

Standard Installation Guide for Galileo SSL

Galileo SSL Client v3.0.1

Version 1.0

04 October 2018

THE INFORMATION CONTAINED IN THIS DOCUMENT IS CONFIDENTIAL AND PROPRIETARY TO TRAVELPORT.

Copyright

Copyright © 2006–2018 Travelport and/or its subsidiaries. All rights reserved.

Travelport provides this document for information purposes only and does not promise that the information contained in this document is accurate, current or complete. This document is subject to change without notice. No part of this document 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 licensee's personal use without the prior written permission of Travelport and/or its subsidiaries.

Trademarks

Travelport and/or its subsidiaries may have registered or unregistered patents or pending patent applications, trademarks copyright, or other intellectual property rights in respect of the subject matter of this document. The furnishing of this document does not confer any right or license to or in respect of these patents, trademarks, copyright, or other intellectual property rights.

All other companies and product names are trademarks or registered trademarks of their respective holders.

Contents

Introduction	1
What's New	1
Minimum Software Requirements	2
Installer Requirements	3
Downloading Galileo SSL Client	3
Installing Galileo SSL	3
Before Installing Galileo SSL Client	4
Standard Galileo SSL Installation	5
Installation Environments for Galileo SSL	7
Typical Agency Workstation Environment	8
Gateway Mode for a Citrix Load-Balanced (Cluster) or MTS Environment	9
Stand-Alone Citrix or MTS Environment	11
Configuring Galileo SSL for Supported Products	12
Configuring Galileo Desktop/Smartpoint for Galileo SSL in a Typical Agency Workstation Environment	12
Configuring Galileo Desktop/Smartpoint in Gateway Mode for a Citrix Load-Balanced (Cluster) or MTS Environment.....	13
Configuring Galileo Desktop/Smartpoint in a Stand-Alone Citrix or MTS Environment.....	14
Configuring Travelport Booking Feed for Galileo SSL	14
Configuring a TN3270 Emulator for Galileo SSL	15
Configuring XML Select for Galileo SSL	16
Configuring Customer Proxy Servers for Galileo SSL	17
Appendix A: SSL Client Configuration Parameters	19
Appendix B: DNS/VIP Addresses	21
Copy System Access	21
Add-Ons Workaround	21
Transient DNS Changes	22
Appendix C: Troubleshooting	23
Telnet	23
SSL Thumbprints.....	23

Introduction

SSL (Secure Sockets Layer) is a commonly used protocol for managing the security of a message transmission on the internet. Galileo SSL enables agencies to use their existing computers and print servers to access the Apollo and Galileo Computer Reservation Systems (CRS) over the public internet via an encrypted, secured connection.

What's New

The updates for Galileo SSL Client 3.0.1 are:

- Improved reliability of the Galileo SSL thumbprint passcode.

When an agent is provisioned, Travelport maps a Galileo SSL thumbprint to the agent's Client ID as part of the authentication mechanism to the Travelport domain.

Previously, agents may have required a reset to their SSL thumbprint for certain changes, such as an upgrade to their computer's operating system. If the thumbprint was reset, the associated Client ID no longer mapped to the new thumbprint passcode, and Galileo SSL connectivity failed.

With Galileo SSL Client 3.0.1, an encrypted copy of the thumbprint passcode is now stored locally on the agent's machine or agency server. This local copy of the passcode reduces the need to reset the passcode.

For more information, see *SSL Thumbprints* on page 23.

- An installation option to either retain the existing communication (TCP/IP) configuration or select Galileo SSL's default communication configuration. See Step 3 in *Standard Galileo SSL Information* on page 5.

Minimum Software Requirements

The following requirements are needed for the SSL installation. These requirements comply with the June 2018 updates to the Payment Card Industry Data Security Standard (PCI DSS).

Supported Product	<p>SSL is implemented for agencies that run these Travelport products:</p> <ul style="list-style-type: none"> ▪ Travelport Smartpoint ▪ Galileo Desktop 1.01 and later ▪ Travelport Booking Feed (TBF) ▪ PM Browser ▪ XML Select ▪ Products that use a TN3270 emulator for connectivity ▪ Products that use a proxy server for connectivity <p>No changes for SSL will be made for current internet-dependent products and services, such as:</p> <ul style="list-style-type: none"> ▪ Galileo Web Services (GWS) ▪ Galileo Flight Integrator (GFI) <p>Note: Galileo Print Manager (GPM) is no longer supported by Travelport. If you are currently using GPM, please upgrade to GPM.NET, which does not require a separate installation of the Galileo SSL Client. GPM.NET is currently available in most locations. See your Travelport representative for details.</p>
Internet Access	<p>To support internet access:</p> <ul style="list-style-type: none"> ▪ Allow SSL service on port 443 through firewall or other customer infrastructure. ▪ Set idle timeouts on port 443 connections at 3600 seconds or higher. ▪ If using an HTTP proxy, ensure the proxy idle timeout on port 443 is set to 3600 seconds or higher.
Operating System	<p>Galileo SSL Client v3.0.0 must be installed on a Microsoft® Windows operating system that supports Microsoft .NET Framework 4.6.2 or later:</p> <ul style="list-style-type: none"> ▪ Windows 7 Service Pack 1 ▪ Windows Server 2008 R2 ▪ Windows 8.0 or Windows 8.1 <p>Windows 8.1 is recommended. A free update from Windows 8.0 to Windows 8.1 is available.</p> <ul style="list-style-type: none"> ▪ Windows 2012 or Windows 2012 R2 ▪ Windows 10 <p>These Windows 10 updates are recommended:</p> <ul style="list-style-type: none"> ○ Windows 10 Anniversary (includes .NET Framework 4.6.2) ○ Windows 10 Creators (includes .NET Framework 4.7) ○ Windows 10 Fall Creators (includes .NET Framework 4.7.1) <p>Note: Windows 10 Student (10 S) is NOT compatible with Smartpoint.</p> <p>Important!</p> <p>Other versions of Microsoft Windows, including Windows XP and Windows Vista are NOT compatible with Microsoft .NET Framework 4.6.2 or later.</p>

Software Framework

Microsoft® .NET Framework 4.6.2 or later.

- If a supported version of .NET Framework is not present, the Galileo SSL Client installation process displays a message and then stops. After you install .NET Framework 4.6.2, run the Galileo SSL Client installer again.
- Some supported products include .NET Framework 4.6.2 or later in their product installations. See specific product Installation Guides for details.
- A free version of .NET Framework can be downloaded from www.Microsoft.com. From the Microsoft site, search for **.NET Framework 4.6.2**.



Installer Requirements

Before you install Galileo SSL:

- Ensure that the SSL connection is installed under the supervision of someone with a working knowledge of your office hardware.
- The installer has administrative rights.

Downloading Galileo SSL Client

The Galileo SSL v3.0.1:

- Is available for download as of 04 October 2018 on Travelport Marketplace at <https://www.travelportmarketplace.com/Product/-Galileo-SSL-301>.
- Is Included in the installation for Travelport Smartpoint v8.2 for Travelport Apollo and Travelport Galileo. (Pending release in 2019.)
- May be available from regional portals or other locations provided by your Travelport representative.

Installing Galileo SSL

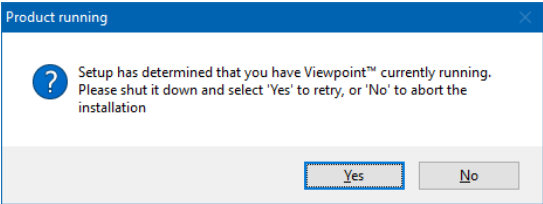
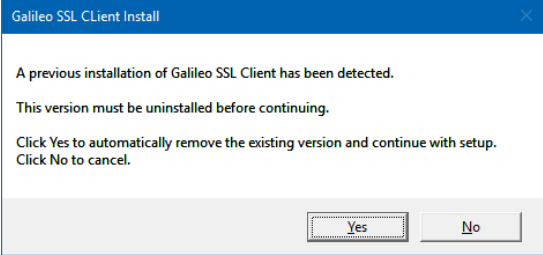
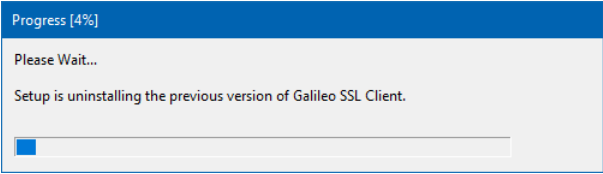
The instructions for installing and configuring Galileo SSL can vary not only by supported product, but also by type of environment. Therefore, before installing Galileo SSL and configuring your supported products, follow the steps in *Before Installing Galileo SSL Client*.

- Review this section for installation prerequisites and the Basic Installation information.
- Review the *Installation Environments for Galileo SSL* section on page 7 and install Galileo SSL based on the selected environment.
- Go to *Configuring Galileo SSL for Supported Products* on page 12 for instructions on configuring the supported products that will use the Galileo SSL connection.

Note: Configuration requirements for supported products may vary depending on the environment in which they are installed. Be sure to confirm the appropriate environment before proceeding with the configuration instructions.

Before Installing Galileo SSL Client

Before installing Galileo SSL Client, confirm the following prerequisites.

Prerequisite	Details
Ensure that one of the supported products is installed.	See <i>Minimum Software Requirements</i> on page 2 for a list of Travelport products that use Galileo SSL.
Close any supported applications.	<p>If one of the supported applications is running, a message is displayed. For example:</p>  <p>Close the associated application and click Yes.</p>
Do NOT uninstall previous versions of Galileo SSL Client.	<p>If Galileo SSL Client was previously installed, you do not need to manually uninstall previous versions. If a previous version is present, the installation process displays the following dialog box:</p>  <p>Click Yes to display the Progress message.</p> 
When installing the SSL in a Server Mode environment, allow proper firewall and virus software throughput.	<p>Proper throughput ensures proper UDP and TCP/IP network protocol exceptions required for related applications. This throughput applies to firewall and virus software running on the SSL server and down-stream workstations connecting through the server.</p> <p>Please see the firewall configuration specifications for your application.</p>
Back up customized configuration settings.	<p>In Galileo SSL 3.0.1, an option was added to the installation to retain customized configuration settings. However, as a precaution, the configuration file should be backed up to retain customized settings for connection profiles, proxy settings, and other changes.</p> <ol style="list-style-type: none"> 1. Copy SSLClientService.exe.Config. By default, this file is located in <i>c:\Program Files (x86)\Galileo\SSL</i>. 2. If customized configurations are not retained after installing Galileo SSL Client or Travelport Smartpoint, replace the new SSLClientService.exe.Config file with the back-up copy. 3. Restart the Galileo SSL Tunnel service.

Standard Galileo SSL Installation

The standard Galileo SSL installation applies to installations for all supported products, unless otherwise noted.

Note: Be sure to review the *Installation Environments for Galileo SSL* on page 7 **BEFORE** installing Galileo SSL. This section provides details for installing Galileo SSL on single machines or various types of networked environments.

1. Close any supported products.
2. Launch the Galileo SSL installation. The method of delivery for this installation can vary by region; the installation location and other details are provided by your Travelport representative.

Note: The installation checks for the presence of Microsoft .NET Framework version 4.6.2 or later. If the correct version is already installed, the installation will continue. If Microsoft .NET Framework version 4.6.2 or later is not found, the Galileo SSL Client installer stops.

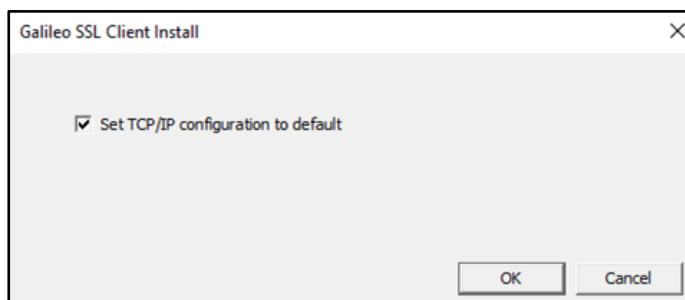
The Galileo SSL Client Install displays.

3. Select or deselect the check box for **Set TCP/IP configuration to default**.

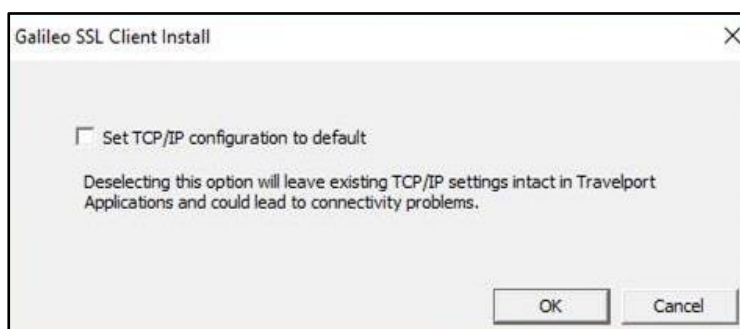
This check box selection varies depending on whether the installation detects an existing version of Galileo SSL.

New Installations

For new installations, in which a previous version of Galileo SSL is not detected, the default TCP/IP configuration is selected.

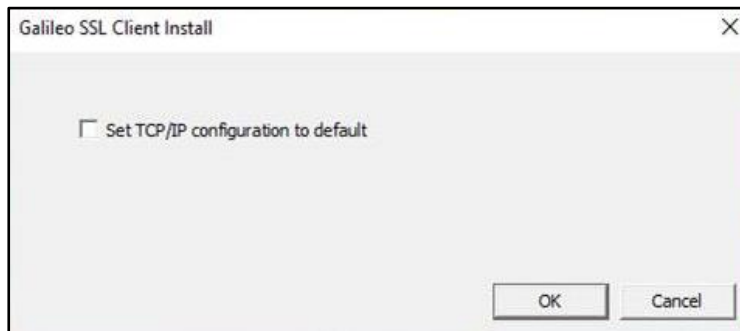


If you deselect this option, any existing TCP/IP configurations for Travelport applications are used. These existing configurations may vary for each Travelport application, and these settings should be validated to ensure that they do not lead to connectivity problems.

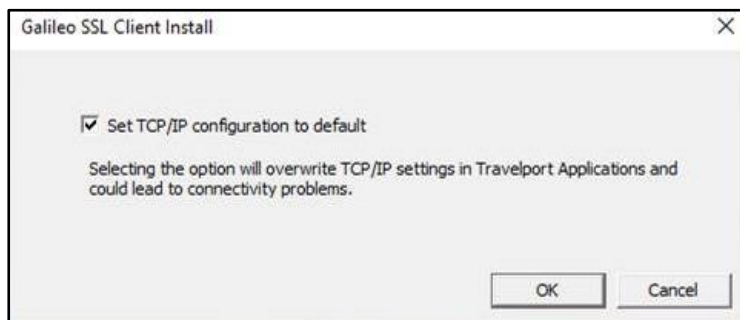


Updated Installations

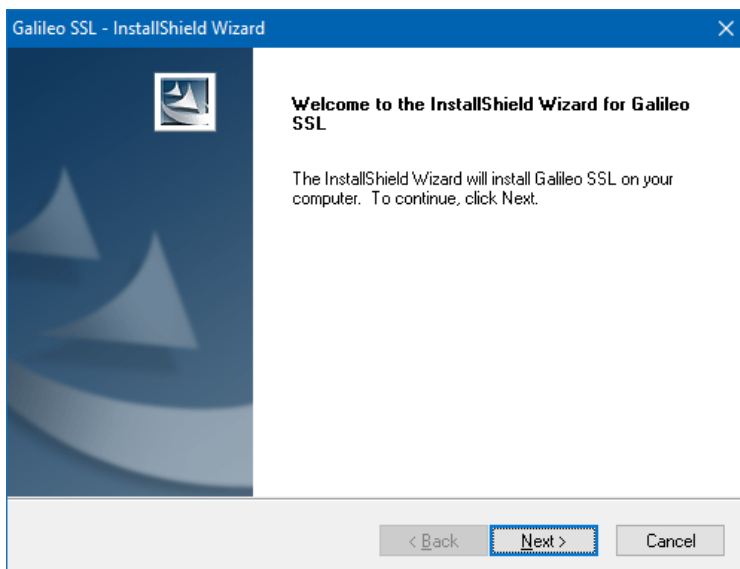
For updated installations, in which a previous version of Galileo SSL is detected, the default TCP/IP configuration is not selected. Therefore, the existing TCP/IP configuration is retained.



If this option is selected, the default TCP/IP configurations for Travelport applications are used and any customized settings are overwritten. Therefore, these settings should be validated to ensure that they do not lead to connectivity problems.

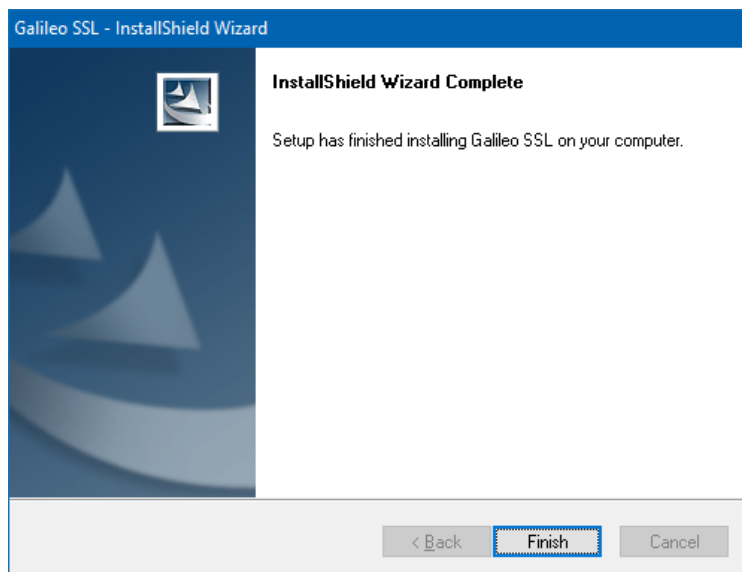


4. Click **OK** to display the Welcome window.



3. Click **Next**. The Terms and Conditions window appears.
4. Click the radio button *I acknowledge that I have read and agree to the terms and conditions*.
5. Click **Next**.

The Finish window displays.



6. Click **Finish**.
7. After installing Galileo SSL, go to *Configuring Galileo SSL for Supported Products* on page 12 for instructions on configuring the supported products that will use the Galileo SSL connection.

Installation Environments for Galileo SSL

SSL can be installed in a variety of environments. The installation type for your agency depends on the way the network is configured and the specific environment setup. The three most common environments are:

- Typical Agency Workstation
See *Typical Agency Workstation Environment* on page 8.
- Gateway Mode for Citrix Load Balanced (Cluster) or MTS
See *Gateway Mode for a Citrix Load-Balanced (Cluster) or MTS Environment* on page 9.
- Stand-Alone Citrix or MTS
See *Stand-Alone Citrix or MTS Environment* on page 11.

Note: Please contact your Travelport representative if you need assistance with other types of installation environments.

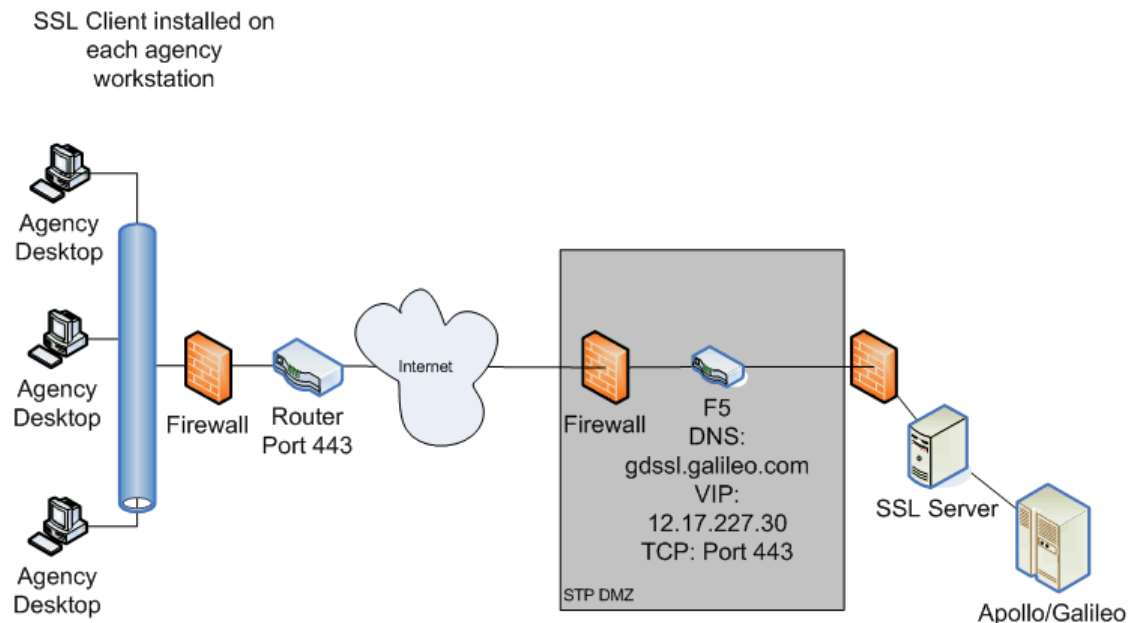
After installing Galileo SSL, see *Configuring Galileo SSL for Supported Products* on page 12 to configure your associated supported products.

Typical Agency Workstation Environment

In the typical agency workstation environment, supported products are installed separately on each agency workstation. Therefore, the Galileo SSL Client must also be installed on each agency workstation.

Environment Diagram

The following diagram shows the typical agency workstation environment after the Galileo SSL Client is installed.



1. The Galileo SSL Client is installed on each workstation to route traffic via port 443.
2. Client launches the supported product, such as Galileo Desktop or Smartpoint.
3. Data flows to a shared ISP router, which routes all traffic to Travelport's SSL environment.

Note: The DNS/VIP numbers depend on the location. See *Appendix B: DNS/VIP Addresses* on page 21 to determine the correct numbers for your location.

Installing Galileo SSL

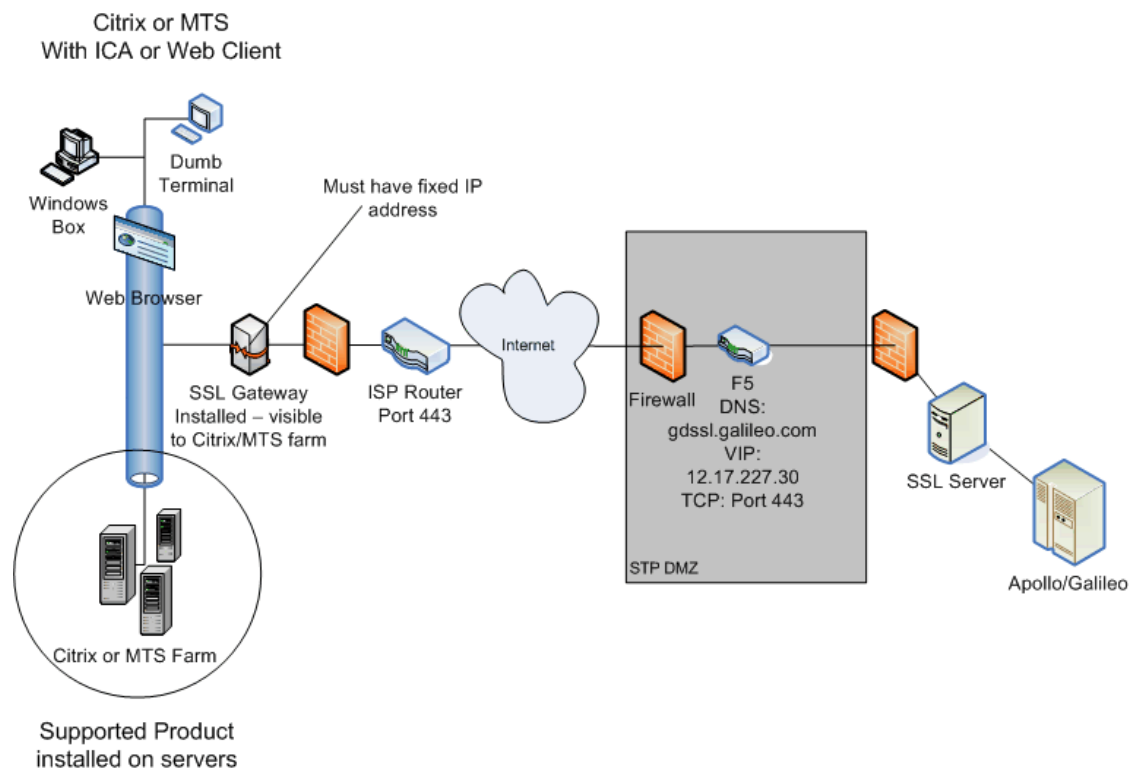
To install SSL in a typical agency workstation environment:

1. Use the *Standard Galileo SSL Installation* on page 5. Galileo SSL must be installed separately on each workstation.
2. Verify that Galileo SSL is installed on the workstation.
 - a. From the **Start** menu, select the **Control Panel**.
 - b. Double-click **Add or Remove Programs** to display the Add or Remove Programs dialog box.
 - c. If Galileo SSL has installed successfully, the currently installed programs list includes *Galileo SSL*.
3. After installation, refer to *Configuring Galileo SSL for Supported Products* on page 12 to determine additional configuration requirements for your supported products.

Gateway Mode for a Citrix Load-Balanced (Cluster) or MTS Environment

In a load-balanced Citrix or MTS environment, in which the supported products are installed on servers, the Galileo SSL Client is installed on the SSL Gateway machine.

Environment Diagram



1. Client launches Citrix or Microsoft Terminal Server (MTS) with an Integrated Connection Agent (ICA) or Web Client.
2. On a load-balanced farm, the load-balancing software connects to the least-utilized server.
3. The server then starts an instance of the supported software.
4. When the supported software is launched, it searches for the configuration file for the IPCS fixed (static) IP address of the SSL Gateway.
 - Each instance of the supported software must have the IPCS configured for the SSL Gateway's fixed IP.
 - The SSL Client must have a fixed IP address or, for advanced users, a DNS name.
5. The SSL Gateway provides a path to authentication and a secure encrypted shared connection to Travelport's SSL environment.

Note: The DNS/VIP numbers depend on the location. See *Appendix B: DNS/VIP Addresses* on page 21 to determine the correct numbers for your location.

Installing Galileo SSL

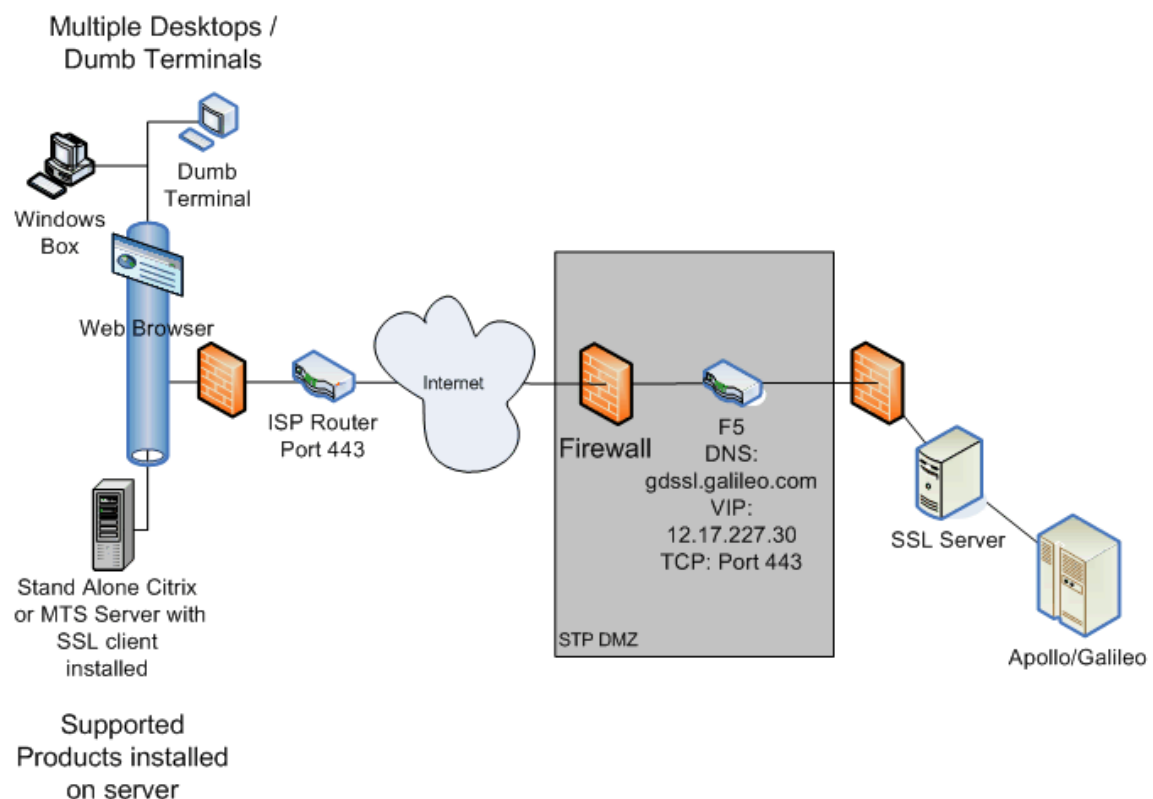
To install SSL in Gateway Mode for a Citrix Load Balanced (Cluster) or MTS environment:

1. Install SSL on the Gateway machine using the *Standard Galileo SSL Installation* on page 5.
2. Open the configuration file **SSLClientService.exe.config** using Notepad.
3. Add the following line to the <appSettings> section for the SSL Gateway:

```
<add key="Server Mode" value="enabled" />
```
4. After installation, refer to *Configuring Galileo SSL for Supported Products* on page 12 to determine additional configuration requirements for your supported products.

Stand-Alone Citrix or MTS Environment

Environment Diagram



1. Client launches Independent Computing Architecture (ICA) to a single Citrix or MTS server.
2. The MTS or Citrix server starts an instance of the supported software.
3. When the supported software is launched, it uses the loopback address to authenticate via the SSL Loopback Tunnel.
4. The SSL Client provides a path to authentication and a secure encrypted shared connection to Travelport's SSL environment.

Note: The DNS/VIP numbers depend on the location. See *Appendix B: DNS/VIP Addresses* on page 21 to determine the correct numbers for your location.

Installing Galileo SSL

To install SSL in a stand-alone Citrix or Microsoft Terminal Server environment:

1. Install SSL on the stand-alone or MTS server using the *Standard Galileo SSL Installation* on page 5.
2. Verify that SSL is installed and running by opening the Task Manager and finding the entry **SSLClientService.exe**.
3. After installation, refer to *Configuring Galileo SSL for Supported Products* on page 12 to determine additional configuration requirements for your supported products.

Configuring Galileo SSL for Supported Products

After installing Galileo SSL for the appropriate installation environment, you must configure your supported products to use the Galileo SSL connection.

Important! Configuration requirements for a supported product can vary depending on the environment in which it is installed. Be sure to confirm the appropriate environment before proceeding with the configuration instructions.

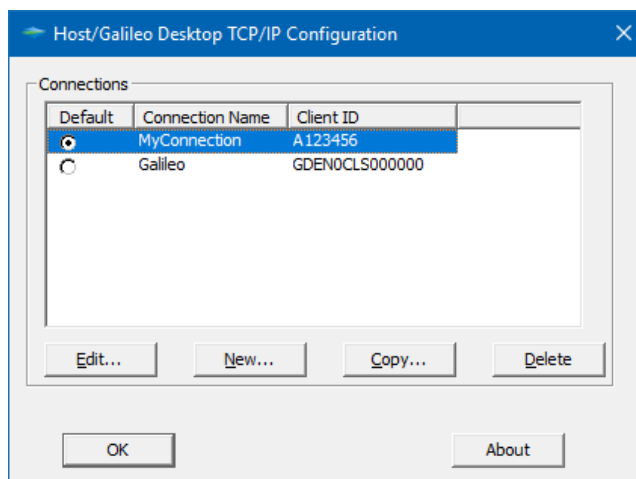
Configuring Galileo Desktop/Smartpoint for Galileo SSL in a Typical Agency Workstation Environment

After the Galileo SSL installation is completed, the installation automatically changes the Primary and Secondary IPCS Addresses for all Client IDs to use **127.0.0.1** for Galileo SSL access. At the time of installation, all present Client IDs are updated.

Note: If you use multiple Client IDs and traditional land-line access, the addresses must be manually configured back to the original addresses. For example: 216.113.159.193 and 216.113.159.198.

To configure Galileo Desktop for Galileo SSL:

1. Close Galileo Desktop.
2. From the **Start** menu, select the **Control Panel**.
3. Double-click the **Galileo TCP/IP** icon to display the Host/Galileo Desktop TCP/IP Configuration dialog box.



4. Select your connection and click **Edit** to display the Connection dialog box.
5. In **Client Identifier**, verify that the Client ID is correct.
6. Confirm that **Use Fixed Configuration Server Addresses** is selected.
7. Confirm that the **Primary IPCS Address** and **Secondary IPCS Address** are 127.0.0.1.

Note: If you use multiple Client IDs and traditional land-line access, the addresses must be manually configured back to the original addresses. For example: 216.113.159.193 and 216.113.159.198.

8. Select **Force Download**.

9. Click **OK**.

Note: Advanced Users Only: In Gateway mode, you might want to select *Use Domain Name Services (DNS)*. This would be the DNS Host Name of the Gateway mode server configured on your local network.

Configuring Galileo Desktop/Smartpoint in Gateway Mode for a Citrix Load-Balanced (Cluster) or MTS Environment

To configure Galileo Desktop, modify each Citrix-supported application configuration file to reflect the fixed IP of the SSL Gateway.

1. Stop the Galileo SSL Service:
 - a. Right-click **My Computer** and choose **Manage** to open the Computer Management dialog box.
 - b. Open **Services and Applications > Services**.
 - c. Select the Galileo SSL Service and click **STOP**.
 - d. Keep this dialog box open to restart the service later.
2. Navigate to the Galileo Desktop Users directory, which is typically in a \MACHINE folder.
3. Right-click **dat32com.ini** and choose **Open With > Choose Program > Notepad**.
4. Find the following text in the configuration file – there are two instances:

```
IPCName=
PrimaryIPCS=###.###.###.###
SecondaryIPCS=###.###.###.###
```


5. Modify the Primary and Secondary IPCS addresses to reflect the fixed IP address of the SSL Gateway.
6. Choose **File > Save**.
7. Restart the Galileo SSL Service:
 - a. Select the Galileo SSL Service on the Computer Management dialog box and click **START**.
 - b. Close the dialog box.

Configuring Galileo Desktop/Smartpoint in a Stand-Alone Citrix or MTS Environment

To configure Galileo Desktop in a Stand-Alone Citrix or Microsoft Terminal Server environment:

1. Stop the Galileo SSL Service:
 - a. Right-click **My Computer** and choose **Manage** to open to Computer Management dialog box.
 - b. Open **Services and Applications > Services**.
 - c. Select the Galileo SSL Service and click **STOP**.
 - d. Keep this dialog box open to restart the service later.
2. Navigate to each `\\(Users)\\(Remote Users Home Directory)`.
3. Right-click **dat32com.ini** and choose **Open With > Choose Program > Notepad**.
4. Find the following text in the configuration file – there are two instances:

```
IPCName=
PrimaryIPCS=###.###.###.###
SecondaryIPCS=###.###.###.###
```
5. Modify the Primary and Secondary IPCS addresses to reflect the loopback IP address 127.0.0.1.
6. Choose **File > Save**.
7. Restart the Galileo SSL Service:
 - a. Select the Galileo SSL Service on the Computer Management dialog box and click **START**.
 - b. Close the dialog box.

Configuring Travelport Booking Feed for Galileo SSL

These configuration instructions apply to Travelport Booking Feed (TBF) implementations in all environments.

Note: If your TBF implementation uses more than one queue, contact your Galileo support person.

To configure TBF for Galileo SSL:

1. Stop the Galileo SSL Service:

- a. Right-click **My Computer** and choose **Manage**.
 - b. Open **Services and Applications > Services**.
 - c. Select the Galileo SSL Service and click **STOP**.
2. Install Galileo SSL on the machine that runs the TBF Client Adapter.
 3. Modify the **SSLClientService.exe.config** file.
 - a. Navigate to the Galileo SSL installation folder (e.g., *c:\Program Files\Galileo\SSL*).
 - b. Right-click the **SSLClientService.exe.config** file and select **Open With > Notepad**.
 - c. Add the following lines with the TBF information, under the <appSettings> section if you are installing TBF after previously installing the SSL Client:

```
<add key="GIDS QueueName Override" value="<your queueName here>" />
```

(**Note:** This will work for single or multiple clients using the same queue name.)
 - d. Save and close SSLClientService.exe.config.
 4. Open the Galileo IDS Configuration adapter utility.
 5. In the TBF Application Properties dialog box, change the **MQ Host Name** destination to **127.0.0.1**.
 6. Click **Apply**.
 7. Restart the Galileo SSL Service:
 - a. Select the Galileo SSL Service on the Computer Management dialog box and click **START**.
 - b. Close the dialog box.

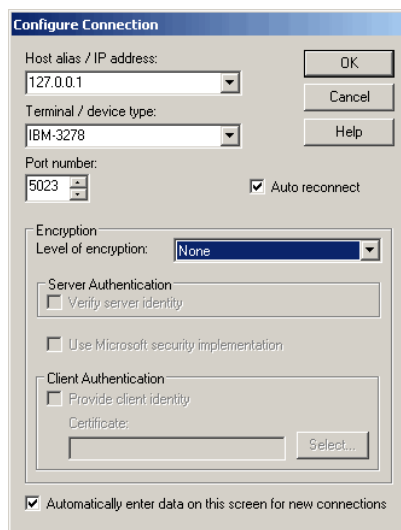
Configuring a TN3270 Emulator for Galileo SSL

These configuration instructions apply to TN3270 Emulator implementations in all environments. Travelport has two different TN3270 endpoints, which you need to configure separately. To install and configure SSL on a machine that uses a TN3270 emulator to connect:

1. Install SSL. Use the same installation instructions as specified for Galileo Desktop.
2. Launch the TN3270 emulator.
3. Navigate to the session configuration options.
4. Navigate to host IP Address field and add or replace the host IP with the loopback address (127.0.0.1), and the following port to route traffic to the Galileo TN3270 Gateway:
 - a. Port 5024 for VS1 (e.g., RoomMaster)
 - b. Port 5025 for GVM (e.g., Taste)

Note: If you need access to both end-points, create two different “profiles” in your TN3270 emulation software to allow you to “select” the system you will use. You can give them a meaningful name, such as “RoomMaster” and “Taste”.

Your application settings might vary from the following example:



Configuring XML Select for Galileo SSL

These configuration instructions apply to XML Select implementations in all environments. When installing the Galileo SSL Client in an XML Select environment, the HCM Manager is automatically configured with the loopback settings.

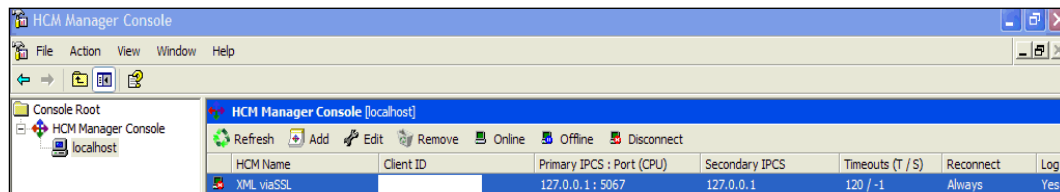
To install Galileo SSL in an XML Select environment:


1. Launch the installation.
2. The installation checks for the presence of Microsoft.NET version 2.0. If already installed, the SSL installation continues.
 - a. If Microsoft.NET version 2.0 is not found, the download starts automatically. The download is approximately 23 MB.
 - b. When the download completes, if you are prompted with a security message to run or not run, click **Run**.
 - c. Follow the Microsoft.NET install prompts to install.
 - d. After the .NET install, the SSL software installation automatically continues.
3. The Welcome screen displays.
Click **Next**.
4. The Terms and Conditions screen displays.
Click **Yes** to accept.
5. The Finish screen displays.
Click **Finish**.

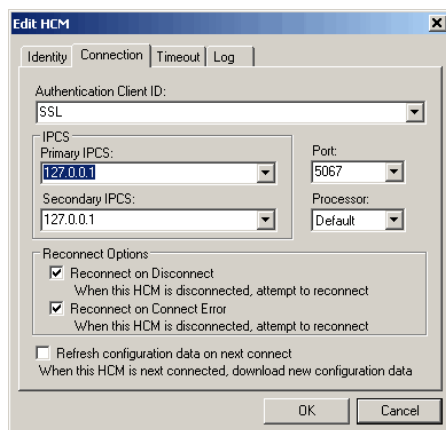
Verify that the Primary IPCS is set to the loopback address (127.0.0.1):

1. Choose **Start > Programs > XML Select > HCM Manager Console**.

- The HCM Manager Console screen should look similar to the following, with the Primary IPCS configured to the loopback address 127.0.0.1 and Port 5067.



- To manually verify these settings, select the HCM Name and click the **Edit**  button.
- Click the **Connection** tab. The Edit HCM dialog box should look similar to the following:



NOTE: SSL has not been tested on the Galileo Test and Copy systems.

Configuring Customer Proxy Servers for Galileo SSL

These configuration instructions apply to customer proxy servers in a typical agency workstation environment only.

This section describes installing SSL to support customer proxy servers. Customer proxy servers service the requests of clients by forwarding requests to other servers. To install SSL to support customer proxy servers:

- Install SSL on the Gateway machine. Use the same installation instructions as specified for Galileo Desktop.
- Stop the Galileo SSL Service:
 - Right-click **My Computer** and choose **Manage**.
 - Open **Services and Applications > Services**.
 - Select the Galileo SSL Service and click **STOP**.
- Enable proxy server support by adding the IP Address or DNS name of the proxy server in the **SSLClientService.exe.config** file.
- Navigate to the default install folder. For example, *C:\Program Files\Travelport\SSL*.
- Right-click the file and choose **Open With > Notepad**.

6. Add the following lines in the <AppSettings> section with the information for the customer:

```
<add key="Proxy Server Address" value="customer proxy"/>
```

```
<add key="Proxy Server Port" value="customer proxy port"/>
```

```
<add key="Proxy Server Username" value="customer proxy username"/>
```

```
<add key="Proxy Server Password" value="customer proxy password"/>
```

8. Choose **File > Save**.
9. Restart the Galileo SSL Service:
 - a. Select the Galileo SSL Service in the Computer Management dialog box and click **START**.
 - b. Close the dialog box.

Note: When using an HTTP proxy, please ensure that the proxy idle timeout on port 443 is set to 3600 seconds or higher.

Appendix A: SSL Client Configuration Parameters

The reference table below provides various parameters used when installing and configuring the SSL.

Literal key to use in .config file	When used, the key specifies:	Default, if not specified
SSL (GDAS) Server		
SSL Server Address	The PRODUCTION GDAS Server to use	gdssl-atl.galileo.com
Copy SSL Server Address	The COPY GDAS Server to use	gdsslpp-atl.galileo.com
SSL Server Port	The servers port to target	443
LCN Complex		
Configuration Server Address	The PRODUCTION IPCS address to target	216.113.159.193 and 216.113.159.198
Copy Configuration Server Address	The COPY IPCS address to target. (Now redundant parameter. COPY GDAS server is targeted instead.)	
Configuration Server Port	The IPCS port to use	5067
Client IPC Port	The primary port we listen on for IPC requests (now redundant parameter)	
Client IPCS Port	The port we listen on for IPCS requests	5067
Copy IPCS Prepend String	Prepending a zero to the existing Copy Client ID is required for Copy system access	"0"
Other Endpoints		
MQ Server	The MQ Server IP address used for printing	57.8.16.41
MQ Printing Port	The MQ Server IP port used for printing	1414
GIDS Server	The TBF Server IP address to use	57.8.16.41
GIDS Port	The TBF Server IP port to use	1415
GIDS QueueName Override	The target TBF queue to use if the automatic generation does not work (uses primary FP ClientID). See the <i>Configuring TBF for Galileo SSL</i> section regarding multiple queues.	<not configured>
TN3270 Server	The TN3270 server to target	57.8.81.14
TN3270 Port	The TN3270 server port to target	5023
PM Browser Server	The HTTP server to send PM Browser requests	57.8.16.39

Literal key to use in .config file	When used, the key specifies:	Default, if not specified
PM Browser Server Port	The HTTP server port to send PM Browser requests	80
PM Browser Listen Port	The port we listen on for PM Browser traffic	8765
Proxy Server Configuration		
Proxy Server Address	The IP address/DNS name of a proxy server to use, if required	<not configured>
Proxy Server Port	The IP port of a proxy server to use, if required	<not configured>
Proxy Server Username	The user name of the proxy server permissions, if required.	<not configured>
Proxy Server Password	The password of the proxy server permissions, if required.	<not configured>
General Configuration		
Server Mode	Enables SSL Client Server Mode. Traffic from local network machines will be accepted. To enable, set to "Enabled".	<not configured>
Spoof Version 3	Test config parameter. Do not use.	False
Disable Redirects	Prevents automatic redirection to preferred GDAS SSL servers. To enable, set to "True".	False
Keepalive Seconds	The period in seconds between TCP/IP low-level keepalives. May be tuned to avoid networking issues regarding lost connections.	120
Trace Level Override	Changes the tracing level of the SSL Client. Values may be Critical, Error, Warning, Information, Verbose or All.	Warning

Appendix B: DNS/VIP Addresses

The firewall must allow TCP connections to these endpoints on port 443:

DNS	VIP
gdssl.galileo.com	216.113.159.225
gdssl-atl.galileo.com	216.113.159.226
sslfpemea.galileo.com	216.113.159.227

For Copy system access, the following should also be included (also port 443):

DNS	VIP
gdsslpp-atl.galileo.com	216.113.131.33

Copy System Access

To direct a client ID to the Travelport copy system complex, add a leading "zero" to your client ID. If your copy system client ID is *wgal1000*, use *0wgal1000* in your client to target the copy systems. Copy system access is available in v1.7 and later of the SSL retro client.

For XML Select users who test against a copy environment, use the following DNS:

DNS: gdsslpp-atl.galileo.com

VIP: The copy system IP address range that needs to be added to copy/test Client IDs is:
10.5.225.125-10.5.226.125

Galileo Desktop can connect to the Production and non-production system simultaneously using this feature. Client IDs without the leading zero will connect to Production, while Client IDs with the leading zero will connect to non-production.

Add-Ons Workaround

A desktop add-on is a feature, such as Relay, Rapid Reprice, WebFares, Point and Click, ARNE, or AutoServiceFee. These add-ons check the "Host=" statement in the WIN.INI file to validate which host is configured. Galileo Desktop treats all Client IDs that start with "G" as Galileo and all others as Apollo, and sets this host= statement accordingly.

The new SSL copy access requires that you prepend a zero in front of the Client ID so that a Galileo Copy Client ID triggers the application to set the win.ini as *host=Apollo*. The workaround for copy applies to a Galileo Copy Client ID. You need to configure with the zero, then change the host in win.ini back to *host=Galileo*.

To begin, open the **win.ini** file, and make the following change:

Before:

```
[Focalpoint]
SWDIR=C:\fp\swdir\
DATADIR=C:\fp\datadir\
MACHINEDIR=C:\fp\machine\
Host=Apollo
```

After:

```
[Focalpoint]
SWDIR=C:\fp\swdir\
DATADIR=C:\fp\datadir\
MACHINEDIR=C:\fp\machine\
Host=Galileo
```

Transient DNS Changes

The DNS to which you are assigned will remain the same (see the **Default** labels in the Access column in the DNS/VIP table), unless a problem arises and all users on that DNS are moved to another DNS. This migration is transparent, except that if you ping or trace your assigned DNS, the VIP will display the new system to which traffic is going. Upon completion of the fix, you will be switched back to your original VIP.

Appendix C: Troubleshooting

Telnet

Being able to telnet from your operating system is a prerequisite as a download from the SSL server. To test whether you can telnet from your operating system, you must be able to launch a telnet application. In Windows XP, you can launch telnet from a DOS prompt. In Windows Vista, a third-party application is required. To test via telnet whether you can connect to the SSL VIP:

1. Launch your telnet application.
2. Enter the following commands (below). If you can connect, you will receive a blank screen. Press the **Enter** key to drop the connection.
 - telnet gdssl.galileo.com 443
 - telnet gdssl-atl.galileo.com 443
 - telnet sslfpemea.galileo.com 443

Note: You may receive the following message:

Could not open connection to the host, on port 443: Connect failed.

This message indicates there is a connectivity issue between the workstation and the Galileo SSL farm. This should be investigated by the agency network personnel. It is most likely a firewall rule issue. See the instructions on firewall rules and configuration for your installation type.

SSL Thumbprints

When an agent is provisioned, Travelport maps a Galileo SSL thumbprint to the agent's Client ID as part of the authentication mechanism to the Travelport domain.

In Galileo SSL Client 3.0.0 and earlier, agents may have required a reset to their SSL thumbprint for certain changes, such as an upgrade to the agent's operating system. If the thumbprint was reset, the associated Client ID no longer mapped to the new thumbprint passcode, and Galileo SSL connectivity failed.

As of Galileo SSL Client 3.0.1, an encrypted copy of the thumbprint passcode is stored locally. This local copy of the passcode reduces the need to reset the passcode.

Security of the thumbprint passcode is preserved by encryption using standard Windows APIs, which restrict decryption to the local machine and only if a specific key is known. That key is hardcoded in the Galileo SSL Client.

Thumbprint Locations

The securely encrypted thumbprint passcode is stored in up to four locations on the computer.

Windows 64-Bit

GD SSL Configuration Path

C:\Program Files (x86)\Galileo\SSL\SSLClientService.exe.Config

Thumbprint Path

- C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Travelport.GDAS.Thumb.bin
- HKEY_USERS\DEFAULT\Software\Galileo International\Connectivity
- HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Galileo International\Connectivity
- C:\Program Files (x86)\Galileo\SSL\SSLClientService.exe.Config

Windows 32-Bit

GD SSL Configuration Path

C:\Program Files\Galileo\SSL\SSLClientService.exe.Config

Thumbprint Path

- C:\Windows\System32\config\systemprofile\AppData\Local\Travelport.GDAS.Thumb.bin
- HKEY_USERS\DEFAULT\Software\Galileo International\Connectivity
- HKEY_LOCAL_MACHINE\SOFTWARE\Galileo International\Connectivity
- C:\Program Files\Galileo\SSL\SSLClientService.exe.Config

Resetting Thumbprints

Local storage of the thumbprint passcode reduces the need to reset thumbprint passcodes.

However, if a reset is required for the thumbprint, two options are available:

- Travelport offers an automated Thumbprint Reset Tool. Please contact your Travelport Helpdesk to obtain more information about the SSL Thumbprint Automated Reset Tool.
- A configuration setting to force the Galileo SSL client to reinitialize the thumbprint and store the thumbprint in any of the four locations on the machine.
 1. Go to the Galileo SSL Config file, which is located in either:
 - C:\Program Files (x86)\Galileo\SSL\SSLClientService.exe.config.
 - C:\Program Files\Galileo\SSL\SSLClientService.exe.Config

2. Change the configuration setting to:

```
<add key="Rewrite Local Thumbprint Values" value="TRUE"/>
```

Fallback

If it is necessary to fall back or reinstall Galileo SSL, a backup of the agent's prior configuration and communication settings has been saved on the agent's computer at

C:\TravelportSSL\SSLClientService.exe.config.bak.