MDE-4880A

Passport® V8.02+ Third-party Partner Device Access Rules
February 2010

Introduction

IMPORTANT INFORMATION
The following information is applicable only to sites where all the Passport® systems have been upgraded completely to V8.02 or later (V8.02+). **DO NOT** implement the following processes at sites that do not use Passport V8.02+ software on all the systems.

Purpose

This document provides information on the rules for third-party devices to access and communicate with Passport V8.02+ systems. The Passport system's architecture uses a Gilbarco® Firewall Virtual Private Network (VPN) Router to manage traffic and adhere to compliance standards. The Gilbarco Firewall VPN Router replaces the blue colored Linksys® router on existing Passport sites.

IMPORTANT INFORMATION
The Passport system **MUST** use the Gilbarco Firewall VPN Router to ensure appropriate communication for Local Area Network (LAN) and Wide Area Network (WAN) devices. Failure to install the Gilbarco Firewall VPN Router as per Gilbarco requirements affects communication and compromises on site compliance. **DO NOT** discard the old router at existing sites (or your lab system), as the site may need it to expand the number of available ports on the new Gilbarco Firewall VPN Router.

All Passport V8.02+ system installations use the settings as described in this document. The IP-enabled third-party devices (like Back Office System, Loyalty Server, and Security Camera) communicate with the Passport system through the Gilbarco Firewall VPN Router DMZ port. Back Office Systems can use file shares or FTP with the appropriate access rule and IP Address, as described in "Third-party Device Configuration" on page 5.

Certain configurations, such as remote access through a WAN or use of dual routers may require additional installation precautions for compliance. Refer to MDE-4743 Passport PA-DSS Implementation Guide and MDE-4866 Passport Firewall Router Configuration and Service Manual for additional installation recommendations.

Table of Contents

Related Documents

Document Number	Title	GOLD Library
MDE-4743	Passport PA-DSS Implementation Guide	Passport
MDE-4866	Passport Firewall Router Configuration and Service Manual	• Passport • Service Manual

Abbreviations and Acronyms

Term	Description
ASC	Authorized Service Contractor
CAT	Customer Activated Terminal
CRIND®	Card Reader IN Dispenser
CWS	Cashier Workstation
DMZ	Demilitarized Zone
FAQ	Frequently Asked Questions
FTP	File Transfer Protocol
GSM	Gilbarco Security Module
IP	Internet Protocol
LAN	Local Area Network
MOC	Major Oil Company
POS	Point Of Sale
VPN	Virtual Private Network
WAN	Wide Area Network

Important Changes with the Passport V8.02+ System

BP® and ConocoPhillips Sites

Both BP and ConocoPhillips sites follow the same third-party device configuration standards for the Passport V8.02+ system architecture. However, in the future, these networks may require sites to place all the third-party devices on the Hughes® Fortigate device instead of the Gilbarco Firewall VPN Router. They may require only FTP connections with these devices, removing the file share access.

Note: If any of the MOC networks require changes to the Passport V8.02+ system architecture, Gilbarco will advise third-party vendors and update this document prior to field release.

Images

Beginning with V8.02, all Passport system images must be loaded from scratch. The process of switching or restoring previous images in a lab setting is extremely complex. Attempting to restore a previously saved image may result in loss of data and make the Enhanced Dispenser Hub unusable.

Communications

Due to the Passport system's PA-DSS compliance implementation, third-party devices can no longer ping the Passport Server (third-party devices are not a part of the Passport LAN now). However, the Passport system can ping the device.

Secondary Router

Refer to MDE-4866 Passport Firewall Router Configuration and Service Manual for instructions on the use of a non-Gilbarco secondary router.

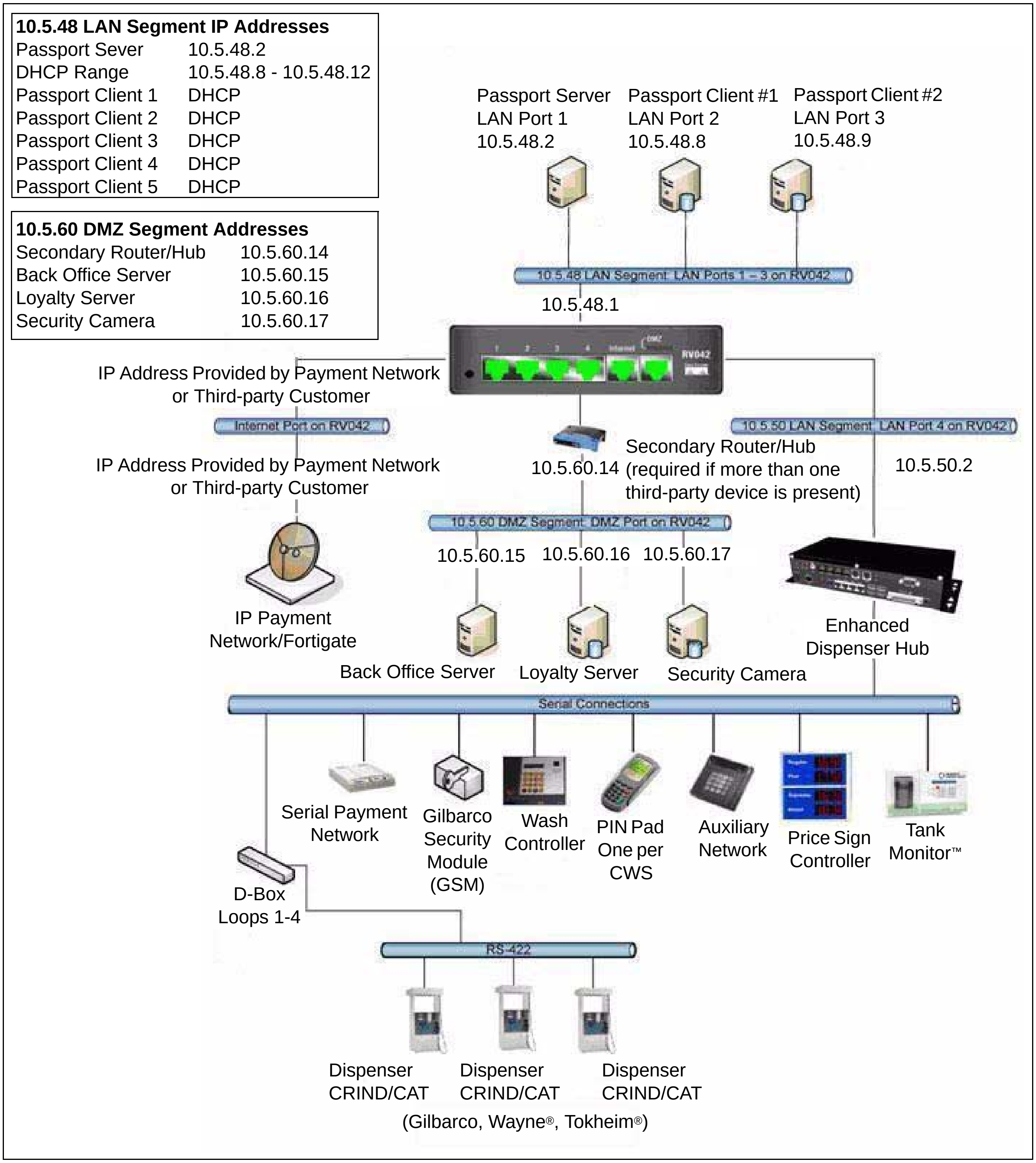
The following documents will be available on the Point Of Sale (POS) Partner Portal, after the supporting documents for Passport V8.02 have been released to production.

Document Number	Document	Back Office	Loyalty Server	Price Sign	Security Camera	Auxiliary Network
MDE-4829	Passport V8.02 Software Installation Manual	Y	Y	Y	Y	Y
MDE-4822	Enhanced Dispenser Hub Installation Manual	Y	Y	Y	Y	Y
MDE-4823	Passport System Enhanced Dispenser Hub Start-up and Service Manual	Y	Y	Y	Y	Y
MDE-4603	Auxiliary Network Hardware Installation and Software Module Manual	-	-	-	-	Y
MDE-4674	Passport Electronic Price Sign Interface Manual	-	-	Y	-	-
MDE-3618	Point Of Sale System Hardware Start-up and Service Manual	Y	Y	Y	Y	-
MDE-4866	Passport Firewall Router Configuration and Service Manual	Y	Y	Y	Y	Y
MDE-4842	Passport Software Upgrade Manual for Passport V6.01/V7.00/V8.00 to V8.02 and Later	Y	Y	Y	Y	Y

Passport Enhanced Dispenser Hub Site Architecture

The Passport Enhanced Dispenser Hub Site architecture is shown in Figure 1.

Figure 1: Passport Enhanced Dispenser Hub Site Architecture



10.5.48 LAN Segment IP Addresses	
Passport Sever	10.5.48.2
DHCP Range	10.5.48.8 - 10.5.48.12
Passport Client 1	DHCP
Passport Client 2	DHCP
Passport Client 3	DHCP
Passport Client 4	DHCP
Passport Client 5	DHCP

10.5.60 DMZ Segment Addresses	
Secondary Router/Hub	10.5.60.14
Back Office Server	10.5.60.15
Loyalty Server	10.5.60.16
Security Camera	10.5.60.17

Passport Server LAN Port 1 10.5.48.2
Passport Client #1 LAN Port 2 10.5.48.8
Passport Client #2 LAN Port 3 10.5.48.9
10.5.48 LAN Segment: LAN Ports 1 – 3 on RV042
10.5.48.1
RV042
IP Address Provided by Payment Network or Third-party Customer
Internet Port on RV042
IP Address Provided by Payment Network or Third-party Customer
10.5.50 LAN Segment: LAN Port 4 on RV042
Secondary Router/Hub (required if more than one third-party device is present)
10.5.60.14
10.5.50.2
10.5.60 DMZ Segment: DMZ Port on RV042
10.5.60.15
10.5.60.16
10.5.60.17
IP Payment Network/Fortigate
Back Office Server
Loyalty Server
Security Camera
Enhanced Dispenser Hub
Serial Connections
Serial Payment Network
Gilbarco Security Module (GSM)
Wash Controller
PIN Pad One per CWS
Auxiliary Network
Price Sign Controller
Tank Monitor™
D-Box Loops 1-4
RS-422
Dispenser CRIND/CAT
Dispenser CRIND/CAT
Dispenser CRIND/CAT
(Gilbarco, Wayne®, Tokheim®)

Third-party Device Configuration

Firewall VPN Router Port Management

Turn on the DMZ gate, using the IP Addresses assigned specifically for the third-party devices. The following table lists the DMZ segments and the corresponding IP addresses.

10.5.60 DMZ Segment	IP Addresses
Secondary Router/Hub	10.5.60.14
Back Office Server	10.5.60.15
Loyalty Server	10.5.60.16
Security Camera	10.5.60.17
Subnet Mask	255.255.255.192
Default Gateway	10.5.60.1

RV042 Third-party Access Rules

The following table lists the access rules for the third-party devices.

Third-party LAN	□	Allow	All Traffic [1]
BOSShare	□	Allow	BOSShare [139]
BOSFTP	□	Allow	FTP [21]
WANFTP	□	Allow	FTP [21]

Third-party LAN is used for Loyalty Server, IP-based Security Camera, and Back Office Systems, where data is pushed from the Passport Server to the Back Office System. The Authorized Service Contractor (ASC) must enable this rule during installation.

BOSShare is used for Back Office Systems that access the Passport Server through File Share. The ASC must enable this rule during installation. The Back Office System must access the Passport Server using 10.5.60.1 as the IP Address. The IP Address 10.5.48.2 or POSServer01 can no longer be used for accessing the Passport Server.

BOSFTP is used for Back Office Systems that access the Passport Server through FTP. The ASC must enable this rule during installation. The Back Office System must access the Passport Server using 10.5.60.1 as the IP Address. The IP Address 10.5.48.2 or POSServer01 can no longer be used for accessing the Passport Server.

WANFTP is used for customers of MOC and Back Office Systems that access the Passport Server through FTP over the WAN connection. The ASC must enable this rule during installation. The Back Office System must access the Passport Server using 10.5.60.1 as the IP Address.

Note: 1) Only devices originating from the DMZ can access the server through 10.5.60.1. If using the WAN port for FTP, you can access the server through the IP Address assigned to the RV042 Internet port and not through 10.5.60.1.

2) WANFTP is used only for private network connections through the WAN port and is ***NEVER*** *used for public internet connections.*

Frequently Asked Questions (FAQ)

Following are the frequently asked questions on troubleshooting the third-party devices.

FAQ 1: The third-party device cannot ping the Passport Server.

Solution

Third-party devices (Loyalty Server, Security Camera, and Back Office System) no longer reside on the Passport LAN. This is by design and is necessary for Passport PA-DSS compliance. Unlike the old Passport system architecture, you cannot ping the Passport Server through the DMZ port.

FAQ 2: The third-party device (Loyalty Server, Security Camera, and Back Office System) cannot communicate with the Passport Server.

Solution

To solve this problem, proceed as follows:

1. Ensure that the third-party device is connected to the following:
   - The **Gilbarco Firewall VPN Router** through the **DMZ Port**
   - A Router/hub attached to the **Gilbarco Firewall VPN Router DMZ Port**, when multiple third-party devices are present at the site

2. Ensure that the **DMZ Port** is enabled in the Gilbarco Firewall VPN Router’s Port Management configuration.

3. Ensure that the third-party device is not configured for DHCP (refer to steps 4 and 5).

4. Use the static IP Address 10.5.60.1 for the Passport Server.
   Note: Do not use POSServer01 or 10.5.48.2.

5. Ensure that the appropriate static IP Address is assigned to the third-party device. Refer to “Firewall VPN Router Port Management” on page 5.

6. Ensure that the appropriate **Access Rule** is enabled for all the third-party devices (Third-party LAN, BOSShare, BOSFTP, or WANFTP). Refer to “RV042 Third-party Access Rules” on page 5 for related information.

© 2010 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-4880A Passport® V8.02+ Third-party Partner Device Access Rules · February 2010