deploy a new device on-site, including configuring the device, downloading applications, and testing the device prior to deployment.
- **System administrators or site managers** change passwords, perform routine tests and device maintenance, and configure devices for remote diagnostics and downloads.

To perform the subset of tasks that corresponds to a job, select the appropriate system mode menus and execute the corresponding procedures.

Local and Remote Operations

The system mode operations available on a V^x810 can be divided into the following two categories or types:

- **Local operations** address a stand-alone device and do not require communication or data transfers between the device and a host computer or another VFI device. Perform local system mode operations to configure, test, and display information about the device.
- **Remote operations** require communication between the device and a host computer or another VFI device over a cable connection. Perform remote system mode operations to download applications to the device, upload software from one device to another, or perform diagnostics.

This chapter contains descriptions on how to perform local system mode operations. For information on performing remote operations, such as downloads, refer to the [Performing Downloads](#) section.

Verifying Device Status

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

- If no application is loaded onto system SRAM or flash ROM, the message **DOWNLOAD NEEDED** appears on the display screen.



From this point, press F2 and F4 to access system mode and perform the required download.

- If an application is loaded onto system SRAM or flash ROM, an application-specific prompt appears. The application is running and the device is in normal mode. If all installation steps are complete, the device can process transactions.

Entering System Mode

To prevent unauthorized use of the system mode menus, the V^x810 OS requires a system password each time you enter system mode. After entering the correct password, the device enters system mode and displays the first system mode main menu, **SYS MODE MENU 1**. From here you can cycle through the system mode main menus.

File Groups

The V^x810 operating system implements a file system in non-volatile, battery-backed SRAM, and in non-volatile flash ROM memory. Files are assigned to one of 15 groups for access control. Each group has a separate CONFIG.SYS file, and each group is protected by a separate password. Groups are referred to as Group *n* or GID*n* throughout this manual.

The following rules apply to the V^x810 file group system:

- The primary application must be downloaded onto Group 1.
- On power up and after a restart, the device defaults to Group 1 as the controlling group.
- Group 1 applications have access to files stored in all other groups.
- Applications stored in Groups 2 to 14 have access only to their own respective files and to 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.
- Groups 1–15 are empty until they are filled through a download.

For more information on managing file groups, refer to the Verix V Operating System Programmers Manual, VPN 23230.

Passwords

Passwords for the V^x810 are enforced by the Verix V operating system (OS) in compliance with PCI PED password requirements. These requirements include the requiring of two passwords for sensitive operations; and, the requiring of all passwords to be at least five characters in length.

Downloading and IPP Keyloading are considered sensitive operations that require two passwords, the System Mode password, followed by the GID1 password. The OS will require the user to enter the GID 1 password every time the user selects these operations in System Mode, regardless of whether the operation has already been previously selected in the current System Mode session. For example, the DOWNLOAD operation will require a password each time it is selected, even if the user performs a second DOWNLOAD operation immediately after the first DOWNLOAD operation is completed and does not exit System Mode.

The OS will require *all* passwords to be at least five characters and up to ten characters in length for System Mode and all GIDs.

System Mode Password The default, factory-set password for System Mode is “**Z66831**.” Use the following key sequence to enter this password:

1 ALPHA ALPHA 6 6 8 3 1 then press **ENTER**

File Group Passwords The default, factory-set password for file group 1 (GID1) is also “**Z66831**.” For file groups 2-15 (GID2-GID15), password is **<EMPTY>** by default.

Password Maintenance The OS supports two methods by which passwords can be changed. Passwords can either be changed manually, or by downloading a password change parameter. You can change a password at any time, provided you know the current password.



CAUTION If you change the System Mode password but forget it later on, no password recovery method is available. Without the password, you will not be able to access System Mode operations and will be prevented from requesting downloads, performing remote diagnostics, or changing any of the information already stored in memory. The device can, however, continue to process transactions in Normal mode.

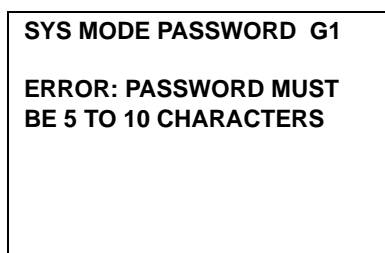
If you forget or lose the System Mode password of your device, please contact your local VeriFone representative for assistance.

When you key in a password, an asterisk (*) appears for each character you type. These asterisks prevent your password from being seen by an unauthorized person. You can use the **ALPHA** key to change the characters or symbols you enter. This does not cause additional asterisks to appear.

Manual Password Change

A user can change the System Mode password or any GID password from the Passwords submenu in System Mode. The user must choose a password at least five characters long and no more than ten characters long.

If the user attempts to enter a new password less than five characters long, the OS will sound a beep and the screen will display an error message (see [Figure 16](#)):



```
SYS MODE PASSWORD G1
ERROR: PASSWORD MUST
BE 5 TO 10 CHARACTERS
```

Figure 16 Error message for insufficient password length

To return to the New Password prompt, press ENTER. Re-enter the new password, and then press ENTER. To abort the password change, press CANCEL.

If the user attempts to enter more than ten characters for the new password, the password will be set to the first ten characters entered.

Download Password Change

A user can set the System Mode password or any GID password by downloading a Password Change parameter from any download server (VeriCentre, DDL, or customer-developed server).

If the downloaded password is at least five characters long and no more than ten characters long, the OS will accept the new password.

If the downloaded password is more than ten characters long, the OS will truncate the downloaded password to the first ten characters and will accept the new truncated password.

If the downloaded password is less than five characters long, the OS will accept the new password. The OS will initially accept the new “short” password, but the next time an operation is performed where the password is required, the user will be prompted to change the password to a valid password before the requested operation can be performed.

For operations which do not require a password, the OS will continue to operate normally and any applications loaded on the device will be unaffected.

CAUTION

It is possible for a download server to change a password to one which can not be entered on the V^x810 keypad. In this case, the device could be rendered unusable, depending on which password is changed and the specific configuration of the device.

NOTE

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

Previous versions of the OS will allow a password to be as short as one character. If a customer has configured a device with “short” passwords and upgrades its OS to the PCI PED password-compliant OS, the device will follow the logic described in [Download Password Change](#).

This means that the OS will not enforce the five-character minimum password requirement until the user attempts to perform an operation which requires a password. When a password-requiring operation is performed, the user will be required to change the password to a compliant password before the operation can be performed.

Any applications loaded on the device will be unaffected by the new OS.

System Mode Menus

The Vx810 has 3 system mode menus.

Table 5 System Mode Menus

SYS MODE MENU 1	SYS MODE MENU 2	SYS MODE MENU 3
EDIT PARAMETERS F2	MEMORY FUNCTIONS F2	CONTRAST F2
DOWNLOAD F3	TERMINAL INFO F3	PASSWORDS F3
RESTART F4	CLOCK F4	IPP KEY LOAD F4

On successful entry of the system password, **SYS MODE MENU 1** appears.

To return to a previous menu, press the **PF1** key (below the up arrow). To go to the next menu, press the **PF2** key (below the down arrow). Pressing the **ENTER** key also cycles you through the system mode menus. To return to the main system mode menu and cancel any changes, press the **CANCEL** key.

Each menu option may immediately execute an operation upon selection, or it may contain a submenu or a series of prompts.

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.

System Mode Procedures

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

- 1 When a main system mode menu appears, select an option by pressing the appropriate function key.
- 2 Complete the operation.
- 3 Return to the main system mode menu.

Procedure descriptions are arranged in the following tabular format:

Table 6 Procedural Description Example

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

The Display column indicates what appears on the 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 ALL CAPS. For example, **DOWNLOAD NEEDED**.
- If text is enclosed in parentheses, the actual text or message may vary depending on the application installed. For example, in (Application Prompt), the normal font is used and text is typed in title case.

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 for that particular system mode menu option.

A submenu row indicates a specific menu invoked 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 save changes from a submenu and return to the menu screen.
- Press the **CANCEL** key to exit any submenu without saving changes.

Entering System Mode The following describes how to enter system mode after you have turned on the VX810.



On successful completion, some operations automatically exit system mode and restart the device. Other operations require that you exit system mode and restart the device. To manually exit system mode, select **RESTART (F4)** in **SYS MODE MENU 1**.

Table 7 Entering System Mode

Display	Action
<p style="text-align: center;"> VERIFONE VX810 QG000829 03/29/2007 VERIX ★DEFAULT CERTIFICATE★ COPYRIGHT 1997-2007 VERIFONE ALL RIGHTS RESERVED </p>	<p>At startup, the device displays a copyright notice screen that shows the device model number, the OS version of the VX810 stored in the device's flash ROM memory, the date the firmware was loaded onto the device, and the copyright notice.</p> <p>This screen appears for three seconds, during which time you can enter system mode by simultaneously pressing F2 and F4.</p> <p>You can extend the display period of this screen by pressing any key during the initial three seconds. Each key press extends the display period an additional three seconds.</p>
<p>(Application Prompt) or DOWNLOAD NEEDED ★GO FILE NOT FOUND</p>	<p>If an application already resides on the device, an application-specific prompt is displayed. If no application resides on the device, the following message is displayed:</p> <p>DOWNLOAD NEEDED</p> <p>To enter system mode from this screen, simultaneously press F2 and F4.</p> <p>Note: The device will automatically download the file VeriFone.zip from a USB flash drive without the user having to go through System Mode under the following conditions:</p> <ul style="list-style-type: none"> • The USB flash drive is connected before the device is turned on. • The USB flash drive is inserted when the initial DOWNLOAD NEEDED message is displayed. <p>In both cases, the USB DOWNLOAD COMPLETE message will appear on the screen after the VeriFone.zip file has been downloaded.</p>

Table 7 Entering System Mode (continued)

Display	Action
<pre>SYSTEM MODE ENTRY PASSWORD -----</pre>	<p>If an application prompt appeared and you chose to enter system mode, you are prompted to type the system password.</p> <p>If DOWNLOAD NEEDED appeared, use the default password "Z66831." This password is entered as: 1 ALPHA ALPHA 6 6 8 3 1, then press ENTER.</p> <p>If you enter an incorrect password, the device exits the SYSTEM MODE ENTRY screen. Verify your password and re-enter it.</p> <p>To quit this operation and return to the application prompt or DOWNLOAD NEEDED screen, press CANCEL.</p>
<pre>SYS MODE MENU 1 EDIT PARAMETERS F2 DOWNLOAD F3 RESTART F4 ↑ ↓</pre>	<p>SYS MODE MENU 1 is the first menu displayed. To cycle through to the other menus, press the PF2 key or press ENTER until you reach the desired menu.</p>

Menu 1 In this menu you can edit system parameters, perform downloads, and restart the device.

Table 8 System Mode Menu 1

Display	Action
<div style="border: 1px solid black; padding: 5px;"> <p>SYS MODE MENU 1 EDIT PARAMETERS F2 DOWNLOAD F3 RESTART F4 ↓</p> </div>	<p>To edit system parameters, select EDIT PARAMETERS (F2)</p> <p>To download an application to your device, select DOWNLOAD (F3).</p> <p>To restart the device, select RESTART (F4).</p> <p>To go to the next system mode menu, press PF2 or ENTER.</p>
EDIT PARAMETERS	
<div style="border: 1px solid black; padding: 5px;"> <p>SYS MODE MENU 1 EDIT PARAMETERS F2 DOWNLOAD F3 RESTART F4 ↓</p> </div>	<p>To edit system parameters, select EDIT PARAMETERS (F2)</p> <p>To abort any action at any step, press CANCEL.</p>
<div style="border: 1px solid black; padding: 5px;"> <p>GROUP SELECT GROUP ID: nn APP: NOT EMPTY</p> </div>	<p>Scroll to the group whose parameters you want to edit. Press PF1 to move up the list or PF2 to move down the list. Then press ENTER.</p>
<div style="border: 1px solid black; padding: 5px;"> <p>SYSTEM MODE DOWNLOAD GROUP nn PASSWORD -----</p> </div>	<p>To continue, enter the required password.</p> <p>The default group password is “Z66831.” This is entered as: 1 ALPHA ALPHA 6 6 8 3 1, then press ENTER.</p>
<div style="border: 1px solid black; padding: 5px;"> <p>SYS MODE PASSWORD Gnn PLEASE TRY AGAIN</p> </div>	<p>This message appears if you enter an incorrect password.</p> <p>Press ENTER to try again. Re-enter your password.</p>
<div style="border: 1px solid black; padding: 5px;"> <p>SYS MODE EDIT Gnn FILE CONFIG.SYS</p> </div>	<p>The CONFIG.SYS file is displayed. Press ENTER to continue.</p>

Table 8 System Mode Menu 1 (continued)

Display	Action
<pre> GID 1: NOT EMPTY NEW (F1) PARAMETER: *GO _____ FIND (F2) VALUE: F : VX81 . OUT EDIT (F3) CLEAR (F4) ↑ ↓ </pre>	<p>Do one of the following:</p> <ul style="list-style-type: none"> To create a new parameter, select NEW (F1). Enter a name for the parameter, then press ENTER. Enter a value for the parameter, then press ENTER. To look for an existing parameter, select FIND (F2). Type the name of the parameter, then press ENTER. To edit the value for an existing parameter, scroll through the list of existing parameters by pressing PF1 to move up the list or PF2 to move down the list, then select EDIT (F3). Change the value for the parameter, then press ENTER. To erase an existing parameter, scroll through the list of existing parameters by pressing PF1 to move up the list or PF2 to move down the list, then select CLEAR (F4). Then either select YES (F3) to confirm or NO (F4) to cancel the action.
DOWNLOAD	
<pre> SYS MODE MENU 1 EDIT PARAMETERS F2 DOWNLOAD F3 RESTART F4 ↓ </pre>	<p>To download an application to your device, select DOWNLOAD (F3).</p> <p>To abort any action at any step, press CANCEL.</p>
<pre> SYSTEM MODE DOWNLOAD GROUP ID: nn </pre>	<p>Type the Group ID (valid values are 1 to 15) of the group into which you want to download files to. (Refer to Chapter 6 for detailed download instructions and information.) Then press ENTER to select the group.</p>
<pre> SYSTEM MODE DOWNLOAD GROUP nn PASSWORD ----- </pre>	<p>To continue, enter the required password.</p> <p>The default group password is “Z66831.” This is entered as: 1 ALPHA ALPHA 6 6 8 3 1, then press ENTER.</p>
<pre> SYS MODE PASSWORD Gnn PLEASE TRY AGAIN </pre>	<p>This message appears if you enter an incorrect password.</p> <p>Press ENTER to try again. Re-enter your password.</p>
<pre> SYS MODE DOWNLOAD Gnn SINGLE-APP F3 MULTI-APP F4 </pre>	<p>To download a single application, select SINGLE-APP (F3).</p> <p>To download multiple applications, select MULTI-APP (F4).</p>

Table 8 System Mode Menu 1 (continued)

Display	Action
<div style="border: 1px solid black; padding: 5px;"> <p>SYS MODE DOWNLOAD Gnn FULL F3 PARTIAL F4</p> </div>	<p>For a full download, select FULL (F3). For a partial download, select PARTIAL (F4). To return to SYS MODE MENU 1, press the PF1 key.</p>
<div style="border: 1px solid black; padding: 5px;"> <p>SYS MODE DOWNLOAD Gnn COM2 F3</p> </div>	<p>Select the download source, COM 2 (F3).</p>
<div style="border: 1px solid black; padding: 5px;"> <p>SYS MODE DOWNLOAD Gnn UNIT RECEIVE MODE WAITING FOR DOWNLOAD</p> </div>	<p>The device is ready to receive a download from the selected source.</p>
<div style="border: 1px solid black; padding: 5px;"> <p>SYS MODE DOWNLOAD Gnn *** _ _ _ _ _ DOWNLOADING NOW</p> </div>	<p>During download, a line of asterisks appears that shows the percentage of completion. Each asterisk equals approximately 10% of the download. When the download is completed, the device will restart. You can cancel a download in progress by pressing CANCEL. This will also restart the device.</p>
RESTART	
<div style="border: 1px solid black; padding: 5px;"> <p>SYS MODE MENU 1 EDIT PARAMETERS F2 DOWNLOAD F3 RESTART F4 ↓</p> </div>	<p>Select RESTART F4 to exit system mode and restart the device.</p>



NOTE Before performing a download to flash ROM memory in an initialized device (one that contains an application), reclaim all available flash ROM space. Unlike SRAM, unused flash ROM and duplicate flash ROM information are not automatically reclaimed during a download. To reclaim this space, perform a defragment operation from system mode (refer to the procedure [flash ROM FILES F3](#)). This operation makes all files in flash ROM memory contiguous. You must also clear some or all flash ROM memory if your device does not have enough space for the impending download.

Menu 2 In this menu, you can perform memory functions, view device configuration information, or set the device clock.

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 keypad using the device's built-in keyed file editor. Each record has two parts: a key name and a key value. The search key is a variable-length string, or key name, that identifies the record. The information assigned to the search key is contained in a separate variable-length string, 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 device 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.



NOTE For a complete list of the ASCII characters supported by the V^x810 series, as well as their decimal and hexadecimal equivalents, please refer to [Appendix C](#).

CONFIG.SYS: Protected and Non-protected Records

The concept of protected and non-protected records applies only to the CONFIG.SYS files in your device. Prior to a download, the recommended procedure is to clear SRAM files.

Protected records in the file Group 1 CONFIG.SYS file are retained in a full application download and when SRAM is cleared. Protected records are those with search keys beginning with an asterisk (*) or a pound/hash symbol (#).

Non-protected records are all other CONFIG.SYS files, and records of other files. These records are deleted in a full application download and when SRAM is cleared.

Editing CONFIG.SYS with an External Editor

You can create and edit the CONFIG.SYS files of V^x810 applications through an IBM PC-compatible computer when you download files to the device. For more information on editing an application's CONFIG.SYS file, refer to the VeriCentre Reference Manual, VPN 24698, and the Verix V Operating System Programmers Manual, VPN 23230, or contact your local VeriFone representative.



NOTE The Verix V OS in the V^x810 will support all non-modem-related VeriCentre operations, including full/partial downloads and compressed downloads, but not VeriCentre-initiated downloads because this requires a modem.

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

Table 9 System Mode Menu 2

Display	Action												
<div style="border: 1px solid black; padding: 5px;"> <p>SYS MODE MENU 2 MEMORY FUNCTIONS F2 TERMINAL INFO F3 CLOCK F4</p> <p>↑ ↓</p> </div>	<p>To perform memory functions, select MEMORY FUNCTIONS (F2).</p> <p>To view device configuration information, select TERMINAL INFO (F3).</p> <p>To set the device clock, select CLOCK (F4).</p> <p>To go to the previous system mode menu, press PF1. To go to the next system mode menu, press PF2 or ENTER.</p>												
MEMORY FUNCTIONS ► USAGE													
<div style="border: 1px solid black; padding: 5px;"> <p>SYS MODE MENU 2 MEMORY FUNCTIONS F2 TERMINAL INFO F3 CLOCK F4</p> <p>↑ ↓</p> </div>	<p>To perform memory functions, select MEMORY FUNCTIONS (F2).</p> <p>To abort any action at any step, press CANCEL.</p>												
<div style="border: 1px solid black; padding: 5px;"> <p>SYS MODE MEM FUNCS RAM: 2048 FLASH: 4096</p> <p style="text-align: right;">USAGE F2 DIRECTORIES F3 CLEAR MEM F4</p> </div>	<p>This screen shows the amount of installed SRAM and flash ROM memory.</p> <p>To view memory usage, select USAGE (F2).</p>												
<div style="border: 1px solid black; padding: 5px;"> <p>MEMORY USAGE</p> <table style="width: 100%; border-collapse: collapse;"> <tr> <td>RAM FILES</td> <td style="text-align: right;">6</td> </tr> <tr> <td style="padding-left: 20px;">INUSE</td> <td style="text-align: right;">1 KB</td> </tr> <tr> <td style="padding-left: 20px;">AVAIL</td> <td style="text-align: right;">1907 KB</td> </tr> <tr> <td>FLASH FILES</td> <td style="text-align: right;">1</td> </tr> <tr> <td style="padding-left: 20px;">INUSE</td> <td style="text-align: right;">6 KB</td> </tr> <tr> <td style="padding-left: 20px;">AVAIL</td> <td style="text-align: right;">3450 KB</td> </tr> </table> </div>	RAM FILES	6	INUSE	1 KB	AVAIL	1907 KB	FLASH FILES	1	INUSE	6 KB	AVAIL	3450 KB	<p>Selecting USAGE (F2) displays the following information:</p> <ul style="list-style-type: none"> • Number of files in SRAM memory • Total KB of SRAM memory in use • Total KB of SRAM memory available • Number of files in flash ROM memory • Total KB of flash ROM memory in use • Total KB of flash ROM memory available
RAM FILES	6												
INUSE	1 KB												
AVAIL	1907 KB												
FLASH FILES	1												
INUSE	6 KB												
AVAIL	3450 KB												

Table 9 System Mode Menu 2 (continued)

Display	Action
MEMORY FUNCTIONS ► DIRECTORIES	
<div style="border: 1px solid black; padding: 5px;"> <p>SYS MODE MENU 2 MEMORY FUNCTIONS F2 TERMINAL INFO F3 CLOCK F4</p> <p>↑ ↓</p> </div>	<p>To perform memory functions, select MEMORY FUNCTIONS (F2).</p> <p>To abort any action at any step, press CANCEL.</p>
<div style="border: 1px solid black; padding: 5px;"> <p>SYS MODE MEM FUNCS RAM: 2048 FLASH: 4096</p> <p>USAGE F2 DIRECTORIES F3 CLEAR MEM F4</p> </div>	<p>This screen shows the amount of installed SRAM and flash ROM memory.</p> <p>To view directory information, select DIRECTORIES (F3).</p>
<div style="border: 1px solid black; padding: 5px;"> <p>SYS MODE DIRECTORY GROUP ID: nn</p> <p>RAM FILES F3 FLASH FILES F4</p> </div>	<p>Type the Group ID (valid values are 1 to 15) of the group whose directory you want to view.</p> <p>To view the files in SRAM memory for the selected group, select RAM FILES (F3).</p> <p>To view the files in flash ROM memory for the selected group, select FLASH FILES (F4).</p>
MEMORY FUNCTIONS ► CLEAR MEM	
<div style="border: 1px solid black; padding: 5px;"> <p>SYS MODE MENU 2 MEMORY FUNCTIONS F2 TERMINAL INFO F3 CLOCK F4</p> <p>↑ ↓</p> </div>	<p>To perform memory functions, select MEMORY FUNCTIONS (F2).</p> <p>To abort any action at any step, press CANCEL.</p>
<div style="border: 1px solid black; padding: 5px;"> <p>SYS MODE MEM FUNCS RAM: 2048 FLASH: 4096</p> <p>USAGE F2 DIRECTORIES F3 CLEAR MEM F4</p> </div>	<p>This screen shows the amount of installed SRAM and flash ROM memory.</p> <p>To clear memory information, select CLEAR MEM (F4).</p>
<div style="border: 1px solid black; padding: 5px;"> <p>SYS MODE MEMORY GROUP ID: nn</p> </div>	<p>Type the Group ID (valid values are 1 to 15) of the group whose memory you want to erase, then press ENTER.</p>

Table 9 System Mode Menu 2 (continued)

Display	Action
<div style="border: 1px solid black; padding: 5px;"> <p>SYS MODE MEMORY GROUP nn PASSWORD -----</p> </div>	<p>To continue, enter the required password. If you enter an incorrect password, the following message appears:</p> <p>SYS MODE PASSWORD Gnn PLEASE TRY AGAIN</p> <p>Press ENTER to try again. Re-enter your password.</p>
<div style="border: 1px solid black; padding: 5px;"> <p>SYS MODE MEMORY CLEAR CONFIG.SYS F2 CLEAR Gnn FILES F3 CLEAR ALL GROUPS F4</p> </div>	<p>To clear the CONFIG.SYS records for the selected group, select CLEAR CONFIG.SYS (F2).</p> <p>To clear the other files stored in the selected group, select CLEAR Gnn FILES (F3).</p> <p>To clear the other files stored in all groups, select CLEAR ALL GROUPS (F4).</p>
<div style="border: 1px solid black; padding: 5px;"> <p>SYS MODE MEMORY CLEAR ALL F2 KEEP PROTECTED VARIABLES F3</p> </div>	<p>Selecting CLEAR CONFIG.SYS (F2) will further display the following options:</p> <ul style="list-style-type: none"> • Select CLEAR ALL (F2) to clear all CONFIG.SYS records, including both protected and non-protected records. • Select KEEP PROTECTED VARIABLES (F3) to clear non-protected CONFIG.SYS records but retain protected CONFIG.SYS records.
<div style="border: 1px solid black; padding: 5px;"> <p>RAM & FLASH CLEARED COALESCING FLASH</p> </div>	<p>This message will be displayed when clearing is completed.</p>
TERMINAL INFO ► SYSTEM INFO	
<div style="border: 1px solid black; padding: 5px;"> <p>SYS MODE MENU 2 MEMORY FUNCTIONS F2 TERMINAL INFO F3 CLOCK F4 ↑ ↓</p> </div>	<p>To view device configuration information, select TERMINAL INFO (F3).</p> <p>To abort any action at any step, press CANCEL.</p>
<div style="border: 1px solid black; padding: 5px;"> <p>SYS MODE MENU SYSTEM INFO F2 DIAGS AND LOGS F3</p> </div>	<p>To view system information, select SYSTEM INFO (F2).</p>

Table 9 System Mode Menu 2 (continued)

Display	Action
<p>SYS MODE TERM INFO</p> <p>SERNO 303-000-040</p> <p>PTID 12000000</p> <p>PART M28150302DMO</p> <p>REV 1</p> <p>OS VER QG000829</p> <p style="text-align: center;">↓</p>	<p>Selecting SYSTEM INFO (F2) shows the following information:</p> <ul style="list-style-type: none"> • Device Serial Number (9-character, numeric code) • Permanent Device ID Number (8-character, numeric code) • Device Part Number (12-character alphanumeric code) • Hardware Revision Number (2-character numeric code) • System OS Version (8-character alphanumeric code)
<p>SYS MODE TERM INFO</p> <p>MODL VX810</p> <p>CTRY GEN</p> <p>KEYPAD 0</p> <p>DISPLAY 128128</p> <p>MAG RDR 3</p> <p style="text-align: center;">↑ ↓</p>	<ul style="list-style-type: none"> • Hardware Model: VX810 • Country of Manufacture: GEN = Generic • Keypad Type: 0 = TelCo, 1 = Calculator, 2 = Singapore • Display Resolution: 128 x 128 pixels • Magnetic Stripe Reader Type
<p>SYS MODE TERM INFO</p> <p>PINPAD 1</p> <p>LIFE 143457</p> <p>RSET 070613131233</p> <p>RCNT 171</p> <p>TAMPER DETECTED N</p> <p style="text-align: center;">↑ ↓</p>	<ul style="list-style-type: none"> • Integrated PIN Pad: 1 = Yes, 0 = No • Running Life (in seconds) • Last Reset Date & Time (in YYMMDDHHMMSS format, where YY = year, MM = month, DD = day, HH = hour, MM = minute, and SS = second) • Reset Count – either through application control, system mode request, or a power cycle. • Occurrence of Tampering: Y = Yes, N = No
<p>SYS MODE TERM INFO</p> <p>CERT 234000</p> <p>HEAP 772</p> <p>STACK 1708</p> <p style="text-align: right;">NEXT CERT F3</p> <p style="text-align: center;">↑</p>	<ul style="list-style-type: none"> • CERT indicates the certificate numbers pertaining to the device. Pressing NEXT CERT (F3) will show the other certificate numbers. • HEAP indicates the memory designation used by the OS. • STACK indicates the memory set aside by the OS for running tasks.

Table 9 System Mode Menu 2 (continued)

Display	Action
TERMINAL INFO ► DIAGS AND LOGS	
<p>SYS MODE MENU 2 MEMORY FUNCTIONS F2 TERMINAL INFO F3 CLOCK F4</p> <p>↑ ↓</p>	<p>To view device configuration information, select TERMINAL INFO (F3).</p> <p>To abort any action at any step, press CANCEL.</p>
<p>SYS MODE MENU SYSTEM INFO F2 DIAGS AND LOGS F3</p>	<p>To perform system diagnostic tests and view log information, select DIAGS AND LOGS (F3).</p>
<p>SYS MODE DIAGS SMART CARD DIAG F2 KEYBOARD DIAG F3 MAG CARD DIAG F4</p> <p>↓</p>	<p>To run a test on any inserted ICC or SAM cards, select SMART CARD DIAG (F2).</p> <p>To run a test on the keypad, select KEYBOARD DIAG (F3).</p> <p>To run a test on the magnetic stripe reader (MSR), select MAG CARD DIAG (F4).</p>
<p>SYS MODE DIAGS SCREEN DIAG F2 IPP DIAG F3</p> <p>↑ ↓</p>	<p>To perform a diagnostic test on the screen, select SCREEN DIAG (F2).</p> <p>To perform a diagnostic test on the internal PIN pad, select IPP DIAG (F3).</p>
<p>SYS MODE DIAGS REMOTE DIAGS F2 DEBUGGER F3</p> <p>↑ ↓</p>	<p>The REMOTE DIAGS (F2) functions are reserved for VeriFone use only.</p> <p>To use the debugging tool, select DEBUGGER (F3).</p>
<p>SYS MODE DIAGS ERROR LOG F2 TAMPER LOG F3</p> <p>↑</p>	<p>To view the error logs, select ERROR LOG (F2).</p> <p>To view the tamper logs, select TAMPER LOG (F3).</p>

Table 9 System Mode Menu 2 (continued)

Display	Action
TERMINAL INFO ► DIAGS AND LOGS ► SMART CARD DIAG	
<div style="border: 1px solid black; padding: 5px;"> <p>SYS MODE MENU 2 MEMORY FUNCTIONS F2 TERMINAL INFO F3 CLOCK F4</p> <p>↑ ↓</p> </div>	<p>To view device configuration information, select TERMINAL INFO (F3).</p> <p>To abort any action at any step, press CANCEL.</p>
<div style="border: 1px solid black; padding: 5px;"> <p>SYS MODE MENU SYSTEM INFO F2 DIAGS AND LOGS F3</p> </div>	<p>To perform system diagnostic tests and view log information, select DIAGS AND LOGS (F3).</p>
<div style="border: 1px solid black; padding: 5px;"> <p>SYS MODE DIAGS SMART CARD DIAG F2 KEYBOARD DIAG F3 MAG CARD DIAG F4</p> <p>↓</p> </div>	<p>To run a test on any inserted ICC or SAM cards, select SMART CARD DIAG (F2).</p>
<div style="border: 1px solid black; padding: 5px;"> <p>VOYAGER VER 02080000 DRVR VER 070329161412 PHILIP VER 2.0 6/06 SMART CARD TEST F3 LIST SYNC DRIVERS F4</p> </div>	<p>The screen displays system and driver information pertaining to the SAM slots available.</p>
<div style="border: 1px solid black; padding: 5px;"> <p>TEST CUST SLOT F1 SAM1 F2 SAM2 F3 SAM3 F4</p> </div>	<p>Selecting SMART CARD TEST (F3) will display this screen. Select the SAM card slot you want to test.</p> <ul style="list-style-type: none"> • Customer Card slot (F1) • SAM Card 1 slot (F2) • SAM Card 2 slot (F3) • SAM Card 3 slot (F4)

Table 9 System Mode Menu 2 (continued)

Display	Action
<div style="border: 1px solid black; padding: 5px;"> <p>SAM 1 POWER UP: PASSED GET ATR: PASSED</p> </div>	This is the screen that is displayed when an inserted SAM card is successfully tested.
<div style="border: 1px solid black; padding: 5px;"> <p>SAM 2 POWER UP: FAILED</p> </div>	This is the screen that is displayed when there is no inserted SAM card in the slot being tested.
TERMINAL INFO ► DIAGS AND LOGS ► KEYBOARD DIAG	
<div style="border: 1px solid black; padding: 5px;"> <p>SYS MODE MENU 2 MEMORY FUNCTIONS F2 TERMINAL INFO F3 CLOCK F4</p> <p>↑ ↓</p> </div>	<p>To view device configuration information, select TERMINAL INFO (F3).</p> <p>To abort any action at any step, press CANCEL.</p>
<div style="border: 1px solid black; padding: 5px;"> <p>SYS MODE MENU SYSTEM INFO F2 DIAGS AND LOGS F3</p> </div>	To perform system diagnostic tests and view log information, select DIAGS AND LOGS (F3) .

Table 9 System Mode Menu 2 (continued)

Display	Action																																																
<div style="border: 1px solid black; padding: 5px;"> <p>SYS MODE DIAGS SMART CARD DIAG F2 KEYBOARD DIAG F3 MAG CARD DIAG F4</p> <p style="text-align: center;">↓</p> </div>	<p>To run a test on the keypad, select KEYBOARD DIAG (F3).</p> <p>Pressing a key on the device, will return a corresponding keycode. These are listed as follows:</p>																																																
<div style="border: 1px solid black; padding: 5px;"> <p>SYS MODE KBD TEST KEYCODE 00</p> </div>	<table border="1"> <thead> <tr> <th>Key</th> <th>Keycode</th> <th>Key</th> <th>Keycode</th> </tr> </thead> <tbody> <tr> <td>F1</td> <td>FA</td> <td>ENTER</td> <td>(n/a)</td> </tr> <tr> <td>F2</td> <td>FB</td> <td>0</td> <td>30</td> </tr> <tr> <td>F3</td> <td>FC</td> <td>1</td> <td>31</td> </tr> <tr> <td>F4</td> <td>FD</td> <td>2</td> <td>32</td> </tr> <tr> <td>ALPHA</td> <td>0F</td> <td>3</td> <td>33</td> </tr> <tr> <td>S1</td> <td>61</td> <td>4</td> <td>34</td> </tr> <tr> <td>S2</td> <td>62</td> <td>5</td> <td>35</td> </tr> <tr> <td>S3</td> <td>63</td> <td>6</td> <td>36</td> </tr> <tr> <td>S4</td> <td>64</td> <td>7</td> <td>37</td> </tr> <tr> <td>CANCEL</td> <td>(n/a)</td> <td>8</td> <td>38</td> </tr> <tr> <td>CLEAR</td> <td>08</td> <td>9</td> <td>39</td> </tr> </tbody> </table>	Key	Keycode	Key	Keycode	F1	FA	ENTER	(n/a)	F2	FB	0	30	F3	FC	1	31	F4	FD	2	32	ALPHA	0F	3	33	S1	61	4	34	S2	62	5	35	S3	63	6	36	S4	64	7	37	CANCEL	(n/a)	8	38	CLEAR	08	9	39
Key	Keycode	Key	Keycode																																														
F1	FA	ENTER	(n/a)																																														
F2	FB	0	30																																														
F3	FC	1	31																																														
F4	FD	2	32																																														
ALPHA	0F	3	33																																														
S1	61	4	34																																														
S2	62	5	35																																														
S3	63	6	36																																														
S4	64	7	37																																														
CANCEL	(n/a)	8	38																																														
CLEAR	08	9	39																																														

TERMINAL INFO ► DIAGS AND LOGS ► MAG CARD DIAG

<div style="border: 1px solid black; padding: 5px;"> <p>SYS MODE MENU 2 MEMORY FUNCTIONS F2 TERMINAL INFO F3 CLOCK F4</p> <p style="text-align: center;">↑ ↓</p> </div>	<p>To view device configuration information, select TERMINAL INFO (F3).</p> <p>To abort any action at any step, press CANCEL.</p>
<div style="border: 1px solid black; padding: 5px;"> <p>SYS MODE MENU SYSTEM INFO F2 DIAGS AND LOGS F3</p> </div>	<p>To perform system diagnostic tests and view log information, select DIAGS AND LOGS (F3).</p>
<div style="border: 1px solid black; padding: 5px;"> <p>SYS MODE DIAGS SMART CARD DIAG F2 KEYBOARD DIAG F3 MAG CARD DIAG F4</p> <p style="text-align: center;">↓</p> </div>	<p>To run a test on the magnetic stripe reader (MSR), select MAG CARD DIAG (F4).</p>
<div style="border: 1px solid black; padding: 5px;"> <p>SYS MODE TRK 1: NO DATA TRK 2: NO DATA TRK 3: NO DATA</p> </div>	<p>The V×810 has 3-track, high coercivity, bi-directional MSR heads. Initially, each track will indicate NO DATA.</p>

Table 9 System Mode Menu 2 (continued)


Display	Action
<p>SYS MODE TRK 1: VALID DATA TRK 2: VALID DATA TRK 3: VALID DATA</p>	<p>When you swipe a magnetic stripe card through the MSR slot, a successful read would indicate VALID DATA for each track.</p> <p>An unsuccessful read may indicate any one of the following:</p> <ul style="list-style-type: none"> • NO START • PARITY ERR
<p>TERMINAL INFO ► DIAGS AND LOGS ► SCREEN DIAG</p>	
<p>SYS MODE MENU 2 MEMORY FUNCTIONS F2 TERMINAL INFO F3 CLOCK F4</p> <p>↑ ↓</p>	<p>To view device configuration information, select TERMINAL INFO (F3).</p> <p>To abort any action at any step, press CANCEL.</p>
<p>SYS MODE MENU SYSTEM INFO F2 DIAGS AND LOGS F3</p>	<p>To perform system diagnostic tests and view log information, select DIAGS AND LOGS (F3).</p>
<p>SYS MODE DIAGS SCREEN DIAG F2 IPP DIAG F3</p> <p>↑ ↓</p>	<p>To perform a diagnostic test on the screen, select SCREEN DIAG (F2).</p>
	<p>A successful screen test is indicated by all 128 x 128 pixels being shaded BLACK.</p> <p>Any part of the screen that is not shaded black indicates defective pixels.</p>

Table 9 System Mode Menu 2 (continued)

Display	Action
TERMINAL INFO ► DIAGS AND LOGS ► IPP DIAG	
<div style="border: 1px solid black; padding: 5px;"> <p>SYS MODE MENU 2 MEMORY FUNCTIONS F2 TERMINAL INFO F3 CLOCK F4</p> <p>↑ ↓</p> </div>	<p>To view device configuration information, select TERMINAL INFO (F3).</p> <p>To abort any action at any step, press CANCEL.</p>
<div style="border: 1px solid black; padding: 5px;"> <p>SYS MODE MENU SYSTEM INFO F2 DIAGS AND LOGS F3</p> </div>	<p>To perform system diagnostic tests and view log information, select DIAGS AND LOGS (F3).</p>
<div style="border: 1px solid black; padding: 5px;"> <p>SYS MODE DIAGS SCREEN DIAG F2 IPP DIAG F3</p> <p>↑ ↓</p> </div>	<p>To perform a diagnostic test on the internal PIN pad, select IPP DIAG (F3).</p>
<div style="border: 1px solid black; padding: 5px;"> <p>INTERNAL PIN PAD IPP8 EMUL01A 07/05 0D SN: 0000000000000000 MODE: VISA BAUD: 1200</p> <p style="text-align: right;">RESET F3 EXIT F4</p> </div>	<p>To perform a diagnostic test on the internal PIN pad, select IPP DIAG (F3).</p> <p>To reset the internal PIN pad settings, select RESET (F3).</p> <p>To exit this option, select EXIT (F4).</p>
TERMINAL INFO ► DIAGS AND LOGS ► REMOTE DIAGS	
<div style="border: 1px solid black; padding: 5px;"> <p>SYS MODE MENU 2 MEMORY FUNCTIONS F2 TERMINAL INFO F3 CLOCK F4</p> <p>↑ ↓</p> </div>	<p>To view device configuration information, select TERMINAL INFO (F3).</p> <p>To abort any action at any step, press CANCEL.</p>
<div style="border: 1px solid black; padding: 5px;"> <p>SYS MODE MENU SYSTEM INFO F2 DIAGS AND LOGS F3</p> </div>	<p>To perform system diagnostic tests and view log information, select DIAGS AND LOGS (F3).</p>

Table 9 System Mode Menu 2 (continued)

Display	Action
<pre> SYS MODE DIAGS REMOTE DIAGS F2 DEBUGGER F3 ↑ ↓ </pre>	<p>To perform remote diagnostic tests, select REMOTE DIAGS (F2).</p> <p>This option is reserved for VeriFone use only, and requires the loading of a Device Management Agent.</p>
TERMINAL INFO ► DIAGS AND LOGS ► DEBUGGER	
<pre> SYS MODE MENU 2 MEMORY FUNCTIONS F2 TERMINAL INFO F3 CLOCK F4 ↑ ↓ </pre>	<p>To view device configuration information, select TERMINAL INFO (F3).</p> <p>To abort any action at any step, press CANCEL.</p>
<pre> SYS MODE MENU SYSTEM INFO F2 DIAGS AND LOGS F3 </pre>	<p>To perform system diagnostic tests and view log information, select DIAGS AND LOGS (F3).</p>
<pre> SYS MODE DIAGS REMOTE DIAGS F2 DEBUGGER F3 ↑ ↓ </pre>	<p>To use the debugging tool, select DEBUGGER (F3).</p> <p>The debugging tool is included in the SDK, but is not stored in the terminal memory of a factory unit. It must be signed, downloaded, and authenticated before it can be used.</p>
<pre> SYS MODE FILE FILE GROUP nn </pre>	<p>Type the Group ID (valid values are 1 to 15) of the files you want to debug. Then press ENTER.</p>
<pre> LOAD DBMON.OUT </pre>	<p>This message is displayed when the debugger tool is run.</p>
<pre> SYSTEM MODE FILE GROUP nn PASSWORD ----- </pre>	<p>To continue, enter the required password.</p>

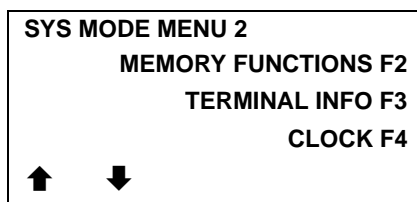
Table 9 System Mode Menu 2 (continued)

Display	Action														
TERMINAL INFO ► DIAGS AND LOGS ► ERROR LOG															
<div style="border: 1px solid black; padding: 5px;"> <p>SYS MODE MENU 2 MEMORY FUNCTIONS F2 TERMINAL INFO F3 CLOCK F4</p> <p>↑ ↓</p> </div>	<p>To view device configuration information, select TERMINAL INFO (F3).</p> <p>To abort any action at any step, press CANCEL.</p>														
<div style="border: 1px solid black; padding: 5px;"> <p>SYS MODE MENU SYSTEM INFO F2 DIAGS AND LOGS F3</p> </div>	<p>To perform system diagnostic tests and view log information, select DIAGS AND LOGS (F3).</p>														
<div style="border: 1px solid black; padding: 5px;"> <p>SYS MODE DIAGS ERROR LOG F2 TAMPER LOG F3</p> <p>↑</p> </div>	<p>To view the error logs, select ERROR LOG (F2).</p>														
<div style="border: 1px solid black; padding: 5px;"> <p>SYS MODE ERR LOG</p> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%;">TYPE</td> <td>1</td> </tr> <tr> <td>TASK</td> <td>2</td> </tr> <tr> <td>TIME</td> <td>030904092217</td> </tr> <tr> <td>CSPR</td> <td>4000030</td> </tr> <tr> <td>PC</td> <td>704201A0</td> </tr> <tr> <td>LR</td> <td>70420140</td> </tr> <tr> <td>ADDR</td> <td>00000000</td> </tr> </table> </div>	TYPE	1	TASK	2	TIME	030904092217	CSPR	4000030	PC	704201A0	LR	70420140	ADDR	00000000	<p>The error log screens display internal diagnostic information about the most recent unrecoverable software error.</p> <p>If you report a problem with your device, you may be asked to provide this information.</p>
TYPE	1														
TASK	2														
TIME	030904092217														
CSPR	4000030														
PC	704201A0														
LR	70420140														
ADDR	00000000														

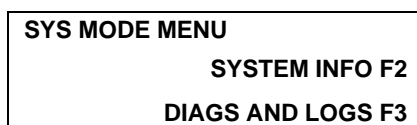
Table 9 System Mode Menu 2 (continued)

Display	Action
	<p>This first screen displays the following:</p> <ul style="list-style-type: none"> • TYPE (Error Type), where the error type code is: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> 1 = Data abort: attempt to access data at an invalid address 2 = Program abort: attempt to execute code at an invalid address • TIME (time of crash): clock time of the error in the format <i>YYMMDDhhmmss</i>, where <i>YY</i> = year, <i>MM</i> = month, <i>DD</i> = day, <i>hh</i> = hour, <i>mm</i> = minute, and <i>ss</i> = 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 <p>Note: LR may not always contain the current return address.</p> <ul style="list-style-type: none"> • ADDR (fault address): contains the illegal address that the application was trying to access • After making any notations, press the key under the down arrow (PF2) to view additional error log information, if shown.

TERMINAL INFO ► DIAGS AND LOGS ► TAMPER LOG



To view device configuration information, select **TERMINAL INFO (F3)**.
To abort any action at any step, press **CANCEL**.



To perform system diagnostic tests and view log information, select **DIAGS AND LOGS (F3)**.

Table 9 System Mode Menu 2 (continued)

Display	Action
<div style="border: 1px solid black; padding: 5px;"> <p>SYS MODE DIAGS ERROR LOG F2 TAMPER LOG F3 ↑</p> </div>	To view the tamper logs, select TAMPER LOG (F3) .
<div style="border: 1px solid black; padding: 5px;"> <p>TAMPER LOG 18-OCT-05 23:10 TAMPER CODE 0 00 04 10-OCT-05 12:05 TAMPER CLEAR 10-OCT-05 12:00 TAMPER CODE 2 00 00</p> </div>	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 DD-MON-YY format, while the time is displayed as a 24-hour clock.
TERMINAL INFO ► CLOCK	
<div style="border: 1px solid black; padding: 5px;"> <p>SYS MODE MENU 2 MEMORY FUNCTIONS F2 TERMINAL INFO F3 CLOCK F4 ↑ ↓</p> </div>	To set the device clock, select CLOCK (F4) . To abort any action at any step, press CANCEL .
<div style="border: 1px solid black; padding: 5px;"> <p>SYS MODE CLOCK INCREMENT HOUR F1 EDIT TIME F2 EDIT DATE F3 DECREMENT HOUR F4</p> </div>	To adjust the current time one hour forward, select INCREMENT HOUR (F1) . To adjust the time, select EDIT TIME (F2) . To adjust the date, select EDIT DATE (F3) . To adjust the current time one hour back, select DECREMENT HOUR (F4) .
<div style="border: 1px solid black; padding: 5px;"> <p>SYS MODE TIME CURRENT TIME: 10 : 01 : 50 NEW TIME: _ _ : _ _ : _ _</p> </div>	Selecting EDIT TIME (F2) , will prompt you to enter new time values. Enter the new time in HH:MM:SS format, then press ENTER .

Table 9 System Mode Menu 2 (continued)

Display	Action
<p>SYS MODE DATE CURRENT DATE: 06 / 15 / 07 NEW DATE: __ / __ / __</p>	<p>Selecting EDIT DATE (F3), will prompt you to enter new date values. Enter the new date in MM/DD/YY format, then press ENTER.</p>
<p>SYS MODE CLOCK TIME AND DATE 10 : 01 : 50 06 / 15 / 07</p>	<p>After adjusting the time or date, the new time and date setting is displayed.</p>

Menu 3 In this menu you can adjust screen contrast, change passwords, or perform IPP key loading.

Table 10 System Mode Menu 3

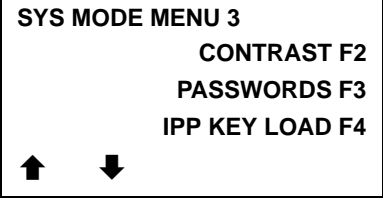
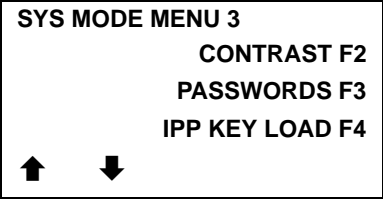
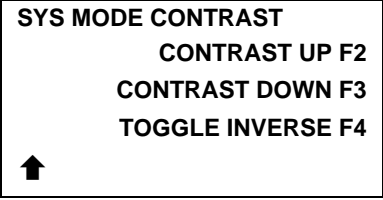
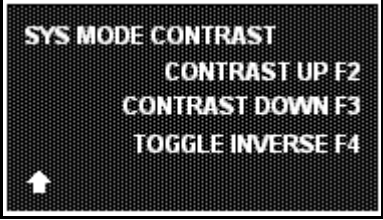
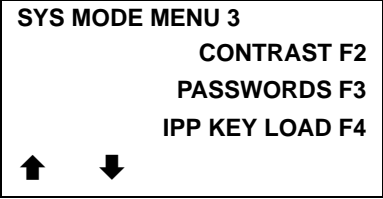
Display	Action
	<p>To adjust screen contrast, select CONTRAST (F2).</p> <p>To change passwords, select PASSWORDS (F3).</p> <p>To perform IPP key loading, select IPP KEY LOAD (F4).</p> <p>To go to the previous system mode menu, press PF1.</p> <p>To go to the next system mode menu, press PF2 or ENTER.</p>
CONTRAST	
	<p>To adjust screen contrast, select CONTRAST (F2).</p> <p>To abort any action at any step, press CANCEL.</p>
	<p>To increase screen contrast, select CONTRAST UP (F2).</p> <p>To decrease screen contrast, select CONTRAST DOWN (F3).</p>
	<p>To invert the screen, select TOGGLE INVERSE (F4).</p> <p>From having black text on a white background, the screen will have white text on a black background.</p> <p>To bring the screen back to its original setting, select TOGGLE INVERSE (F4) again.</p>
PASSWORDS	
	<p>To change passwords, select PASSWORDS (F3).</p> <p>To abort any action at any step, press CANCEL.</p>

Table 10 System Mode Menu 3 (continued)

Display	Action
<div style="border: 1px solid black; padding: 5px;"> <p>SYS MODE PASSWORD FILE GROUP nn F2 SYS MODE ENTRY F3</p> </div>	<p>To change the password for a file group, type the Group ID (valid values are 1 to 15) of the group whose password you want to change. Then select FILE GROUP nn (F2).</p> <p>To change the password for System Mode Entry, select SYS MODE ENTRY (F3).</p>
<div style="border: 1px solid black; padding: 5px;"> <p>SYS MODE PASSWORD GROUP nn PASSWORD -----</p> </div>	<p>To continue, enter the required password.</p> <p>The default group password is "Z66831." This is entered as: 1 ALPHA ALPHA 6 6 8 3 1, then press ENTER.</p>
<div style="border: 1px solid black; padding: 5px;"> <p>SYS MODE PASSWORD Gnn PLEASE TRY AGAIN</p> </div>	<p>This message appears if you enter an incorrect password.</p> <p>Press ENTER to try again. Re-enter your password.</p>
<div style="border: 1px solid black; padding: 5px;"> <p>SYS MODE PASSWORD Gnn NEW -----</p> </div>	<p>Enter the new password, then press ENTER.</p>
<div style="border: 1px solid black; padding: 5px;"> <p>SYS MODE PASSWORD Gnn AGAIN-----</p> </div>	<p>Re-enter the new password, then press ENTER.</p>
<div style="border: 1px solid black; padding: 5px;"> <p>SYS MODE PASSWORD Gnn PLEASE TRY AGAIN</p> </div>	<p>This message is displayed if the entry and re-entry of the new password does not match. Press ENTER to continue.</p>
<div style="border: 1px solid black; padding: 5px;"> <p>SYS MODE PASSWORD Gnn PASSWORD CHANGED</p> </div>	<p>This message is displayed upon successful changing of the password.</p>
IPP KEY LOAD	
<div style="border: 1px solid black; padding: 5px;"> <p>SYS MODE MENU 3 CONTRAST F2 PASSWORDS F3 IPP KEY LOAD F4 ↑ ↓</p> </div>	<p>To perform IPP key loading, select IPP KEY LOAD (F4).</p> <p>To abort any action at any step, press CANCEL.</p>

Table 10 System Mode Menu 3 (continued)

Display	Action
<p>SYS MODE PASSWORD GROUP nn PASSWORD -----</p>	<p>To continue, enter the required password. The default group password is “Z66831.” This is entered as: 1 ALPHA ALPHA 6 6 8 3 1, then press ENTER.</p>
<p>SYS MODE PASSWORD Gnn PLEASE TRY AGAIN</p>	<p>This message appears if you enter an incorrect password. Press ENTER to try again. Re-enter your password.</p>
<p>INTERNAL PIN PAD KEY LOADING MODE BYTES SENT 0 BYTES RCVD 0 END F4</p>	<p>A communication channel is opened through COM2 to the IPP to allow key loading. The number of bytes sent and received is displayed. Press END (F4) when done. The system will restart.</p>
<p>KEY LOADING STOPPED: TIMER EXPIRED</p>	<p>This message is displayed if no data is sent within 1.25 minutes. Press END (F4) to continue. The system will restart.</p>



File Authentication

This chapter discusses the VeriShield file authentication security architecture, VeriShield 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, system deployers, site administrators, or entities authorized to download files to the Vx810 (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 Vx810 using the VeriShield File Signing Tool (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 Vx810 uses the VeriShield security architecture, which has both physical and logical components. The logical security component of the VeriShield architecture, which is part of the 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 Vx810 to logically secure access to the device by controlling who is authorized to download application files to that device. 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 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 the Vx810.

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** 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.

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

Table 11 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 V^x810 clients – either internally within VeriFone or externally to sponsors.

All certificates issued by the VeriFone CA for the V^x810 platform, and for any VeriFone platform with the VeriShield 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

- A **sponsor certificate** certifies a client's sponsorship of the device. 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 device.

-
- A **signer certificate** certifies the right to sign and authenticate files for devices 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 device, 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 device sponsor has authorized to sign, download, and authenticate applications to run on the sponsor's device.

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 Vx810, 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 device'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 device for deployment.

Development Process

In this process:

- 1** The application developer creates an application file.
- 2** The developer assigns a name to the application file.
- 3** The application file becomes a required input for the VeriShield File Signing Tool (included in the SDK).
- 4** The default certificate (VXSIGN.CRT) and default key (VXSIGN.KEY) included in the SDK are inputs for the VeriShield File Signing Tool.
- 5** Using the application file, default certificate, and default key, the VeriShield File Signing Tool creates a signature file (*.p7s).
- 6** The signature file and the original application file are loaded onto a development device, where the following actions occur:
 - a** The device's operating system searches for signature files.
 - b** When a signature file is found, the operating system 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.

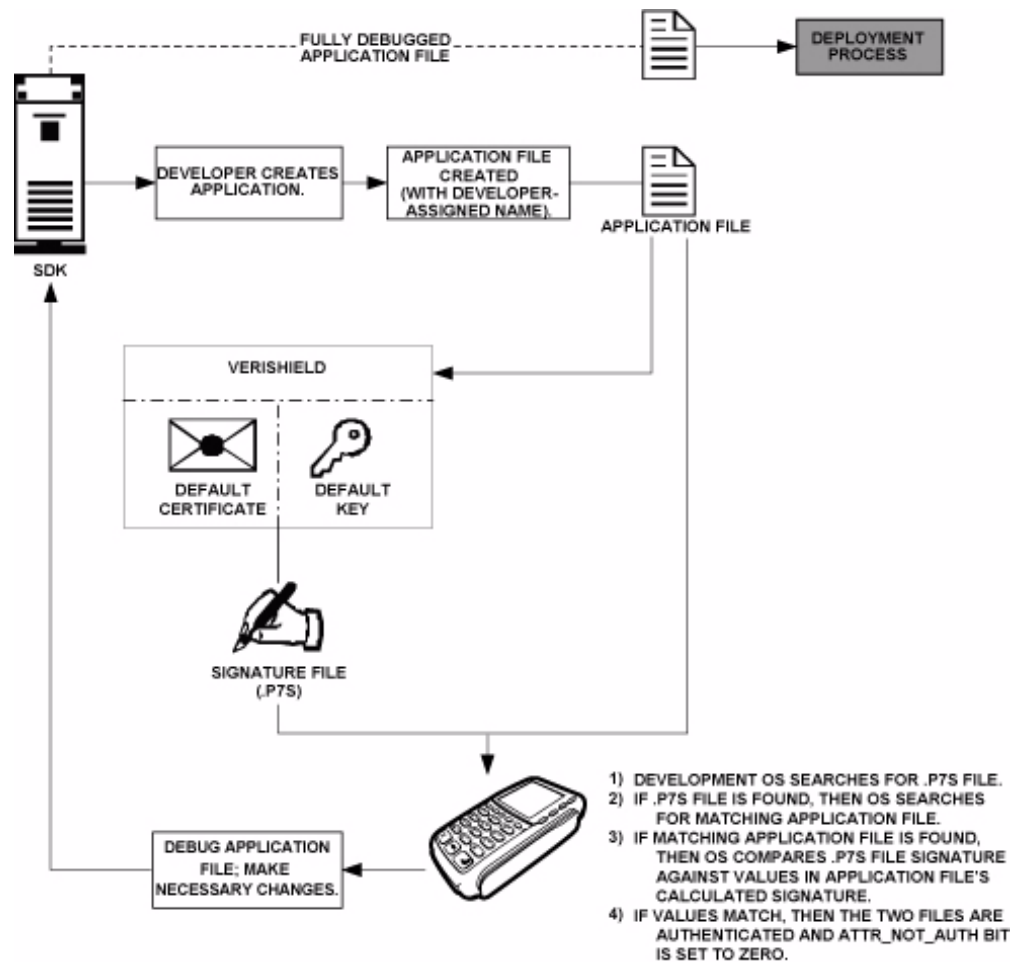


Figure 17 The Development Process

Pre-Deployment Process

In this process:

- 1 A sponsor goes to the VeriFone CA Web site and requests certificates for deployment devices.
- 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.

The following diagram describes the pre-deployment process.

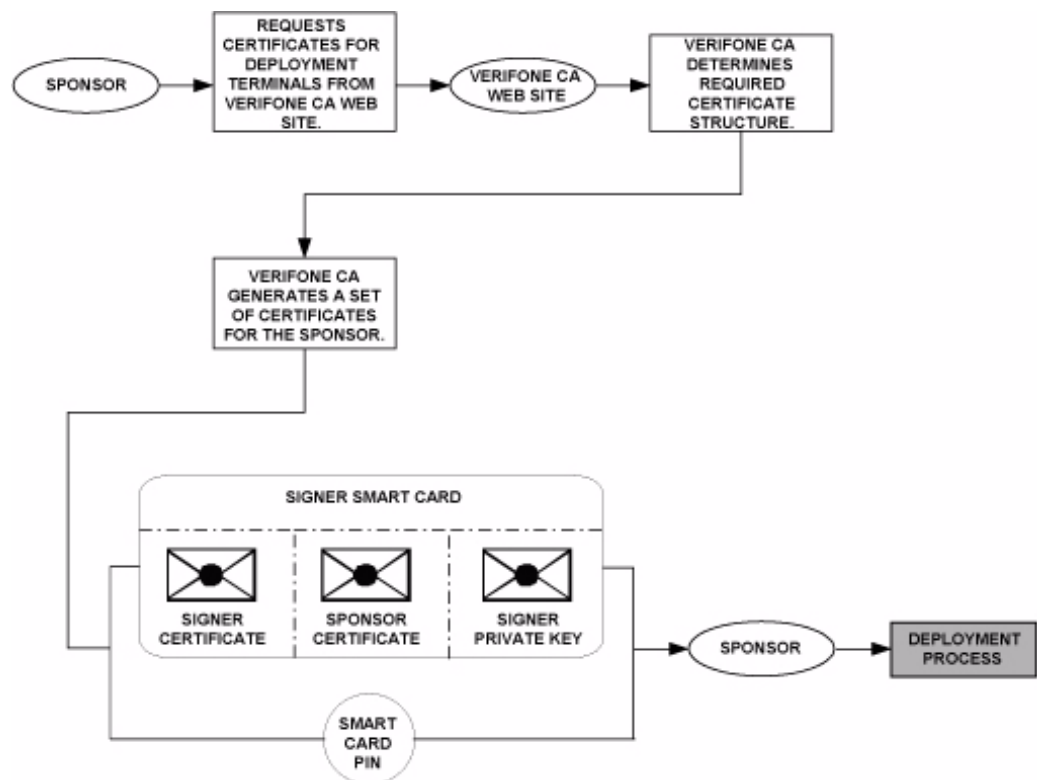


Figure 18 The Pre-Deployment Process

Deployment Process

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.
- 2 VeriShield extracts the signer key, signer certificate, and sponsor certificate from the smart card.
- 3 VeriShield uses the extracted data, along with the application file, to create a signature file (*.p7s).
- 4 VeriShield 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 onto a deployment device, where the following actions occur:
 - a The device's operating system searches for signature files.
 - b If a signature file is found, the operating system 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 device (otherwise, the executable remains stored in the device's memory but is not allowed to run).

The following diagram describes the deployment process.

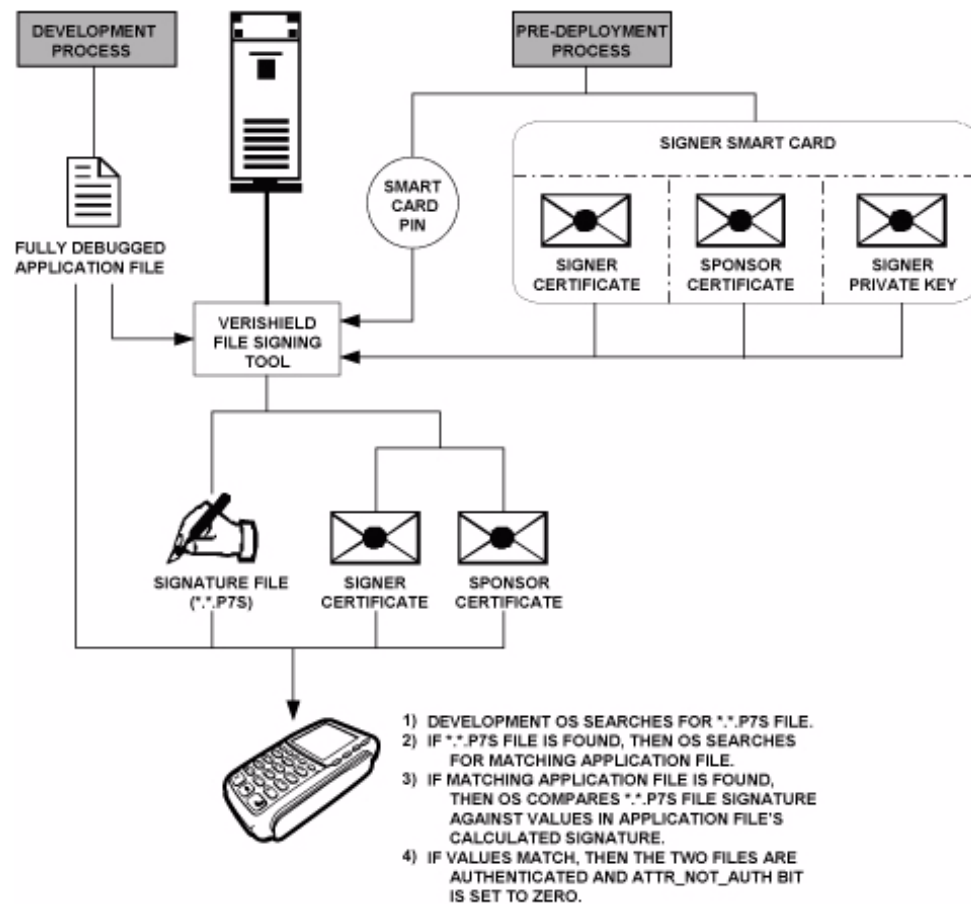


Figure 19 The Deployment Process

Planning for File Authentication

File authentication is an integral part of every V^x810 device. To safeguard the device'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 device.

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 below.

Table 12 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 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 security architecture.

In most cases, application designers make these decisions based on specifications provided by the device 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 V^x810 each time you perform an application download.

When the file authentication module detects a new signature file after a device 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 device's memory, but is not authenticated or allowed to run on the device until the signature files for the application executable files are processed by the file authentication module after a subsequent download procedure and device restart.

Determine Successful Authentication

To ensure the Vx810's logical security, never assume that a target file was authenticated simply because it downloaded onto the Vx810 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 device 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 device 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 device beeps as an alert.

An application 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 that will confirm that all of the files it uses is successfully authenticated on download completion, and when the application executes the first time following a restart.

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 device, the ATTR_NOT_AUTH bit is automatically set to 1. If the modified file is an executable, it is no longer allowed to run.



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.

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 device 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.

To manage hierarchical relationships between certificates, certificate data is stored in device's 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 device's certificate tree. This requirement can be met in two ways:

- The higher-level certificate may have already been downloaded onto the device 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 onto each V^x810 device upon manufacture. When you take a new V^x810 device out of its shipping carton, certificate data is already stored in the device's certificate tree. In this just-out-of-the-box condition, the V^x810 is called a development device.

Typically, a sponsor requests an additional set of digital certificates from the VeriFone CA to establish sponsor and signer privileges. This additional set of certificates are downloaded onto the V^x810 when the device is being prepared for deployment and replaces the default certificate. When this procedure is complete, the V^x810 is called a deployment device.

Adding New Certificates

When you add a new certificate file to a V^x810, the file authentication module detects it by filename extension (*.crt). On restart, the device attempts to authenticate the certificate under the authority of the resident higher-level certificate stored in the device'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 device's certificate tree depends on if 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 device's certificate tree. The corresponding certificate file (*.crt) is deleted from that file group's SRAM.
- 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.

Certificate Tree Restoration

The Verix V OS in the V^x810 supports certificate tree restoration. When a certificate tree is restored, any custom certificate is cleared. The DUKPT PIN entry limit bucket is also cleared.

Development Devices

A development device is a Vx810 still maintaining the original factory set of certificates in its certificate tree. This set of certificates includes several higher-level system certificates and a special client certificate called a default signer certificate.

In the development device, the level of logical security provided by the file authentication module is minimal, even though applications must still be signed and authenticated before they can run on the device. In most application development and test environments, tight security is not required, and the flexibility offered by the Vx810 development device is more important.



NOTE With the factory set of certificates stored in the device's memory, anyone who has the Vx810 SDK and VeriShield File Signing Tool can generate valid signature files for downloading and authenticating files on the Vx810 platform.

Deployment Devices

While the application development process is being completed and while the new application is being tested on a development device, a sponsor can order specific sponsor and signer certificates from the VeriFone CA to use to logically secure sponsor and signer privileges when the Vx810 is prepared for deployment.

Customer-specific sponsor and signer certificates are usually downloaded onto a device 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.

When the sponsor and signer certificates are downloaded and successfully authenticated, the device 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 device. Additional certificates can be obtained from the VeriFone CA anytime to implement new sponsor and signer relationships in deployment devices. VeriShield allows for multiple sponsors and signing certificates in a device. This allows the flexibility of unique signatures for each executable or data files.

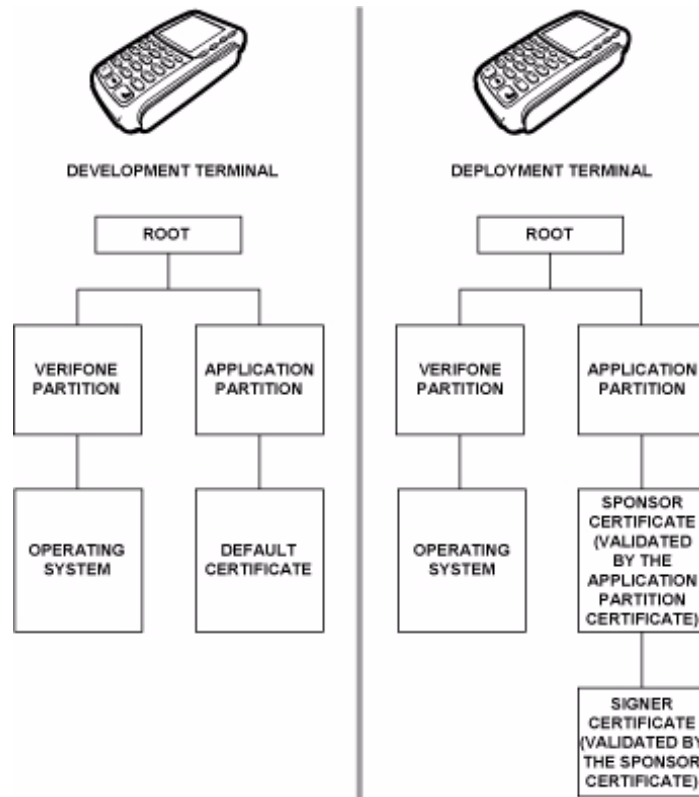


Figure 20 Certificate Trees in Development and Deployment Devices

Permanency of the Certificate Tree

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

The certificate tree file is stored in a reserved area of non-volatile memory and is therefore relatively 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 devices than deployment devices.

Table 13 Differences Between Required Inputs

Development Device	Deployment Devices
<p>Manufacturing inputs to the file signing process are included, together with the VeriShield File Signing Tool in the Vx810 SDK. These inputs make it possible for anyone who has the Vx810 SDK to sign and authenticate files.</p> <p>The following two factory inputs are required for the file signing process, in addition to the application files you want to sign and authenticate:</p> <ul style="list-style-type: none"> • Default signer certificate, with the filename VXSIGN.CRT • Default signer private key, with the filename VXSIGN.KEY <p>Note: A default signer password is not a required entry when using the VeriShield File Signing Tool to sign files for a Vx810 development device.</p>	<p>The required inputs to the VeriShield File Signing Tool must be obtained from the VeriFone CA to logically secure the sponsor and signer privileges for the device.</p> <p>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:</p> <ul style="list-style-type: none"> • Customer signer certificate: This unique certificate is a required input for the VeriShield File Signing Tool and must be downloaded onto the device along with the signature files and target application files to authenticate, unless already downloaded onto the device in a previous operation. • Customer 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 the VeriShield File Signing Tool, but does not have to be downloaded onto the device. • Customer 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 the VeriShield File Signing Tool, but it does not have to be downloaded onto the device. <p>Note: The customer sponsor certificate, which authenticates the customer signer certificate, is usually downloaded onto the device with the customer signer certificate, but it is not a required VeriShield File Signing Tool input when signing files.</p>

Replace a Sponsor Certificate

A sponsor may need to clear the current sponsor certificate from a device 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 device to the development state by:

- Deleting the current sponsor and signer certificates from the device's application partition.
- Restoring the default certificate to the device's application partition.



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

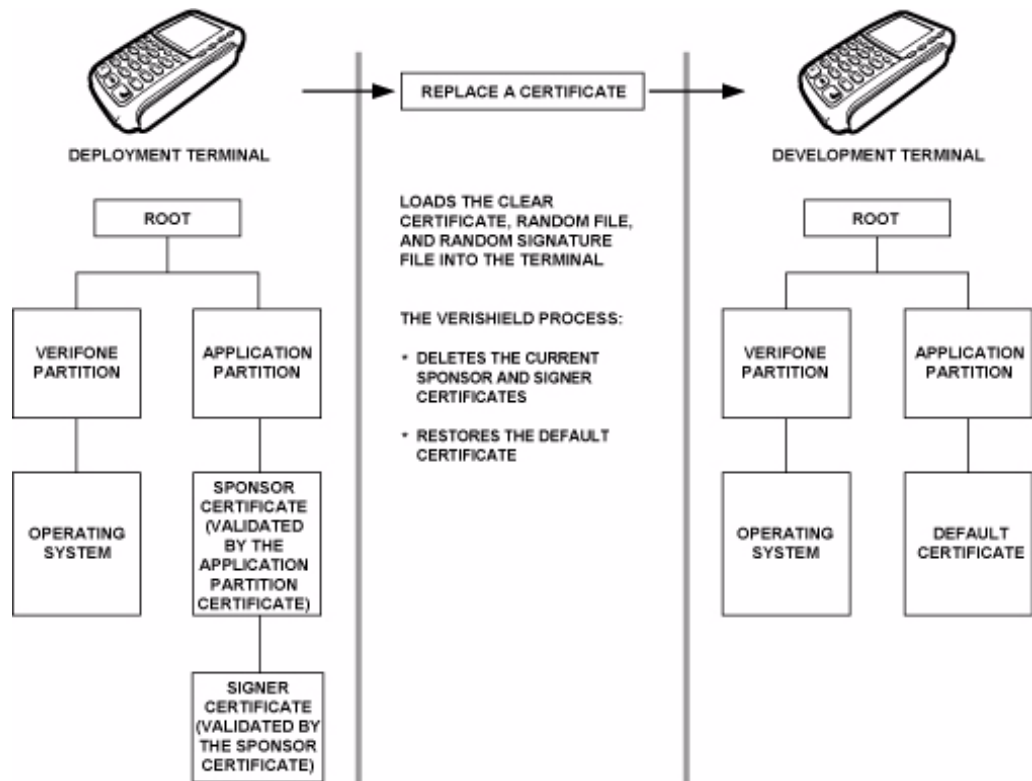


Figure 21 Certificate Replacement Process

File Authentication and the File System

Application Memory Logically Divided Into File Groups

The memory of a V^x810 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 into a device's memory and prevent these applications from overlapping or interfering with each other's operation.

There are a total of 16 file groups. 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.

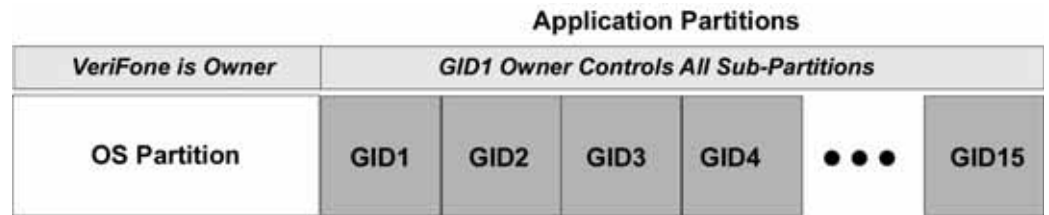


Figure 22 Vx810 Application Memory Partitions



NOTE The Vx810 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

Here are some important Vx810 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 device, 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 device 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 onto GID1 is always the primary application for the device. This application is owned by the primary device sponsor (sponsor A) in cases where there are multiple sponsors.
- The Group 1 application controls any and all secondary applications stored in device's 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 device, each `.OUT` and 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 device, the signature files for the respective applications must be downloaded, together with the corresponding target files, into the specific file groups for which the applications are authorized. If an application is downloaded onto a group for which it is not authorized, file authentication for that application fails.

If, for example, Application B is downloaded onto GID4, where it is authorized to run, but the signature files for all Application B executable files are downloaded onto 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 SRAM or Flash ROM of a File Group

All `*.p7s` files are loaded onto SRAM and contain flags that indicate if the file to verify is stored in SRAM or flash ROM. A signature file must know if its matching application file is stored in SRAM or flash ROM. 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 file system as the target file it authenticates. That is, if the target file is stored in the flash ROM, the signature file is also stored in the flash ROM; if the target file is stored in SRAM, the signature file is also stored in SRAM.

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.



Normally signature files are retained in the device 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 you intend to perform back-to-back downloads, as described in [Chapter 6](#), all signature files must be retained in the Vx810's application memory, together with the target application files they authenticate.



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 V Operating System Programmers Manual.

Restrictions on Downloading Different File Types

A typical application download includes a variety of different file types. The following restrictions describe how you can download different kinds of files to the Vx810 and how files are stored in its file system:

Table 14 Download File Extensions

File Type	Restriction
Certificate (*.crt)	<i>Must</i> be downloaded onto the SRAM of the target file group (GID1–GID15) selected in system mode.
Signature (*.p7s)	<i>Must</i> be downloaded onto the SRAM of the target file group (GID1–GID15) selected in system mode.
Operating system	<i>Must</i> be downloaded onto Group 1 SRAM. When the OS files, related certificates and signature files are authenticated, they are automatically moved from Group 1 SRAM 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 SRAM.

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 VeriShield File Signing Tool. This section discusses the use of this tool, which is included in the V^x810 Verix V DTK.

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

You can run the 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 use the FileSign dialog box to make the required entries.



NOTE

The file signing process for operating system files is done for V^x810 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.

System Requirements

The VeriShield 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

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 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 VeriShield 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 SRAM (default location) or in the flash ROM file system. 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.

The following image shows the FileSign dialog box.

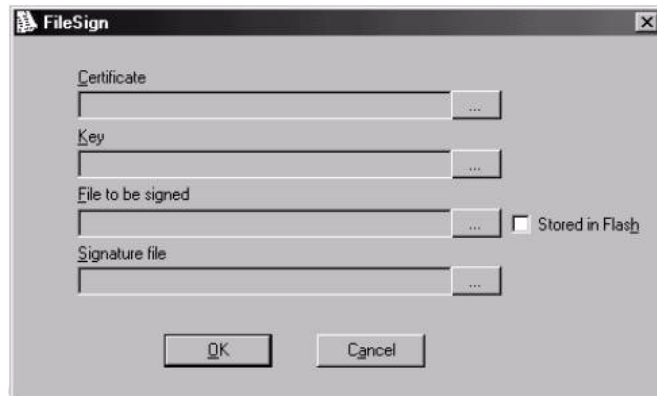


Figure 23 FileSign Dialog Box



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 device, but not for a development device.

Command-Line Entries

The following table lists the switches that make up the command-line mode syntax for the VeriShield File Signing Tool.

Table 15 Command-Line Mode Switches for VeriShield File Signing Tool^a

Switch	Description	Requirements
-C, -c	Signer certificate file name (*.crt).	Required input for development devices and deployment devices. Use the VXSIGN.CRT default signer certificate for development devices. Use the signer certificate issued by the VeriFone CA for deployment devices.
-K, -k	Signer private key filename (*.key).	Required input for development devices and deployment devices. Use the VXSIGN.KEY default signer private key for development devices. Use the signer private key provided by the VeriFone CA for deployment devices.
-P, -p	Signer password for decrypting the signer private key.	Required input only for deployment devices. The VeriFone CA issues and securely conveys this password to an authorized signer.

Table 15 Command-Line Mode Switches for VeriShield File Signing Tool^a

Switch	Description	Requirements
-F, -f	Name of the application file to sign (*.out, *.lib, or other file type).	Required for development devices and for deployment devices.
-S, -s	Name of the signature file (*.p7s) for the VeriShield File Signing Tool to generate for the target application file.	Required for development devices and for deployment devices.
-L, -l	Specifies to store the target application file to sign and authenticate in the flash ROM (drive F:) file system. If you do not use this switch to specify flash ROM as the target file destination, it is stored by default in the SRAM file system (drive I:).	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 onto the target file group's SRAM. 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 flash ROM (F:), its *.p7s file is moved into the flash ROM file system. If, however, you set the *FA variable in the file group's CONFIG.SYS file to 0, all signature files are deleted from SRAM 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.

Command-Line Mode Syntax Example

In the following VeriShield File Signing Tool command-line entry example, note that the syntax used applies to a Vx810 development device with the factory set of certificates, and not to a deployment device. There are two differences:

- The default signer certificate and default signer key file names provided by VeriFone as part of the Vx810 SDK are entered on the command line instead of customer-specific customer signer certificate and customer signer private key file names.
- The switch for signer password (`-P password`) is not used, because a customer signer password is only required to sign and authenticate files for Vx810 deployment devices being prepared for deployment.

Please note also how the command-line mode switches 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 ROM file system instead of the target group's (default) SRAM file system. (The target group for the download must be selected from system mode when the download is performed.)
- The `-f` switch indicates that the application file "file.out" must be signed by the VeriShield File Signing Tool.

Executable files, such as *.out and *.lib files, must always be signed if they are to run on the device 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 default signer certificate to be used for file authentication with the development device, "vxsign.crt."
- The `-k` switch is followed by the name of the default signer private key file, vxsign.key. A signer private key is a required input to the file signing process for development devices and for deployment devices.

Graphical Interface Mode

When you execute the the VeriShield File Signing Tool file, the FileSign dialog box is displayed.

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 flash ROM memory upon download to the device, 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 VeriShield File Signing Tool and generate the signature file; otherwise, press ALT+A or click CANCEL to exit the the VeriShield File Signing Tool.

When the necessary signature files are generated to authenticate the application or applications on the V^x810, perform the application download procedure.

For more information about file authentication within the context of specific download procedures, refer to [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 V^x810.
- Prepare the V^x810 for deployment.
- Maintain V^x810 installations in the field.
- Transfer data to/from V^x810 devices.

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 V^x810 has ports that allow connection to a network or to other VFI devices (for back-to-back downloads).

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 device receiving data. The term upload describes the process of a device sending data.

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

- **Host computer downloads:** Applications, operating systems or OS updates, and associated files transfer from a host PC to the V^x810.
- **Back-to-back downloads:** Applications and associated files transfer from one VFI device to a V^x810 device.

Download Methods

The following three methods are available for file and data downloads through the V^x810 download and upload procedures:

- **Direct downloads:** Files or data transfer directly from the sending system (a host computer) to the receiving V^x810 device. A special cable, VPN 08362-01-R, is used to connect to the RS-232 serial port of the host computer.
- **Back-to-back downloads:** Files and data transfer from a sending VFI device to a receiving V^x810 device.

- **USB downloads:** Files and data are transferred from a USB-connected drive. The device searches for the VeriFone.zip file on the drive and downloads data from it.

NOTE

The device will automatically download the file VeriFone.zip from a USB flash drive without the user having to go through [System Mode](#) under the following conditions:

- The USB flash drive is connected before the device is turned on.
- The USB flash drive is inserted when the initial **DOWNLOAD NEEDED** message is displayed.

In both cases, the **USB DOWNLOAD COMPLETE** message will appear on the screen after the VeriFone.zip file has been downloaded.

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 V^x810:

- **VeriCentre DMM:** Multi-user environment for software downloads. DMM supports Windows NT clients and has a sophisticated database to manage up to 100,000 devices. The V^x810 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 device records.

NOTE

The Veri V OS in the V^x810 will support all non-modem-related VeriCentre operations, including full/partial downloads and compressed downloads, but not VeriCentre-initiated downloads because this requires a modem.

- **DDL.EXE:** Downloads files and data from a development system or another host computer, directly to a V^x810 over a serial cable connection. DDL.EXE is a Windows program included in the Verix V DTK (Verix V 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 the two devices is required. This data transfer procedure, invoked from within system mode, is handled by the OS software and firmware of the sending and receiving V^x810 devices.

Download Content

In general, you can download files and data to a V^x810. 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 device's basic processes and functions. Files that belong to the OS are stored in a reserved area of the device's memory.

A complete OS is downloaded onto each V^x810 during the manufacture. If necessary, download newer versions during application development, or when preparing for deployment to on-site devices.

- **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.

V^x810 applications can be developed by VeriFone, customers, or third parties on customer request. One or more applications must be downloaded onto the V^x810 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 V^x810 is file authentication. For an executable to run on a V^x810, it must be authenticated by the VeriShield file authentication module. For more information 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 onto the device together with the application files to authenticate.

- **Device configuration settings:** Files or records that contain various types of data can also be downloaded onto a V^x810, including CONFIG.SYS variables, passwords for accessing protected system mode functions, and the current date and time (For more information on device configuration settings, see [Chapter 4](#)).

Full and Partial Downloads

When preparing to initiate a download procedure, choose either a full or partial download and the COM 2 port, through the system mode 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.

Table 16 Types of Full and Partial Downloads

Download Type	Description and Effects	Download Methods Supported
Full application download	<p>An entire application, including all executables and data files, transfers from one system to another in a single operation.</p> <p>Files related to the file authentication process and device configuration settings can be included in a full application download. During this process, SRAM is cleared.</p> <p>Following a full application download, the device restarts and the file authentication module is invoked. If application files are authenticated and config.sys *GO variable is set, then the application executes.</p>	<ul style="list-style-type: none"> • Direct downloads • Back-to-back downloads
Partial application download	<p>A subset of application executables, font files, or data files transfer from one system to another to modify or update an existing application.</p> <p>Files related to file authentication and device configuration settings can be included in a partial application download. During this process, SRAM is <i>not</i> cleared.</p> <p>Following a partial application download, the device does not restart and returns control to system mode or the issuing application. The file authentication module is not invoked, nor are any applications allowed to execute, until the device is manually restarted from within system mode.</p>	<ul style="list-style-type: none"> • Direct downloads <p>Note: Partial back-to-back downloads are <i>not</i> supported.</p>

Table 16 Types of Full and Partial Downloads (continued)

Download Type	Description and Effects	Download Methods Supported
Full operating system download	<p>An <i>entire</i> OS version transfers from a host PC to the Vx810.</p> <p>Files related to file authentication and device configuration settings can be included in a full OS download. During this process, SRAM is cleared.</p> <p>Following a full OS download, the device restarts and the file authentication module is invoked. If the OS files are authenticated, the new OS updates (replaces) the existing OS.</p> <p>Application files stored in the memory area where the OS downloads (Group 1) are erased.</p>	<ul style="list-style-type: none"> • Direct downloads <p>Note: Full back-to-back OS downloads are <i>not</i> supported.</p>
Partial operating system download	<p>Either an <i>entire</i> or a <i>partial</i> OS version transfers from a host PC to the Vx810 device.</p> <p>Files related to file authentication and device configuration settings can be included in a partial OS download.</p> <p>Following a partial OS download, the device does not restart and returns control to system mode or the issuing application. The file authentication module is not invoked, and the new OS is not processed until you manually restart the device from within system mode. If the new OS is authenticated, it updates (replaces) the existing OS.</p> <p>Application files stored in the memory area where the OS downloads into (Group 1) are retained.</p>	<ul style="list-style-type: none"> • Direct downloads <p>Note: Partial back-to-back operating system downloads are <i>not</i> supported.</p>

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 devices on-site.
- Full OS downloads are usually performed by VeriFone at the factory and, on occasion, by those who deploy devices on-site to upgrade older devices 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 device configuration settings in a V^x810 and return control to the main application.
- Full downloads restart the device; partial downloads return control to system mode or the issuing application. OS and application downloads can be combined. The file authentication module is not invoked until the device is restarted following the download procedure.

Support for Multiple Applications

The V^x810 architecture supports multiple applications. This means that more than one application can reside in device's memory, and that more than one application can run (execute) on the device.

The application memory of the V^x810 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 V^x810 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 device's 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 onto a specific file group, along with any related files. Select the target file group for the download using system mode 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 device. 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 V^x810 operating system controls physical access to GIDs 1–15 using password-protected system mode functions.

To download data into a specific file group, first enter system mode 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 system mode, 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 SRAM and Flash ROM Memory

The V^x810 application memory partition has two separate file systems:

- SRAM (battery-backed volatile memory, also called SRAM), partition designator I:
- Flash ROM (non-volatile memory), 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 SRAM and others into flash ROM.
- There are also rules that restrict which types of files you can download and store in a file system (SRAM or flash ROM).

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 SRAM.

In a typical download procedure, all files are loaded onto the SRAM file system of the target group selected in system mode. Specific files included in the download package must be redirected, as necessary, to the flash ROM file system of the target group or to the SRAM or flash ROM file system of another file group.

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

Defragment Flash ROM for Application Downloads

Before performing an application download, defragment the device's flash ROM memory. To ensure the best results when performing back-to-back downloads, defragment the flash ROM memory of both the sending and receiving devices. A system mode procedure is also available for clearing the SRAM or flash ROM memory, either entirely or for a specific file group, to prepare a V^x810 for a clean download.

NOTE



The flash ROM defragment operation is not necessary for a V^x810 in a just-out-of-the-box condition. In this case, the device's flash ROM file system is still in factory-new condition.

Redirection of Files During Application Downloads

You can download application files into SRAM or flash ROM memory. By default, files downloaded onto a specific file group are stored in the SRAM of that group. To store a file in the flash ROM memory of that file group, provide instructions to redirect the file to flash ROM 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 (memory area) to download files to.

- Partition designator I: is SRAM: This is the system mode default for downloads.
- Partition designator F: is flash ROM.

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 SRAM of the target group to the flash ROM 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 flash ROM memory (F:) 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 SRAM (Drive I:) 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 SRAM.

For example, the following batch download list loads the executable code file FOO.OUT into the SRAM of the selected file group (default Group 1). Because the signature file, FOO.P7S is included, FOO.OUT is also authenticated when the device 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 flash ROM. Because it follows the inserted zero-length SETDRIVE.I file, GOO.DAT downloads into Group 1 SRAM.

```
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 SRAM or flash ROM file systems, and in specific file groups in a single batch download operation.



You can only use zero-length SETDRIVE.x files for batch application direct downloads, and 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 system mode setting for performing downloads. Using the system mode 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 SRAM 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 system mode. If no number is added to the SETGROUP filename, SETGROUP.1 (GID1) is assumed.

Restrictions on File Redirection

The V^x810 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 onto GID1.
- Because of the way file groups are managed in the V^x810 file system, only two schemes are available for redirecting files during a batch application download:
 - If using system mode 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 system mode 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 SRAM, GOO.OUT into GID2, and COMN.LIB shared library into GID15. When the device 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 device 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 direct downloads, and 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 V^x810 SDK allows you to change the default drive and file group for a direct download by preceding the filenames on the DDL command line with a special filename. The syntax is as follows:

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

where, *drive letter* is I: for SRAM, (default) or F: for flash ROM, and

```
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 flash ROM of the selected target group and the data file `card.dat` into Group 15 SRAM. (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 SRAM and not into flash ROM memory or into another file group.

OS files are downloaded onto Group 1 SRAM 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.

- For full OS downloads, the redirection of OS files into Group 0 is performed automatically, after the device restart, and as part of the download procedure.
- For partial OS downloads, OS files are redirected from the SRAM of Group 1 into Group 0 on manual device restart by selecting the appropriate system mode menu option.

A downloaded OS is processed and authenticated while stored in Group 1 SRAM. 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 device – in both file systems and in all file groups – transfer to the receiving device in a single operation.

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

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 device. This redirection process is transparent during the download.

Briefly, all files initially download into SRAM, and are redirected based on the directory and subdirectory names of the sending device's file system. Signature files must always be authenticated in SRAM. If the target file that the signature file authenticates is stored in flash ROM, the signature file is moved to flash ROM 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 device. If the *FA variable is present in the Group 1 CONFIG.SYS file of the sending device, it must be set to 1 to retain all previously downloaded signature files.

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

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 onto and allowed to run on a Vx810, the file must be digitally signed on the download computer using the VeriShield 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 device 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 device. 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 onto the SRAM 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 device's 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 SRAM 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 V^x810 deployment device for deployment. That is, a sponsor certificate and a signer certificate are downloaded in batch mode to GID1 SRAM of the receiving device, together with the application to authenticate.
- A signature file is generated for each executable that comprises the application on the download computer using the VeriShield File Signing Tool, with the signer certificate, signer private key, and signer password as required inputs. These signature files are also downloaded onto the receiving device.

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 V^x810 deployment device in batch mode.
- 2 When the device restarts after the download, the file authentication module searches the SRAM-based 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 SRAM 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 device 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 device beeps three times. The routine 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 also fails, resulting to an application not authenticated and not allowed to execute on the device.

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

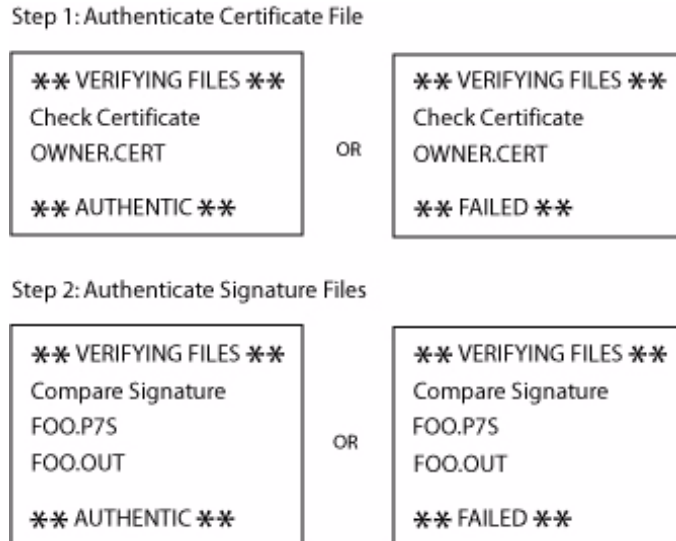


Figure 24 Display Prompts During the File Authentication Process

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 device beeps three times. The routine 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 device 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 are successfully authenticated.

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

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 device file system.

- 6 Certificate files and signature files are retained in the SRAM file system until the file authentication process is complete. These special files are 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 device memory. This is also true for a signature file retained in device 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 device restart.

- 7 When all certificates and signature files are processed and special files are deleted or redirected as required, the device 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 V^x810 file system.

By inserting zero-length SETDRIVE.x and SETGROUP.n files into a download list, you can specify which drive (x = I: SRAM or F: flash ROM) 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 V^x810 file system.

For example, if the device 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 device.

Chapter 5 discussed how signer certificates are required inputs to the VeriShield File Signing Tool when preparing a deployment device. Each signature file generated under that signer certificate contains a logical link that allows the application to authenticate and run on the device only if the signature files and corresponding target files are downloaded onto the target GID.

Although you can store files in any file group simply by selecting the target group in system mode, 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 device.

Download an Operating System Update Provided by VeriFone

Because the operating system software for the V^x810 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 V^x810 device using a PC-to-device direct download procedure. OS files cannot be downloaded onto a V^x810 device in a back-to-back operation.

The file authentication procedure for OS downloads is much the same as that for 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 device 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 SRAM. If you select a target group other than Group 1, the operation fails.
- Before initiating an OS download, either full or partial, ensure that enough memory space is available in Group 1 SRAM to temporarily store the OS files and that any application files can also be stored in Group 1.
- If a full OS download was selected in system mode, the device 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 system mode, the operating system returns control to system mode after the download completes. To process the new OS, you must manually restart the device by selecting the appropriate system mode 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 device's certificate tree, and as signature files for corresponding OS files are detected and authenticated.

- While the new OS is being processed, there is no visible indication on the device display of the progress of processing. When the new OS is processed (this usually takes a few moments), the device restarts automatically and the OS download procedure is complete.

CAUTION

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

**File Authentication
for Back-to-Back
Application
Downloads**

When performing a back-to-back application download between two V^x810 devices, the file authentication process on the receiving device is similar to an application download from a host computer to a standalone V^x810 device. 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 system mode in both devices, select Group 1 as the target group for both devices, and enter all required passwords.
- All signature files required to authenticate the download applications must reside in the memory of the sending device. They must not be deleted through the *FA variable being cleared to 0 on previous downloads.
- Any sponsor and signer certificates downloaded onto and authenticated on the sending device are stored in the certificate tree of that device. When you perform a back-to-back download, certificate files are reconstructed from the data present in the sending device's certificate tree.
- All certificates transfer to Group 1 SRAM on the receiving device, except for the highest-level platform root certificate, which can never be transferred to another device.
- When certificates are detected by the file authentication module of the receiving device, 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 device. Then all signature files are checked.

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

“Synchronized” means that the certificate tree of the receiving device can be no more than one revision out-of-sync with the certificate tree on the sending device or the files on the receiving device 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 device.

- When the back-to-back download completes and all certificates and signature files authenticate, the receiving device restarts. If the name of the *GO application is specified in the Group 1 CONFIG.SYS file of the receiving device, the application executes and the application prompt or logo is displayed on the device.

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 device.

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

Optimize Available Memory Space for Successful Downloads

One certificate file or signature file requires approximately 400 bytes of memory space. The application designer must account for the extra memory required to download and store these special files.

When planning your download procedure, carefully consider the total amount of memory space required to store certificates and signature files and the application files. In some cases, a considerable number of 400-byte signature files reside in device memory at any given time. Here are some general guidelines to follow:

- Know the size of available memory (SRAM and flash ROM) of the receiving device; also in back-to-back downloads, know the size of available memory on both the sending and receiving devices.
- Know in advance how application files are redirected to SRAM or flash ROM and to file groups other than the target group.
- Defragment flash ROM memory before performing a download to optimize the available space in the flash ROM file system.
- Before performing a download, use the system mode menu selections to clear the entire SRAM and flash ROM of a specific file group, as necessary, to ensure proper use of available memory in the target group.

Support for File Compression

For information regarding file compression, refer to the Verix V Operating System Programmers Manual, VPN 23230.

Effect of Downloads on Existing Files and Data

When downloading application files and data to a V^x810 device, an important consideration is the effect of the download procedure on existing application files, files used in the file authentication process, and device configuration settings stored in CONFIG.SYS files in the receiving device. 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 device, 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 device during an application or operating system download (direct and back-to-back). These include the system mode 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 system mode password in a separate, securely-controlled operation. Ensure that this password is retained in a secure place.

- For back-to-back application downloads, clear the SRAM and flash ROM of the receiving device before initiating the download. All application files stored on the receiving device, including CONFIG.SYS settings, are replaced by those of the sending device. System mode and file group passwords are retained on the receiving device.
- For full operating system downloads, Group 1 SRAM 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 on a subsequent operation, together with the certificates and signature files required to authenticate them.

Set Up the Download Environment

The first step in performing a download to a V^x810 device is to establish the physical communication link between the sending and receiving systems required to support the following download methods:

- **Direct serial cable connection for direct application and OS downloads:**
The link is between the COM2 port of a download computer and the COM2 port on the receiving V^x810 device.

A DB9-type serial connectors cable, VPN 08362-01-R, is available for supporting direct downloads. This cable has a 10-pin RJ-45 modular plug on one end for the external dongle or multi-port adapter.

- **Direct serial cable connection for back-to-back application downloads:**
The link is between the RS-232 serial ports of the sending and receiving devices.

A special cable is required for back-to-back downloads, VPN 05651-00. This cable has two 10-pin RJ-45 modular plugs on each end to establish the device-to-device connection.

Cable Connection for Direct Downloads

A special dongle cable, VPN 08362-01-R, is provided for direct downloads. This is the generic cable for all RS-232-based hosts.

The following steps describe how to establish the cable link between the sending host computer and the receiving V^x810 device using the special dongle cable:

- 1 Connect the 14-pin header end of the cable to the V^x810.
- 2 Connect the female DB-9 connector end of the cable to the RS-232 serial port of the host computer.
- 3 Connect an external power brick to the DC jack provided on the DB-9 connector housing.

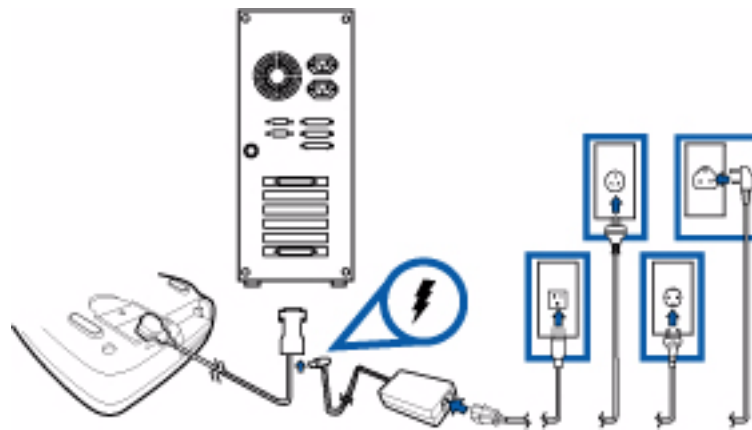


Figure 25 Serial Cable Connection with Multi-Port Adapter

Cable Connection for Back-to-Back Application Downloads

To prepare for a back-to-back application download:

- 1 Connect a MOD10 cable (P/N 05651-XX) between the RS-232 serial ports of the devices using a UART Dongle connected to each device.
- 2 Power up both devices.

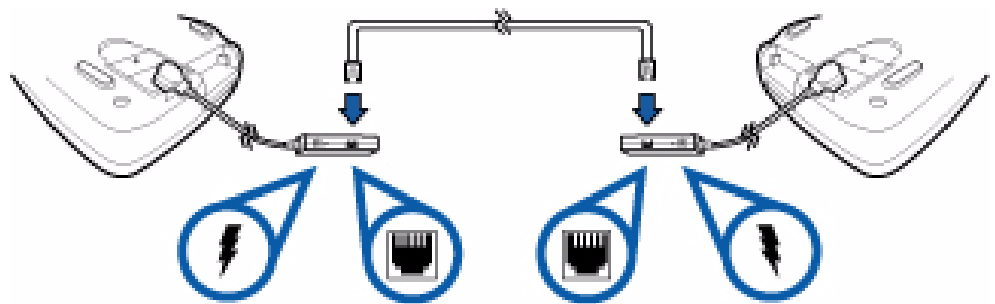


Figure 26 MOD10 Cable Connection Between Two V^x810 Devices

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 (COM2) to the RS-232 serial port (COM2) of the V^x810.

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 files of the file groups to store the application files.
- Certificate files (*.crt) required for file authentication on the receiving device 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 the VeriShield File Signing Tool are located on the host computer. One signature file downloads for each executable (*.out or *.lib) to run on the device.
- The filenames in the batch download list on the host computer indicate which application files to redirect to flash ROM 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 device to avoid accidental overwrites.
- The required system mode and file group passwords are available to make the required system mode menu selections and to prepare the receiving device to receive the application download.
- Sufficient memory space exists in the SRAM of the target group so that it can accept the entire download package, including certificates, signature files, and all data files.
- Use the system mode menu options to clear the entire SRAM or flash ROM or specific file groups on the receiving device (as necessary). Perform a flash ROM defragment (coalesce) operation to optimize the flash ROM file system (as necessary, the application itself can issue a function call to defragment the flash ROM on restart after the download.) For more information on system mode operations, refer to [Chapter 4](#).

Checklist for Effects on Files and Settings in the Receiving Device

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

Direct Application Download Procedure

The following procedure describes how to perform a direct application download from a host download computer into the Group 1 application memory area of a V^X810 deployment device.

Steps described in the Action column are performed directly on the V^X810 device. Notes provided in this column indicate and explain actions you must perform on the host computer.

The following table describes the common steps required for all download and upload procedures.

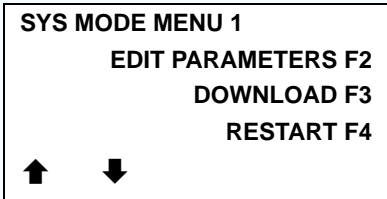
Table 17 Common Steps to Start a Download

Step	Display	Action
1	<p style="text-align: center;"> VERIFONE VX810 QG000829 03/29/2007 VERIX ★DEFAULT CERTIFICATE★ COPYRIGHT 1997-2007 VERIFONE ALL RIGHTS RESERVED </p>	<p>At startup, the device displays a copyright notice screen that shows the device model number, the OS version of the V^X810 stored in the device’s flash ROM memory, the date the firmware was loaded onto the device, and the copyright notice.</p> <p>This screen appears for three seconds, during which time you can enter system mode by simultaneously pressing F2 and F4.</p> <p>You can extend the display period of this screen by pressing any key during the initial three seconds. Each key press extends the display period an additional three seconds.</p>

Table 17 Common Steps to Start a Download (continued)

Step	Display	Action
2	<div style="border: 1px solid black; padding: 5px;"> (Application Prompt) or DOWNLOAD NEEDED *GO FILE NOT FOUND </div>	<p>If an application already resides on the device, an application-specific prompt is displayed. If no application resides on the device, the following message is displayed:</p> <p>DOWNLOAD NEEDED</p> <p>To enter system mode from this screen, simultaneously press F2 and F4.</p> <p>Note: The device will automatically download the file VeriFone.zip from a USB flash drive without the user having to go through System Mode under the following conditions:</p> <ul style="list-style-type: none"> • The USB flash drive is connected before the device is turned on. • The USB flash drive is inserted when the initial DOWNLOAD NEEDED message is displayed. <p>In both cases, the USB DOWNLOAD COMPLETE message will appear on the device screen after the VeriFone.zip file has been downloaded.</p>
3	<div style="border: 1px solid black; padding: 5px;"> SYSTEM MODE ENTRY PASSWORD ----- </div>	<p>If an application prompt appeared and you chose to enter system mode, you are prompted to type the system password.</p> <p>If DOWNLOAD NEEDED appeared, use the default password “Z66831.” This password is entered as:</p> <p>1 ALPHA ALPHA 6 6 8 3 1, then press ENTER.</p> <p>If you enter an incorrect password, the device exits the SYSTEM MODE ENTRY screen. Verify your password and re-enter it.</p> <p>To quit this operation and return to the application prompt or DOWNLOAD NEEDED screen, press CANCEL.</p>

Table 17 Common Steps to Start a Download (continued)

Step	Display	Action
4		<p>SYS MODE MENU 1 is the first menu displayed. To cycle through to the other menus, press the PF2 key or press ENTER until you reach the desired menu.</p> <p>To perform download operations, select DOWNLOAD (F3).</p> <p>To abort any action at any step, press CANCEL.</p>

The following table describes the specific steps required for performing a direct application download.

Table 18 Direct Application Download Procedure

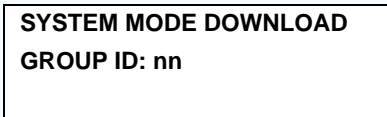
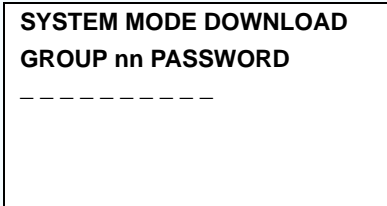
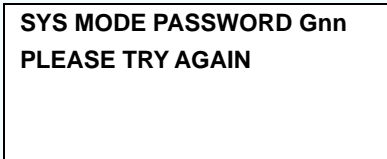


Step	Display	Action
1		Type the Group ID (valid values are 2 to 15) of the group into which you want to download files to. Then press ENTER to select the group.
2		To continue, enter the required password. The default group password is "Z66831." This is entered as: 1 ALPHA ALPHA 6 6 8 3 1 , then press ENTER .
		This message appears if you enter an incorrect password. Press ENTER to try again. Re-enter your password.
3		To download a single application, select SINGLE-APP (F3) . To download multiple applications, select MULTI-APP (F4) .
4		For a full download, select FULL (F3) . For a partial download, select PARTIAL (F4) . To return to SYS MODE MENU 1 , press the PF1 key.

Table 18 Direct Application Download Procedure (continued)

Step	Display	Action
5	<p>SYS MODE DOWNLOAD Gnn COM2 F3</p>	Select the download source, COM 2 (F3) .
	<p>SYS MODE DOWNLOAD Gnn UNIT RECEIVE MODE WAITING FOR DOWNLOAD</p>	The device is ready to receive a download from the selected source.
	<p>SYS MODE DOWNLOAD Gnn *** _ _ _ _ _ DOWNLOADING NOW</p>	<p>During download, a line of asterisks appears that shows the percentage of completion. Each asterisk equals approximately 10% of the download.</p> <p>When the download is completed, the device will restart.</p> <p>You can cancel a download in progress by pressing CANCEL. This will also restart the device.</p>
6	<p>**VERIFYING FILES** CHECK CERTIFICATE (FILENAME.CRT) **AUTHENTIC** or --- FAILED ---</p>	<p>The file authentication module on the receiving device begins to check for new certificate (*.crt) and signature (*.p7s) files included in the download. Then these special files process one at a time; certificates process first, then signature files.</p> <p>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 device beeps three times, allowing you to note which certificate failed to authenticate.</p> <p>The authentication process continues to the next certificate until all new certificates are authenticated.</p>

Table 18 Direct Application Download Procedure (continued)

Step	Display	Action
7	<pre> **VERIFYING FILES** COMPARE SIGNATURE FILENAME.P7S FILENAME.OUT **AUTHENTIC** or --- FAILED --- </pre>	<p>The file authentication module continues to authenticate any new signature files downloaded with the OS files.</p> <p>When the signature file authentication routine starts, the status display informs you of the progress of the authentication process.</p> <p>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 device beeps three times, allowing you to note which signature file failed to authenticate. The authentication process proceeds to the next signature file until all signature files are validated.</p> <p>When all new signature files are authenticated, the device restarts, and the application specified in the *GO variable or the default application in Group 1 executes and starts running on the device.</p>
8	<pre> (Application Prompt) or DOWNLOAD NEEDED </pre>	<p>If the downloaded application successfully authenticates, the corresponding application prompt or logo is displayed upon restart.</p> <p>The device can now process transactions.</p> <p>Note: The message DOWNLOAD NEEDED appears if:</p> <ul style="list-style-type: none"> • 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). <p>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 signature files.</p>

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 (COM2) to the RS-232 serial port (COM2) of the V^x810 device (refer to [Cable Connection for Direct Downloads](#)).

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 device restarts automatically and the new OS is processed, replacing the existing OS. In a partial OS download, the device returns to system mode and the new OS does not process until you manually initiate a device restart from system mode.
- The correct keyed record variables for the download exist in the CONFIG.SYS files of Group 1. (OS files must always download into GID1 SRAM). 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 V^x810 platform.
 - A file called VFI.PED. This file is an encrypted list of the new OS files.
- The required system mode and file group passwords are available to make the required system mode menu selections to prepare the receiving device to receive the application download.
- Sufficient memory space exists in the Group 1 SRAM to accept the OS download package including certificates, signature files, and all data files.
- Use the system mode menu options to clear the entire SRAM or flash ROM or the SRAM of Group 1 on the receiving device (as necessary).

Checklist for Effects on Files and Settings in the Receiving Device

- A full OS download replaces the existing OS and erases all application files from the Group 1 SRAM.
- A partial OS download returns control of the device to system mode and does not erase application files from the Group 1 SRAM.
- Protected records in the CONFIG.SYS files of the receiving device – keyed records that begin with * or # – are not erased.
- An OS download does not overwrite device configuration settings, including the current date and time, and passwords. If required, you can download new device configuration settings together with the OS files.

- ❑ The certificate tree that exists on the receiving device is not modified unless one or more new certificate files required to authenticate the new OS are being downloaded onto the device. When new certificates authenticate on the receiving device, the data they contain is stored in the certificate tree and the certificate files are deleted from the Group 1 SRAM.
- ❑ The certificates and signature files required to authenticate the new OS are processed by the file authentication module of the receiving device the same as application files.
- ❑ When the device restarts and the new OS files process, they are moved out of the Group 1 SRAM into the Group 0 area of the V^x810 file system.

Direct Operating System Download Procedure

The following procedure describes how to perform a direct operating system download from a host computer into the Group 1 SRAM of a V^x810 device.

Steps described in the Action column are performed directly on the V^x810 device. Notes provided in this column indicate and explain actions you must perform on the host computer.

Table 19 Direct Operating System Download Procedure

Step	Display	Action
1	<div style="border: 1px solid black; padding: 5px;"> <p>SYSTEM MODE DOWNLOAD GROUP ID: nn</p> </div>	<p>Type the Group ID (valid values are 1 to 15) of the group into which you want to download files to. Then press ENTER to select the group.</p> <p>Operating system files must <i>always</i> be downloaded onto Group 1.</p>
2	<div style="border: 1px solid black; padding: 5px;"> <p>SYSTEM MODE DOWNLOAD GROUP nn PASSWORD -----</p> </div>	<p>To continue, enter the required password. The default group password is “Z66831.” This is entered as: 1 ALPHA ALPHA 6 6 8 3 1, then press ENTER.</p>
	<div style="border: 1px solid black; padding: 5px;"> <p>SYS MODE PASSWORD Gnn PLEASE TRY AGAIN</p> </div>	<p>This message appears if you enter an incorrect password.</p> <p>Press ENTER to try again. Re-enter your password.</p>
3	<div style="border: 1px solid black; padding: 5px;"> <p>SYS MODE DOWNLOAD Gnn SINGLE-APP F3 MULTI-APP F4</p> </div>	<p>To download a single application, select SINGLE-APP (F3).</p> <p>To download multiple applications, select MULTI-APP (F4).</p>

Table 19 Direct Operating System Download Procedure

Step	Display	Action
4	<div style="border: 1px solid black; padding: 5px; text-align: center;"> <p>SYS MODE DOWNLOAD Gnn FULL F3 PARTIAL F4</p> </div>	<p>For a full download, select FULL (F3). For a partial download, select PARTIAL (F4). To return to SYS MODE MENU 1, press the PF1 key.</p>
5	<div style="border: 1px solid black; padding: 5px; text-align: center;"> <p>SYS MODE DOWNLOAD Gnn COM2 F3</p> </div>	<p>Select the download source, COM 2 (F3).</p>
6	<div style="border: 1px solid black; padding: 5px; text-align: center;"> <p>SYS MODE DOWNLOAD Gnn UNIT RECEIVE MODE WAITING FOR DOWNLOAD</p> </div>	<p>The device is ready to receive a download from the selected source.</p> <p>Initiate the download by executing the proper commands in the download tool running on the host computer (when the receiving device is ready to receive the direct OS download).</p>
	<div style="border: 1px solid black; padding: 5px; text-align: center;"> <p>SYS MODE DOWNLOAD Gnn ***_----- DOWNLOADING NOW</p> </div>	<p>During download, a line of asterisks appears that shows the percentage of completion. Each asterisk equals approximately 10% of the download.</p> <p>When the download is completed, the device will restart.</p> <p>You can cancel a download in progress by pressing CANCEL. This will also restart the device.</p>

Table 19 Direct Operating System Download Procedure

Step	Display	Action
7	**VERIFYING FILES** CHECK CERTIFICATE (FILENAME.CRT) **AUTHENTIC** or --- FAILED ---	<p>When the OS download is complete, the device restarts automatically. The file authentication module on the receiving device begins to check for new certificate (*.cert) and signature (*.p7s) files included in the download. These special files process one at a time; certificates process first, then signature files.</p> <p>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 device beeps three times, allowing you to note which certificate failed to authenticate.</p> <p>The authentication process continues to the next certificate until all new certificates are checked.</p>

Table 19 Direct Operating System Download Procedure

Step	Display	Action
8	<div style="border: 1px solid black; padding: 5px;"> <p>**VERIFYING FILES** COMPARE SIGNATURE</p> <p>FILENAME.P7S FILENAME.OUT</p> <p>**AUTHENTIC** or --- FAILED ---</p> </div>	<p>The file authentication module continues to authenticate new signature files downloaded with the OS files.</p> <p>When the signature file authentication routine starts, the status display informs you of the progress of the authentication process.</p> <p>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 device beeps three times, allowing you to note which signature file failed to authenticate. The authentication process proceeds to the next signature file until all signature files are validated.</p> <p>When all new signature files are authenticated, the device restarts and begins processing the new OS (full download) or it returns control to system mode (partial download).</p> <p>If you are performing a partial download, the device does not restart until you manually press the F4 key in SYS MODE MENU 1. If an application resides on the device following the OS download, it executes on restart.</p> <p>Note: Because a full OS download clears the SRAM, all device applications, related certificates, and signature files must be downloaded to the device when performing this type of download.</p>
9	<div style="border: 1px solid black; padding: 5px;"> <p>(Application Prompt) or DOWNLOAD NEEDED</p> </div>	<p>If you performed a full OS download, the DOWNLOAD NEEDED prompt is displayed.</p> <p>A direct application download on the receiving device can be performed.</p> <p>If you performed a partial OS download and manually restarted the device, the application residing in the device (if any) executes. The application prompt is displayed on device restart, after OS processing, and the application starts.</p>

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 device downloads is also discussed.

Hardware Checklist

- The correct serial cable connects the RS-232 serial ports of the sending and receiving V^x810 devices (refer to [Cable Connection for Back-to-Back Application Downloads](#)).
- Verify that the SRAM size on the receiving device is large enough to receive files uploaded from the sending device. If the SRAM on the sending device is 512 KB, the SRAM on the receiving device must be at least 512 KB.

Software Checklist

- The firmware versions of the sending and receiving devices must be identical or very similar.
- One or more complete and authenticated applications are stored in the GIDs 1–15, SRAM or flash ROM of the sending device. In this type of operation, *all* files stored in application memory of the sending device download to the receiving device.
- Before initiating the download procedure, remember to select Group 1 as the target file group on both the sending and receiving devices. The required system mode and file group passwords must also be available to make the required system mode menu selections on both devices.
- The current CONFIG.SYS variables, date and time, and other device configuration settings on the sending device are those downloaded onto the receiving device. Ensure that the desired settings are correct.
- All signature files required to authenticate the application files being downloaded onto the receiving device are present in the SRAM or flash ROM file system of the sending device.
- The certificate tree of the sending and receiving device 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 devices.
- If application files are downloaded onto the receiving device in previous operations, use the system mode menu options to clear the SRAM and flash ROM file systems of the receiving device before you initiate the back-to-back download procedure. This ensures a clean download.

Checklist for Effects on Files and Settings in the Receiving Device

- A back-to-back application download overwrites existing applications, libraries, or any other files stored in the SRAM of the receiving device.
- All CONFIG.SYS records and settings on the receiving device – protected and non-protected – are replaced by those of the sending device. Ensure that these records and settings on the sending device are correct before initiating the download.
- Passwords on the receiving device are retained.
- Certificates and signature files downloaded onto the receiving device, together with application files, must be processed by the file authentication module on the receiving device on device restart after the back-to-back download completes.

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

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

- ❑ An application upload does not overwrite the existing certificate tree on the receiving device. Any downloaded certificate files are authenticated and 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 source Vx810 device (transfers application files to the receiving Vx810 device).
- 2 Downloading application files from the sending device to a properly configured receiving device.

Prepare Sending Device (PC-to-Device)

- 1 Configure the host PC for an application download operation to the sending device:
 - 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 receiving device to receive.
- 2 Configure the sending device to receive an application download from a PC:
 - From **SYS MODE MENU 1**, set Group 1 and COM2 as the port to receive the download.
- 3 Connect a cable between the RS-232 serial ports of the PC and the sending device.
- 4 Initiate the file transfer on the PC.
- 5 From **SYS MODE MENU 1** on the sending device, select either a full or a partial download using a UART Dongle connected to each device.

The PC transfers files to the sending device.

Download Application Files to Receiving Device

- 1 Configure a sending device for an application download operation to a deployment device:
 - 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 V Programmers Manual.
 - Ensure that the download is exactly what you want your receiving devices to receive.
 - Ensure that previously authenticated files are not changed prior to the file transfer operation.
- 2 Configure the receiving device to receive an application download from the sending device. From **SYS MODE MENU 1**, set Group 1 and COM2 as the port to receive the file transfer.
- 3 Connect a cable, VPN 08362-01-R, between the RS-232 serial ports of the source and receiving devices using a UART Dongle connected to each device.
- 4 From any system mode menu on the sending device, press [*] and enter the GID1 password to initiate the file transfer.
- 5 From **SYS MODE MENU 1** on the deployment device, select either a full or a partial download. The sending device begins to transfer files to the receiving device.

The following diagram describes the procedure for a back-to-back application download from a sending Vx810 device to a receiving Vx810 device.

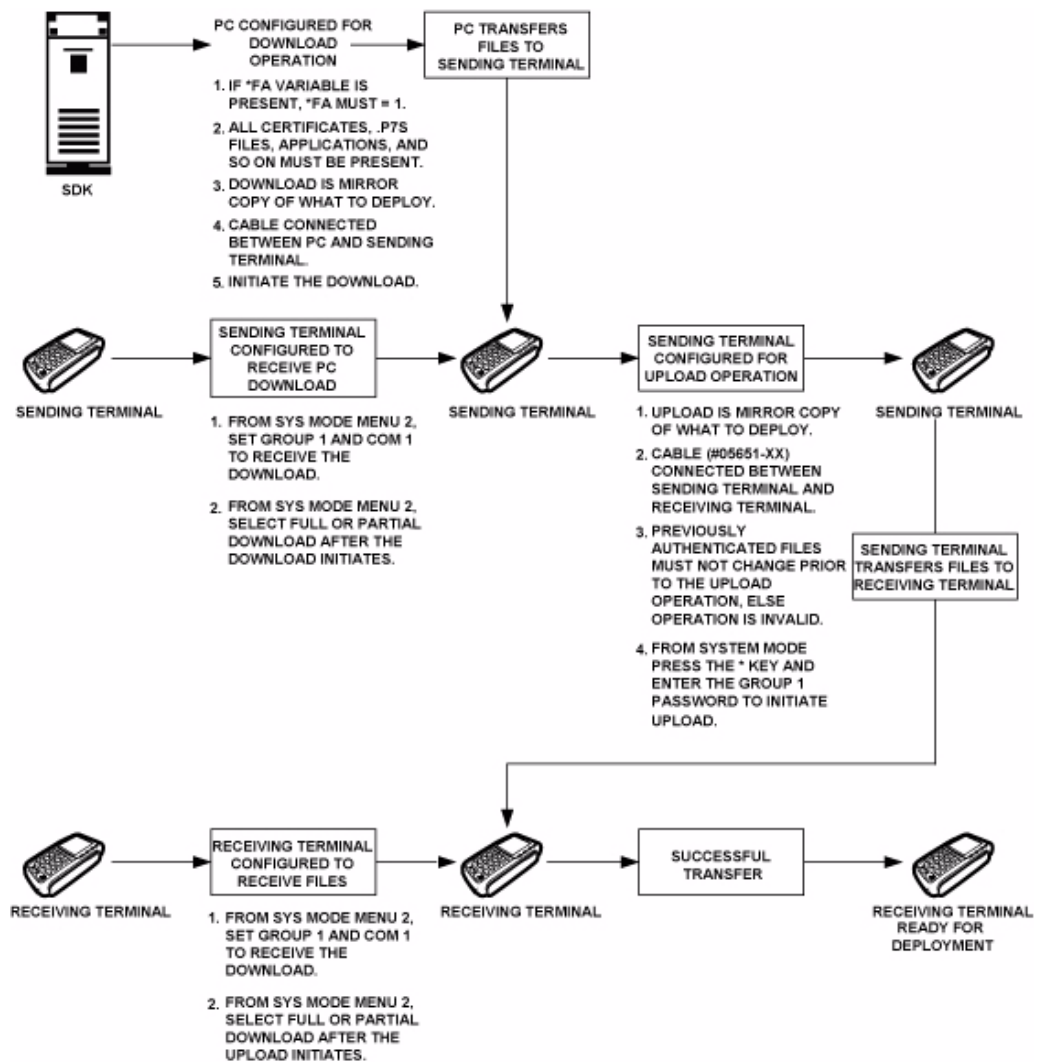


Figure 27 Back-To-Back Download Process

Back-to-back downloads require that one device, the sending device, be loaded with the required applications. The receiving device is the receiving device. The procedure assumes the following:

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



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

- You are performing a full download

Table 20 Back-to-Back Application Download Procedure

Step	Display	Action
1		Connect a MOD10 cable (P/N 05651-XX) between the RS-232 serial ports of the devices using a UART Dongle connected to each device. Then start up both devices.
2	(Application Prompt) or DOWNLOAD NEEDED *GO FILE NOT FOUND	After start up, the sending device displays the application prompt; while the receiving device displays DOWNLOAD NEEDED . For both devices, enter system mode by simultaneously pressing F2 and F4 .
3	SYSTEM MODE ENTRY PASSWORD -----	For both devices, enter the default system password “ Z66831 .” This password is entered as: 1 ALPHA ALPHA 6 6 8 3 1 , then press ENTER .
4	SYS MODE MENU 1 EDIT PARAMETERS F2 DOWNLOAD F3 RESTART F4 ↑ ↓	For the receiving device, select DOWNLOAD (F3) . Enter the system mode password when prompted.
	SYS MODE DOWNLOAD Gnn SINGLE-APP F3 MULTI-APP F4	Select SINGLE-APP (F3) .
	SYS MODE DOWNLOAD Gnn FULL F3 PARTIAL F4	Select FULL (F3) .

Table 20 Back-to-Back Application Download Procedure

Step	Display	Action
	<div style="border: 1px solid black; padding: 5px;"> <p>SYS MODE DOWNLOAD Gnn ****WARNING**** ALL FILES WILL BE CLEARED FROM GROUP 1 CANCEL DOWNLOAD F3 CONTINUE F4</p> </div>	<p>To abort the download, select CANCEL DOWNLOAD (F3).</p> <p>To proceed with the download, select CONTINUE (F4).</p>
	<div style="border: 1px solid black; padding: 5px;"> <p>SYS MODE DOWNLOAD Gnn COM2 F3</p> </div>	<p>Select COM2 (F3) as the download source.</p>
	<div style="border: 1px solid black; padding: 5px;"> <p>SYS MODE DOWNLOAD Gnn UNIT RECEIVE MODE WAITING FOR DOWNLOAD</p> </div>	<p>The device is ready to receive a download from the selected source.</p>
	<div style="border: 1px solid black; padding: 5px;"> <p>SYS MODE DOWNLOAD Gnn ***_----- DOWNLOADING NOW</p> </div>	<p>During download, a line of asterisks appears that shows the percentage of completion. Each asterisk equals approximately 10% of the download.</p>
5	<div style="border: 1px solid black; padding: 5px;"> <p>SYS MODE MENU 1 EDIT PARAMETERS F2 DOWNLOAD F3 RESTART F4 ↑ ↓</p> </div>	<p>For the sending device, press the Asterisk (*) key to enter Upload mode. Enter the system mode password when prompted.</p>
	<div style="border: 1px solid black; padding: 5px;"> <p>SYS MODE UPLOAD ***_----- UPLOADING NOW</p> </div>	<p>To message UPLOADING NOW is displayed.</p> <p>During upload, a line of asterisks appears that shows the percentage of completion. Each asterisk equals approximately 10% of the download.</p>
	<div style="border: 1px solid black; padding: 5px;"> <p>SYS MODE UPLOAD UPLOAD COMPLETE</p> </div>	<p>For the sending device, a message is displayed when the upload is successful.</p> <p>Otherwise, an error message will be displayed.</p>
6	<p>The receiving device begins to validate all files. Allow the receiving device to complete file authentication and reboot the device. An application-specific menu is displayed after the receiving device completes the reboot.</p> <p>The sending device is ready to perform another download.</p>	



Specifications

This chapter describes the technical specifications for the Vx810 device.

Product Specifications

Model	Vx810
Processor	200 MHz Samsung S3C2410 ARM920 32-bit microprocessor
Flash ROM	4MB installed (expandable to 8MB or 16MB)
SRAM	2MB installed (expandable to 4MB)
Operating System	Verix V platform. Built specifically to provide true and secure multi-application capability, as well as dynamic memory allocation and file authentication.
Display	128 x 128 pixel (2.75-inch) graphical LCD with high-contrast white backlighting. Supports 16 lines x 21 characters with standard font set.
Magnetic Card Reader	(Optional) Triple-track. High coercivity. Bi-directional. Compliant to ISO 7810 and ISO 7811.
Primary Smart Card Reader	(Optional) Support for ISO 7816, 1.8V, 3V, 5V or synchronous and asynchronous cards. EMV Level 1 and Level 2 Type approved.
SAM Card Reader	(Optional) 1-3 Security Access Modules
Input Device	Rubber keys: <ul style="list-style-type: none">• 4 ATM-style function keys (F1 to F4)• 4 programmable function keys (PF1 to PF4)• 1 ALPHA key• Main keypad (0 to 9, *, and #)• 3 command keys (CANCEL, CLEAR, and ENTER)
Peripheral Ports	Single multi-connector, which supports power, RS-232, USB Client, USB Host, Ethernet, and power over Ethernet. SDIO interface supports optional expansion module for contactless payments or SD memory card.

Supported Memory Media	SD Memory Card
	<ul style="list-style-type: none"> • Sandisk SD: SDSDB-512 / SDSDB-256 / SDSDB-128
	USB Flash Drive
	<ul style="list-style-type: none"> • Sandisk Cruzer Mini: SDCZ2-256-A10 • Memorex Thumbdrive: 32507725 • Kingston DataTraveler: KUSB DT1256 • PNY USB Flash: PFD256U20RF • Lexar USB Pro: JD256-80-231
Security	3DES encryption, Master / Session and DUKPT key management. PCI-PED approved. VeriShield file authentication.
Audio Output	Monophonic
Physical	Length: 150 mm (5.9 in.). Width: 85 mm (3.3 in.). Height: 32 mm (1.2 in.). Weight: terminal, 270g (0.59 lbs.); full shipping, 850g (1.87 lbs.).
Voltage	Input: AC 100-240V, 50-60Hz. Output: DC 5-12V. 2.5-W maximum consumption.

Environmental, Regulatory and Performance Specifications

The V^x810 meets all the necessary environmental, regulatory and performance standards for its intended use and expected market. VeriFone recognizes its responsibility to minimize the environmental impacts of its operations and products.

The V^x810 is classified as a “portable general purpose” device. It is designed for operation in retail environments where the product is handed over the counter to the consumer for payment transactions, PIN verification, etc.

This device is *not* intended for outdoor use and is certified for indoor use only.

Temperature and Humidity

Operating Temperature and Humidity

- Temperature: 0°C to +40°C (+32°F to +104°F)
- Humidity: 5% to 90% RH, non-condensing

Storage Temperature and Humidity

- Temperature: -40°C to +70°C (-40°F to +158°F)
- Humidity: 15% to 95% RH, non-condensing

Compliance Certifications

Emission Standards

This device is compliant to the following emission standards for information technology equipment: Radiated and Conducted Emissions (EN 55022:1998 / CISPR22 Class A).

Immunity Standards

This device is compliant to the following immunity standards for information technology equipment: Electrostatic Discharge (ESD) Immunity (EN/IEC 61000-4-2:1998), Radiated Immunity (EN 61000-4-3:1998), Electrical Fast Transients (EFT) Burst Immunity (EN/IEC 61000-4-4:1995), Surge (EN/IEC 61000-4-5:1995), Conducted Immunity (EN/IEC 61000-4-6:1996), Magnetic Field Susceptibility (EN/IEC 61000-4-8:1993), Voltage Dips (EN/IEC 61000-4-11:1994), Harmonic Current Emissions (EN/IEC 61000-3-2:1994), Flicker (EN 61000-3-3:1994).

Safety Standards

This device is compliant to the following immunity standards for information technology equipment: UL 1950 (3rd Ed.) and EN 60950 Amend 4 (1997).

Other Standards

This device is compliant to the following PTT certifications: CFR 47 Part 68 and CS-03.

SPECIFICATIONS*Environmental, Regulatory and Performance Specifications*



Care and Maintenance

Your V×810 device is a product of superior design and craftsmanship and should be treated with care. The following suggestions will help you protect your warranty coverage.

- Keep the device dry. Precipitation, humidity, and all types of liquids or moisture can contain minerals that will corrode electronic circuits. If your device does get wet, switch off the power, and allow the device to dry completely before replacing it.
- Do not use or store the device in dusty, dirty areas. Its moving parts and electronic components can be damaged.
- Do not store the device in hot areas. High temperatures can shorten the life of electronic devices, damage batteries, and warp or melt certain plastics.
- Do not store the device in cold areas. When the device returns to its normal temperature, moisture can form inside the device and damage electronic circuit boards.
- Do not drop, knock, or shake the device. Rough handling can break internal circuit boards and fine mechanics.
- Do not use harsh chemicals, cleaning solvents, or strong detergents to clean the device. Use only a soft, clean, dry cloth for cleaning. For best results, use the [VeriFone Cleaning Kit](#).
- Do not paint the device. Paint can clog the moving parts and prevent proper operation.
- Keep the device free from any small, loose items (such as paper clips, staples, or coins) that could accidentally get inside it through an opening, such as the SD card reader slot or the primary smart card reader slot.
- Do not attempt to open the device other than as instructed in this guide. This device has security features that protect it from tampering. For example, if the device's outer casing is opened, file content will be deleted.

These suggestions apply equally to your V×810 device, or any of its attachments or accessories. If your device is not working properly, take it to the nearest authorized service facility for servicing or replacement. For your safety, have this device serviced only by a VeriFone-authorized service provider.

Additional Safety Information

The following are additional information for your safety in using this device.

Power Adapter

Use only the power adapter that came with your device. Adapters for other electronic devices (including other VFI devices) may look similar, but they may affect your device's performance or damage it.

Potentially Explosive Environments

Do not use this device in any area with a potentially explosive atmosphere, and obey all signs and instructions. Potentially explosive atmospheres include areas where you would normally be advised to turn off your vehicle engine. Sparks in such areas could cause an explosion or fire resulting in bodily injury or even death.

Service and Support

For problems concerning your V^x810 device, contact your local VeriFone representative or service provider.

For V^x810 product service and support information:

- USA – VeriFone Service and Support Group, 1-800-VERIFONE (837-4366), Monday - Friday, 8 A.M. - 7 P.M. EST
- International – Contact your VeriFone representative

Product Returns

Before returning a V^x810 device to VeriFone, you must first obtain a Merchandise Return Authorization (MRA) number. The following procedure describes how to return one or more V^x810 devices 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 repair or replacement of their V^x810 devices.

To return a V^x810 device:

- 1 Gather the following information from the printed labels on the bottom of *each* V^x810 device to be returned:
 - Model Name. That is, “V^x810”.
 - Part Number (P/N). 12-digit, alphanumeric code. For example, “M281-503-02-DMO”.
 - Serial Number (S/N). 9-digit, numeric code. For example, “303-000-040”.

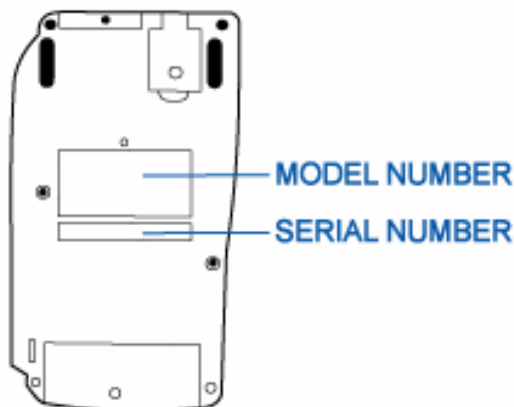


Figure 28 Information Labels on Device Bottom

- 2 Obtain the MRA numbers by doing one of the following:
 - a Call VeriFone toll-free within the United States at 1-800-VERIFONE (837-4366) 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. - 7 P.M. EST.
 - Give the MRA representative the information you gathered in Step 1 and describe the problem that you are having with each V^x810 device.
 - If you are returning several (3 or more) devices, it is advisable to send a fax or email instead.
 - b Send a fax to the “VeriFone MRA Department”.
 - Place the information you gathered in Step 1 in the body of the fax, including a description of the problem you are having with each device. Include also your contact information.
 - Send the fax to 727-953-4172 (U.S.).
 - c Email the VeriFone MRA Department at i_mra_help@verifone.com.
 - Place the information you gathered in Step 1 in the body of your email, including a description of the problem you are having with each device.
 - d Complete the Contact Form found at http://www.verifone.com/aboutus/contact/contact_form.cfm.
 - In the Inquiry field, specify “VeriFone MRA Department” followed by the information you gathered in Step 1 and the description of the problem you are having with each device.
- 3 An MRA representative will contact you and provide you with your MRA numbers.

NOTE

One MRA number must be issued for each V^x810 device you return to VeriFone, even if you are returning several of the same model and problems.

- 4 Send your V^x810 devices to your designated VeriFone service center. Provide the shipping address where the devices will be delivered once repaired or replaced.

Be sure to keep a record of the following items:

- Assigned MRA numbers.
- Part and serial numbers assigned to the V^x810 devices you are returning for service or repair.
- Shipping documentation, such as airway bill numbers used to trace your shipment.

Accessories and Documentation

VeriFone produces the following accessories and documentation for the V^x810. When ordering, please refer to the part number (VPN).

- 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 or power cord fits your needs.

CPS 11212-3A-R DC Power Supply

VPN 07152-02-R AC Power Cord

Connectivity Cables

VPN 08360-01-R Cable 14-PIN Header / IO Box (with 12V DC Power Socket, Mini USB Socket, USB Socket, and RJ48 Socket), 1.0m

VPN 08360-02-R Cable 14-PIN Header / IO Box (with 12V DC Power Socket, Mini USB Socket, USB Socket, and RJ48 Socket), 0.5m

VPN 08361-01-R Cable 14-PIN Header / RJ45, 0.3m Coil

VPN 08362-01-R Cable 14-PIN Header / Power / DB9, 1.38m

VPN 08366-01-R Cable 14-PIN Header / Power, 0.15m

Privacy Shield

VPN 08368-01-R Privacy Shield

Integrated Base Station

VPN 08388-01-R Integrated Base Station

VeriFone Cleaning Kit

VPN 02746-01 Cleaning Kit

Documentation

For the V^x810:

V ^x 810 Certifications and Regulations Sheet	VPN 24960
V ^x 810 Quick Installation Guide	VPN 24961
V ^x 810 Installation Guide	VPN 24963
V ^x 810 Privacy Shield Quick Installation Guide	VPN 24965
Verix V Operating System Programmers Manual	VPN 23230
Verix V Tools Programmers Manual	VPN 23231

Troubleshooting Guidelines

The troubleshooting guidelines provided in the following section are included to assist you to successfully install and configure your V^x810 device. If you have problems operating your V^x810 device, please read through these troubleshooting examples.

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. Typical examples of malfunction you may encounter while operating your V^x810 device and steps you can take to resolve them are listed.

NOTE



The V^x810 device comes equipped with tamper-evident labels. The V^x810 contains no user serviceable parts. Do not, under any circumstance, attempt to disassemble the device. 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 warranty.

CAUTION



Use only a VeriFone-supplied power pack. Using an incorrectly rated power supply may damage the device or cause it not to work as specified. Before troubleshooting, ensure that the power supply matches the requirements specified at the bottom of the device. (See [Chapter 7](#), for detailed power supply specifications.) Obtain the appropriately rated power supply before continuing with troubleshooting.

Display Does Not Show Correct/Readable Info

When the V^x810's display screen does not show correct or clearly readable information:

- Remove and reapply power to the device.
- If the problem persists, contact your local VeriFone service provider.

Blank Display

When the V^x810's display screen does not show any information:

- Check the device's power connection.
- Remove and reapply power to the device.
- If the problem persists, contact your local VeriFone service provider.

Device Does Not Dial Out

If the device does not dial out:

- Check the telephone line connections.
- Check that the telephone line is working by plugging it into a working telephone and listening for a dial tone.
- Replace the telephone cable that connects the device with a cable you know is working correctly.
- If the problem persists, contact your local VeriFone service provider.

Keypad Does Not Respond

If the keypad does not respond properly:

- Check the device's 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.
- Run the system mode keypad diagnostic.
- If the problem persists, contact your local VeriFone representative.

Transactions Fail To Process

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

Check Magnetic Stripe Card Reader

- Perform a test transaction using one or more different magnetic stripe cards to ensure the problem is not a defective card.
- 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.
- If the manual transaction does not work, check the telephone line.
- Run the system mode magnetic stripe card reader diagnostic.
- Contact your VeriFone distributor or service provider.

Check Primary 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.
- Ensure the MSAM cards are properly inserted in the cardholders and that the cardholders are properly secured.
- If the manual transaction does not process, check the telephone line.
- Contact your VeriFone distributor or service provider.



System Messages

This appendix describes system messages, which are grouped into two categories: error messages and information messages.

Error Messages

The following error messages may appear when the V^x810 device is in system mode.

ALREADY DEBUGGING

This message displays when **DEBUGGER F5** in **SYS MODE MENU 2** is selected and the debugging monitor program, **DBMON.OUT**, is already running on the device.

FLASH CHKSUM ERROR

A corrupt file is detected in the flash ROM file system during device 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.

PLEASE TRY AGAIN

This message is displayed if you enter an incorrect system mode password or an incorrect file group password. Repeat the password entry and press **ENTER**.

RAM CHKSUM ERROR

A corrupt file is detected in the SRAM file system at device 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.

** 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 (**XXXXXX** and **YYYYYY**) and try to download the archive again.

Information Messages

The following information messages may appear when the V^x810 device is in system mode.

DOWNLOAD NEEDED

The operating system is unable to start the application specified in the *GO variable for the following reasons:

- Application is not resident in the device.
- The *GO variable is not set in the Group 1 CONFIG.SYS file.
- The application file specified in the *GO variable does not exist in Group 1. (The *GO variable cannot specify an application file stored in a file group other than Group 1.)
- The application or a shared library used by the application either does not exist or is not authenticated. All executables must be authenticated to run on the device.
- There is not enough memory available to run the application requested in the *GO variable.

LOAD DBMON.OUT

This message displays when the **DEBUGGER F5** option in **SYS MODE MENU 2** is selected. The DBMON.OUT debugging monitor program is included in the SDK, but is not stored in the device's memory. To use the debugging tool, you must sign, download, and authenticate the DBMON.OUT application.

LOAD TERMINAL MANAGEMENT AGENT

This message displays if you select **REMOTE DIAGS F3** in **SYS MODE MENU 2** and the (optional) Terminal Management Agent (TMA) software is not resident in the V^x810 device. The TMA software is required to perform remote diagnostics. For more information about support for remote diagnostics, contact your VeriFone service provider.

RECEIVING NOW

In back-to-back downloads, the *Target* (receiving) device displays this message on data transfer initiation when pressing the asterisk key (*). To stop the upload, press **CANCEL** on either device (sending or Target).

SYS MODE CLEAR CLEARING FLASH PLEASE WAIT

This message is displayed when you select **FLASH FILES F3** in **SYS MODE MENU 1** and select **CLEAR GROUP_NN F2** or **CLEAR ALL FILES F3** to clear files from the flash ROM memory of a specific file group (Group 1–15) or from the entire flash ROM memory. This message remains until the files within the file group or all files in flash ROM are deleted.

If you select **CLEAR ALL FILES F3**, only application files stored in the flash-based file system – not the files stored in SRAM – are erased.

SYS MODE CLEAR
CLEARING RAM
PLEASE WAIT

This message is displayed when you select **RAM FILES F2** in **SYS MODE MENU 1** and select **CLEAR GROUP_NN F2** or **CLEAR ALL FILES F3** to clear files from the SRAM of a specific file group (Group 1–15) or from the entire SRAM. This message remains until the files within the file group or all files in SRAM are deleted.

If you select **CLEAR ALL FILES F3**, only the application files stored in SRAM – not the files stored in flash ROM – are erased. If you erase the main application stored in the SRAM file system, the device displays **DOWNLOAD NEEDED** after the VeriFone copyright screen on device restart.

NOTE



Clearing the SRAM does not erase the keyed variable settings stored in protected CONFIG.SYS records – that is, in records that start with an asterisk (*).

SYS MODE DEFRAG
RECLAIMING FLASH
PLEASE WAIT

This message is displayed when you select **FLASH FILES F3**, followed by **DEFRAG F4** in **SYS MODE MENU 1** to perform defragmentation (coalesce) of the flash ROM memory file system. **PLEASE WAIT** remains displayed during the defragmentation process. On successful completion, the device automatically restarts.

SYS MODE DOWNLOAD
DOWNLOADING NOW

An application is being downloaded onto a *receiving* Vx810 device from a host PC directly over a serial cable. This message is also displayed on the Target device in a back-to-back download.

The device 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.

SYS MODE ERROR LOG
TYPE
TASK
TIME
CSPR
PC
LR
ADDR

This information appears when you select **ERROR & Tmpr LOGS F4** in **SYS MODE MENU 2** or on system crash. Select **TAMPER LOG F4** to view a list of possible tamper events. Select **ERROR LOG F3** to display the following information which helps developers interpret the cause of the most recent unrecoverable software error that occurred on the device:

- **TYPE:** The error type code.
- **TASK:** The type of task that was currently executed.
- **TIME:** The clock time when the last error occurred in *YYMMDDhhmmss* format.
- **CSPR:** The register that contains the processor and state condition code.
- **PC:** The register that holds the execution address.
- **LR:** The register that holds the return address of the function call.
- **ADDR:** 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 V Programmers Manual*.

**SYS MODE KBD TEST
KEYCODE NN**

This message is displayed when you initiate a local diagnostic test of the device keyboard through **KEYBOARD DIAG F1** in **SYS MODE MENU 3**. When invoked, the decimal ASCII keycode of each key pressed appears to the right of **KEYCODE**. For example, pressing the **1** key on the device keypad displays the corresponding ASCII code, **31**.

**SYS MODE PASSWORD
FILE GROUP NN
SYS MODE ENTRY**

This message is displayed when you initiate the procedure for modifying existing system mode passwords through **PASSWORDS F2** in **SYS MODE MENU 2**. The menu options displayed allow you to change the password of a file group (**F2**) or the system mode password (**F3**).

**SYS MODE PASSWORD
NEW
AGAIN
PASSWORD CHANGED**

This message is displayed when you select **PASSWORDS F2** in **SYS MODE MENU 2** to modify the existing system mode 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.

**SYS MODE UPLOAD
UPLOADING NOW**

In a back-to-back download, the sending device displays this message when you initiate an upload from the receiving device. To stop the upload, press **CANCEL** on either device.

**TRK1:
TRK2:
TRK3:**

When you invoke a local system mode diagnostic test of the magnetic stripe card reader, status information appears for the data tracks (TRK1, TRK2, and TRK3) on the card.

To perform this test, select **MAG CARD DIAG F2** in **SYS MODE MENU 3** and swipe a magnetic stripe card through the card reader.

NO DATA or **VALID DATA:** A successful test of the magnetic stripe card reader results in one of these two messages for each track. Actual data stored on the card is not displayed.

An error condition 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**

Press **CANCEL** to end the local diagnostic test of the card reader.

```
UNZIP STUFF.ZIP
MYPROG.OUT
MYDATA.TXT
6X8.FON
10X14.FON
...
```

If you are using the file compression module in DMM, information similar to that displayed appears when a compressed file archive downloaded onto the device decompresses (unzipped), and the files extract from the archive.

```
** VERIFYING FILES **
CHECK CERTIFICATE

FILENAME.CRT

** AUTHENTIC **

or

--FAILED--
```

This message is displayed when the file authentication module detects a new digital certificate, together with the filename of the certificate to authenticate, during a download to the V^x810. If the authentication is successful, **AUTHENTIC** is displayed; otherwise, **FAILED** is displayed for five seconds and the device 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**.

```
** VERIFYING FILES **
COMPARE SIGNATURE

MYFILE.P7S
MYFILE.OUT

** AUTHENTIC **

or

--FAILED--
```

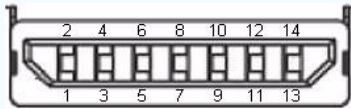
This message is displayed when the file authentication module detects a new signature file, together with the application file for which the signature file was generated, during a download to the V^x810 device. If the authentication is successful, **AUTHENTIC** is displayed; otherwise, **FAILED** appears for five seconds and the device 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.

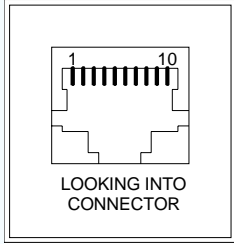
Port Pinouts

The tables in this appendix list pinouts for the V^x810 device, dongles, and cable connectors.

Multi-Port

Connector	Pin	Function	Description
 <p>LOOKING INTO CONNECTOR</p>	1	EXTGND	External Ground
	2	USB_DEVICE-	USB Device Signal (-)
	3	USB_DEVICE+	USB Device Signal (+)
	4	SGND	System Ground
	5	RXD_HOST	RS-232 Receive Data
	6	TXD_HOST	RS-232 Transmit Data
	7	SGND	System Ground
	8	USB_HOST-	USB Host Signal (-)
	9	USB_HOST+	USB Host Signal (+)
	10	SGND	System Ground
	11	EXTPWR	12Vdc External Power
	12	EXTPWR	12Vdc External Power
	13	EXTGND	External Ground
	14	RESERVED	(n/a)

COM Port

Connector	Pin	Function	Description
 <p>LOOKING INTO CONNECTOR</p>	1	NC	No Connection
	2	NC	No Connection
	3	DCD	Data Carrier Detect
	4	DTR	Data Terminal Ready
	5	GND	Signal Ground
	6	RXD	RS-232 Receive Data
	7	TXD	RS-232 Transmit Data
	8	nCTS	RS-232 Clear to Send
	9	nRTS	RS-232 Ready to Send
	10	NC	No Connection



ASCII Table

An ASCII table for the Vx810 is presented below.

Table 21 Vx810 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

Table 21 Vx810 ASCII Table

Dec	Hex	ASCII	Dec	Hex	ASCII	Dec	Hex	ASCII	Dec	Hex	ASCII
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



Application ID An alphanumeric code that identifies an application downloaded onto a device 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 V×810 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 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 device's display panel when power is applied to the device, assuming that an application has already been downloaded onto the device'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 device's application memory to another device's application memory. A terminal-to-terminal application upload require that the sending and receiving device 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 device's serial ports or modem.

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.

Byte A term developed to indicate a measurable number of consecutive binary digits that are usually operated on as a unit.

Carrier Usually, an analog signal that is selected to match the characteristics of a particular transmission system. The carrier signal on a phone line is modulated with frequency or amplitude variations to allow a device to transmit or receive data using a modem. A carrier signal transmits data from a host computer to a V×810 modem dongle over an analog telephone line.

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

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

CONFIG.SYS file A special keyed file that is stored in device 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 V×810 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.

Data Information prepared, often in a particular format, for a specific purpose. Data is to be distinguished from applications or program instructions. In the V×810, application files and data files can be stored in RAM or flash memory.

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

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 device or peripheral.

Direct download The process of transferring files and data from a download computer to a device over a serial cable connection and in a local, as opposed to a remote, system environment.

Display The backlit LCD screen on the V×810 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 device over a communication link to a receiving device.

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 device flash memory.

Flash memory An area of non-volatile memory where files can be stored. The V×810 also has a RAM-based file system. Files can be stored in RAM (drive I :) or in flash (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 device such as a PIN pad terminal, or the data that is entered.

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

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.

Keyed file record ASCII data, or variables, stored in the device's CONFIG.SYS files. A keyed file record consist of two parts: a search key that identifies the record, and the data or variable stored in the record.

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 V×810 is used to enter data and perform operations.

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

Memory A device or medium that can retain information for subsequent retrieval. The term is most frequently used to refer to the internal storage of a computer (or any electronic device) that can be directly addressed by operating instructions. In the V×810, files can be stored in battery-backed RAM or in non-volatile flash memory.

Messages Words and symbols appearing on the display screen which inform the user of the 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.

Modem *Modulator/demodulator*. A device that converts a digital bit stream into an analog signal to transmit over an analog communication channel (modulation), and converts incoming analog signals into digital signals (demodulation). The V×810 modem dongle allows communication with a host computer over a dial-up telephone line.

Non-volatile memory A memory or storage medium that retains data in the absence of power so that the data is available when power is restored. For the V×810, application files and data files can be stored in battery-backed RAM or non-volatile flash memory, according to the requirements of the application.

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

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.

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

Password A group of characters that identify a user to the system so that they can gain access to the system or part of that system. Passwords are used to ensure the security of computer systems by regulating the amount of access freedom. The password used to enter system mode is called the *system mode password*. In the V×810 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 device In a computer system, any equipment that provides the processing device with outside communication. Typical peripheral devices for a POS terminal include PIN pads 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 device 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 device 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 device display asking the user to enter specific information.

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 device and a host computer.

PTID *Permanent Terminal ID*. An optional identifier that can be permanently assigned to a VeriFone device 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 device, 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 V×810, the RAM (or SRAM) is commonly used to store applications and temporary data generated during a transaction.

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

Remote host computer A host computer connected to a Vx810 modem dongle over a dial-up telephone line to download files or data, or to process transactions. The opposite of remote is *local*.

RS-232 A widely used standard interface that covers the electrical connection between data communication equipment, such as a modem, and data terminal equipment, such as a microcomputer or computer terminal. The RS-232 interface standard was developed by the EIA (Electronic Industries Association) and is essentially equivalent to the CCITT's V.24 interface.

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 Vx810, 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 Vx810, a short character string used by an application to identify a keyed file record stored in CONFIG.SYS files. 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.

Serial port A connection point through which digital information is transferred one digital bit at a time. Same as *serial interface*. The Vx810 has one serial port, available at the multiport connector. The main serial port on a download computer is usually assigned the device ID, COM1.

Signature file A digital file with the filename extension *.p7s generated in an industry-standard format by the VeriShield File Signing Tool. The output of the VeriShield File Signing Tool is a signature file in an industry-standard format.

Swipe The action of sliding a magnetic stripe card through a card reader. The Vx810 card reader has a bi-directional swipe direction. The user must hold the card so that the magnetic stripe is faces in and towards the keyboard.

System Mode For the Vx810, system mode temporarily disables normal mode operations, allowing you to perform local functions such as downloads, diagnostics, and other operations that cannot be performed while the application is running.

At startup, the device displays a copyright notice screen that shows the version of Vx810 system firmware stored in device flash memory, the date it was loaded onto the device, and the copyright notice. This screen appears for three seconds. To enter system mode, simultaneously press the F2 and F4 keys during this three-second period. Pressing any other keys during that period resets the copyright notice screen to display an additional three seconds.

System mode password A unique set of characters entered by the user to access the system mode local functions of the device. A default password is supplied with each device. For the Vx810, the default system password set at manufacture is: **Z66831**.

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

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

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

Terminal Any device capable of sending and receiving data over a data link, such as a telephone line or a RS-232 cable. Some devices, such as the Vx810, 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 applications to download to that terminal. For ZonTalk 2000 downloads, the V×810 terminal ID is stored in the *ZT record in the CONFIG.SYS file. This variable should not exceed 10 characters in length.

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.

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 device, such as the one that is integrated in the V×810.

Transaction An exchange of data resulting in a transfer of goods, services, value, 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.

Volatile memory A type of memory where the contents are destroyed if the power supply to the memory is interrupted. When volatile memory, such as SRAM, is used for crucial applications, it is often back up by battery-supplied power.



Numerics

3DES **12, 128**

A

accessories **135**

B

back-to-back application downloads **120**

 effects on files and settings **120**

 hardware checklist **120**

 procedure **121**

 software checklist **120**

back-to-back downloads **87, 121**

C

Certificate Authority, VeriFone **63**

cleaning kit **135**

D

data entry modes

 normal mode **16**

 system mode **16**

device status

 verifying **32**

digital certificate **64**

digital signature **64**

direct application downloads **109**

 effects on files and settings **110**

 hardware checklist **109**

 procedure **110**

 software checklist **109**

direct downloads **87**

direct operating system downloads **115**

 effects on files and settings **115**

 hardware checklist **115**

 procedure **116**

 software checklist **115**

documentation **135**

downloads

 content **89**

 methods **87**

 back-to-back downloads **87**

 direct downloads **87**

 USB downloads **88**

 tools **88**

 VeriCentre **88**

 VeriCentre DMM **88**

DUKPT **12, 73, 128**

E

EMV **9, 12, 127**

error messages **139**

F

file authentication

 Certificate Authority, VeriFone **63**

 file system **77**

 authenticate files **79**

 file groups **77**

 restrictions on downloading **80**

 how it works **66**

 introduction **63**

 planning **70**

 files **70**

 requirements **70**

 signature files **70**

 successful authentication **71**

 processes **66, 72**

 adding new certificates **73**

 certificate tree restoration **73**

 deployment **66, 68**

 deployment devices **74**

 development **66**

 development devices **74**

 hierarchical relationships between
 certificates **72**

 permanency of the certificate tree **75**

 pre-deployment **66, 67**

 replace a sponsor certificate **77**

 required inputs to the file signing process **76**

special files **64**

- digital certificate **64**
- signer certificate **65**
- sponsor certificate **65**
- digital signature **64**
- signer private keys **64**

file groups **33****H**host computer downloads **87****K**

keypad

- command keys **19**
 - cancel key **19**
 - clear key **19**
 - enter key **19**
- data entry modes **16**
 - normal mode **16**
 - system mode **16**
- keys **15**
- programmable function keys **19**

M

magnetic stripe card reader

- how to use **30**

MSAM cards

- installing **24**
- replacing **24**

Nnormal mode **16****P**PCI-PED **12, 128**power pack **22, 135**

primary smart card reader

- how to use **30**

product (V×810)

- features and benefits **12**
 - flexibility and future-proofing **12**
 - reliability and security **12**
 - ultra sleek PIN pad **13**

overview **11****S**

service and support

- accessories and documentation **135**
 - cleaning kit **135**
 - connectivity cables **135**
 - documentation **135**
 - integrated base station **135**
 - power pack **135**
 - privacy shield **135**
- product returns **133**

setup

- cable connections **26**
 - ethernet connection **29**
 - other VFI devices **26**
 - powered USB **28**
 - RS-232 connection **27**
 - Standard USB **27**
 - USB download support **28**

location **21**

MSAM cards

- installing **24**
- replacing **24**

options **26**

- privacy shield **26**

power supply **29**unpacking **22**Signer private keys **64**

specifications

- environmental, regulatory and performance **128**
 - temperature and humidity **128**

product **127**

- audio output **128**
- display technology **127**
- flash ROM **127**
- input device **127**
- magnetic stripe reader **127**
- model **127**
- operating system **127**
- primary smart card reader **127**
- processor **127**
- security access module card reader **127**
- SRAM **127**
- supported memory media **128**
- voltage **128**

SSL **12**

- system mode **16**
 - entering **32, 39**
 - menus **37**
 - menu 1 **41**
 - DOWNLOAD **42**
 - EDIT PARAMETERS **41**
 - RESTART **43**
 - menu 2 **44**
 - MEMORY FUNCTIONS **45**
 - CLEAR MEM **46**
 - DIRECTORIES **46**
 - USAGE **45**
 - TERMINAL INFO **47**
 - CLOCK **58**
 - DIAGS AND LOGS **49**
 - DEBUGGER **55**
 - ERROR LOG **56**
 - IPP DIAG **54**
 - KEYBOARD DIAG **51**
 - MAG CARD DIAG **52**
 - REMOTE DIAGS **54**
 - SCREEN DIAG **53**
 - SMART CARD DIAG **50**
 - TAMPER LOG **57**
 - SYSTEM INFO **47**
 - menu 3 **60**
 - CONTRAST **60**
 - IPP KEY LOAD **61**
 - PASSWORDS **60**
 - operations **32**
 - local operations **32**
 - remote operations **32**
 - passwords **33**
 - file group passwords **34**
 - maintenance **34**
 - manual password change **35**
 - system mode password **34**
 - procedures **37**
 - when to use **31**

T

- troubleshooting
 - blank display **137**
 - device does not dial out **138**
 - display does not show correct/readable info **137**
 - keypad does not respond **138**

U

- USB downloads **88**

V

- VeriCentre **88**
- VeriCentre DMM **88**
- VeriShield **12, 63, 64, 66, 81**
 - command-line entries **82**
 - command-line mode syntax example **84**
 - graphical interface mode **84**
 - operating modes **81**
 - system requirements **81**



VeriFone, Inc.
2099 Gateway Place, Suite 600
San Jose, CA, 95110 USA
Tel: (800) VeriFone (837-4366)
www.verifone.com

V^x810

Reference Guide

