



# Galileo International

Technical Support Documentation

## Firewall & Proxy Specifications

*For Focalpoint® , Viewpoint™ & Galileo Print Manager™*  
(GALILEO® and APOLLO® PRODUCTION SYSTEMS)

### Copyright

Copyright © 2001-2005 Galileo International. All rights reserved.

Information in this document is subject to change without notice. The information described in this document is furnished to Galileo International subscribers, or their representatives, and is provided as is under a license agreement or nondisclosure agreement. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or any means electronic or mechanical, including photocopying and recording for any purpose other than the subscriber's personal use without the written permission of Galileo International.

### Trademarks

Apollo, Galileo, the Globe Device, Galileo Print Manager and Viewpoint are registered trademarks, trademarks or service marks of Galileo International in the United States and/or other countries.

Galileo International may have patents or pending patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. The furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property rights except as expressly provided in any written license agreement from Galileo.

---

## Introduction

This document outlines configuration changes that may be required by a firewall administrator to allow Galileo's Focalpoint®, Viewpoint™ and Galileo Print Manager™ (GPM) applications to establish a session with Galileo's computer reservation system (CRS) hosts. Galileo International provides this information as a guide only. The term "Inbound" indicates traffic passing into the subscriber's network from the reservation system. The term "Outbound" indicates traffic passing out of the subscriber's network to the reservation system).

Configuration of a firewall placed between the computer(s) running Focalpoint, Viewpoint and GPM and the Galileo® or Apollo® host system(s) is the sole responsibility of the Galileo customer. It is strongly recommended that the subscriber or firewall administrator contact their respective firewall providers prior to making changes to support Galileo International products. Galileo International does not provide technical or help desk support in these types of configurations.

To identify which reservation system you will be accessing, please contact your Travel Management Company or refer to your system access contract. In general Galileo International subscribers outside North America access the Galileo® reservation system while North American subscribers access the Apollo® reservation system.

## What is Focalpoint® and Viewpoint™?

Interaction with the Galileo® and Apollo® host systems are provided through two applications installed at the end user's workstation.

Focalpoint® is Galileo's proprietary terminal emulation program. Cryptic inputs formats are used to send requests to the host system to complete a travel reservation. Viewpoint™ provides a Graphical User Interface (GUI) to build a travel reservation using a simplified, Microsoft Windows™ based, point and click environment.

The requirements for customer firewalls are the same for both Focalpoint and Viewpoint.

## What is Galileo Print Manager™?

Galileo Print Manager™, commonly referred to as "GPM" or "Print Manager", is a Windows™ based software product that manages host-printing functions (Ticket Printer, Invoice Printer and Back Office Interface (MIR)). The PC that runs this software may be dedicated to this function or, the GPM software may be installed on a computer that is also running Galileo's Focalpoint® or Viewpoint™ reservation products.

Earlier versions of Galileo Print Manager were known as Focalpoint Print Manager or "FPM" (v3 .x) and Document Production Software or "DPS" (v2.x).

Galileo Print Manager™ will enter a "sleep mode" after 300 seconds (5 minutes) of inactivity (TCP socket is dropped). Subsequently, before a host print job can be processed, a "wake-up message" (TCP SYN) is sent. For wake-up to successfully occur, the PC running the Print Manager software must have a static IP address. If Network Address Translation (NAT) is used, the 'inside address' must be statically mapped to the 'outside address'. GPM WILL NOT work properly with PAT or port address translation.

Most Galileo® or Apollo® subscribers will use Galileo Print Manager™. Firewall Administrators should contact their Travel Management Company to determine if this application will be used.

---

## How do I determine my access type to Apollo/Galileo?

Access to the CRS host systems is provided either;

- Via a dedicated TCP/IP frame relay circuit
- or
- Via the Internet using a Virtual Private Network (VPN) connection to Galileo International

Virtual Private Connections can be established one of two ways;

- Software VPN - Using either Nortel Networks Contivity VPN Client software (strongly recommended) or Microsoft's PPTP VPN Protocol (not recommended) or,
- Site To Site VPN - Galileo has both a "managed" solution where Galileo provides all of the necessary components, and an "un-managed" solution which allows our customers to use their own internet connection and their own routers or firewalls to create the VPN.

This document will describe the firewall configuration for the following types of connection:

- **TCP/IP Frame Relay / Galileo Managed SDSL:** When Galileo installs a dedicated Frame Relay or SDSL (Synchronous Digital Subscriber Line), Galileo will also install and configure a site premise router. This router can be connected either to the Local Area Network or to a Galileo customer provided router.
- **Internet/VPN using Software VPN Client:** With an Internet Service Provider (ISP) connection to the Internet, a VPN tunnel is created using either Nortel Networks Contivity VPN Client software or Microsoft's PPTP VPN protocol. Galileo VPN connections are configured for split tunneling, allowing our customers to retain access to the internet while connected to the reservation service. Customers using Galileo's FocalpointNet™ product will use this type of connection.
- **Internet/VPN using hardware: For details on using your own router or firewall to establish a peer to peer VPN connection to Galileo, see the [Un-Managed VPN Support Agreement](#).**

Before proceeding with configuring your firewall, identify which connection type you will be using to access the Galileo® or Apollo® reservation system. Follow the configuration specifications on the following pages that apply to your connection type.

---

## What Galileo devices will you need to reach?

### □ **Configuration Servers: (Dedicated Frame Relay Circuits & “Galileo Managed VPN”)**

**Purpose:** The Configuration Servers, sometimes referred to as “Config Servers”, provide initial configuration authentication. This initial configuration is sometimes referred to as a “download”.

**Protocol Used:**

UDP (User Datagram Protocol / Protocol 17)

TCP/IP (Transmission Control Protocol/Internet Protocol / Protocols 4 & 6)

### □ **IP Concentrators: (Dedicated Frame Relay Circuits & “Galileo Managed VPN”)**

**Purpose:** The IP Concentrators, referred to as IPCs, translate the TCP/IP packet into a format accepted by the Galileo<sup>®</sup> or Apollo<sup>®</sup> reservation system.

**Protocol Used:**

TCP/IP (Transmission Control Protocol/Internet Protocol / Protocols 4 & 6)

### □ **VPN Switch: (Internet/VPN Subscribers Only)**

**Purpose:** The VPN Switch authenticates the VPN client, either Nortel Extranet or Microsoft PPTP, onto the Galileo<sup>®</sup> or Apollo<sup>®</sup> reservation system.

**Protocol Used:** Based on the VPN client being used.

- Extranet IPsec =
  - ISAKMP (UDP protocol on port 500)
  - ESP (IP, Encapsulation Security Payload / Protocol 50)
  - AH (IP, Authentication Header / Protocol 51)
  - UDP 4500 to UDP 4500 (IPsec w/PAT, NAT Traversal)
- Microsoft PPTP = GRE (General Routing Encapsulation / Protocol 47)
- Note, IPsec is the recommended connection. Microsoft’s PPTP client should not be used without first consulting your Galileo technical representative.
- Note, the UDP and TCP packets shown for dedicated circuits are ‘encapsulated’ and encrypted when using an Internet/VPN connection and do not need to be permitted in addition to permitting ISAKMP, ESP and AH.

### □ **DNS SUPPORT:**

The computer running the Nortel VPN client software must be able to ‘resolve’ and ‘reach’ the appropriate DNS name for the option you just choose in the next section. If you have ICMP turned on, you should be able to ping the appropriate name from the following list (based on the option you choose in the next section) and receive a reply.

- fpnetipsec.galileo.com
- fpnetnatt.galileo.com
- fpnetpptp.galileo.com

---

## Configuring a Firewall for a dedicated TCP/IP circuit

**NOTE:** This configuration should only be used when access to the reservation system is via a dedicated communication line provided by Galileo. **If you are accessing the reservation system via the Internet, please refer to the instructions on page 6 – Configuring a Firewall for access via the Internet/VPN. The instructions in this section DO NOT apply to VPN connections over the Internet. See Appendix B for access to Copy or Test Systems.**

### PROTOCOLS:

- TCP/IP (Protocols 6 & 4)
- UDP (Protocol 17)

### GALILEO DESTINATION NETWORKS:

- Network: 57.8.8 1.0 Subnet 255.255.255.0
- Network: 198.177.164.0 Subnet 255.255.255.0
- Do NOT filter these destination networks.
- Test by pinging 57.8.81.13 and 198.177.164.151

### PORTS:

- UDP Port 5067 to Apollo or Galileo (Application configuration requests are sent to this port)
- UDP Port 5067 from Apollo or Galileo (Configuration requests from Galileo Desktop are returned to this port)
- UDP Port 5068 from Apollo or Galileo (Configuration requests from Focalpoint v3.5 and Galileo Print Manager are returned to this port)
- TCP Port 2748 to Apollo host (Focalpoint and Viewpoint applications use this). Responses are returned on a random TCP port. (Generally U.S., Canada, Mexico & Japan)
- TCP Port 2749 to Galileo host (Focalpoint and Viewpoint applications use this). Responses are returned on a random TCP port. (Generally in countries other than the U.S., Canada and Japan)

### Galileo Print Manager (GPM) Only

- GPM requires all of the items listed above plus what is mentioned next.**
- GPM functions as a 'print server', and as such, the software does not originate or establish a TCP session. A 'wake up message' from Galileo to the computer running this software instructs GPM to establish the TCP session outbound to the IPC complex. The firewall must be configured to allow this inbound TCP session to be built, as well as the outbound TCP session used for print data.
  - Message Type = TCP
  - **Origination IP addresses = 57.8.81.13 and 57.8.81.1 13**
  - **Origination Port = any**
  - Destination IP address = static IP address of computer running GPM software
  - **Destination Port = TCP 5069**
  - IMPORTANT, you cannot simply open TCP port 5069 between your network and Galileo's network.
  - NOTE: Galileo Print Manager MUST be assigned a static IP address for the wake-up process to work properly. If you are NATTING, you need a static NAT entry for the PC running GPM.

---

## Configuring a Firewall for Access Using Software VPN Client via the Internet.

**NOTE:** This configuration should only be used when access to the reservation system is via a dial-up or dedicated Internet connection. **If you are accessing the reservation system via a circuit provided by Galileo, refer to page 5 – Configuring a Firewall for Dedicated TCP/IP Circuit. The instructions on this section DO NOT apply to dedicated, point-to-point frame relay connections. If you plan to use a hardware VPN device, see separate [Un-Managed VPN Document](#).**

There are two VPN options, Follow the instructions based on the client you are using::

- IPsec (recommended) using Nortel's Contivity VPN Client
- PPTP (not recommended) using Microsoft's PPTP VPN Client

### PROTOCOLS:

- TCP/IP (Protocols 6 & 4)
  - Nortel Contivity VPN Client Only (IPsec)
    - UDP (Protocol 17)
    - ISAKMP: UDP protocol on port 500
    - IPsec: ESP & AH (Protocols 50 & 51)
    - UDP Source Port 4500 to UDP Destination Port 4500 (Not always required. In some cases where IPsec is used over PAT and NAT Traversal is in place this will be required. See <http://www.ietf.org/internet-drafts/draft-ietf-ipsec-nat-t-ike-08.txt> for more details.)
  - Microsoft PPTP VPN Client Only
    - PPTP: GRE (Protocol 47 mapped to port 1723)

### DESTINATION DNS Name & IP ADDRESSES for VPN Switches:

- There are three 'connection points' available to Galileo's VPN
- There are advantages and disadvantages to the following connection points.

Connection Destination	Connection Type
<a href="http://fpnetipsec.galileo.com">fpnetipsec.galileo.com</a>	Nortel Contivity IPsec VPN Client Use this if your routers or firewalls do not require or support
<a href="http://fpnetnatt.galileo.com">fpnetnatt.galileo.com</a>	Nortel Contivity IPsec VPN Client Use this if your routers or firewalls require support for IPsec over PAT (NAT Traversal)
<a href="http://fpnetpptp.galileo.com">fpnetpptp.galileo.com</a>	Microsoft PPTP

---

# Configuring a Firewall for Access Using Software VPN Client via the Internet. (cont.)

## Required Port and Protocol Information:

- UDP500 for isakmp
- Protocol 50 (IPSec ESP)
- UDP4500 for NAT-T
- TCP 1723 PPTP Å Applies only if using Microsoft PPTP\*
- Protocol 47 GRE Å Applies only if using Microsoft PPTP\*

\*Note, Galileo STRONGLY recommends you use the Nortel Contivity VPN Client software instead of Microsoft's PPTP. If you intend to use Microsoft's client, you should contact Galileo prior to doing so. There are special considerations which must be taken into account.

Changes made in May 2005 require our customers making software VPN connections to Galileo to configure access-lists to permit standard IPSEC protocols as follows:

### New information for customers (IPSec)

<u>Source</u>	<u>Destination</u>	<u>Protocol</u>	<u>Port</u>
Agency LAN IP or 3rd party Router	Public IP 198.151.32.0/24	udp (17)	500
Agency LAN IP or 3rd party Router	3rd party Router	Public IP 198.151.32.0/24	ipsec esp (50) N/A
Agency LAN IP or 3rd party Router	Public IP 198.151.32.0/24	udp (17)	4500
198.151.32.0/24	Agency LAN IP or 3rd party Router	Public IP 198.151.32.0/24	500
198.151.32.0/24	Agency LAN IP or 3rd party Router	Public IP ipsec esp (50)	N/A
198.151.32.0/24	Agency LAN IP or 3rd party Router	Public IP udp (17)	4500

### New information for customers (IPSec)

Agency LAN IP or 3rd party Router Public IP 198.151.32.0/24 TCP (47) 1723  
198.151.32.0/24 Agency LAN IP or 3rd party Router Public IP TCP (47) 1723  
See <http://www.microsoft.com> for more information on setting up GRE for PPTP.

## DNS SUPPORT:

The computer running the Nortel VPN client software must be able to 'resolve' and 'reach' the appropriate DNS name for the option you just choose above. If you have ICMP turned on, you should be able to ping the appropriate name from the following list (based on the option you choose above) and receive a reply. If, for some reason, ICMP is disabled on your network, you will not be able to ping the following three 'destinations'.

- Option #1 PING [fpnetipsec.galileo.com](http://fpnetipsec.galileo.com) (Nortel IPSec Client, default)
- Option #2 PING [fpnetnatt.galileo.com](http://fpnetnatt.galileo.com) (Nortel IPSec Client, use with IPSec over PAT)
- Option #3 PING [fpnetpptp.galileo.com](http://fpnetpptp.galileo.com) (Microsoft PPTP, requires GRE)

**Once the VPN tunnel has been established, you MUST be able to ping the following by DNS names. Even if your firewall(s), router(s) or both have ICMP disabled, you should be able to "ping" inside the VPN tunnel. It's important to be able to ping by DNS name, and not just by IP address. The Focalpoint and Galileo Print Manager software may not work properly if DNS is not properly configured, allowing you to ping the following two 'names'.**

'Config' Server = [vpnipcs.galileo.com](http://vpnipcs.galileo.com) ( should respond and resolve to 172.20.200.2) IP

Concentrator = [vpnipc.galileo.com](http://vpnipc.galileo.com) (should respond to and resolve to 172.20.200.1)

---

## Frequently Asked Questions

### **How do I know if my Firewall will support access to the Galileo® and Apollo® systems?**

Subscribers using a direct, dedicated connection to the Internet should not have problems providing the port and protocol settings addressed in this document can be supported. Internet/VPN access subscribers must be able to support the ports and protocols as well as support the VPN technologies of the Nortel Extranet IPsec client or Microsoft PPTP.

### **My firewall performs port address translation. Will that be an issue?**

The Focalpoint/Viewpoint and Galileo Print Manager applications per se do work with PAT, although we highly recommend that you use NAT for the computer running Galileo Print Manager. With an Internet/VPN connection to Galileo's host systems, success with using PAT will depend upon your firewall(s) and router(s) and their ability to support IPsec over PAT.

### **My firewall performs NAT for the Local Area Network users and Internet Access is via a proxy server. Why can't I get Focalpoint® or Viewpoint™ working correctly?**

The Focalpoint® and Viewpoint™ authentication process allows for one and only one Network Address Translation mapped for both inbound and outbound traffic. Attempts have been unsuccessful with subscribers performing "double-NATting" so Galileo strongly recommends either performing a single Address Translation or selecting another solution.

### **Do I have to open all the ports, protocols and IP addresses specified for my configuration?**

Failure to support one of the configuration requirements in this document will prevent authentication to the Galileo® or Apollo® reservation system. If policies or procedures prevent opening the ports, protocols or IP subnets as specified, it is recommended that another method of connection be used to access the reservation service.

### **I have completed all the steps in configuring the firewall but still cannot get access to the reservation service. Where do I go for help?**

For liability reasons, Galileo International employees are not permitted to touch or configure firewalls owned and maintained by a subscriber. The information included in this document is complete and accurate as of the date published. In the event you are still unable to access the reservation service, contact the vendor who provided the firewall or the firewall manufacturer's technical support desk.

### **Why must the Galileo Print Manager™ use a fixed or static IP address when installed at a dedicated TCP/IP site?**

Galileo Print Manager (GPM) is much like an HP Jet Direct or other Ethernet print server. The computer running GPM, and the GPM application, do not originate the request for the print job. Print jobs are formatted on the Galileo host systems, and sent, unsolicited by GPM, to the computer running the GPM software. Before a print job can be sent, a TCP session must be initiated by, and established with a Galileo 'host'. This "wake-up message" is generated from Galileo/Apollo and is viewed by firewalls as an unsolicited IP packet to the Print Manager PC. For the TCP session to establish properly, the IP address must be known by the Galileo host. That means the IP address of the computer running GPM should not change after the initial authentication process. If the computer's IP address does change, select the Tools menu on GPM, then select Auto-configure, make sure the status bar shows (bottom left of the application) "Listening for a connection" and there are entries under the GTIDs tab. Close GPM, save the changes when prompted to do so, and restart GPM. Note, you may need to contact Galileo to have changed made to our configuration server(s) if the IP address of the computer running GPM changes.

---

## Frequently Asked Questions (cont.)

**You indicate that the Galileo Print Manager™ requires TCP messages to be accepted on port 5069 for the wake-up to be successful. The firewall administrator must understand that the source TCP port is random, or from any to 5069.**

Galileo Print Manager™ (GPM) is designed to minimize network traffic. The TCP session between GPM and the computers that send it print job has a time out value of 300 seconds. If the TCP session has timed out, before a print job can be sent, the Galileo host systems must re-establish the TCP session. (This is a standard SYN, SYN-ACK, ACK sequence). Your firewall must be configured to allow this process to take place. Refer to the “Galileo Print Manager (GPM) Only” section on page #5 of this document for more details.

### **The Print Manager is not waking up. What’s wrong?**

The first test to perform is to bring the Print Manager up manually (refer to the instructions for Installing the Galileo Print Manager™). If documents print when the Print Manager is manually connected, then the problem most definitely is firewall or routing related. Refer to the “Galileo Print Manager (GPM) Only” section on page #5 of this document for details on how to configure your router(s) and firewall(s) properly.

If problems persist, please contact your Galileo or Apollo Account Representative to arrange for further technical assistance.

### **My Travel Management Company uses a DOS based “Print Server” to issue travel documents. Do I need to open ports for that device too?**

No. The Focalpoint Print Servers use a different technology that does not require a wake-up message to be received. Standard Focalpoint® or Viewpoint™ firewall configurations will be sufficient.

---

## Appendix A

### Special Configurations for Galileo Customers Using “GIDS”

#### U.S. SUBSCRIBERS ONLY

##### Galileo IDS

**Purpose:** Galileo IDS is a product which sends data to a customer provided SQL database. The data is created at the mainframe level, and forwarded to the customer’s SQL server when any new booking is created or an existing booking is modified.

##### **Protocol Used:**

- TCP/IP (Transmission Control Protocol/Internet Protocol / Protocols 4 & 6)
- Standard SQL message

**Ports to be Open:** 1415 / TCP Traffic / Inbound Only

<b>TCP/IP Frame Relay or Managed VPN or Un-Managed VPN</b>	<b>Internet or Software VPN</b>
gidsmq.galileo.com** 57.8.16.41	<a href="http://gidsvpn.galileo.com">gidsvpn.galileo.com</a> 198.151.32.111
** The DNS name is not used except for internal Galileo employees who use Galileo’s internal DNS servers. Galileo customers should use the IP address. NOTE, to access GIDS over a dedicated Galileo connection requires special configuration by	

---

## Appendix B

### Special Configurations for Developers & Others Who Require Access To “Copy” or “Test” Systems

#### Various Host System Names & Aliases

	Apollo Host	Galileo Host	Comment
Production	1V	PRE, also known as 1G	Live system
Pre-production	CAPA or CAPG (both are the same-CAPG is back up to CAPA), also known as Copy	CRE, also known as Copy	Generally used by developers holding valid Galileo API licenses to test their coding prior to putting applications into production. Work done here does not impact travelers or any real data. Passenger Name Records (PNR) and Booking Files (BF) should still be routinely cancelled and dates chosen for bookings at least 6 months out. Must have “Test” in name field.
Test - "must go to read/write DB"	TAPC	TRE	Generally used by TPF developers. RARELY is access required by non-Galileo or non-Airline entities. Requires special permission to use. PNRs and BFs should still be routinely cancelled and dates chosen for bookings at least 6 months out. Must have “Test” in name field.

\*\*\*\* Refresh of Pre-Production is normally every 90 days \*\*\*\* Dates of Production DB capture and dates of the refresh are communicated about every 90 days.

**NOTE:** This configuration should only be used when access to the reservation system is via a dedicated communication line provided by Galileo. Connections to pre-production / copy systems over a VPN require special permission. If permission is granted, details will be supplied at that time.

---

## **GALILEO NETWORKS, PROTOCOLS AND PORTS – Pre-Production, a.k.a. “Copy” Systems:**

### **Pre-Production – Apollo Host**

- Network: 57.8.72.0 Subnet 255.255.255.0
- Network: 198.177.164.176 Subnet 255.255.255.240
- UDP Port 5067 to Apollo
- UDP Port 5068 from Apollo (response to BootP requests are returned on this port)
- TCP Port 5067 to Apollo host. Responses are returned on a random TCP port.
- TCP Any to TCP Port 5069 (GPM only)
- Primary ‘Config’ Server = 57.8.72.203 or 198.177.189.184 (doesn’t work for TAPC)
- IP Concentrator / Secondary ‘Config’ Server = 57.8.72.203 or 198.177.189.184 (doesn’t work for TAPC)

### **Pre-Production – Galileo Host**

- Network: 57.8.72.0 Subnet 255.255.255.0
- UDP Port 5067 to Galileo
- UDP Port 5068 from Galileo (response to BootP requests are returned on this port)
- TCP Port 5068 to Galileo host. Responses are returned on a random TCP port.
- TCP Any to TCP Port 5069 (GPM only)
- Primary ‘Config’ Server = 57.8.72.203
- IP Concentrator / Secondary ‘Config’ Server = 57.8.72.203

### **Note to Galileo Employees**

- Port 2748 in CDS record – Production and Test (TAPC) Apollo core
- Port 22748 in CDS record – Pre-Production Apollo core
- Port 2749 in CDS record – Production and Pre-Production Galileo core
- Port 2769 in CDS record – Test (TAPC) Galileo core