Introduction

Purpose

This manual provides instructions to upgrade a Passport® system running Version 8.02, 8.03, 8.06, 8.07, or 9.00 to Version 10.00.

IMPORTANT INFORMATION

Read all the sections of this manual in their entirety before starting the upgrade.
Note: During the upgrade the site will be unable to sell fuel and merchandise using the Passport system. Estimated time to complete the upgrade is 4 to 6 hours under normal circumstances.

Table of Contents

Requirements

Following requirements are essential for the upgrade of a Version 8.02, 8.03, 8.06, 8.07, or 9.00 Passport system to Version 10.00:

- Passport system Remote Access Service (RAS) connection is functional.
- The Passport system being upgraded is running software Version 8.02, 8.03, 8.06, 8.07, or 9.00.
- Upgrade must be performed by a Gilbarco®-certified Authorized Service Contractor (ASC).

IMPORTANT INFORMATION

Access to the Security Manager Report and proper function of all its passwords must be verified BEFORE starting the upgrade procedures outlined in the manual. If the Security Manager Report is not at hand or the passwords are invalid, contact Technical Support IMMEDIATELY, as system security must be disabled to proceed.

Required Tools

Following tools are required for upgrading the V10.00 software (also required for service calls):

- Automated Software Upgrade (ASU) V05.1.05E Service Pack or later (KS335 004DV)
- Enhanced Dispenser Hub (EDH) Disk Maintenance V01.1.01B or later CD (KS342 001DV)
- Passport V10.00 Recovery Image Universal Serial Bus (USB) Drive (S704-20003FD)
  Note: To create a USB thumb drive, refer to MDE-5037 How to Create a Bootable 16 GB USB Drive from the V04.0.11 or Later WinPE CD.
- Passport Application CD V10.00.XX.01
- Passport Service Pack CD V10.00.XX.01D at minimum
- Passport Windows® PE Recovery CD [V04.0.24 or later (S327-04024)] for use in case of error or failure
- Spare Monitor and PS2 Keyboard for connecting to the EDH
- Recommended spare parts for the Passport system service, including spare parts for the EDH
- Laptop for configuring the Firewall Router
- Security Manager Report

Service Packs

Following are recommended minimum Passport Versions and Service Packs for migration to Version 10.00:

Customer	Version and Minimum Service Pack
BP®	V8.02 R OR V8.06 D
Chevron®	V8.02 T
CITGO®, HPS-Dallas, Marathon, Phillips 66®, WorldPay™	V8.03 K
Concord	V8.02 W
ExxonMobil®	V8.02 W
HPS-Chicago	V8.03 M
NBS®/Cenex®, Irving Oil	V8.02 R OR V8.07 B
Shell®	V8.02 Q OR V9.00 C

Note: IOL (V8.05) does not upgrade to V10.00.

IMPORTANT INFORMATION

The Service Pack minimums listed above or later MUST be installed on the Passport system BEFORE starting the procedures in this document. If the Passport system is not running at least the Version and Service Pack listed above, you MUST upgrade to the recommended minimum Version and Service Pack BEFORE continuing.

Specifications

IMPORTANT INFORMATION

Verify the systems being upgraded are not model PX51 series. PX51 hardware series is not supported by Passport V10.00 software. This information may be obtained from the Model/Serial Tag on the top of the case.

If the hardware at this store is a PX51, the unit MUST be upgraded to a PX52 using *MDE-4656 Motherboard Kit (M02870K003KS) Installation Instructions for the Passport System.*

Server/Client Recovery Image

Product	Version Number
PX52 - V10.00	Must be 32.7.06
PX50, 51, 41, or 42	Not Supported

EDH Recovery Image

Passport V10.00 EDH Image version numbers are 40.8.10 and 40.8.11.

PIN Pad Support

Passport V10.00 software supports the following PIN pads:

- Ingenico® 3070
- Ingenico 6550
- Ingenico iSC250
- Ingenico iPP320

IMPORTANT INFORMATION

Do NOT plug an iSC250 PIN Pad into an EDH installed with less than Passport V10.00 Service Pack D. Installing the PIN pad before applying Service Pack D or higher will result in downloading an invalid configuration file to the PIN pad, rendering the PIN pad unusable.

Related Documents

Document Number	Title	GOLD℠ Library
MDE-2597	Gilbarco Security Module (GSM) PA0258XXXXXX Installation and Service Instructions	POS Peripheral Devices
MDE-2856	Site Inspection/Preventive Maintenance Checklist	Site Prep
MDE-3620	Point of Sale Systems Site Preparation Manual	Site Prep
MDE-3765	Console Installation Checklist	Gilbarco Forms

Document Number	Title	GOLD℠ Library
MDE-3816	Passport Hardware Start-up and Service Manual	Passport
MDE-3817	CMOS BIOS Setup for Passport PX52/PX51/PX50 Systems	Passport
MDE-3839	Passport System Installation Addendum	Passport
MDE-3911	Passport System Printer Quick Reference Guide	• POS Peripheral Devices • Passport
MDE-4157	Passport Combined Cashier/Manager Workstation	Passport
MDE-4158	Passport Cashier Workstation	Passport
MDE-4159	Passport Standalone Manager Workstation	Passport
MDE-4304	Connecting the Tank Monitor™ Device to the Passport System	• Passport • Environmental Products
MDE-4318	Passport Competitive Pump and CRIND® (CPC) Hardware/Software Start-up and Service Manual	Competitive Pump and CRIND
MDE-4603	Passport Auxiliary Network Hardware Installation and Software Module Manual	Passport
MDE-4656	Motherboard Kit (M02870K003KS) Installation Instructions for the Passport System	Passport
MDE-4674	Passport Electronic Price Sign Interface Manual	Passport
MDE-4696	Ingenico PIN Pad Kits (PA0379XXXXX, PA0380XXXXX, PA0412XXXXXXX, and PA0411XXXXXXX) Installation Instructions	POS Peripheral Devices
MDE-4822	Passport Enhanced Dispenser Hub Installation Instructions	• Passport • Service Manual
MDE-4823	Passport System Enhanced Dispenser Hub Start-up and Service Manual	• Passport • Service Manual
MDE-4830	Passport V8.02+ POS System Reference Manual	Passport
MDE-4831	Passport V8.02+ Cashier Workstation (CWS) Quick Reference Guide	Passport
MDE-4832	Passport V8.02+ Manager Workstation (MWS) Quick Reference Guide	Passport
MDE-4834	Passport System Recovery Guide for Passport V8.02+	Passport
MDE-4835	Passport V8.02+ What's New	Passport
MDE-4866	Passport Firewall Router Start-up and Service Manual	Passport
MDE-4880	Passport V8.02+ Third-party Partner Device Access Rules	Passport
MDE-4891	Enhanced Dispenser Hub (Passport V8.02+)	Passport
MDE-4905	Passport Approved Launcher Application User Instructions	Passport
MDE-4922	Passport Software Installation Manual for V8.02+ on PX52 Hardware Platforms with Pre-loaded Server and Enhanced Dispenser Hub	Passport
MDE-4941	Passport V8.02+ and Later Remote Access through Virtual Network Computing (VNC)	Passport
MDE-4954	Passport Start up and Service Manual for the Cisco® Firewall Router (Q13708-08)	Passport
MDE-5037	How to Create a Bootable 16 GB USB Drive from the V04.0.11 or Later WinPE CD	Passport
MDE-5167	Gilbarco Deployment Service (GDS) Start-up and Service Manual	Passport
MDE-5171	Insite360 Passport Configuration and Troubleshooting Manual for Passport V10 and Later	Passport

Abbreviations and Acronyms

Term	Description
ASC	Authorized Service Contractor
ASU	Automated Software Upgrade
BIOS	Basic Input/Output System
CAT	Card Activated Terminal
CCN	CRIND Control Node
CPC	Competitive Pump and CRIND
CPU	Central Processing Unit
CRIND	Card Reader in Dispenser
CWS	Cashier Workstation
D-Box	Distribution Box
DMZ	Demilitarized Zone
EDH	Enhanced Dispenser Hub
EMV®	Europay®, MasterCard®, and Visa®
EPP	Encrypting PIN Pad
EPS	Electronic Payment System
FTP	File Transfer Protocol
GDS	Gilbarco Deployment Service
GOLD	Gilbarco Online Documentation
GSM	Gilbarco Security Module
GUI	Graphical User Interface
HPS	Heartland Payment Systems
IP	Internet Protocol
ISP	Internet Service Provider
IT	Information Technology
LAN	Local Area Network
LCD	Liquid Crystal Display
LED	Light Emitting Diode
MAC	Message Authentication Code
MOC	Major Oil Company
MPD®	Multi Product Dispenser
MWS	Manager Workstation
NGP	Next Generation Payment
PCN	Pump Control Node
POS	Point of Sale
RAS	Remote Access Service
SCR	Secure Card Reader
SID	Screened Image Display
SPOT	Secure Payment Outdoor Terminal
TAC	Technical Assistance Center
TCP/IP	Transmission Control Protocol/Internet Protocol
USB	Universal Serial Bus
VGA	Video Graphic Adapter

Term	Description
VNC	Virtual Network Computing
VPN	Virtual Private Network
WAN	Wide Area Network

Upgrading to Passport V10.00

To upgrade a Version 8.02, 8.03, 8.06, 8.07, or 9.00 Passport system to Version 10.00, proceed as follows:

Before You Begin

Before beginning the upgrade process, complete the following tasks:

1 **Pre-upgrade Checklist** - This checklist found in "Appendix A: Pre-upgrade Checklist" on page 26 must be reviewed and items must be completed well before the day of the upgrade. If items in this list are not complete, actions must be taken before starting the upgrade to V10.00.

IMPORTANT INFORMATION
DO NOT CONTINUE UNTIL ALL ITEMS ARE CHECKED OFF THIS LIST.

2 **Manager Consultation** - It is preferred that before arriving on the site, the technician or wholesaler has provided the Manager's Punch List found in "Appendix C: Manager's Punch List" on page 30. Check with the manager to ensure he has the punch list. If not, provide it and go through the list to ensure he understands all items.

3 **Obtain Current Security Manager Report** - Enable Remote Support for the EDH through Security Manager and record the 'Passport' password in a safe location and destroy it after the upgrade is complete. Test to ensure you can connect to the EDH with the password and the Passport Tech credentials on the report are correct. If not, reprint the Security Manager Report. If the Security Manager Report is not available or the passwords are invalid, contact Technical Support IMMEDIATELY, as system security must be disabled to proceed.

4 **Passport RAS Verification** - Ensure Gilbarco support can connect to the Passport system in case you encounter issues later in the upgrade process.

To enable the Remote Support Connection on the Passport system, proceed as follows:

a Hold **Ctrl**, **Alt**, and **P**.

b Login using:
i) Username: Gilbarco
ii) Password: Passport

c Select **Remote Support** on the System Maintenance toolbar.

d Select **Ena. Dial In** (green phone) - if the button is not active, Remote Support is already enabled.

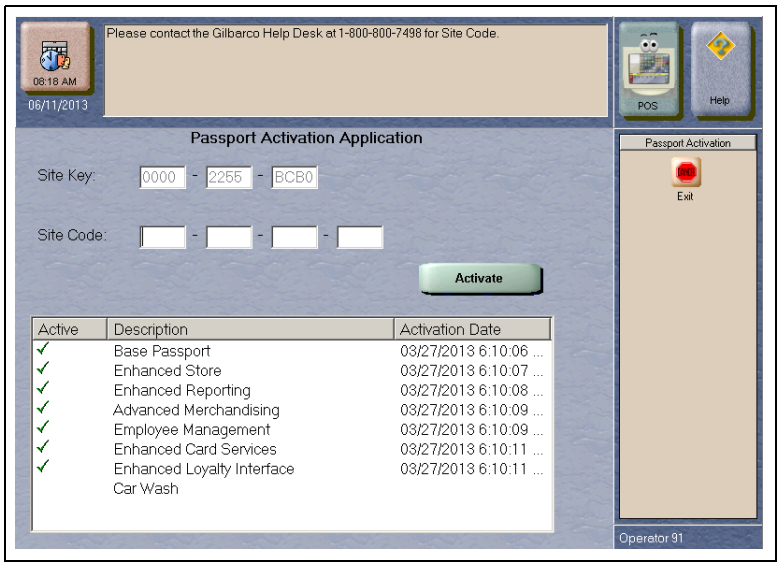
After you have **Dial In** enabled and are certain the RAS phone line is connected properly to the back of the Passport Server, call the RAS number using your cell phone or a separate land line. After two to three rings, if you hear the modem pick up and a series of high pitch noises, you have successfully enabled the modem to contact Gilbarco to verify RAS. If the line rings but never picks up, you have a problem with RAS and must troubleshoot. For assistance with troubleshooting, contact Gilbarco's Technical Assistance Center (TAC) group.
Note: Ensure that no other devices are sharing the RAS line when testing.

5 **Recommended Steps**

- Check the system event viewer on the Server and EDH for DISK, ATAPI, NTFS errors by accessing event viewer from Level 2 System Maintenance. Access the event viewer by bringing up a command prompt and type: **eventvwr**. If any errors are found, contact Passport TAC for assistance at 1-800-743-7501.
- From System Recovery on the Passport Server and EDH, go to **Tools** > **Save Image** to D:\Gilbarco\Images and verify that an image can be created in 20 minutes (you can stop the process after confirming the time) and delete the image if necessary. If estimated time is greater than 20 minutes, contact Passport TAC for assistance at 1-800-743-7501.
- Access Windows Explorer and go to C:\EPSFiles\DLH. If there are any files in the DLH folder, delete them.

6 **Access Feature Activation** in Manager Workstation (MWS) and write down the activate bundles for reference and verification after the upgrade is completed.

Figure 1: MWS Feature Activation Application



7 Verify whether Third-party Printer or Software is installed.
The upgrade to Passport V10.00 software does not convert or move forward any of the third-party drivers that may be required for support of non-Gilbarco equipment, such as VNC, Bullzip (PDF Printing), third-party printers other than OKI® Data, and other connections or hardware that the site may use. Before beginning the upgrade, ensure the customer has all third-party software available for reloading after the upgrade is complete.

If store personnel have used the Approved Launcher Application to save files on the Passport Server **C:** drive, the files will be deleted as part of this V10.00 upgrade. Gilbarco recommends copying these installer files to the Passport Server **D:** drive before the reimage upgrade.

The upgrade to Version 10.00 reimages the Passport Server to Windows XP® and the EDH to Windows 7.

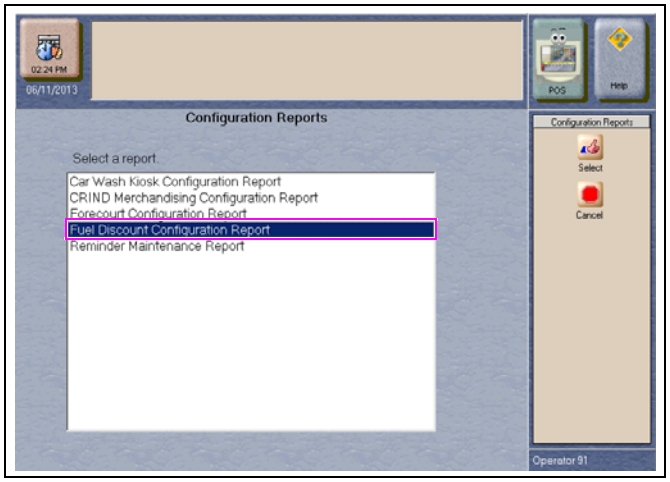
8 Contact Loyalty Provider
Contact the store's loyalty provider to inform them that you are performing a Passport V10.00 upgrade and verify whether the loyalty provider needs to update their configuration or device.

9 Print Configuration Reports.

a Navigate to **MWS** > **Reports** > **Configuration Reports**.

b Select **Fuel Discount Configuration Report**.

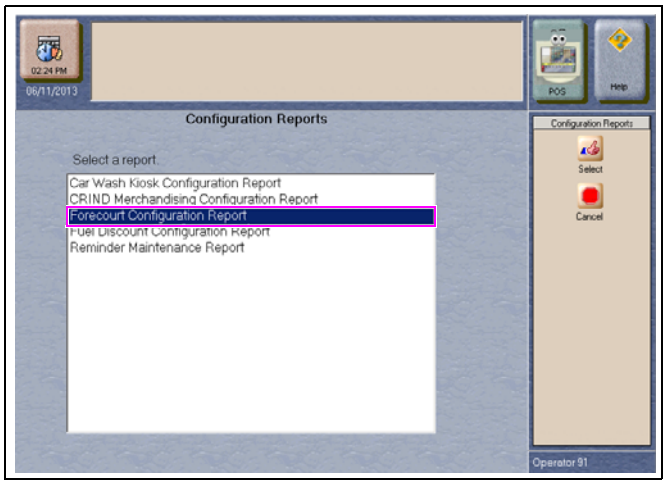
Figure 2: Fuel Discount Configuration Report



c Select **Print**. The report prints at the report printer.

d Select **Forecourt Configuration Report**.

Figure 3: Forecourt Configuration Report



e Select **Print**. The report prints at the report printer.

10 Block Dispensers and Shut Down Forecourt

a Using the preferred process for your company, the store, and within local and federal regulations, block off access to all dispensers in the forecourt area so fuel cannot be dispensed during the upgrade.

IMPORTANT INFORMATION
IT IS HIGHLY RECOMMENDED THAT DISPENSERS NOT BE OPERATED IN STANDALONE MODE AS THIS MAY CREATE PROBLEMS WITH DISPENSER RUNNING TOTALS AND RESULT IN POSSIBLE DATA LOSS.

b Press the **All Stop** key on the Cashier Workstation (CWS) to further secure the forecourt from activity.

Figure 4: All Stop Key

c Customers may choose to keep the store open and sell merchandise using cash only or some other type of device for payment other than the Passport system. Ensure adherence to all local, federal, and Major Oil Company (MOC) safety policies.

IMPORTANT INFORMATION
The Passport system cannot be used for any store functions during the upgrade process.

d If the store manager wishes to close the store, post signs wherever customers may attempt to enter the store notifying them an upgrade is taking place.

IMPORTANT INFORMATION
If any dispensers are bagged off on arrival for a known problem, isolate them in the Distribution Box (D-Box) and turn them off. If this task is not performed, it can cause issues when downloading the rest of the CRIND devices. Also, record the reason for any bagged dispensers and report to the Gilbarco Support Center for record keeping purposes.

11 Perform a Store Close

Store Close should only be performed after all transactions have completed and Forecourt has been blocked off properly.

a Give onsite personnel the go ahead to perform their typical Store Close procedures.

b Have the store manager validate the information on the reports to relieve possibility for data discrepancies. Ensure the network reports indicate there are no transactions in Store and Forward.

c If discrepancies are found, do not start the upgrade until they are clearly understood or the store manager indicates the discrepancies do not require clarification. Contact Passport TAC for assistance if required.

12 Prepare Dispensers for Download

To prepare the dispensers for downloading, proceed as follows:

a Power down the D-Box by removing AC power.

b If dispenser firmware/CRIND Basic Input/Output System (BIOS) upgrades are needed for optimal performance, then follow the appropriate steps to complete the firmware/CRIND BIOS upgrades.

c Perform the appropriate cold start procedure for each dispenser at the site. Dispensers running 22.5.30 CRIND firmware will need to be cold started manually after the upgrade has completed before restoring AC power to the D-Box.

d Leave the D-Box powered off until the software upgrade completes.

IMPORTANT INFORMATION
ENSURE ALL PUMP SETTINGS ARE CAPTURED BEFORE UPGRADING PUMP FIRMWARE, AS THIS WILL REQUIRE RELOAD OF THE DATA. IF CONFIGURATIONS AT THE DISPENSER DO NOT MATCH PASSPORT, DISPENSERS MAY REMAIN OFFLINE AFTER THE CRIND DOWNLOAD PORTION OF THE SOFTWARE UPGRADE.

e Ensure all Clients are online and there are no Clients in Register Setup that have been removed.

13 **Remove all USB devices from the Passport Server, Clients, and EDH** (mouse, keyboard, report printer, etc.) before starting the upgrade.

14 **Refer to the appropriate Passport V10 network addendum document** for specific instructions regarding coordination with the payment network before and after the upgrade.

Following is a list of the Passport V10 network addendum documents for your reference. Download the appropriate document from GOLD on the Gilbarco extranet.

Network Addendum MDE and Title
MDE-5087 Passport V10 Network Addendum for HPS-Dallas Generic
MDE-5088 Passport V10 Network Addendum for BP
MDE-5089 Passport V10 Network Addendum for CITGO
MDE-5090 Passport V10 Network Addendum for Shell
MDE-5091 Passport V10 Network Addendum for WorldPay
MDE-5092 Passport V10 Network Addendum for Marathon
MDE-5095 Passport V10 Network Addendum for NBS/Cenex
MDE-5096 Passport V10 Network Addendum for ExxonMobil
MDE-5098 Passport V10 Network Addendum for Concord
MDE-5111 Passport V10 Network Addendum for Irving Oil
MDE-5115 Passport V10 Network Addendum for Phillips 66
MDE-5116 Passport V10 Network Addendum for Chevron
MDE-5122 Passport V10 Network Addendum for Valero
MDE-5125 Passport V10 Network Addendum for Sunoco®
MDE-5177 Passport V10 Network Addendum for HPS-Chicago

Call the payment network to advise of the upgrade to Version 10.00 Passport software and validate with the network that all batches are settled. Proceeding without a settled batch will cause data loss and reports will not settle properly.

IMPORTANT INFORMATION
Verify the Passport units are not PX51. Passport V10.00 does not support PX51 hardware. If the Passport units are PX51, they MUST be upgraded to PX52 using *MDE-4656 Motherboard Kit (M02870K003KS) Installation Instructions for the Passport System*. If hardware is PX52, proceed to step 15.

15 Installing the ASU Service Pack

Install ASU V05.1.05E (or later) Service Pack through Software Upgrade Manager before attempting the V10.00 upgrade. This ASU Service Pack updates the ASU components on the system to facilitate the V10.00 upgrade.

To install the ASU V05.1.05E Service Pack, proceed as follows:

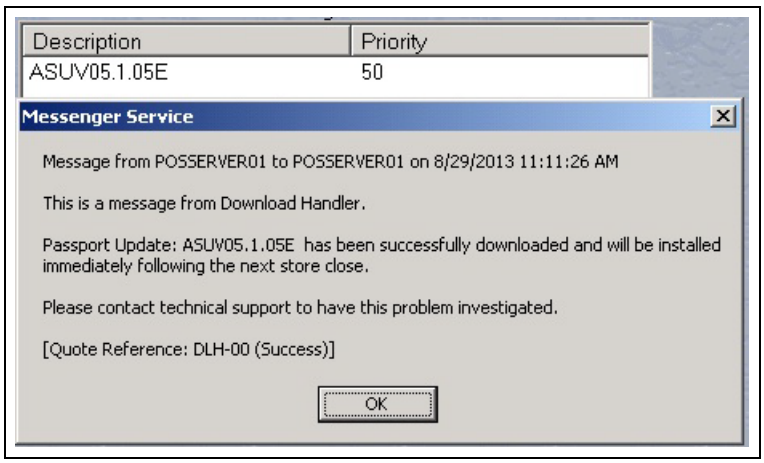
a Log into Passport MWS to access Software Upgrade Manager from **MWS** > **Set Up** > **Store** > **Software Upgrade Manager**.

b Place the ASU V05.1.05E CD in the CD-ROM drive on the MWS.

c Select **Download from CD** from **Software Manager**.

d Wait for the Download Complete message. This should take no more than five minutes. The Messenger Service screen appears.
Note: If the download does not complete within 5 minutes, repeat step 15 on page 12 .

Figure 5: Messenger Service Window



e Click **OK**.

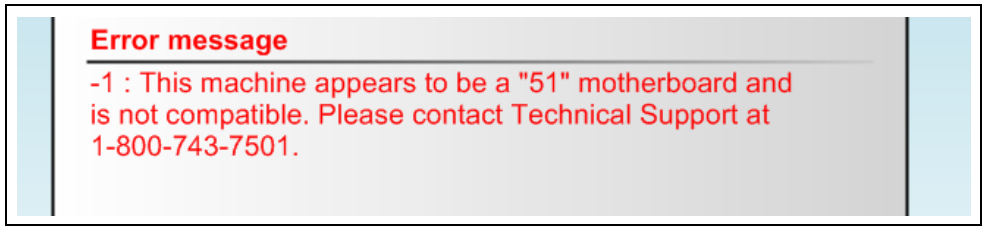
f Remove the CD from the CD-ROM drive.

g Select **Install Software**.

h Click **Yes** to indicate that dispensers will be offline during upgrade.

i ASU V05.1.05E validates the Passport system hardware set. If the unit is PX51, the following PX51 error message appears.

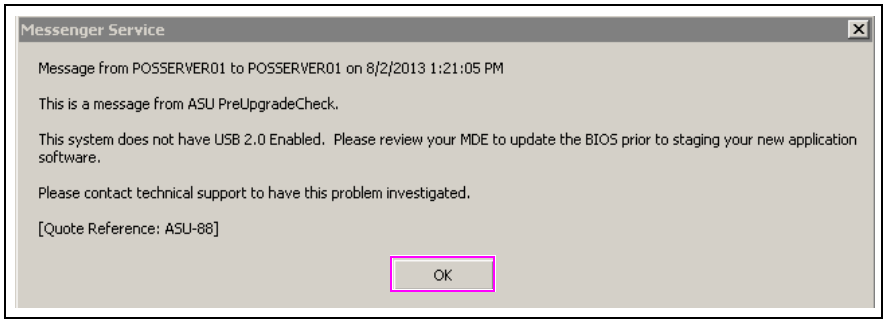
Figure 6: PX51 Error Message



If this error appears, you must contact Gilbarco technical support.

j ASU V05.1.05E also verifies that USB 2.0 is enabled on the Passport Server. If USB 2.0 is not enabled, the USB 2.0 error message appears as shown in Figure 7.

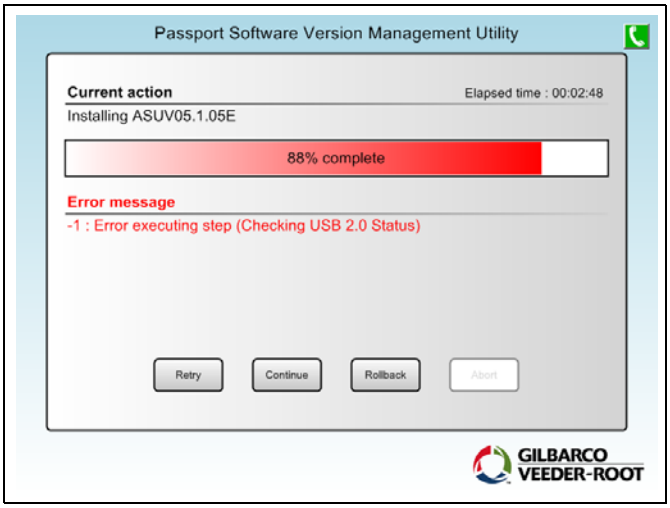
Figure 7: USB 2.0 Error Message



k Click **OK**.

16 Enable USB 2.0 on the Passport Server

Figure 8: Passport Software Version Management Utility



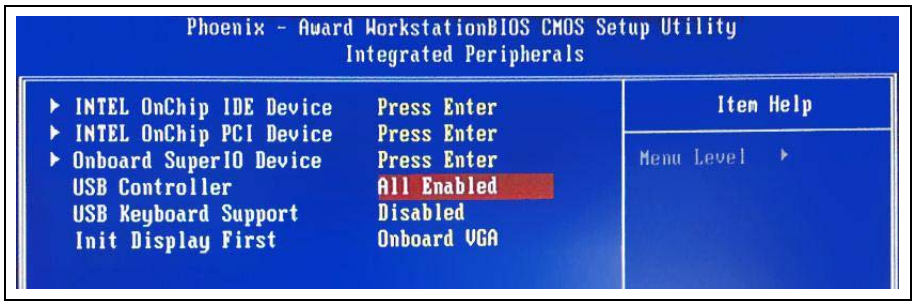
If the **Passport Software Version Management Utility** displays the error message “Error executing step (Checking USB 2.0 Status)” as shown in Figure 8, proceed as follows:

a Reboot the Passport Server and enter the BIOS configuration by pressing the **Del** key on reboot.

b Enter the BIOS Password **PASSASC**, when prompted.

c Browse to **Integrated Peripherals** and ensure **ALL ENABLED** is selected for USB Controller and USB 2.0 Controller.

Figure 9: Enabling USB Setting



d Press **F10** to save and reboot.

e Report any failure to Passport TAC at 1-800-743-7501. If no errors occurred, proceed to the next step.

17 If you receive a message indicating the ASU package successfully installed on the system, continue to step 18.

18 **Install EDH Disk Maintenance** to fix potential EDH drive partition issues. This procedure repartitions the EDH D:\ drive from 10 GB to 30 GB to accommodate large V10.00 image files.

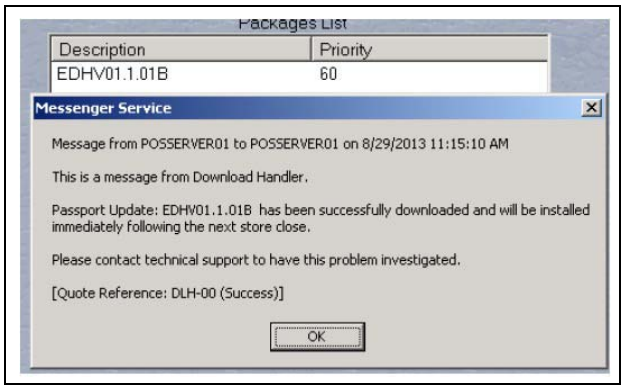
a Log into the Passport system MWS to access Software Upgrade Manager from **Set Up** > **Store** > **Software Upgrade Manager**.

b Place the EDH Disk Maintenance CD in the CD-ROM drive on the MWS.

c Select **Download from CD** from **Software Manager**.

d Wait for the Download Complete message.

Figure 10: Messenger Service Window



e When it displays, click **OK**. Remove the CD from the CD-ROM drive.

f Select **Install Software**.

g Click **Yes** to indicate the dispensers will be offline during upgrade.

h Report any failure to Gilbarco technical support at 1-800-743-7501. If no errors or failures occur, proceed to "Installing Passport V10.00".

IMPORTANT INFORMATION
This process may take some time and duration may vary site-to-site based on a range of circumstances. You may check progress by checking the green EDH hard drive light or plug a Video Graphic Adapter (VGA) monitor into the EDH.

Installing Passport V10.00

To install Passport V10.00, proceed as follows:

1 Insert the **S704 Recovery Image USB Drive** into an available USB port on the back of the Passport Server (USB ports on the front of the unit are not active).

2 Insert the Passport V10.00 Base Software Disk into the CD/DVD Drive.

3 Wait for 10 to 15 seconds while the Windows Operating System recognizes the USB drive.

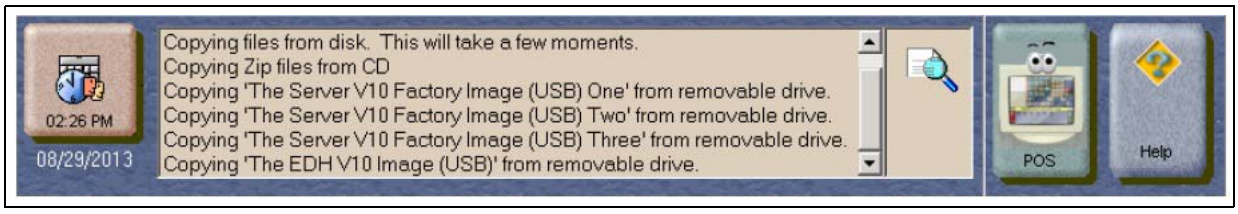
IMPORTANT INFORMATION
It is critical to wait the allotted time to allow the Windows Operating System to recognize the USB drive before pressing **Download from CD** in the Software Upgrade Manager. Use Windows Explorer to verify the USB drive is present.

4 Navigate to **Set Up** > **Store** > **Software Upgrade Manager**.

5 Select **Download from CD**.

6 Select **OK**. The following message appears indicating files are being copied. This process takes about two to three minutes to complete.

Figure 11: Software Upgrade Manager - Copying Files

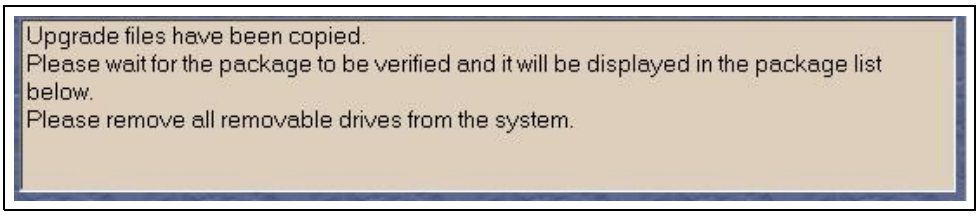


When the files from the CD are copied, the CD tray opens. Remove the CD and close the tray.

7 The USB file copy continues. This process takes about 5 to 10 minutes.

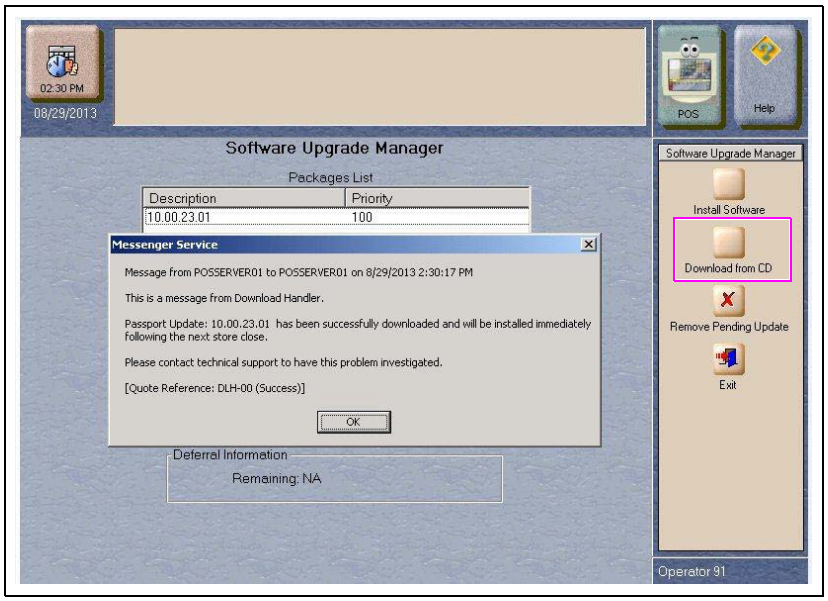
8 When the file copy completes, the message indicating the file copy is successful appears.

Figure 12: Software Upgrade Manager - Files Copied Successfully



9 Following this, the Messenger Service Prompt appears as shown in Figure 13, indicating the files are downloaded and ready for installation.

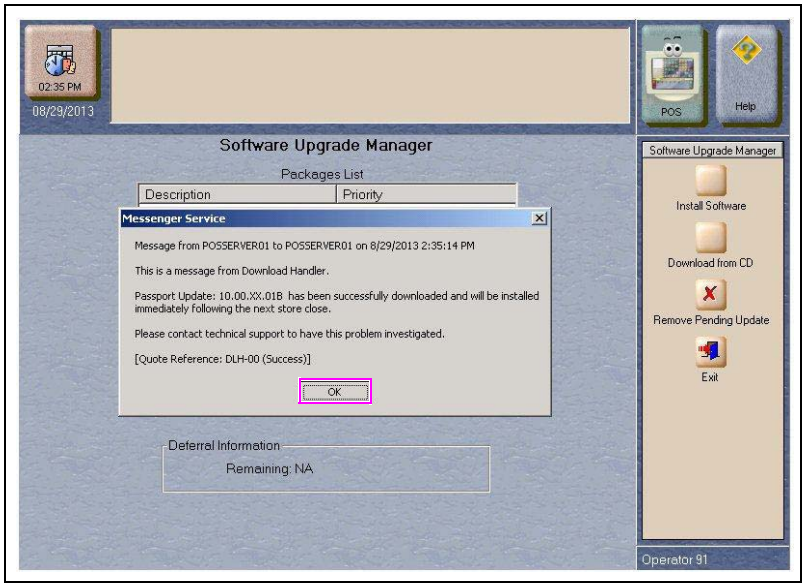
Figure 13: Messenger Service Prompt - Screen 1



10 After this message appears, insert the latest version of the Service Pack CD into the Server CD drive bay and press the **Download from CD** button for a second time.

11 After the Service Pack is copied and staged, the following message appears.

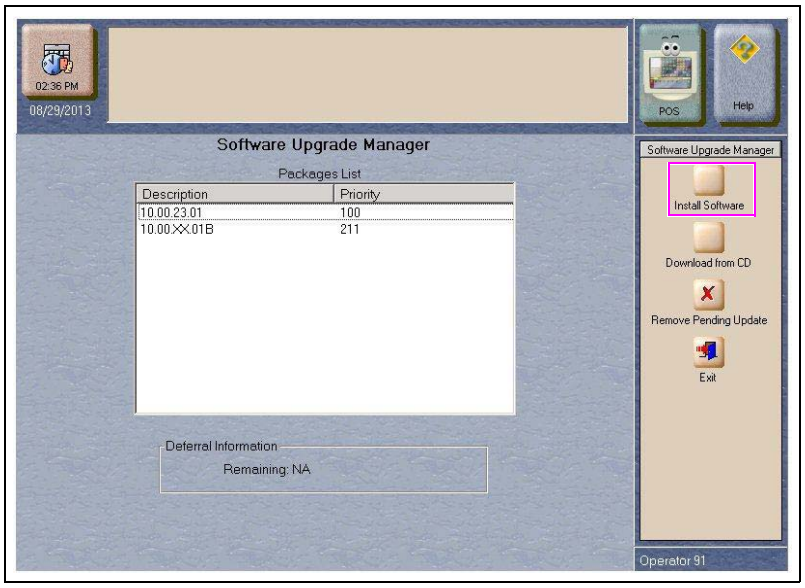
Figure 14: Messenger Service Prompt - Screen 2



Select **OK**.

12 The Software Upgrade Manager screen must appear as shown in Figure 15 (Service Pack letter is determined by the latest release).

Figure 15: Software Upgrade Manager Screen

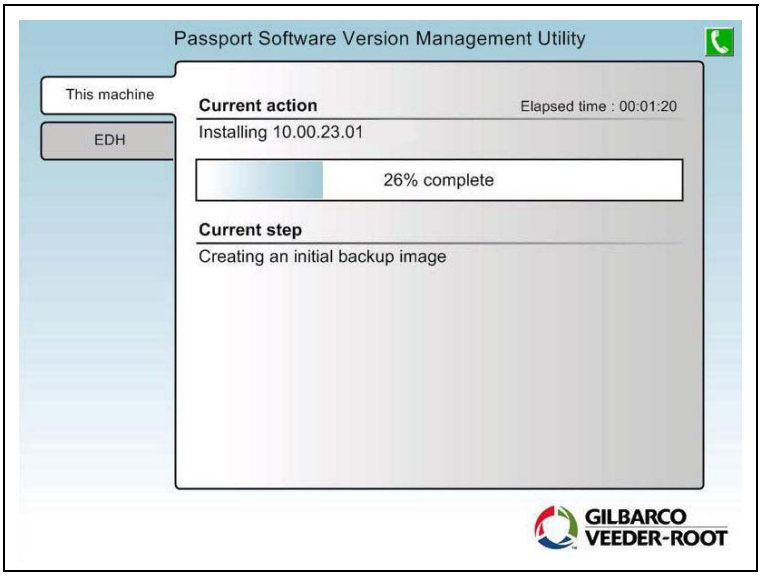


13 Click the **Install Software** button to begin the V10.00 upgrade.

14 Wait and monitor the installation. This part of the upgrade may take up to 2 1/2 hours.

15 When the upgrade starts, the Server, Combo, and Clients display on the ASU screen. From this point the software upgrade is automated for the Server, Combo, Clients, and EDH, and requires no intervention unless an error appears. To view the status of each machine, click the appropriate tab.

Figure 16: Automated Software Upgrade Screen



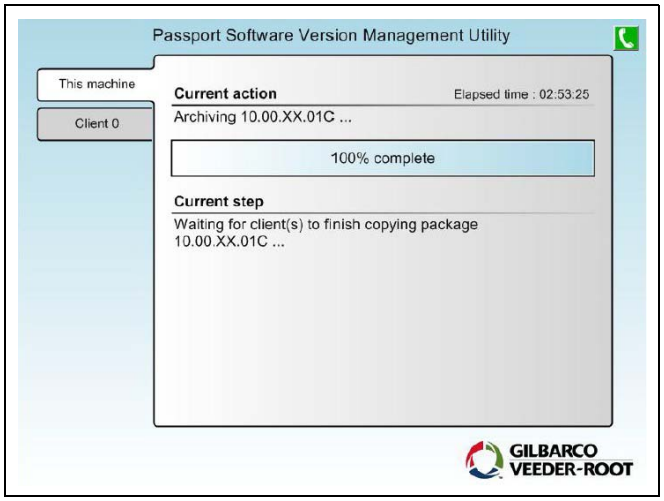
V10.00 Upgrade Process Differences

The V10.00 upgrade has some differences from previous reimage upgrades. The differences are as follows:

- The image that is applied on the MWS and CWS is 90% pre-installed to reduce upgrade time.
- Backup images on all machines are completed at the same time at the beginning of the upgrade.
- ASU screen shows the progress status for saving images and transfer of large Enhanced Dispenser Hub files.
- At 54% MWS reboots and applies a partially installed image and reboots again.
- After the MWS steps have completed, the EDH and Client Workstations upgrade at the same time.

- Client Workstations reimage in succession and should complete before the EDH completes. They appear as Client 0 for a short time after the image is applied and are quickly renamed to their previous name or number.

Figure 17: Client 0



- During the upgrade (typically around 50%) the MWS, CWS, and EDH perform a reimage by booting into the WinPE partition. You will not see updates on the ASU screen during this time, but can see that activity is going on by looking at the screen. As the EDH does not have a screen (unless you plug one in), the flashing green hard drive LED will let you know things are in progress. If the EDH does not come back up after 20 minutes, attach a monitor and call Gilbarco technical support.
- The machines reboot after installing the base application and again after the Service Pack.

IMPORTANT INFORMATION
Reimaging the Server and Client may cause the touch screen to lose calibration. Recalibrate each touch screen after completing the V10.00 upgrade.

Figure 18: Service Pack Upgrade

Note: This screen appears when a Server or Client has completed applying the preinstalled image and ASU is starting up.

Completing the Upgrade

To complete the upgrade, proceed as follows:

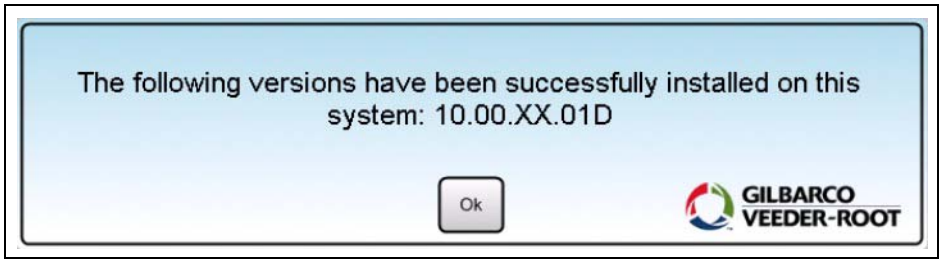
IMPORTANT INFORMATION

If the following message appears, select **No**.

1 Upgrade Complete Message

On completion of the software upgrade, a message pop-up appears indicating the software was successfully installed.

Figure 19: Upgrade Complete Message



2 CRIND Download

Perform the following tasks after the software upgrade completes and the CRIND devices are downloading:

a Power on the D-Box, if powered down on a previous step for CRIND upgrade or because of known download issues with 22.5.30 CRIND firmware on The Advantage® Series or Encore® 300 dispensers.

b For Encore 500, Encore 700, and Eclipse® dispensers the download process begins automatically without cold start when the EDH upgrade is complete and the EDH accepts the new configuration from the MWS.

c CRIND download is complete when the CRIND displays are at the normal idle screen.

Note: It is possible to check the CRIND download status from the Point of Sale (POS) by selecting the dispenser icon in the Forecourt section and then selecting DIAG. Download status information displays if the download is in progress and each dispenser on the forecourt has a flashing green and black arrow.

d After all CRIND devices have downloaded the DIAG button on the CWS show dispensers as IDLE.

3 Verify Single-line dispenser keypads

Verify the CRIND keypad mapping is correct for single-line dispensers on the Forecourt. For additional information, refer to "Appendix F: Single-line CRIND Keypad Configuration" on page 56.

4 Install Third-party Software

a Locate third-party software, such as printer, VNC, Bullzip, etc.

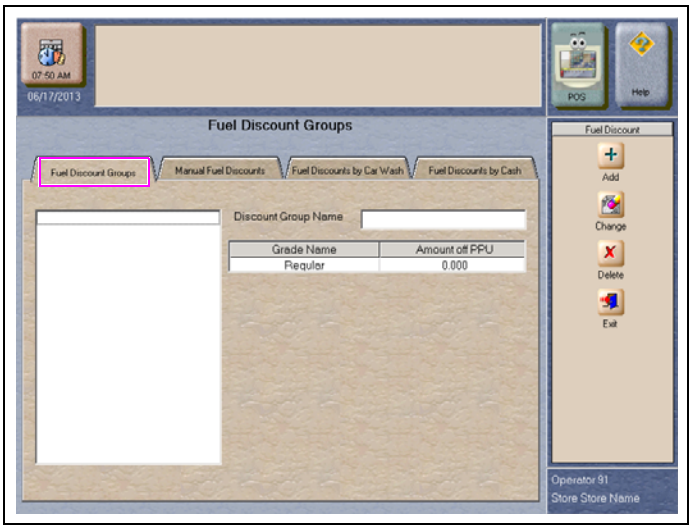
b Refer to *MDE-4905 Passport Approved Launcher Application User Instructions* for installing third-party software.

5 Fuel Discount Programming

After the CWSs have completed the upgrade process, review fuel discount programming to ensure discounting parameters are equivalent to those programmed before the upgrade.

a Review **MWS** > **Fuel** > **Fuel Discount Maintenance** programming (specifically Fuel Discount Groups) and assist the store manager in making necessary changes. Refer to the network addendum for instructions on changes that may be required (see step 14 on page 11 for a list of Passport V10 network addendum documents).

Figure 20: Fuel Discount Maintenance



b Review **MWS** > **Set Up** > **Network** > **Fuel Discount Configuration** programming and assist the store manager in making necessary changes to apply fuel discounts to card types. Refer to the network addendum for instructions on changes that may be required (see step 14 on page 11 for a list of Passport V10 network addendum documents).

6 Verify Time and Time Zone after Upgrade on Server, Clients, and EDH

Ensure the Time and Time Zone on the Passport Server, Clients, and EDH are correct for the store's location.

7 Verify Network Changes

Refer to the network addendum to determine whether network changes are required or you must contact the network after the upgrade (see step 14 on page 11 for a list of Passport V10 network addendum documents).

8 Validating Credit and Debit Operations

a Run a test transaction for credit and debit at the forecourt and inside to validate transactions are approved by the host network.

b Confirm that transactions are not being authorized in Store and Forward.

9 Upgrading the Passport Firewall Router, if required

The original release of the black Cisco Router may not allow traffic through the Demilitarized Zone (DMZ) properly and could prevent third-party interfaces that rely on the DMZ to come online. If you have the router shown in Figure 21 (ii), refer to "Appendix D: Upgrading Cisco VPN Router (RV042) Software to V4.1.1.01-tm" on page 31 for instructions on validating or upgrading the router firmware.

Figure 21: Linksys® and Cisco Routers

(i)

Router with Updated Firmware

(ii)

Firmware Must Be Checked and Updated, if Required

10 Feature Bundle Activation

To perform feature activation, contact the Gilbarco Help Desk.

V10.00 introduces a new feature, Multiple Loyalty Interface, which the store may find beneficial. This feature allows the store to offer more than one loyalty program. The customer may select from the available loyalty programs which one to apply to the transaction.

Figure 22 and Figure 23 provide comparison feature bundle activation screenshots pre-V10.00 and post-V10.00 respectively.

Figure 22: Passport Feature Bundle Activation (Pre-V10.00)

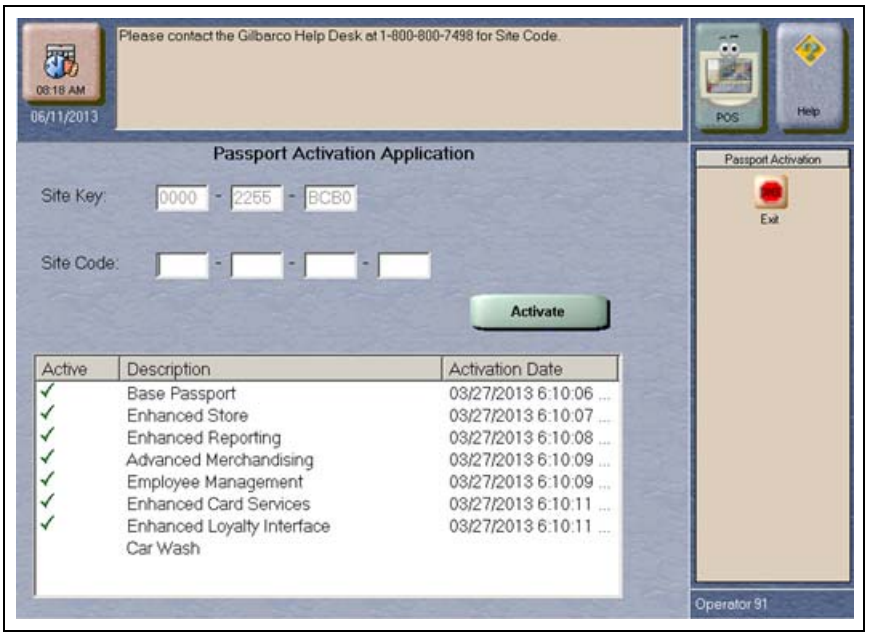
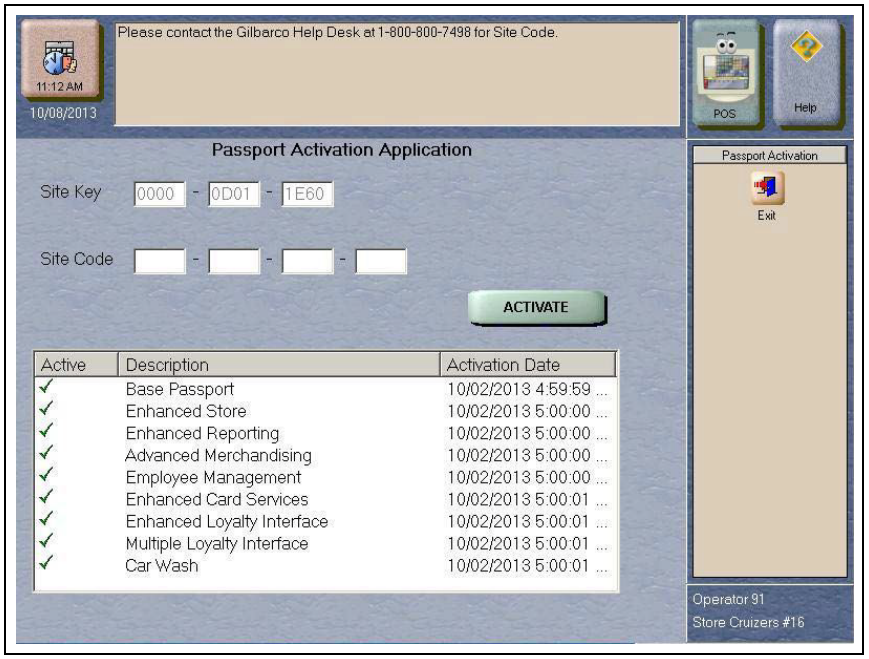


Figure 23: Passport Feature Bundle Activation V10.00



11 RAS Verification
Repeat step 4 on page 6 to ensure RAS is still functional.

12 Disable RAS and EDH Remote Support.

13 Check the Report Printer Font

a Select **Start** > **Printers and Faxes**.

b Right-click **Okidata printer** and select **Printing Preferences**.

c Click the **Job Options** tab.

d Increase or decrease scale per site specifications.

e Press **Apply** and then **OK**.

14 Finalize Training with Onsite Personnel
Review the network addendum with the store manager.

a Review the Reports section.

b Review the Passport Onsite Training Checklist in "Appendix B: CRIND/Pump Software/ Firmware Recommendations" on page 27 and answer any questions the store manager has regarding the topics listed.

15 Open the Store
Perform the following tasks to open the store:

a Remove all blockades from dispensers and POS positions.

b Allow the site to begin trading.

c Monitor the site operation for 15 to 25 minutes to confirm all operations are smooth and contact the Gilbarco TAC support team with any concerns.

16 Before leaving the location
Give the store manager the Security Manager Report and destroy any loose pieces of paper you may have used to store password information temporarily.

Appendix A: Pre-upgrade Checklist

The following table lists the items required before performing the Passport V10.00 upgrade. Check the items off as you complete them.

Checklist Item	Item Definition	Complete
ASC Completed Online Training Course	Contact training@gilbarco.com to enroll in the V10.00 upgrade course.	
Security Manager Report	Must be available in case of failure during upgrade. Verify that Security Manager password function properly before beginning the upgrade. Contact TAC if unable to locate for instructions on disabling security and loading V10.00 with minimal data loss.	
Passport Running V8.02 or Later	Upgrade paths from Passport versions previous to V8.02 are not supported. Software versions earlier than V8.02 must be upgraded to V8.02, 8.03, 8.06, 8.07, or 9.00 before upgrading to V10.00.	
Dispenser Firmware Minimums Met	"Appendix B: CRIND/Pump Software/Firmware Recommendations" on page 27. Gilbarco recommends upgrading dispenser firmware to the latest version if the site intends to implement new functionality, such as Contactless payment, fuel price changes, loyalty, etc.	
Internet Connectivity Confirmed	If there are issues with the Internet connection or other network infrastructure issues, who do you call to ensure you have the IT/ISP contact information available in the event of Internet connectivity issues? Gilbarco is not structured to support site level network connectivity outside the Passport Local Area Network (LAN). *Note: Customers using third-party network infrastructure management companies like Cybera® or MegaPath® may be required to contact these companies well in advance to open up the required ports on their router and to have static IP addresses assigned.*	
Notify Network	Notify the network that you will be performing a software upgrade so they can make any necessary changes on their end.	

Appendix B: CRIND/Pump Software/Firmware Recommendations

IMPORTANT INFORMATION
Gilbarco provides the following information regarding pump and dispenser hardware and software versions in production at the time of development and release of Passport software. Gilbarco recommends that, for optimum performance, these versions be installed at the time of or prior to upgrading the site. Gilbarco has tested Passport software using a sample subset of these versions. Gilbarco provides no warranty, expressed or implied, covering the following hardware and software versions, other versions, or combination of versions operating in the field.

CRIND BIOS Versions

CRIND BIOS Versions	Current Production Release
Single-line and Monochrome (InfoScreen® not supported)	20.9.10
SMARTPad™/MOC EPP	22.5.40
EPP and SCR	42.2.10
Barcode Scanner	25.1.70
SPOT	N/A
Exceptions	N/A

Encore/Eclipse/Automated Attendant (500 Series)

Encore/Eclipse/Automated Attendant (Series 500)	Current Production Release
CRIND Control Node (CCN) Software	3.2.50
Pump Control Node (PCN) Software	
PCN 1	1.8.30
PCN 2	2.8.30
Door Node Software	1.0.47 or higher

Encore 700 Series (NGP)

Encore 700 Series (NGP)	Current Production Release
CRIND Platform Software	2.0.14

Pump Firmware

Pump Firmware	Current Production Release
Advantage Firmware	70.9.92
Advantage Single-hose MPD	72.4.30
Advantage Fixed Blender	77.4.30
Blender Software Chip	10.6.5
Advantage Selectable Blender	75.6.10
Blender Software Chip	10.6.5
Advantage Super High	82.1.10
Advantage Optimized MPD	30.2.41
Advantage Optimized Single-hose MPD	32.1.01
Advantage Optimized Six-hose Blender	37.1.4
Advantage Optimized Single-hose Blender	35.5.20
E300 MPD: Enhanced Security	20.2.24
E300 Single-hose MPD: Enhanced Security	22.2.14
E300 Six-hose Blender: Regular	27.1.10
E300 Single-hose Blender: Sunoco	25.1.90
Others - Enhanced Security	25.3.20
E300 Ultra-Hi™ Regular	20.1.10
Enhanced Security	20.2.24
E300 MPD with Proportional Control Valve: Regular	10.1.10
Enhanced Security	10.2.23
E300 Single-hose MPD with Proportional Control Valve: Regular	12.1.20
Enhanced Security	12.2.14
E300 Six-hose Blender with Proportional Control Valve	17.1.10
E300 Single-hose Blender with Proportional Control Valve: Regular	15.2.20
Enhanced Security	15.3.20
Salesmaker Pro Blender	62.2
MPD Precision Blender	68.1
Legacy®	70.9.92
Legacy Ultra-Hi: Program Pump Preset	84.2.8
5-button Preset	84.3.41
MPD 1 or 3 with Screened Image Display (SID)	53.7.1
MPD with Liquid Crystal Display (LCD)	54.3.10

Display Firmware

Display Firmware	Current Production Release
Modular	53.7.1
MPD-LCD	54.3.10
Monochrome CPU Board	15.1.70
Color E500S	1.2.10

Competitive Dispensers

Competitive Dispensers	Version Release Date
Wayne®	
Legacy CAT (Vista 1, Vista 2) US Market	6.6 - 7/15/2004
Dual CAT (Vista 3) US Market	105.00 - 1/12/2004
Canadian Secure Dual CAT Canada Market	101.00 - 12/20/2000
qCAT (Ovation Series) US Market	207.00 - 5/13/2004
iX CAT (Ovation Series - Blue Board) US Market	2.01 - 8/18/2008
iX US EPP (Ovation Series - Blue Board, Tokheim® Retrofit Kits) US Market	1.1.28.0/1.2.16.0 - 1/31/2012
iXPAY R2 (Ovation Series, Vista 4 - Red Board/Blue Board, Tokheim Retrofit Kits) US Market	2.2.18.0 - 3/9/2012
iXPAY EMV (Ovation Series, Vista 4 - Red Board/Blue Board, Tokheim Retrofit Kits) Canada Market	2.2.15.0 - 3/27/2012
Tokheim	N/A

Competitive Pump and CRIND Software and Firmware

Passport software supports an interface to Wayne and Tokheim electronics using current communication protocols. It is recommended that the software and firmware in competitive equipment be cross-referenced with the appropriate vendor to ensure it is current and supports site operation requirements (for example, fuel discounting, loyalty, and so on). If the software and firmware are NOT current (or does not support site operation requirements) then the competitive equipment must be upgraded as per the vendor's requirements.

Appendix C: Manager's Punch List

Provide this punch list to site personnel 24-48 hours before the upgrade. This will ensure they are aware of the upgrade, the things they must do in preparation, and the impact the upgrade will have on their business day.

- It is recommended that a store close be performed the day of the upgrade.
- Print all necessary period and network reports before the day of the upgrade.
- The upgrade process takes 4-5 hours if no issues are encountered. During this time, the site will not be able to sell fuel or merchandise through the POS.
- Here are a few things the manager can do to minimize down time:

  - Document the following site information:

Store Number	
Site Address	
Site Phone Number	
Network Site ID	

  - Present the technician performing the upgrade with the Security Manager Report (without this report, your store will be closed an additional 4 to 5 hours to disable Passport System Security and perform system recovery. In addition, all historical network data will be lost as a result of disabling system security.

  - Close out tills on additional registers as early as possible and start preparing for your store close as soon as the technician arrives on site.

- It is highly recommended that dispensers are not operated in a standalone mode during the upgrade. This can cause issues with total reconciliations between the POS and dispensers resulting in additional down time. Gilbarco will not be held accountable for additional down time related to activity that allows dispensers to operate in a standalone mode during the upgrade.

- If the site uses a third-party company to manage their Internet connection, they must ensure that the appropriate ports are open on the third-party routing device to allow Internet connectivity. In some cases, this can take up to a week to implement.

Appendix D: Upgrading Cisco VPN Router (RV042) Software to V4.1.1.01-tm

IMPORTANT INFORMATION
Before upgrading the firmware, determine if Passport Primary Router replacement or upgrade is required by verifying the software version. The original release of the black Cisco Router does not allow traffic properly through the DMZ and will prevent third-party interfaces relying on the DMZ from coming online. Due to this, Loyalty connections cannot be made.

Confirming Current Passport Firewall Configuration

Figure 24: Linksys Router and Cisco Router

(i)

Router with Updated Firmware

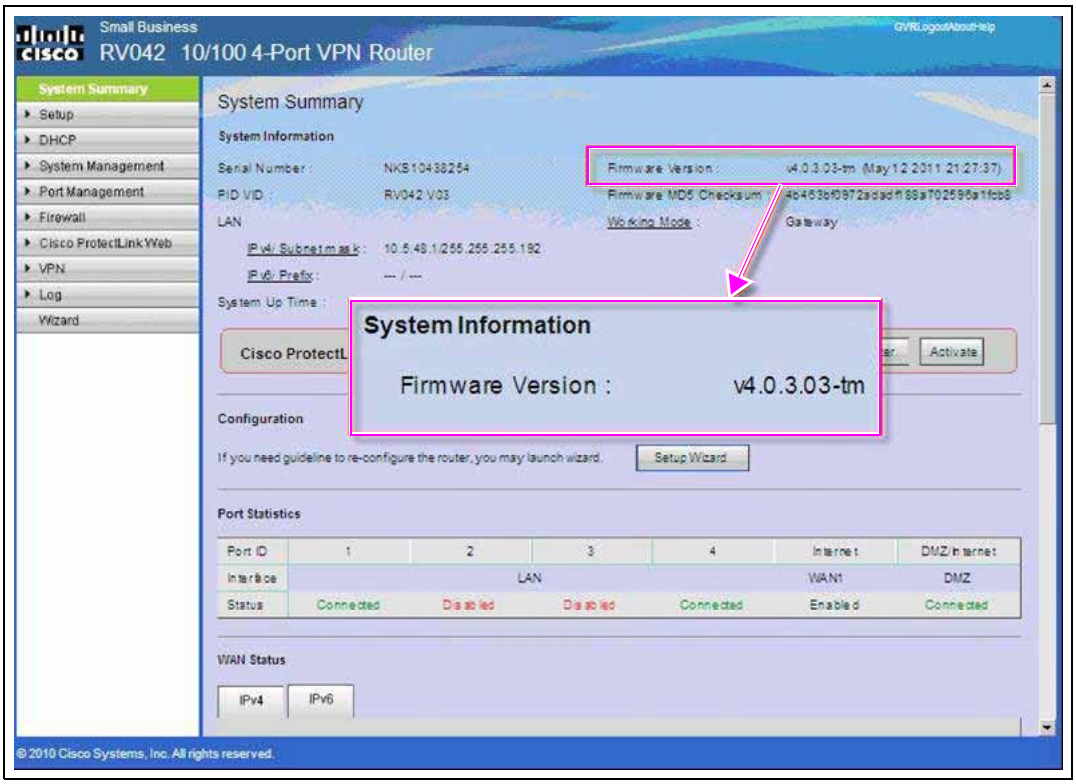
(ii)

Firmware Must Be Checked and Updated, if Required

Connect to the router using Passport Image Control Panel through System Maintenance. Verify the current router configuration by accessing the System Summary section and performing the following upgrade steps.

If the current version is earlier than V4.1.1.0-tm, the router must be upgraded. An example of a router that requires upgrade is shown in Figure 25.

Figure 25: System Summary Screen



Note: The firmware upgrade file RV0XX-V4.1.1.01-tm-20111109-code.bin may be downloaded from the Gilbarco File Transfer Protocol (FTP) Server at: ftp://ftp.gilbarco.com/Passport/Peripherals/Router config 8.02/Cisco Router 08-B.

VPN Router Upgrade Process

IMPORTANT INFORMATION
Before proceeding with the firmware upgrade, it is **HIGHLY recommended** that you have a spare secure Firewall Router onsite for backup purposes in case the upgrade fails due to a power fail and/or a corrupted file downloaded from the FTP site, either a Linksys (Q13708-07 A/B) or Cisco (Q13708-08 A/B) Firewall Router will suffice.

To upgrade the VPN Router, proceed as follows:

IMPORTANT INFORMATION
Ensure all cables connected to the Secure Firewall Router are properly labeled. All devices connected to the Secure Firewall Router must be disconnected before upgrading the Secure Firewall Router. Failure to remove all connections before upgrading the Secure Firewall Router can render the Secure Firewall Router inoperable. After removing all connections to the Secure Firewall Router, connect your laptop to Port 1 on the Secure Firewall Router.

Configuring the Laptop

To program the laptop to use a Static IP Address to communicate on the Firewall Router's LAN, use the following procedures:

IMPORTANT INFORMATION
This procedure requires familiarity with the laptop's hardware and software. To successfully utilize these steps: • Ensure that you have a functional Ethernet® Adapter. • Disable any native or third-party Firewall applications. In addition, all pop-up blocker software must be DISABLED TEMPORARILY. The programming GUI for the replacement Firewall Router requires that pop-up windows be allowed. Failure to disable pop-up blockers will prevent you to access and program the Firewall Router.

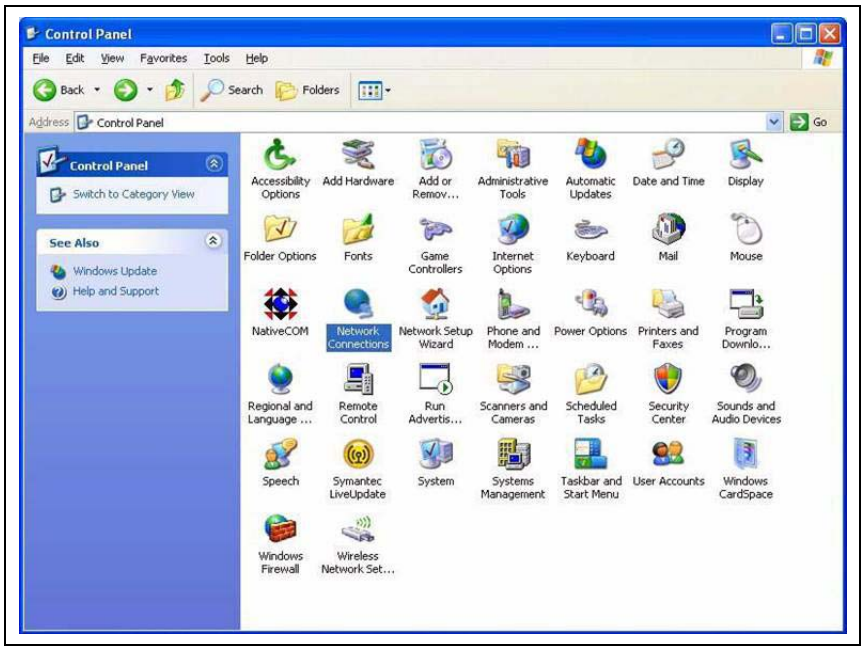
Accessing the Control Panel

To access the Control Panel, proceed as follows:

1 Click **Start** > **Run**. The Run window appears.

2 Type **Control** in the **Open** field and press **Enter**. The Control Panel window appears.

Figure 26: Control Panel



Changing Network Connection Properties

To change the network connection properties, proceed as follows:

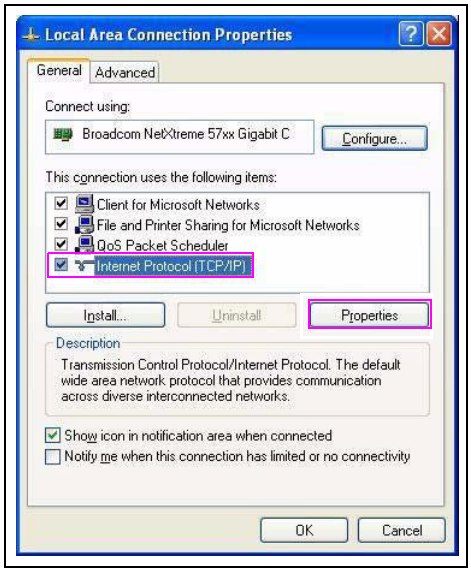
1 Double-click the **Network Connections** icon. The Network Connections window appears.

Figure 27: Network Connections Window

2 Locate the LAN connection used by laptop's Ethernet Adapter.
Note: The name of the connection may vary based on the hardware configured.

3 Right-click the appropriate LAN connection and click **Properties**. The Local Area Connection Properties window appears.

Figure 28: Local Area Connection Properties Window



4 Select **Internet Protocol (TCP/IP)** from the list.

5 Click **Properties**.

IMPORTANT INFORMATION
Make note of the current IP address programming. You must refer to the settings to change the Ethernet Adapter settings for normal usage.

6 Select **Use the following IP address**.

7 Enter the following values in the Internet Protocol (TCP/IP) Properties window:
- IP Address: **10.5.48.18**
- Subnet Mask: **255.255.255.192**
- Default Gateway: **10.5.48.1**

IMPORTANT INFORMATION
10.5.48.18 must be used for the laptop to prevent potential address conflicts. Improper IP address configuration may result in a site down condition when all devices are connected to the router.

8 Click **OK** when programming is complete.

Configuring the Laptop to Access the Router

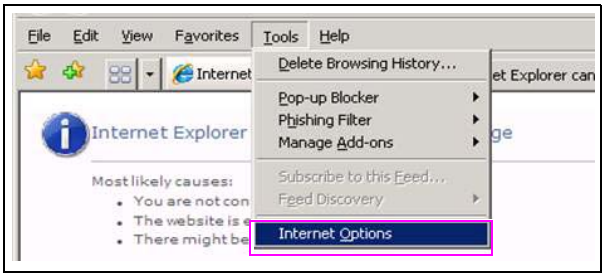
Note: The following procedures MUST be performed on the laptop to access and configure the Firewall Router (must be done only once).

IMPORTANT INFORMATION
The replacement Firewall Router uses only HTTP Secure (HTTPS) to access router configuration. The router's HTTPS address must be added as a trusted site on the laptop; otherwise, Internet Explorer® is unable to display the configuration GUI.

1 Open **Internet Explorer** on the laptop.

2 Navigate to **Tools** > **Internet Options** from the Internet Explorer toolbar.

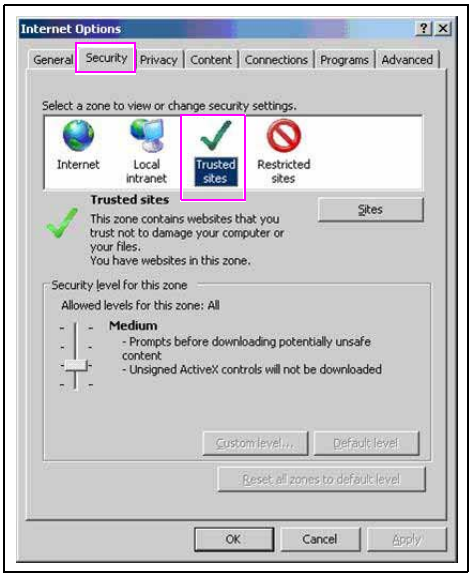
Figure 29: Internet Options



The **Internet Options** window appears.

3 Click the **Security** tab and select **Trusted Sites**.

Figure 30: Trusted Sites

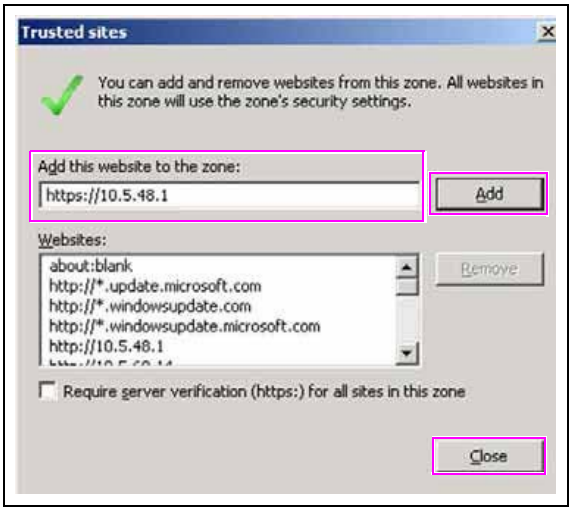


4 Click **Sites**.

Figure 31: Sites Button

The Trusted Sites window appears.

Figure 32: Trusted Sites Window



5 Type **https://10.5.48.1** in the **Add this website to the zone** field.

6 Click **Add**.

7 Click **Close**.

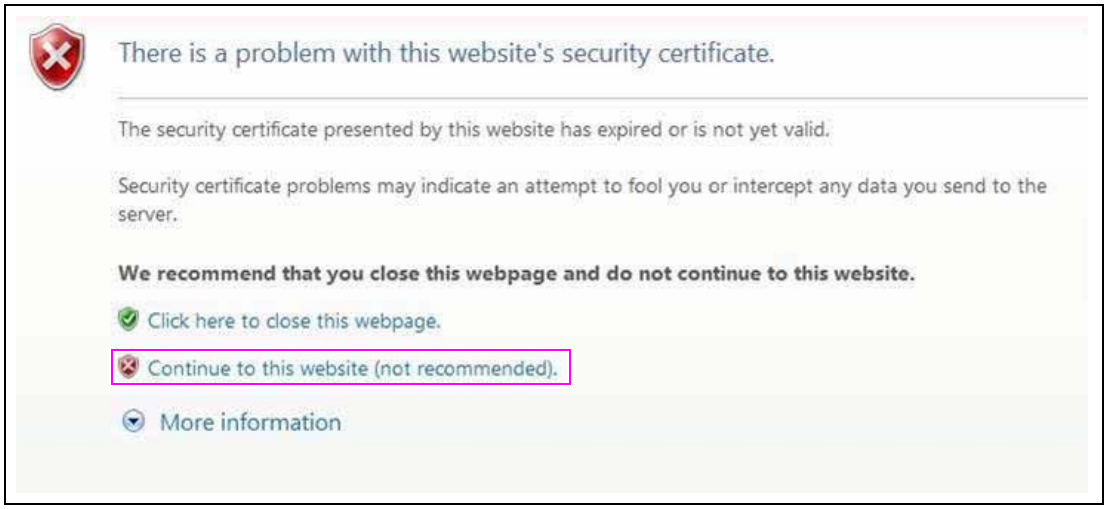
8 Click **OK** on the Internet Options window.

Configuring the Firewall Router

To configure the Firewall Router, proceed as follows:

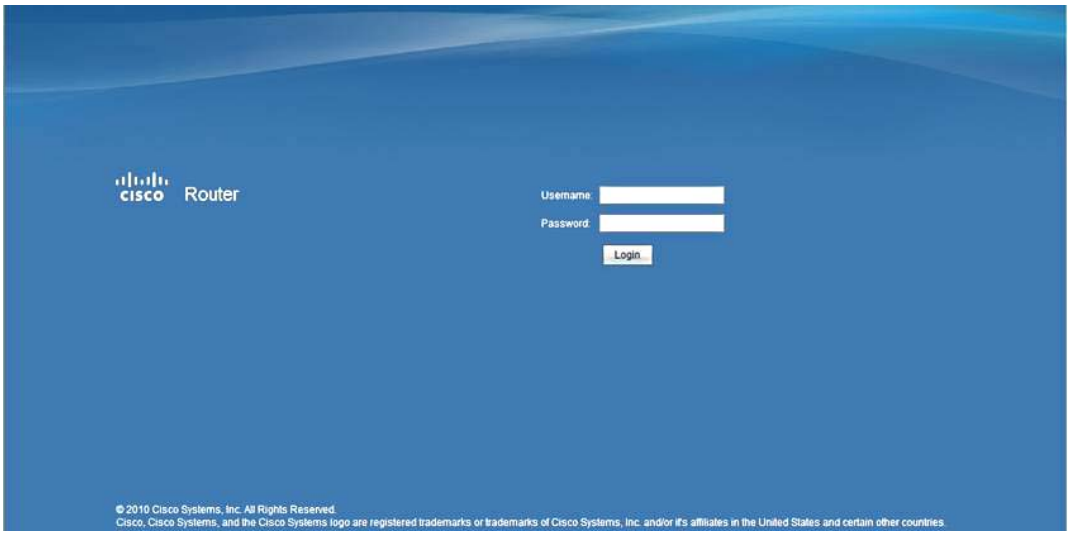
1 Select **Internet Explorer** to access the RV042 Router by typing **https://10.5.48.1** in the address bar and pressing **Enter**.
*Note: You may encounter a screen indicating a problem with the website's certificate. If so, click **Continue to this website (not recommended)**.*

Figure 33: Security Certificate Issue



2 Log in using the router Username and Password from the Security Manager Report.

Figure 34: Login Screen



*Note: Default Username is **GVR** and default Password is **GVRRV02**.*

If done correctly, the screen shown in Figure 35 appears. This is the same screen to confirm the current firmware version.

Figure 35: System Summary Screen

Creating a Backup of Router Configuration

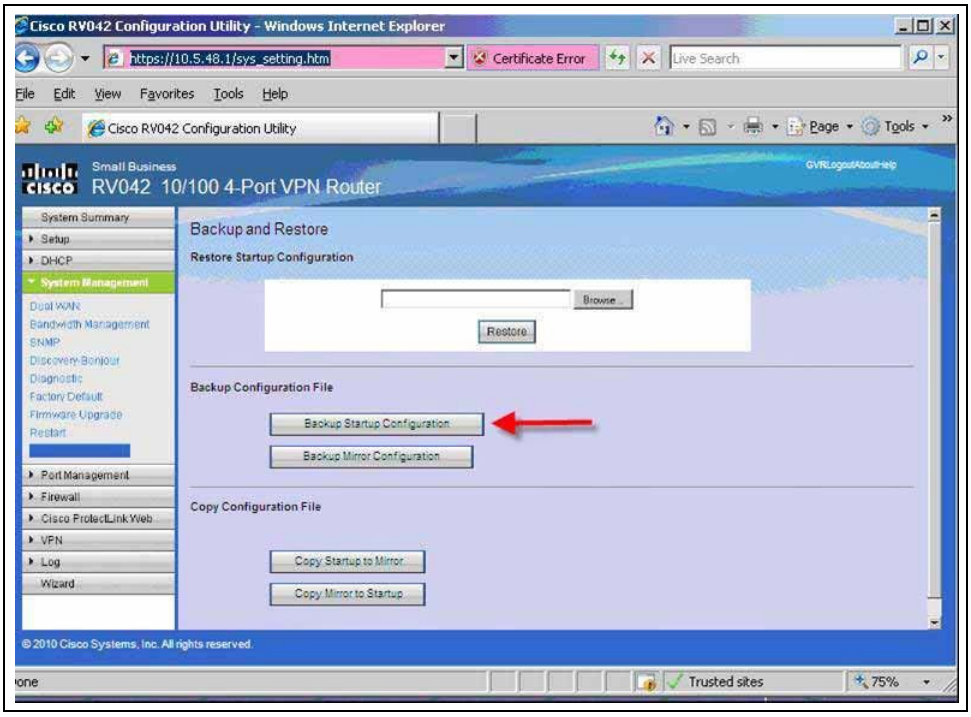
The Firewall Router supports the ability to back up and export configuration files. This function may be used to assist in system recovery, new installations, and router replacements.

IMPORTANT INFORMATION
Exporting router configuration must occur ONLY at this point of configuration. To adhere with compliance requirements, the router configuration must NOT be exported after the site has changed the administrator password.

To back up the configuration that has been previously programmed, proceed as follows:

1 Click the **System Management** tab and select **Backup**.

Figure 36: Backup and Restore Screen



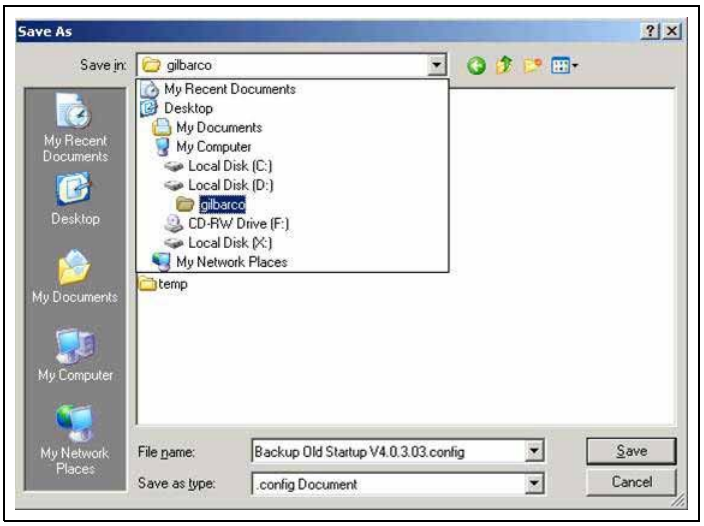
2 Click **Backup Startup Configuration**. The File Download window appears with the message: **Do you want to save this file?**

Figure 37: File Download Window

3 Click **Save**.

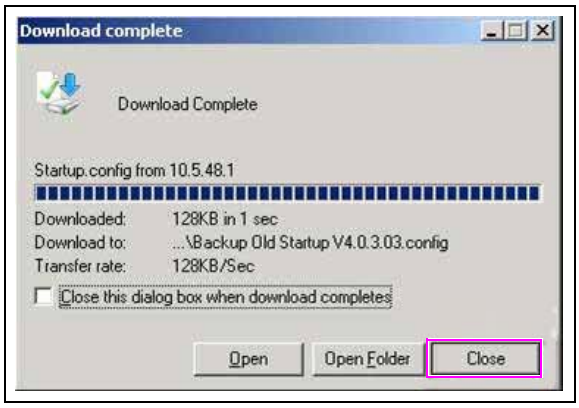
4 Select a location to save the router configuration file. This may also be stores within a device at the location, such as a folder on the D: drive on the Passport Server or an external media provided by the store manager or owner.
Note: The initial backup can be placed on the laptop until the upgrade is complete.

Figure 38: Save As Window



5 Enter a name for the file and click **Save**. The Download Complete window appears.

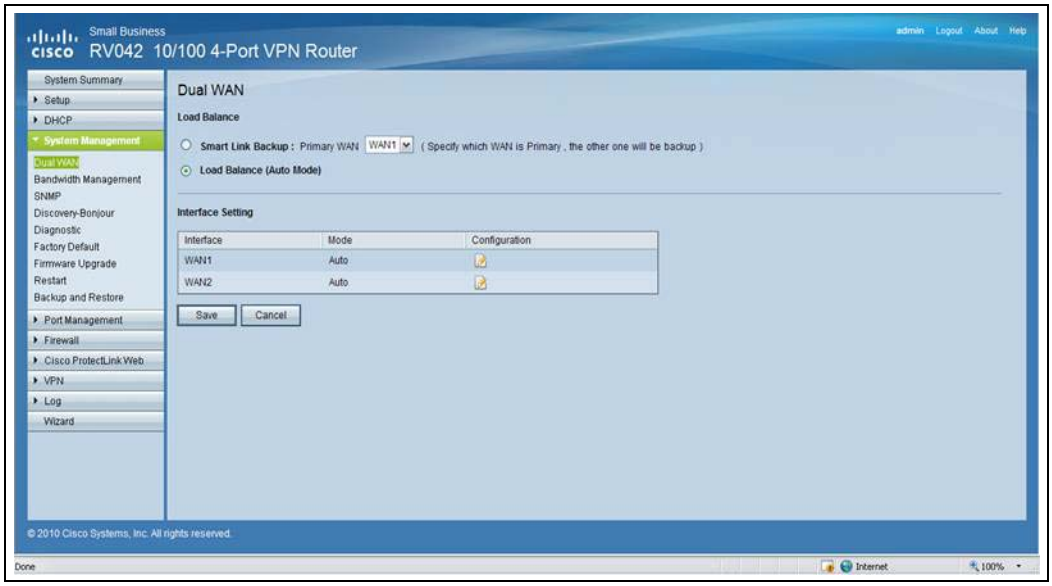
Figure 39: Download Complete Window



6 Click **Close**.

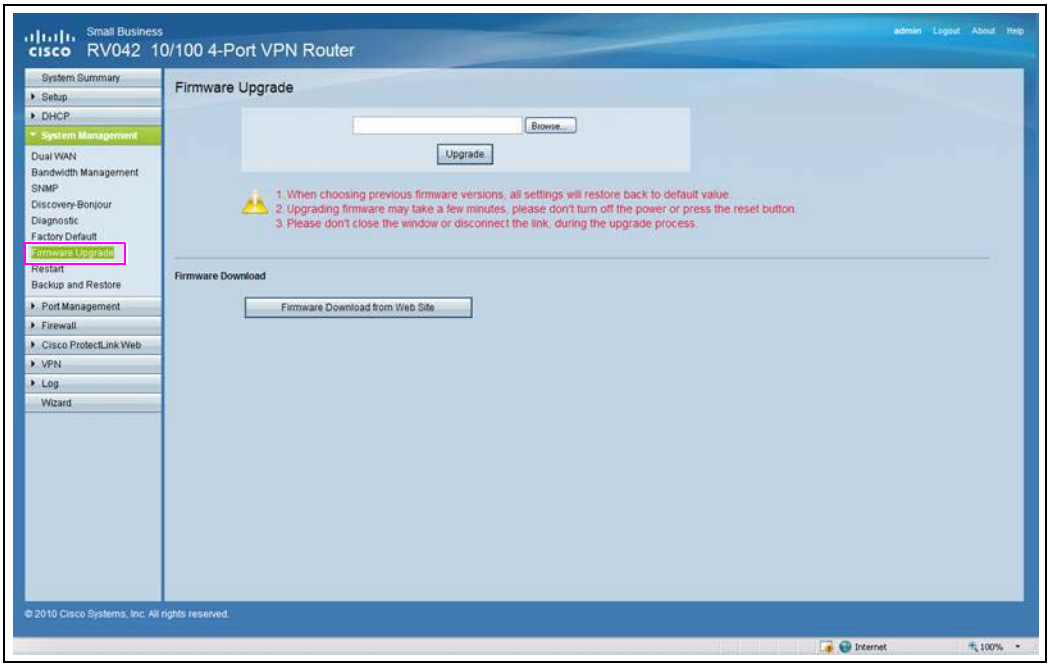
7 After the initial back up is complete, use the drop-down menu and select **System Management**. The Dual WAN screen appears.

Figure 40: Dual WAN Screen



8 Select **Firmware Upgrade**.

Figure 41: Firmware Upgrade Screen



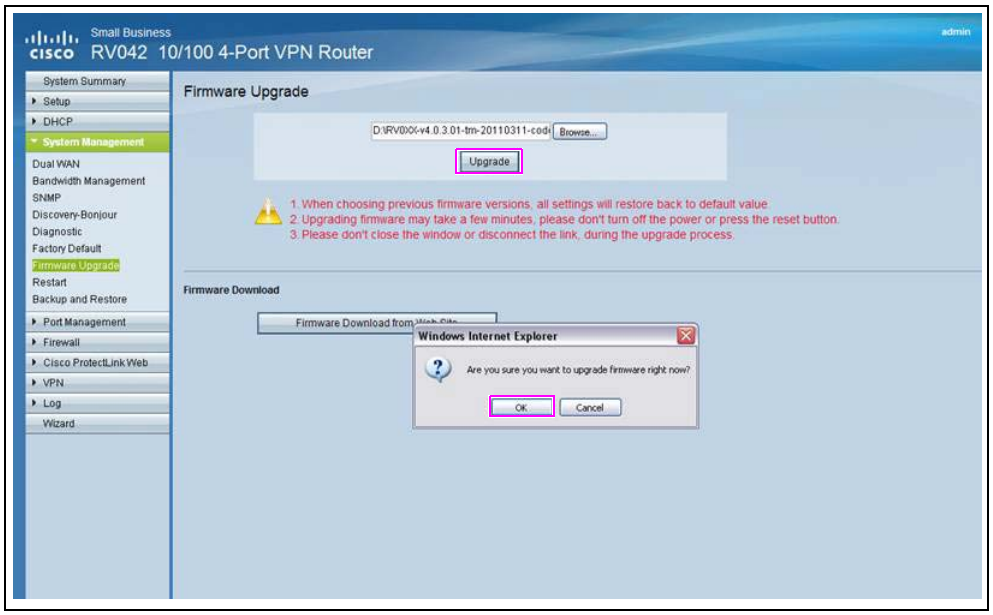
9 Navigate to the directory where the bin file is located using the **Browse** button and then select **RV0XX-V4.1.1.01-tm-20111109-code.bin**.

10 Select **Open** to load the file into the Firmware Upgrade window. The screen indicates the file uploaded.

Figure 42: Firmware Upgrade - File Uploaded

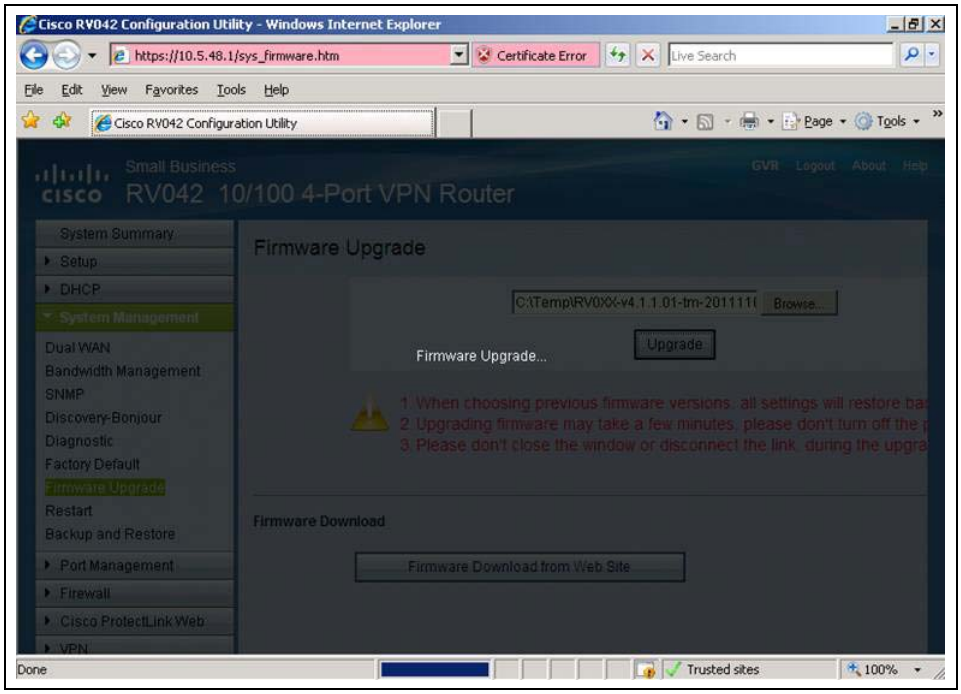
11 Click **Upgrade** to start the process and then click **OK** to continue the upgrade.

Figure 43: Start Firmware Upgrade



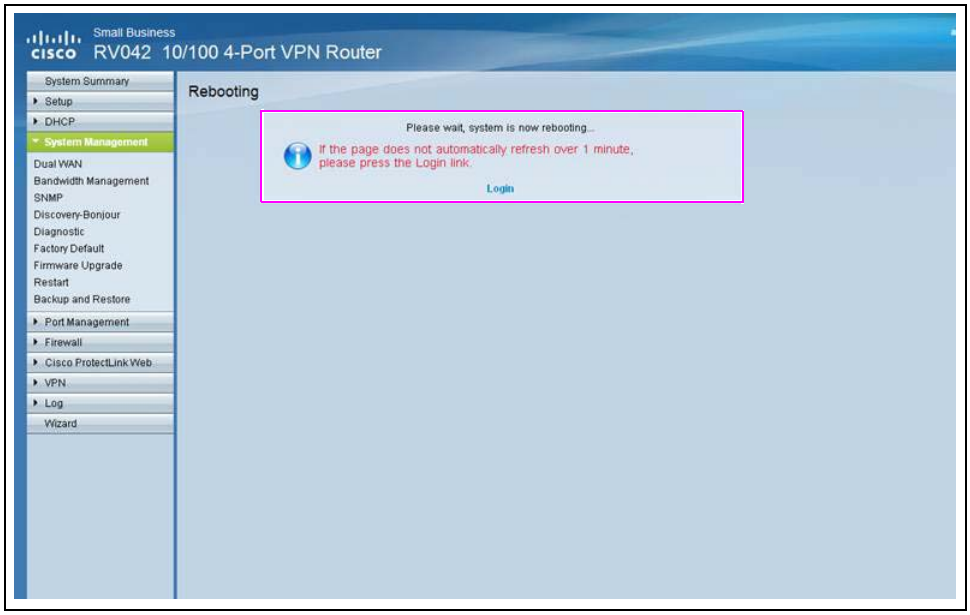
As the process continues, the Firmware Upgrade Processing screen appears. The actual screen may appear slightly different, depending on the Windows version running on the laptop.

Figure 44: Firmware Upgrade Processing Screen



12 When the process is completed, the Rebooting screen appears.

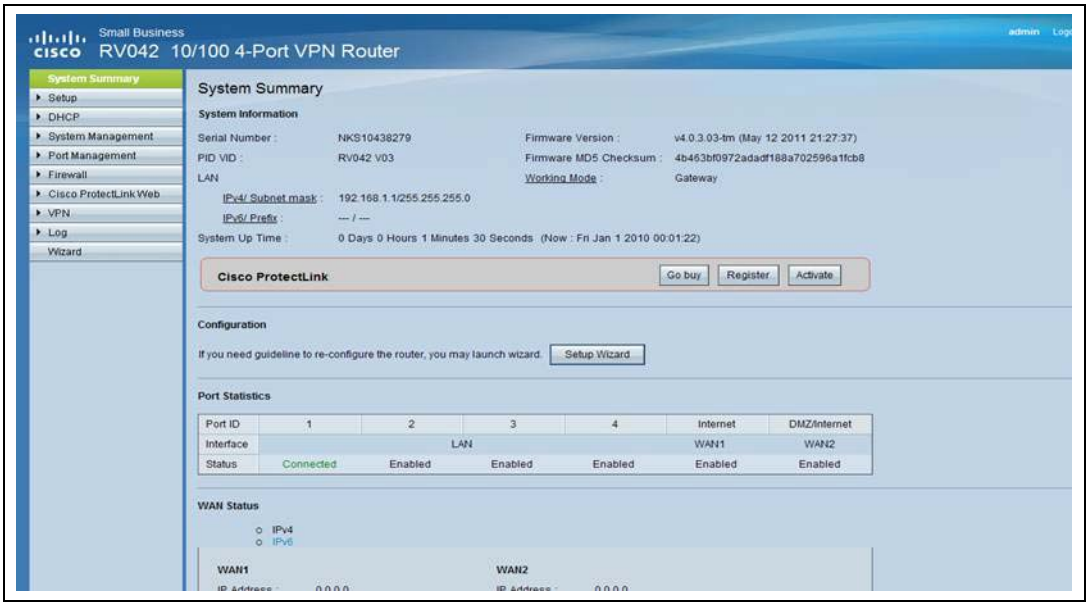
Figure 45: Rebooting Screen



The VPN Router reboots to complete the upgrade.

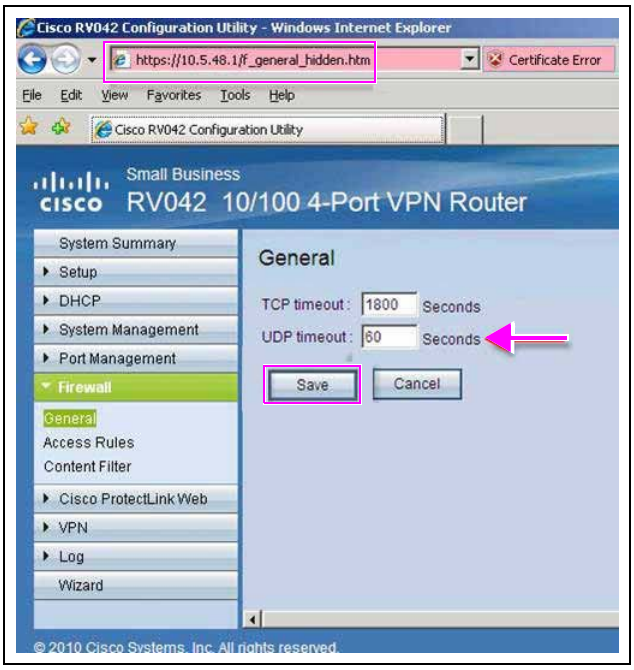
13 After the upgrade is completed, sign back onto the VPN Router and confirm the new version is V4.1.1.01-tm.

Figure 46: System Summary Screen



14 Navigate to **Firewall** > **General** using the drop-down menu and type **https://10.5.48.1/f_general_hidden.htm** in the address bar. Change the UDP timeout value to 60 and click **Save**.

Figure 47: General Tab



15 Reconnect all Passport devices to the Cisco Router that were previously disconnected when the laptop was first connected.

Repeat steps 1 on page 39 through 6 on page 41 to back up the new configuration to the **D:** drive.

16 Select the **Administrative Command Prompt** icon in the Image Control Panel screen and then ping all devices (Server, Clients, EDH, etc.).

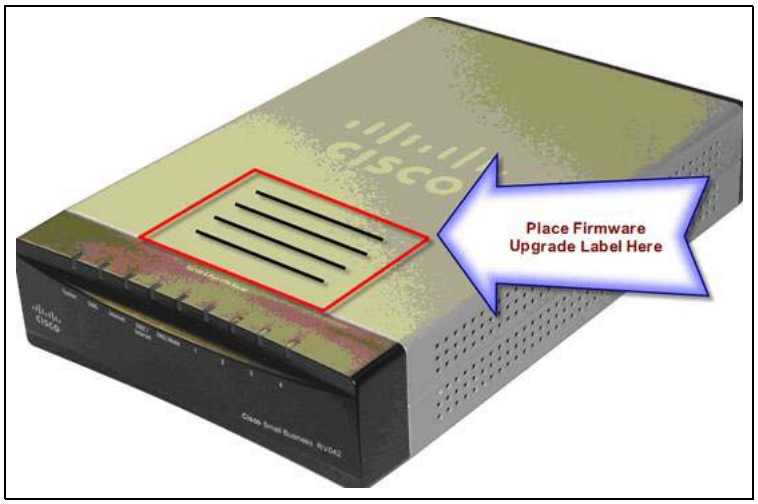
17 After all devices (Server, Clients, EDH, and so on) have been successfully pinged, return the site back to normal operation and verify if the Network is online and third-party devices are working properly, such as Loyalty.

18 After the firmware has been successfully updated and tested, place the supplied label (provided in the software kit) to the Cisco Router [Q13708-08B (firmware V4.1.1.01)] as shown in Figure 48.

⚠ WARNING

Place the label only on the designated area, so as to not block ventilation.

Figure 48: Placing Firmware Upgrade Label



Appendix E: FTP Server Changes for V10.00

This section is not necessary for most Passport stores. Read and ensure you understand this section fully before using these instructions.

Default FTP Configuration

FileZilla Server is a well-known FTP Server that supports both basic FTP and FTPS. Unlike the previous FTP Server, FileZilla Server does not use windows accounts to control access. Account details are stored in configuration file. Passport default configuration contains the following account information:

Account	Root Folder
BackOffice	C:\Passport\XMLGateway
Bos_access	C:\Passport\XMLGateway
GilbarcoFTP	C:\Passport\XMLGateway

Authentication

Both FTPS and FTP are enabled by default, but Gilbarco recommends that customers disable FTP and force all connections to FTPS. FTP is enabled out of the box to allow customers to make this move when their Back Office system vendors are ready.

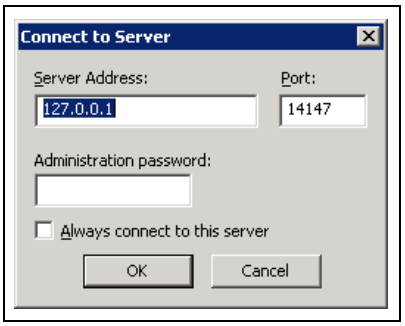
Accessing FileZilla Server Configuration Tool

IMPORTANT INFORMATION
Modify the FileZilla Server configuration IF AND ONLY IF the store uses unique FTP user credentials for their Back Office.

You can launch the configuration tool in two ways:

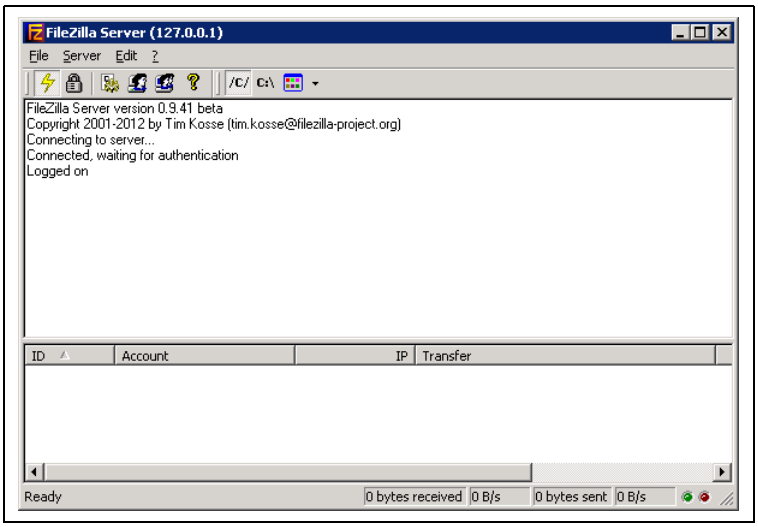
- Launch **Passport Image Control Panel**, and then press the **Add FTP User** button.

Figure 49: FileZilla Server



Enter the password and click **OK**.
Note: If you do not have the password, contact Gilbarco technical support.

Figure 50: FileZilla Server



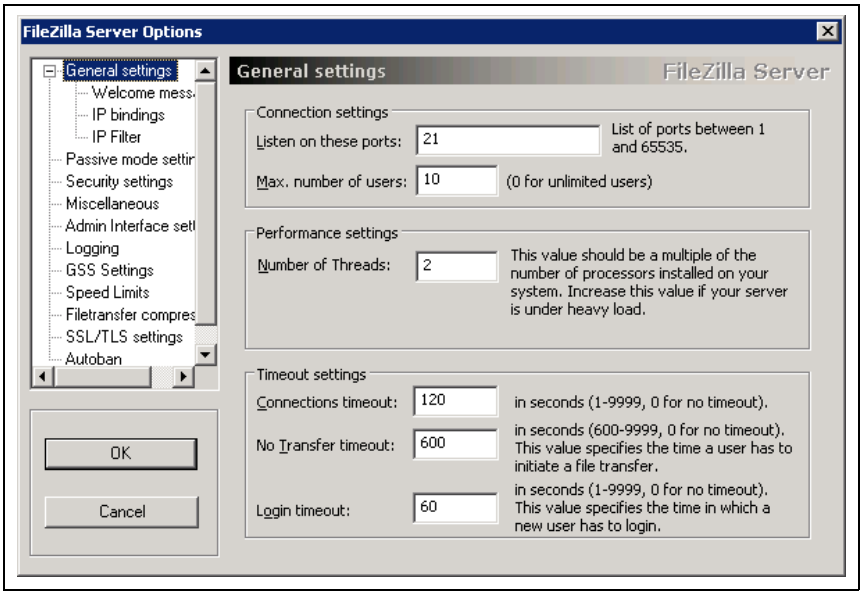
Forcing All Access to FTPS

IMPORTANT INFORMATION
DO NOT force all access to FTPS unless you have confirmed with the store manager or owner that the Back Office System vendor, or other third-party vendors that do file transfer as part of their interface to the Passport system, have implemented FTPS in their software and are ready to support FTPS at this store.

To disable FTP connections, forcing all connections to FTPS, perform the following steps:

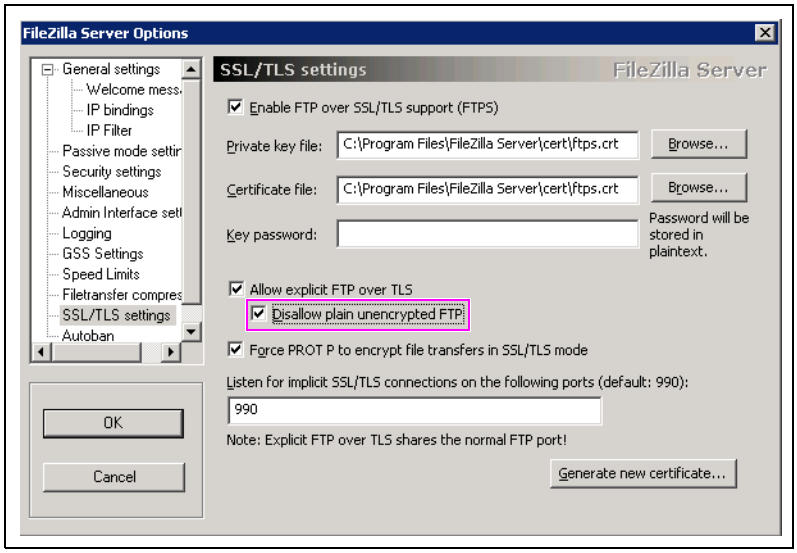
1 From the main menu, select **Edit** > **General Settings**.

Figure 51: FileZilla Server General Settings



2 From the cascading menu on the left side bar, select **SSL/TLS Settings**. Ensure **Disallow plain unencrypted FTP** is checked.

Figure 52: Disallow Plain Unencrypted FTP



Basic FTP connections will now be refused.

Adding Custom Accounts

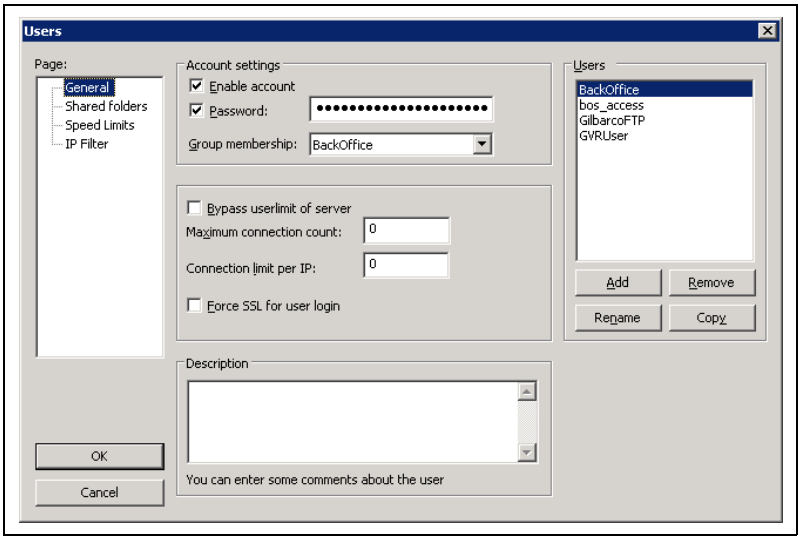
Customers may wish to add their own accounts (users) for Back Office vendors or other purposes. The FileZilla Server FTP Server associates a group of users or a single user with a home folder and allows you to control the level of access the group or single account has to that folder.

Adding a User

To add a user to the Passport Server, proceed as follows:

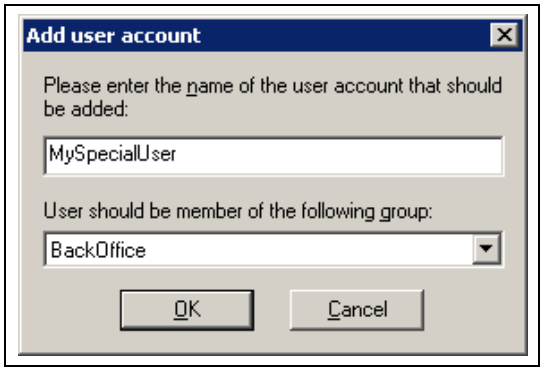
1 Select **Edit** > **Users**.

Figure 53: Edit Users



2 Click **Add**.

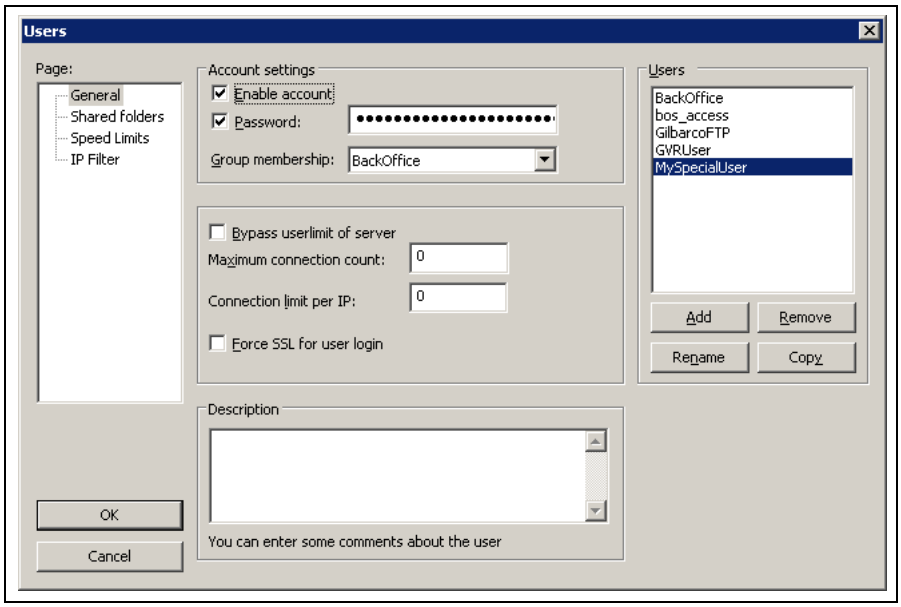
Figure 54: Add User Account



3 Enter the name of the user and select the BackOffice group.

4 Select **OK**. The **Users** window appears with the added new user.

Figure 55: New User



5 Select the **Password**: check box and enter the desired password. The new user account should match the configuration as shown in Figure 55.

Configuring FTPS Access for a Back Office Connected Through the Router DMZ

MDE-4866 Passport Firewall Router Start up and Service Manual describes how to add a secondary router through the DMZ port. In this scenario, the IP address for the router DMZ is 10.5.60.1; a secondary router acts as 10.5.60.14; and, for the purpose of discussion, the machine attempting to communicate with the FTP Server is 10.5.60.16.

Configuring the Router

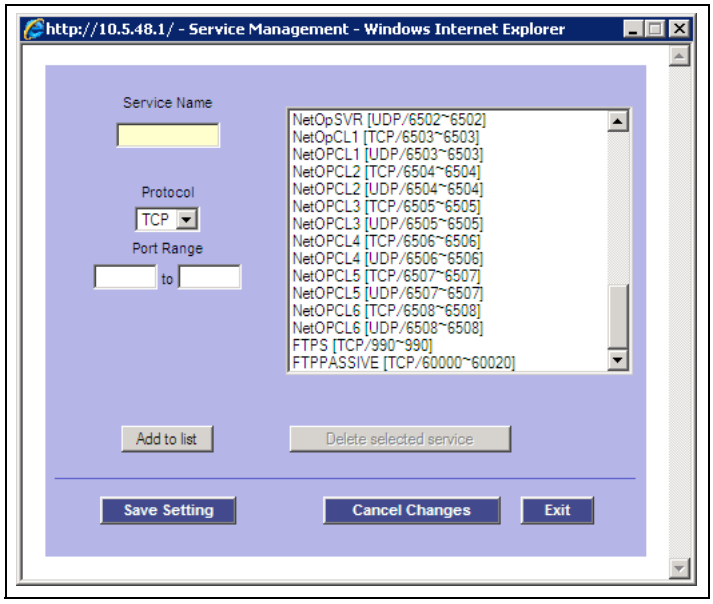
To configure the router, proceed as follows:

1 Log into the router. Select **Setup** > **Forwarding** > **Service Management**.

2 Add the following services:

Service Name	Protocol	Port Range
FTPS	TCP	990 to 990
FTPPASSIVE	TCP	60000 to 60020

Figure 56: Service Management



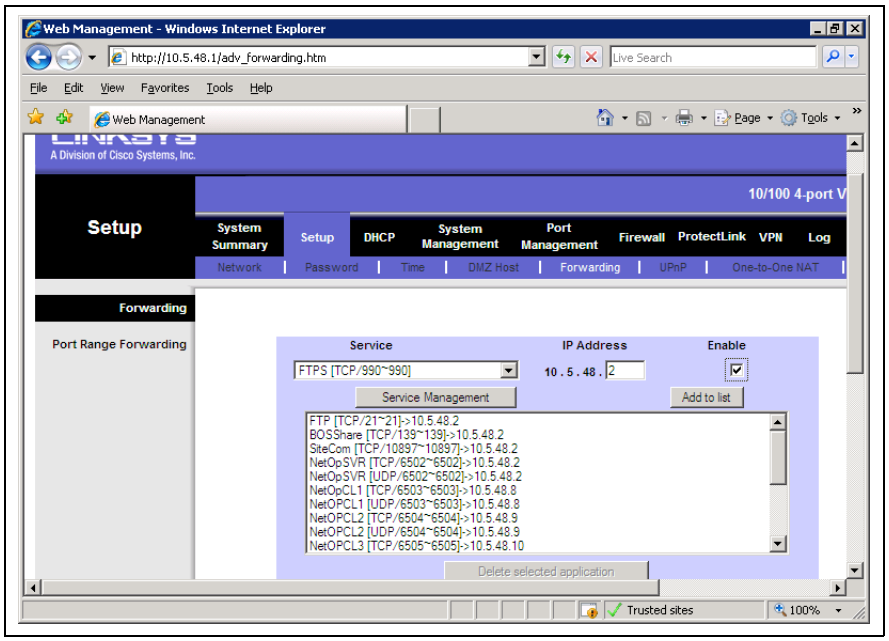
The FTPS entry is for port 990, the port for implicit FTPS connections.

The FTP Passive entry is a range of ports that needed to forward to allow DMZ Clients to make the “passive” data connections.

3 After saving the service entries, add the following forwarding rules:

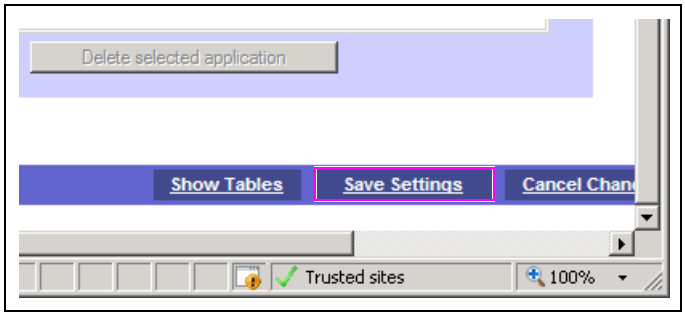
Service	IP Address	Enable
FTPS	10.5.48.2	Yes
FTPPASSIVE	10.5.48.2	Yes

Figure 57: Forwarding Rules for FTPS



4 Select **Save Settings** when completed.

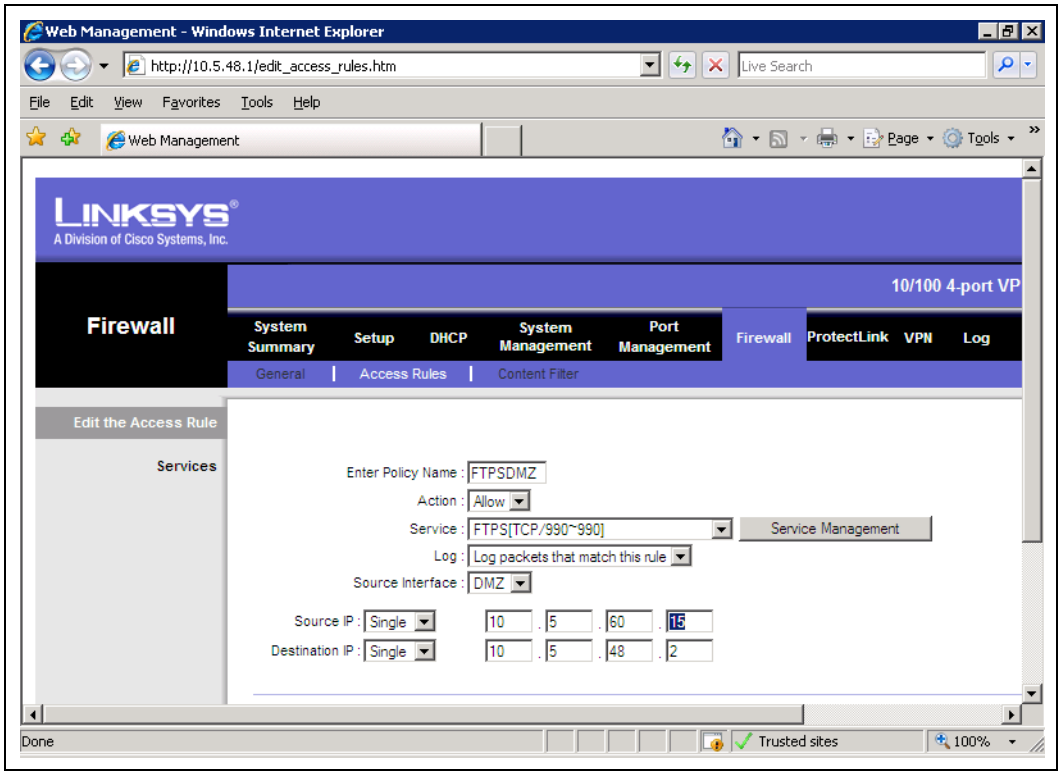
Figure 58: Save Settings



5 Navigate to **Firewall** > **Access Rules**.

6 Add a new rule (FTPSDMZ) to allow connections from the DMZ on port 990 (FTPS) to 10.5.48.2.

Figure 59: Adding New Rule



7 Select **Save settings**.

Configuring FileZilla Server for Passive FTP

To configure FileZilla Server for Passive FTP, proceed as follows:

1 Launch the FTP Server interface on the Server.

Figure 60: Connect Server

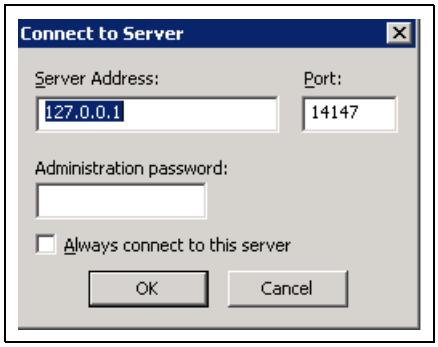
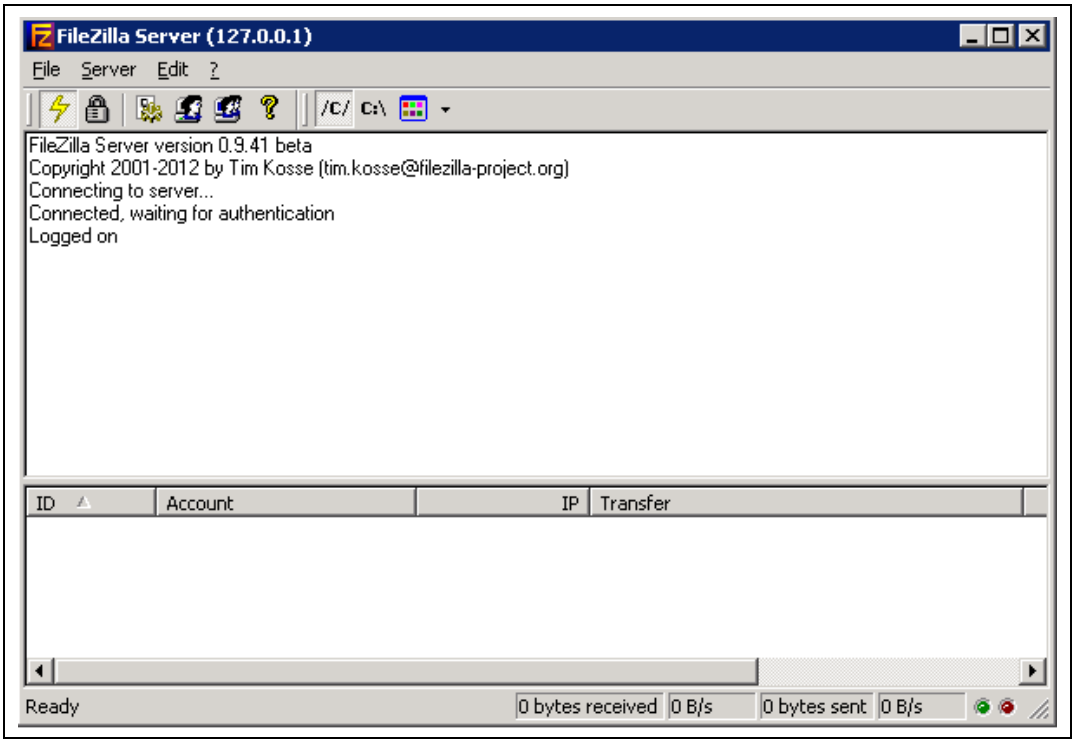
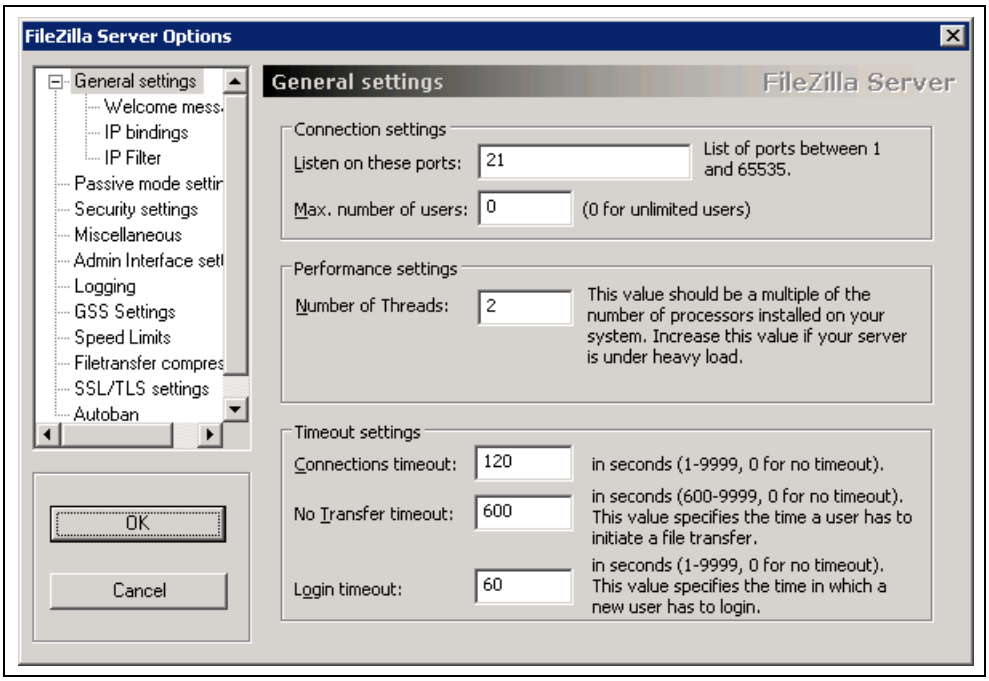


Figure 61: FileZilla Server Interface



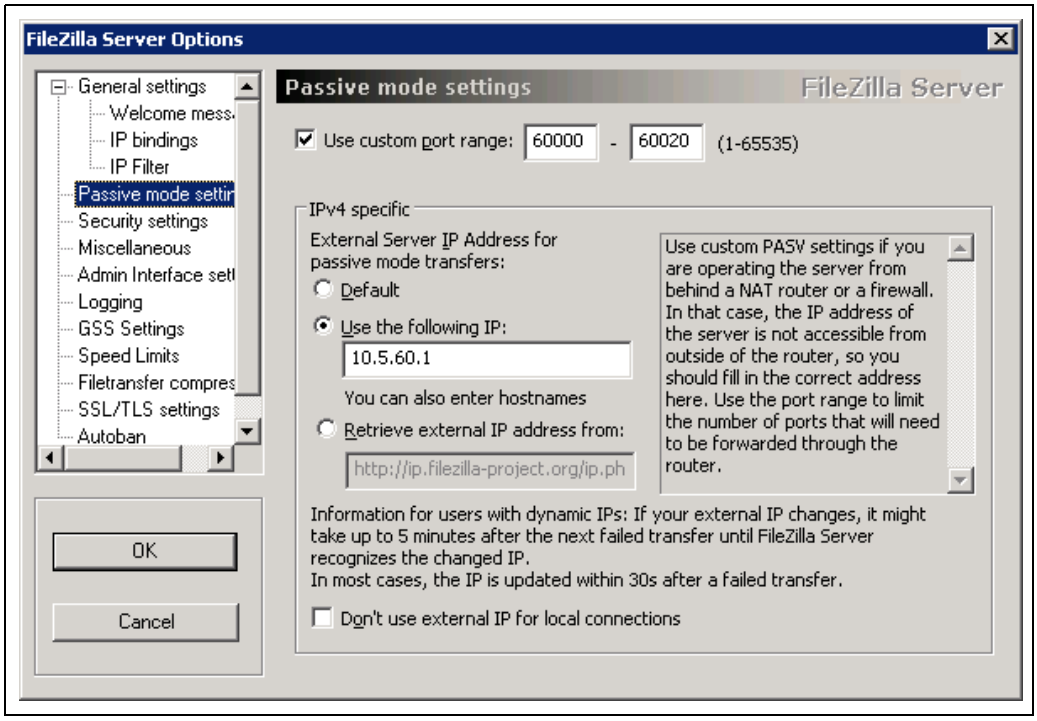
2 From the main menu, select **Edit** > **Settings**.

Figure 62: FileZilla Server Options



3 Using the left sidebar, navigate to **Passive mode settings**.

Figure 63: Passive Mode Settings



4 Enable **Use custom port range** and enter the range 60000 – 60020. In the IPv4 specific frame, select **Use the following IP** and enter 10.5.60.1 (the DMZ address on the router).

5 Ensure **Don't use external IP for local connections** is not selected.

6 Click **OK** to save the settings.

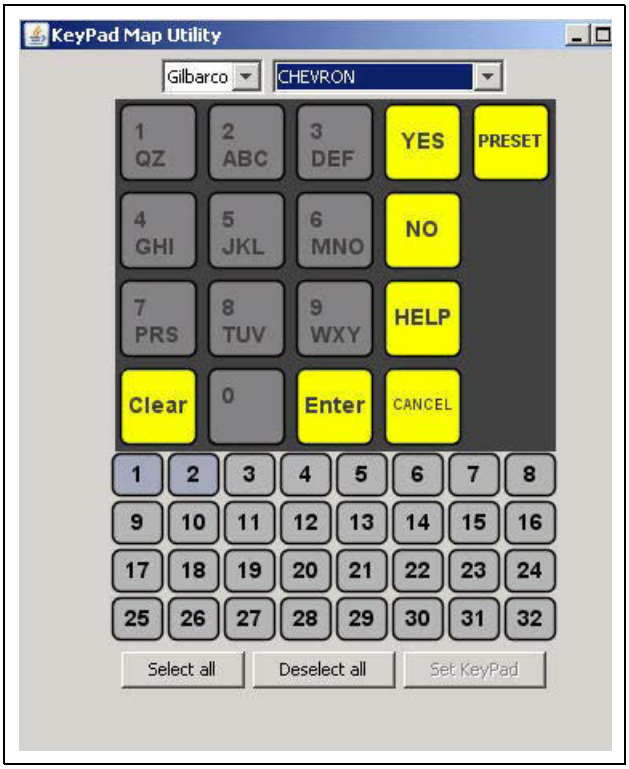
Appendix F: Single-line CRIND Keypad Configuration

If Single-line display CRIND devices are in use, it is necessary to select the appropriate CRIND keypad. To select the CRIND keypad, proceed as follows:

1 On the Passport Server, select **Windows Explorer** and go to **C:\Passport\Installs\bin**.

2 Double-click **changekeypadid.bat**. The **KeyPad Map Utility** window appears.

Figure 64: KeyPad Map Utility



3 Use the drop-down menu to select the appropriate keypad type.

4 Select **Set KeyPad**. A pop-up window appears indicating the Passport system must be restarted for these changes to take effect.

5 Select **OK**.

6 Select **Exit**.

7 Close **Windows Explorer**.

Appendix G: Enable or Disable Force Pay - Debit Key Prompt

A dispenser configured with the Force Pay option causes the CRIND to display prompting to the customer regarding method of payment selections and suppresses the call signal from the dispenser until the customer selects a method of payment for the transaction.

Note: Although Texaco branded locations usually use the Force Pay option, Chevron branded locations and non-branded locations on the Chevron network may enable the Force Pay option, as well, at the store owner's discretion. If these locations use single-line CRIND display dispensers, the CRIND keypad overlay may require replacement to provide proper payment key selections.

To enable or disable the Force Pay option for CRIND devices, proceed as follows:

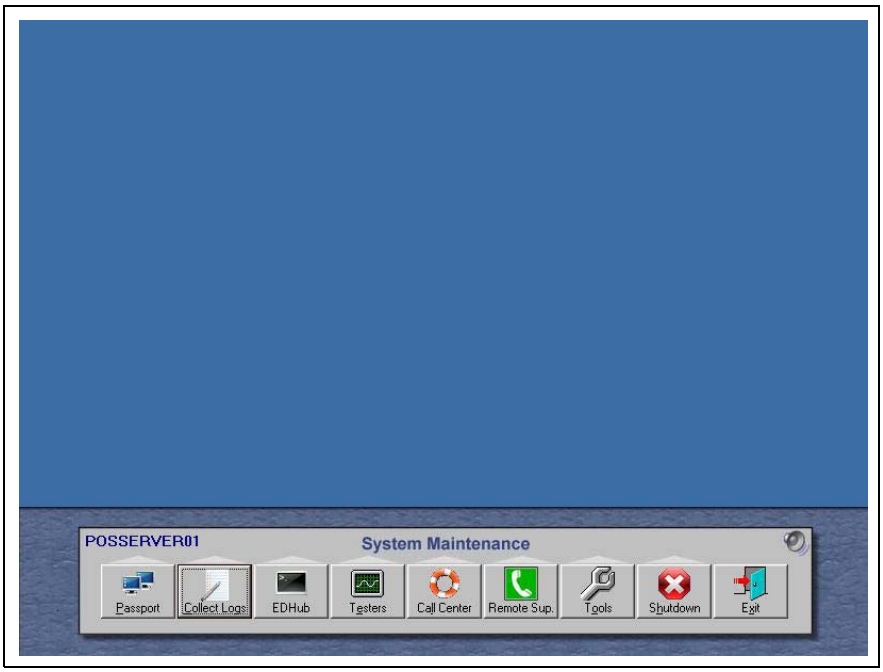
1 Access **System Maintenance** by pressing and holding the **CTRL**, **ATL**, and **P** keys on the Passport Server keypad. The System Maintenance login screen appears.

2 Enter the appropriate User Name and Password for Level 2 System Maintenance access. The System Maintenance toolbar appears.

Figure 65: System Maintenance Toolbar

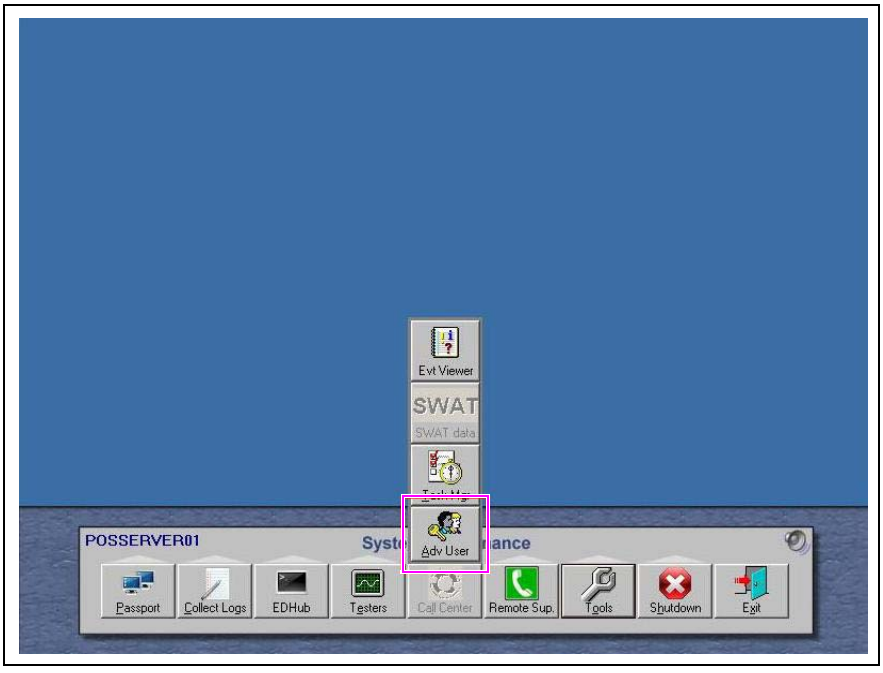
3 Select **Passport** > **Stop**. This stops all Passport processes. The Passport Server touch screen appears as a Windows desktop with no icons and the System Maintenance toolbar.

Figure 66: Passport Processes Stopped



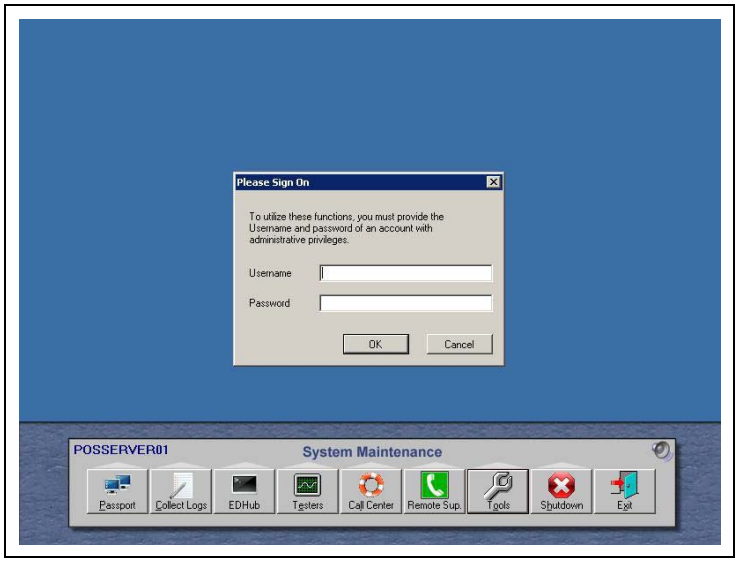
4 Select **Call Center** > **Adv User** on the System Maintenance toolbar.

Figure 67: Call Center > Adv User



5 The **Please Sign On** window appears.

Figure 68: Please Sign On

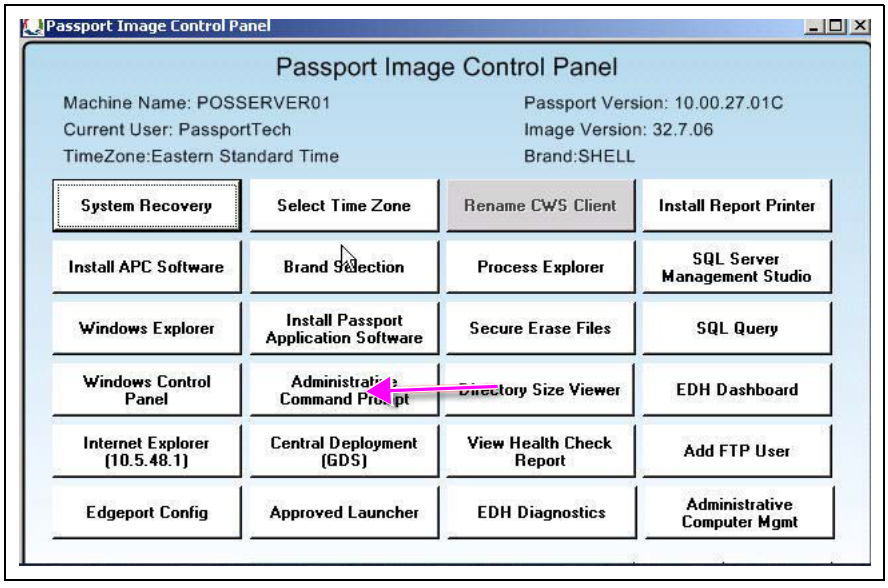


6 Enter the appropriate Username and Password. Select **OK**. The Passport Image Control Panel appears.

IMPORTANT INFORMATION

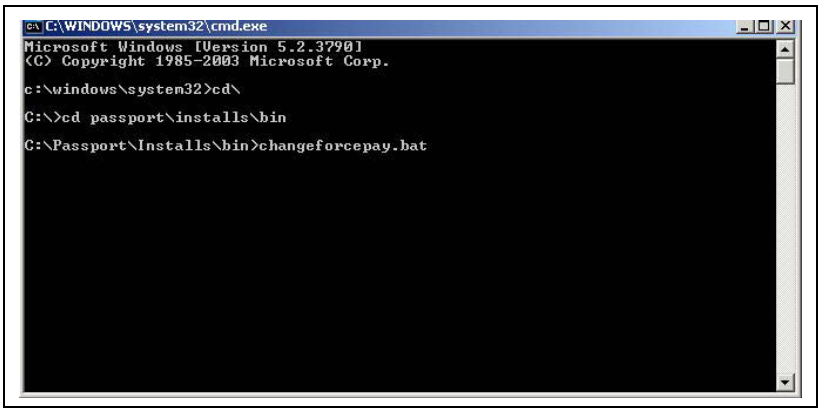
If you do not have the appropriate password, contact Gilbarco technical support. Field service technicians and Gilbarco personnel must keep Usernames and associated Passwords confidential to ensure Passport system security. Gilbarco is not responsible for incurred damage resulting from unauthorized entry.

Figure 69: Passport Image Control Panel



7 Select **Administrative Command Prompt**. The Administrative Command Prompt window appears.

Figure 70: Administrative Command Prompt



8 Type the following commands, pressing the **Enter** key after each line:

cd

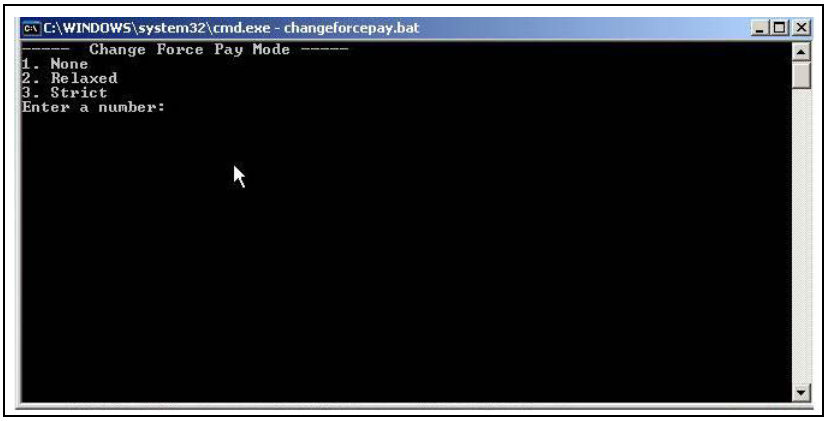
cd passport\installs\bin

9 Type the following command and then press the **Enter** key:

changeforcepay.bat

10 The script runs for changing Force Pay Mode.

Figure 71: Change Force Pay Mode



11 Type the number corresponding to the appropriate Force Pay Mode. The following table lists the options and their descriptions:

Option	Description
1. None	Disable Force Pay Mode and use typical CRIND prompting and operation.
2. Relaxed	CRIND devices display Force Pay Mode prompting, but the CRIND devices generate call signals if the customer lifts the handle without selecting a method of payment.
3. Strict	CRIND devices display Force Pay Mode prompting and do not generate call signals until the customer makes a method of payment selection.

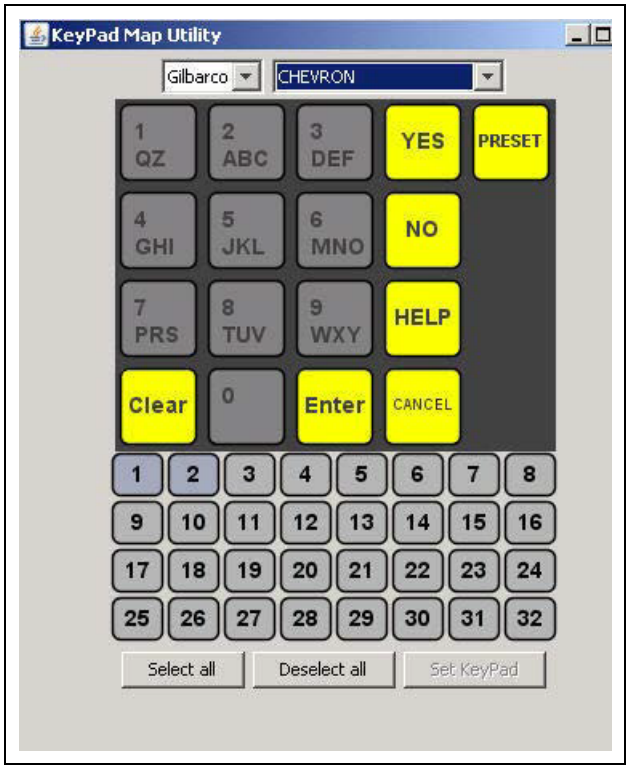
12 Press the Enter key to make the selection and close the window.

13 If all dispensers onsite are monochrome or color, proceed to step 21 on page 62. Otherwise, if any of the dispensers are single-line, proceed with step 14 to configure the appropriate single-line CRIND keypad.

14 On the Passport Server, select **Windows Explorer** and go to **C:\Passport\Installs\bin**.

15 Double-click **changekeypadid.bat**. The **KeyPad Map Utility** window appears.

Figure 72: KeyPad Map Utility



16 Use the drop-down menu to select the appropriate keypad type.

17 Select **Set KeyPad**. A pop-up window appears indicating the Passport system must be restarted for these changes to take effect.

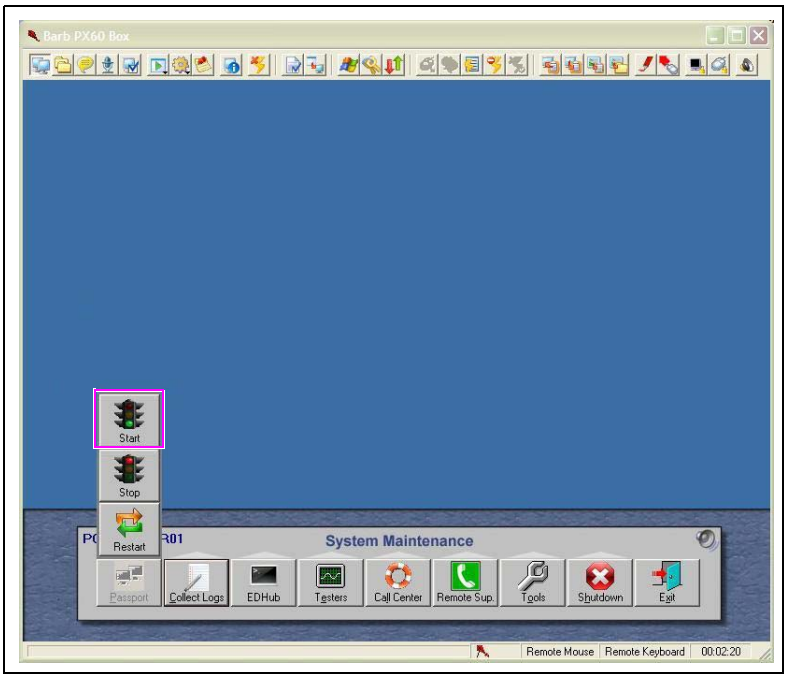
18 Select **OK**.

19 Select **Exit**.

20 Close **Windows Explorer**.

21 Select **Passport** > **Start** on the System Maintenance toolbar to restart the Passport application on the Server.

Figure 73: Passport > Start



22 Select **Exit** on the System Maintenance toolbar to close System Maintenance.

The process to enable or disable Force Pay Mode is complete. All CRIND devices will update with the appropriate Force Pay Mode messaging when Passport application loading is complete.

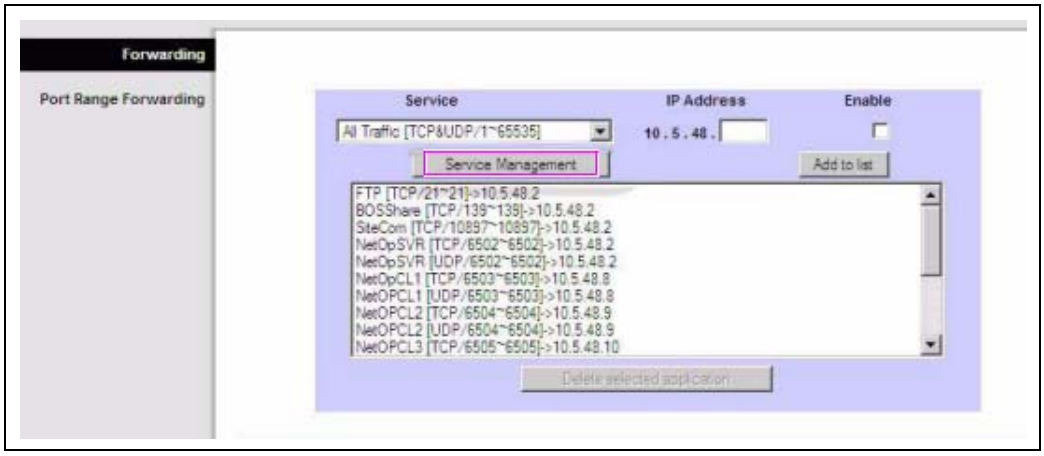
Appendix H: Additional Router Programming for High Speed Remote Support and GDS for ExxonMobil

This section provides additional router programming for high-speed remote support and GDS for ExxonMobil.
Router passwords:

- Linksys (old/pop-up) - Username: admin, Password: GVR09RV042
- Cisco (new/website) - Username: GVR, Password: GVRRV042

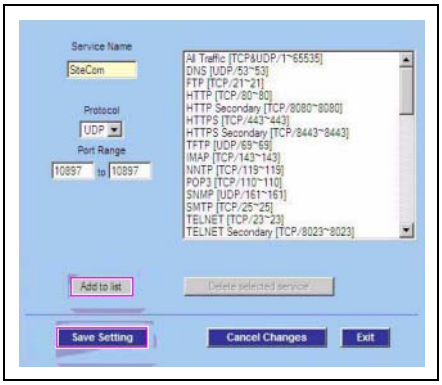
- **For All Sites Hughes® and Cybera** - Add SiteCom UDP: **Setup** > **Forwarding** > **Service Management**

Figure 74: Service Management



- Protocol: UDP
- Port: 10897 - 10897
- Add to list
- Find new SITECOMUDP for SERVICE

Figure 75: SiteCom UDP



- Add 2 at the end of the IP, check Enable, Add to list

Figure 76: Linksys Router

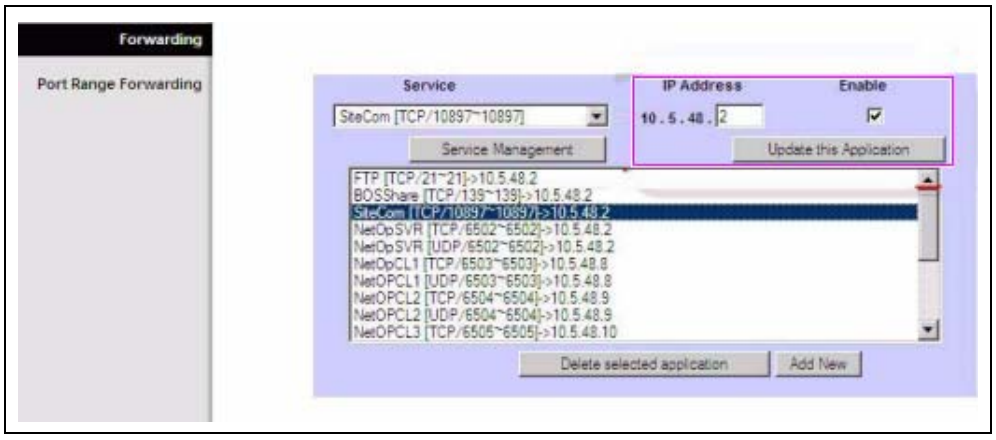
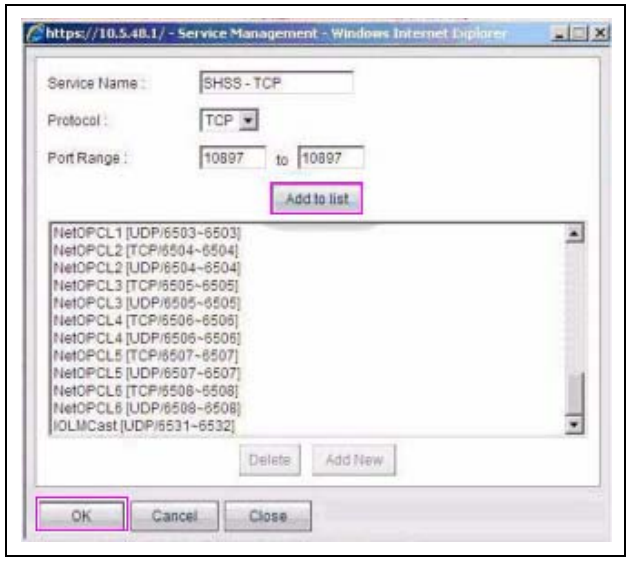


Figure 77: Cisco Router



- Back to **Firewall** > **Access Rules** > **Add New Rule** > **SiteComUDP**

- New SiteComUDP Rules

- **For HUGHES SITES**:

- Source IP Range: 192.168.200.1 ~ 192.168.200.254
- Destination IP Single: 10.5.48.2
- WAN

Add a second **SiteComUDP2**

- Source IP Range: 192.168.202.1 ~ 192.168.202.254
- Destination IP Single: 10.5.48.2
- WAN

- FOR CYBERA SITES:

- Source IP Single: 10.5.60.62
- Destination IP Single: 10.5.48.2
- DMZ

- NetOpUDP, NetOpTCP, SiteComTCP: **Firewall** > **Access Rules**: For NetOps UDP: Edit

- FOR HUGHES SITES:

- Source IP Range: 192.168.200.1 ~ 192.168.200.254
- Destination IP Range: 10.5.48.2 ~ 10.5.48.14
- WAN

Add a second **NetOpsUDP2**

- Source IP Range: 192.168.202.1 ~ 192.168.202.254
- Destination IP Single: 10.5.48.2
- WAN

- FOR CYBERA SITES:

- Source IP Single: 10.5.60.62
- Destination IP Range: 10.5.48.2 ~ 10.5.48.14
- DMZ

- For NetOpsTCP: Edit

- FOR HUGHES SITES:

- Source IP Range: 192.168.200.1 ~ 192.168.200.254
- Destination IP Range: 10.5.48.2 ~ 10.5.48.14
- WAN

Add a second **NetOpsTCP2**

- Source IP Range: 192.168.202.1 ~ 192.168.202.254
- Destination IP Single: 10.5.48.2
- WAN

- FOR CYBERA SITES:

- Source IP Single: 10.5.60.62
- Destination IP Range: 10.5.48.2 ~ 10.5.48.14
- DMZ

- For SiteCom TCP: Edit

- FOR HUGHES SITES:

- Source IP Range: 192.168.200.1 ~ 192.168.200.254
- Destination IP Single: 10.5.48.2
- WAN

Add a second **SiteComTCP2**

- Source IP Range: 192.168.202.1 ~ 192.168.202.254
- Destination IP Single: 10.5.48.2
- WAN

- FOR CYBERA SITES:

- Source IP Single: 10.5.60.62
- Destination IP Range: 10.5.48.2
- DMZ

Figure 78: Hughes Linksys

Figure 79: Hughes Cisco

Figure 80: Cybera Linksys

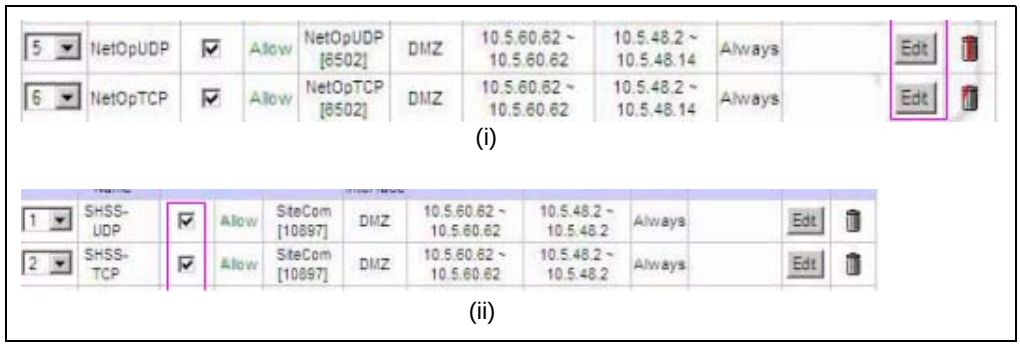
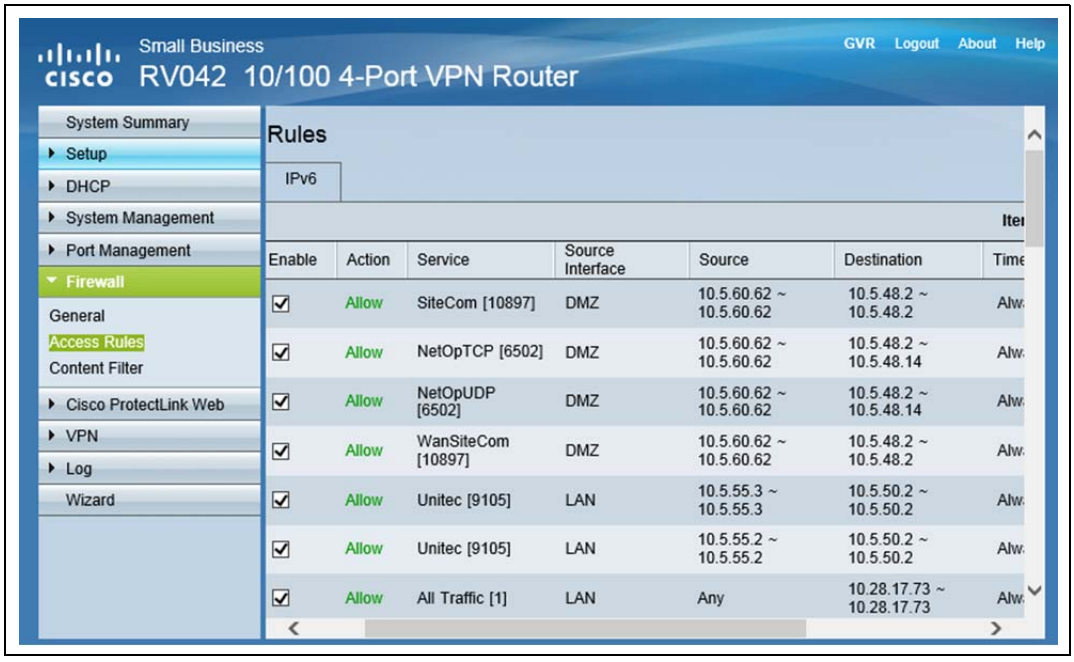


Figure 81: Cybera Cisco



- Configure router for GDS for Cybera sites only, no router changes needed at Hughes sites for GDS:
  - Telnet 64.90.126.115 443 to see if rules need to be set
  - If Telnet fails, connect to router via high speed, **Setup** > **Advanced Routing** and configure as follows:

Figure 82: Advanced Routing

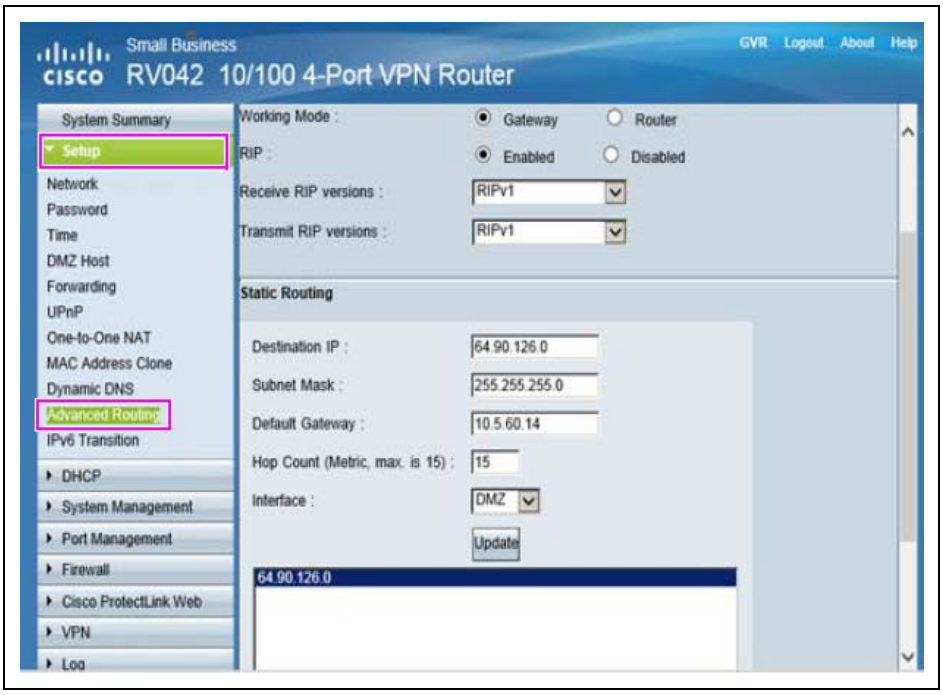
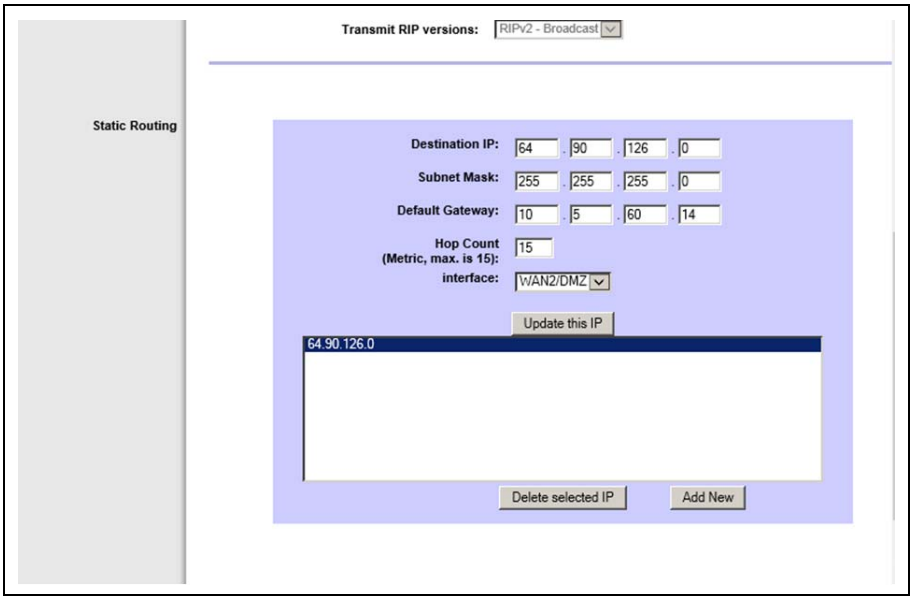


Figure 83: Static Routing



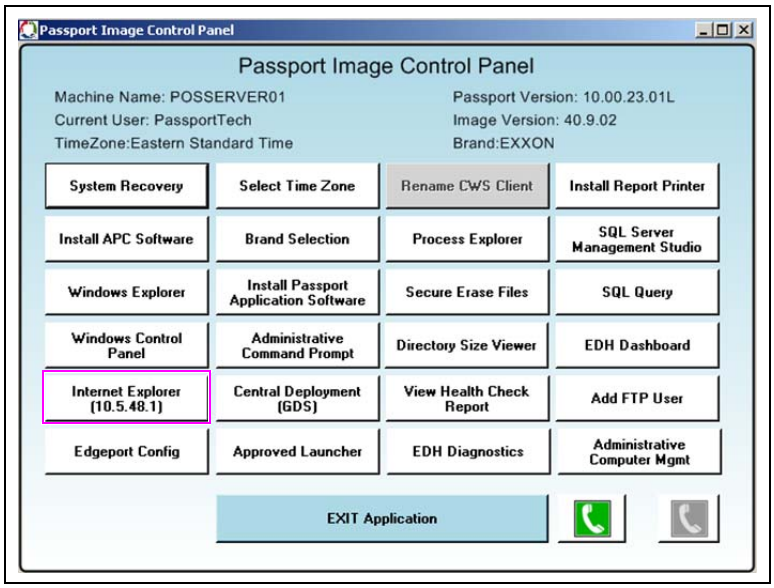
- Default gateway is 10.5.60.14 for secondary router and 10.5.60.62 for Cybera
- Destination IP ends with a 0 (64.90.126.0) so it will cover GDS as well as Insite 360
- Test again using Telnet 64.90.126.115 443
- If telnet fails: tracert 64.90.126.115 to see exactly where communication stops

Configuring Passport for GDS

To configure Passport for GDS, proceed as follows:

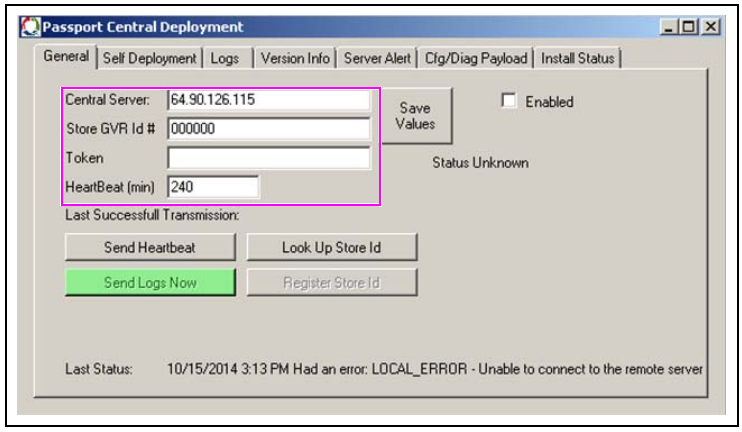
1 Open Image Control Panel - Central Deployment (GDS).

Figure 84: Image Control Panel



2 Enter GVR Store ID# which is obtained from Gilbarco Help Desk (64.90.126.115 will already be entered for Central Server).

Figure 85: Passport Central Deployment



3 Lookup **Store ID** > **Enable** > **Register Store ID** > **Send Heartbeat**.

The Advantage® Series, CRIND®, Encore®, Eclipse®, Gilbarco®, G-SITE®, InfoScreen®, Legacy®, MPD®, and Passport® are registered trademarks of Gilbarco Inc. BP® is a registered trademark of BP p.l.c. Cenex® is a registered trademark of CHS Inc. Chevron® is a registered trademark of Chevron Intellectual Property LLC. Cisco® is a registered trademark of Cisco Systems Inc. CITGO® is a registered trademark of CITGO Petroleum Corporation. Cybera® is a registered trademark of Cybera Inc. EMV® is a registered trademark of EMVCo LLC. Ethernet® is a registered trademark of Xerox Corporation. Europay® and MasterCard® are registered trademarks of MasterCard International Inc. ExxonMobil® is a registered trademark of Exxon Mobil Corporation. GOLD℠ is a service mark of Gilbarco Inc. Hughes® is a registered trademark of The DIRECTV Group Inc. Ingenico® is a registered trademark of Groupe Ingenico. Internet Explorer®, Windows®, and Window® XP are registered trademarks of Microsoft Corporation. Linksys® is a registered trademark of Cisco-Linksys LLC. MegaPath® is a registered trademark MegaPath Group Inc. NBS® is a registered trademark of National Bankcard Services Inc. OKI® is a registered trademark of Oki Electric Industry Company Ltd. Phillips 66® is a registered trademark of Phillips 66 Company. Shell® is a registered trademark of Shell Oil Company. SmartPad™ and Ultra-Hi™ are trademarks of Gilbarco Inc. Sunoco® is a registered trademark of Sunoco Inc. Tokheim® is a registered trademark of Tokheim Group S.A.S. Visa® is a registered trademark of Visa Inc. Wayne® is a registered trademark of Dresser Industries Inc. WorldPay™ is a trademark of WorldPay Limited.

© 2016 Gilbarco Inc.
7300 West Friendly Avenue · Post Office Box 22087
Greensboro, North Carolina 27420
Phone (336) 547-5000 · http://www.gilbarco.com · Printed in the U.S.A.
MDE-5084E Passport® V10.00 Upgrade Instructions · January 2016