SSL (Secure Socket Layer connection)

Installation & Configuration Guide - Updated

Including Instructions for Terminal Server, Citrix & Thin Client Customers

Document Identifier: **SSL Installation and Configuration Guide**
Author: **Austin Burgin & updated by Simon Richards for Galileo Southern Africa**
Date: **13/10/2008 – Updated 06/12/2009**

INDEX

Revision History

Revision	Status	Date	Update Summary
0.01	DRAFT	13 October 08	First UK draft
0.02	DRAFT	15 October 08	Updated with Citrix / Thin Client Configuration Instructions
0.03	DRAFT	22 October 08	Updated with an Index and Fault Finding Instructions
0.0.4	DRAFT	08 December 2009	Updated document for ZA environment & Updated info

Application Overview

Product

This solution allows individual workstations to access the Galileo Host via an SSL (Secure Socket Layer) connection utilising an existing Internet connection, possibly removing the need for Customer Managed VPN or Focalpoint Net Solutions.

Customers are responsible for procuring their own dedicated Internet connection, which can be DSL, cable, T1, etc.
By deploying this solution, Galileo allows an agency to access the Galileo Host via their chosen Internet Service Provider.

Key Points

- Being internet based, the service has no Service Level Agreements or guarantees.
- You must install Focalpoint 3.5 or Galileo Desktop 1.01 or higher on each workstation
- An SSL Client ID will be required per workstation, CMVPN or FPNET Client IDs will not work.
- An SSL Client ID can not be used on multiple workstations as the computer fingerprint is registered.
- You must install the SSL Client on each workstation
- On successfully connecting Galileo for the first time the SSL Client ID GTID will download, the SSL Client ID GTID can only be downloaded once per machine, to reset the SSL Client ID fingerprint contact the Galileo Service Desk.
- For Thin Client or Citrix installations please contact your Galileo Technical Consultant for technical support.

Definition of Secure Socket Layer connection

- SSL, short for *Secure Sockets Layer*, is a protocol for transmitting private documents/information via the internet.
- The Galileo SSL client will enable Galileo Desktop and Galileo Print Managers to access the Galileo Host over the public Internet via an encrypted, secured connection.

Minimum Workstation Requirements

- Focalpoint 3.5, Viewpoint 3.0, or Galileo Desktop 1.01 and higher
  Note: FocalPoint 3.5 and ViewPoint 3.0 are not supported under Vista
- Windows 2000 and higher, if using windows XP, you need to have installed ‘Microsoft Installer 3.1 V2’ on the computer (KB893803)
- Internet Access
- Installer must have Administrative rights
- .Net 2.0 or above needs to be installed, if not present, the install will automatically go out and get it.

Features and Benefits

Feature	Benefit
Access to Galileo via the Internet	No Customer Managed VPN router configuration or FPNET Nortel VPN required.

Technical Overview

Impact to Other Products

Note: Any network problems that a customer faces are more dependant on their ISP. Customers may have to contact their ISP for assistance.

The following products are supported:

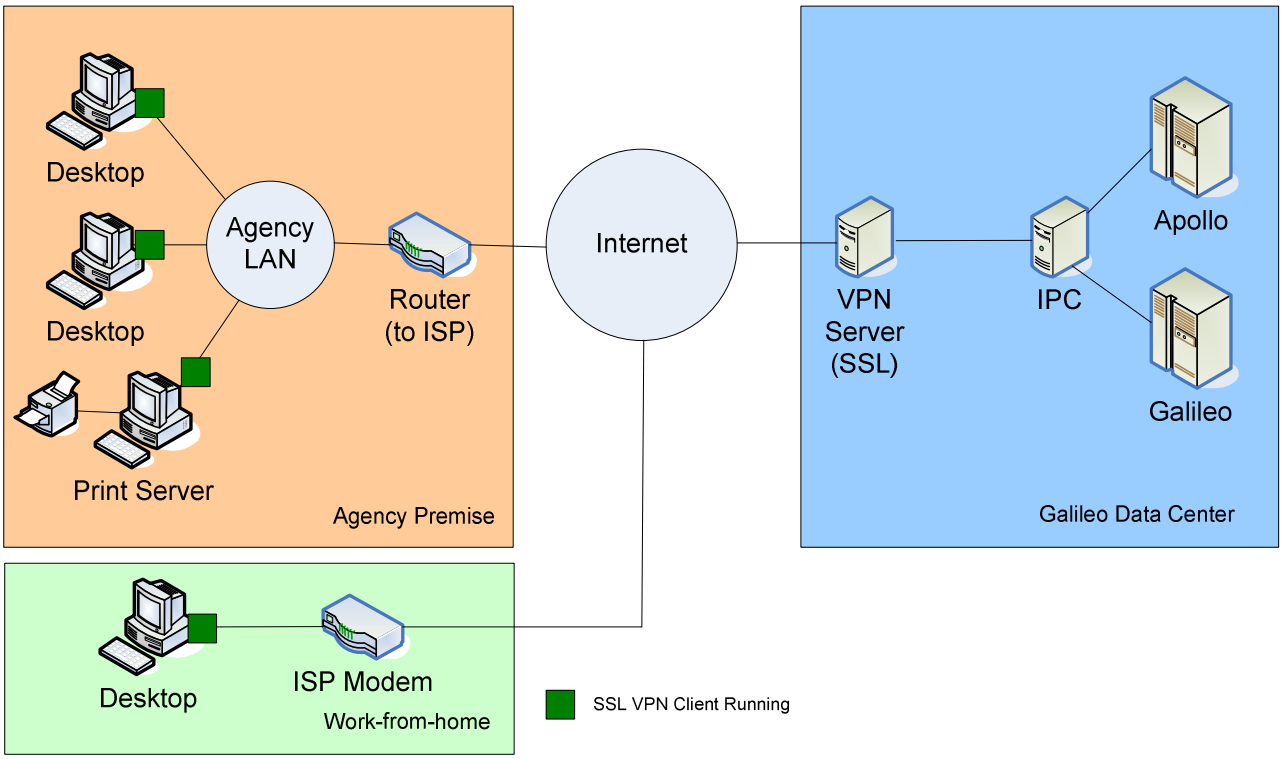
- Galileo Desktop, Focalpoint, Viewpoint host connection
- Print Manager
- Custom Fares
- Galileo Fee Manager
- MQ Print
- PM Browser
- Service Bureau

The following products are not currently supported.

- XML Select
- Anything that isn't Host Access
- Focalpoint Net
- Any other connection to Apollo/Galileo GDS
- NVP / Galileo Rail

- There will be new database (Client IDs) required for customers who migrate from Customer Managed VPN (CMVPN) FocalpointNet to an SSL Connection.

System Overview



Minimum Software Requirements

- Focalpoint 3.5, Viewpoint 3.0, or Galileo Desktop 1.01 and higher
- Windows 2000 and higher
- Internet Access
- .Net 2.0 or above needs to be installed, if not present, the install will automatically go out and get it.
- Microsoft Installer 3.1 v2 (KB893803)

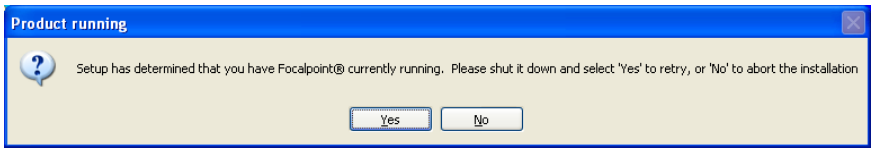
Note:

- *Installer must have Administrative rights*
- *Please install SSL connection under the supervision of someone with a working knowledge of your office hardware.*

Before Installation

- Install only on Focalpoint 3.5, Galileo Desktop 1.01, or higher. If one of these products is not found the following message will display.

- Install on Windows 2000 or higher
- Close Galileo Desktop/Viewpoint or Focalpoint before installation.



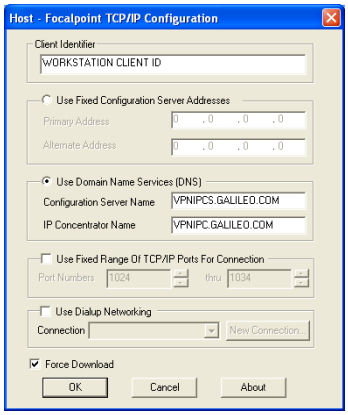
If you are migrating from FPNET please record you existing Focalpoint configuration details before proceeding encase you need to revert back.

Navigate to the Control Panel and double click on the Galileo TCP/IP Icon.

You may need to select the Edit button if you are running Galileo Desktop, record the following information

Client Identifier =

For FPNET customers record the Domain Name Server Names =



Download the SSL Client

Download the latest version of the SSL Client from the Galileo Web Site

http://mamba.galileosa.co.za/software/ssl/GalileoSSLClient_v01.00.0010.exe

Or here

ftp://www.galileosa.co.za/ssl/GalileoSSLClient_v01.00.0010.exe

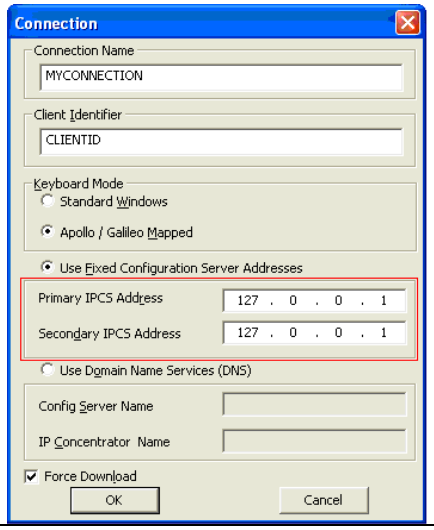
- Please read the SSL installation notes before submitting the Software Download Form
- The installation will automatically uninstall any previous Galileo SSL Client installation

SSL Galileo Desktop Installation

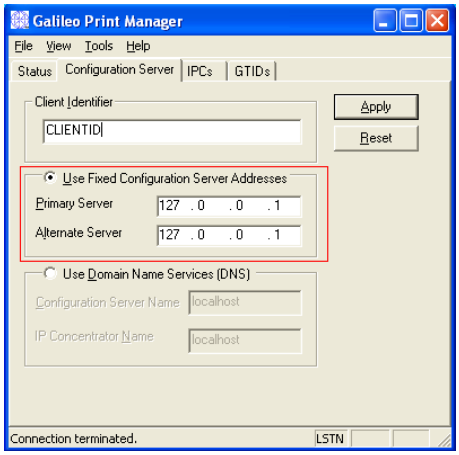
1. Installation over an existing working Galileo Desktop workstation (versions 1.01 and higher) and Galileo Print Manager if installed.

Use these steps to install Galileo SSL over an existing Galileo Desktop workstation.

Close Galileo Desktop and Galileo Print Manager (if applicable).	
Double Click GALILEOSSL.EXE	
The installation will check for the presence of Microsoft.NET version 2.0. If this is already installed the installation will continue.	If Microsoft.NET version 2.0 is not found the download will start automatically. The download is approx 23 MB. a. After the download if prompted with a security message to run or not run, click Run. b. Follow the Microsoft.NET install prompts to install. c. After the install the SSL software installation will automatically continue.
The Welcome Screen displays.	Click Next.
The Terms and Conditions Screen displays.	Click I acknowledge to accept.
The Finish Screen displays.	Click Finish.

The installation automatically changes the Primary and Secondary IPCS Addresses for all Client IDs to use 127.0.0.1 for SSL access. **Note**: If you use multiple Client IDs and any use traditional land line access, the addresses must be manually configured with addresses 57.8.81.13 and 57.8.81.113.	

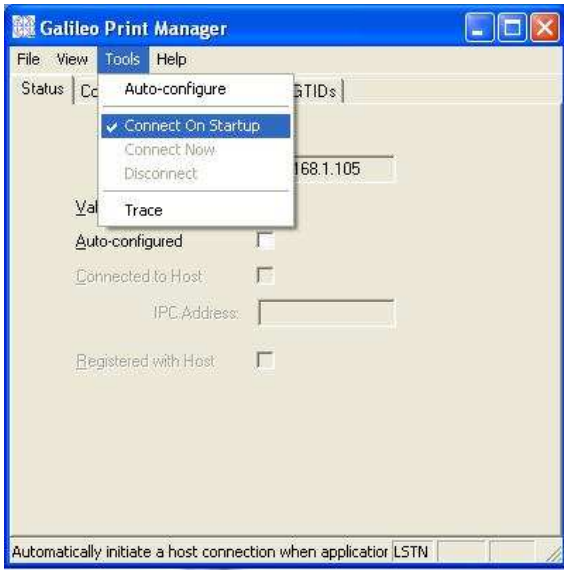
If Galileo Print Manager is installed on the workstation the configuration address will also be automatically updated.



Galileo Print Manager does not automatically wake up so must be configured to “Connect on Startup”. Once connected GPM will stay always connected.

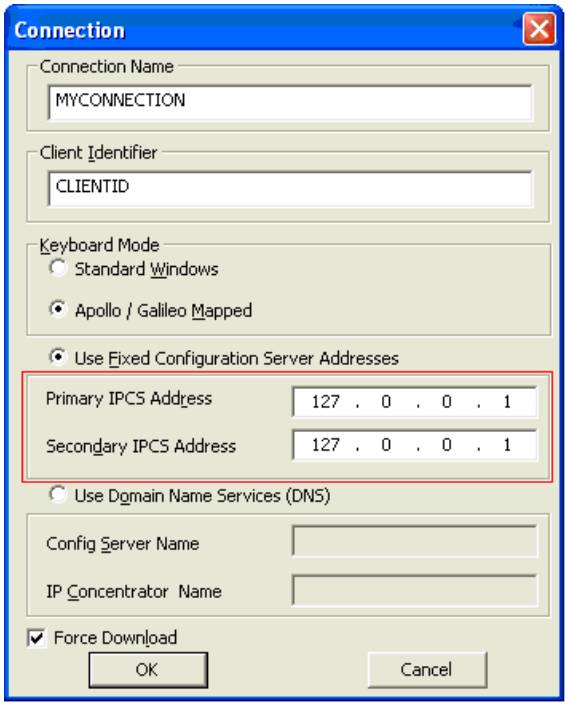
To set this option:

a. From the Tools Menu, Click “Connect On Startup”
b. Click the Configuration Server Tab, then click Apply.
c. From the File Menu, select Save.



2. Configuration of Galileo Desktop on a workstation that has Galileo SSL Software already installed.

Use these steps to Configure Galileo Desktop on a Galileo SSL workstation.

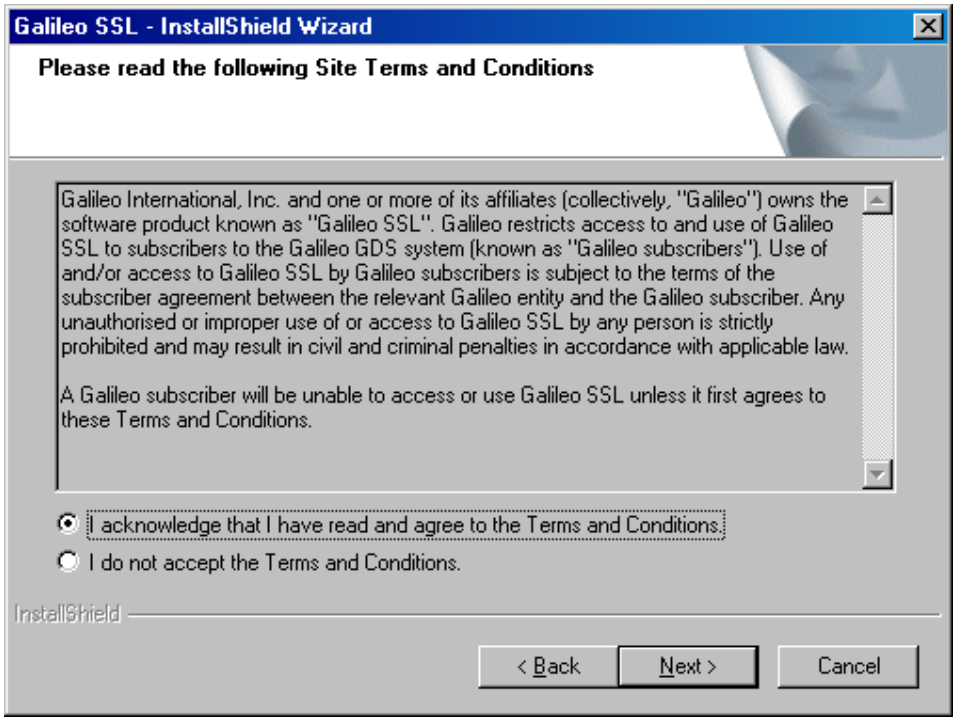
Close Galileo Desktop	
To verify that Galileo SSL is installed.	a. Access Control Panel b. Double Click Add/Remove Programs If the Galileo SSL Software has been installed it will display on the list as “Galileo SSL”
Access the Galileo TCP/IP configuration	a. In Control Panel, click on the Galileo TCP/IP Icon. b. Select your connection and click Edit. c. Verify your Client ID is correct d. Change the Primary and Secondary IPCS addresses to 127.0.0.1 e. Click the force download checkbox f. Click OK. 

Focalpoint 3.5

3. Installation over an existing working Focalpoint 3.5 workstation.

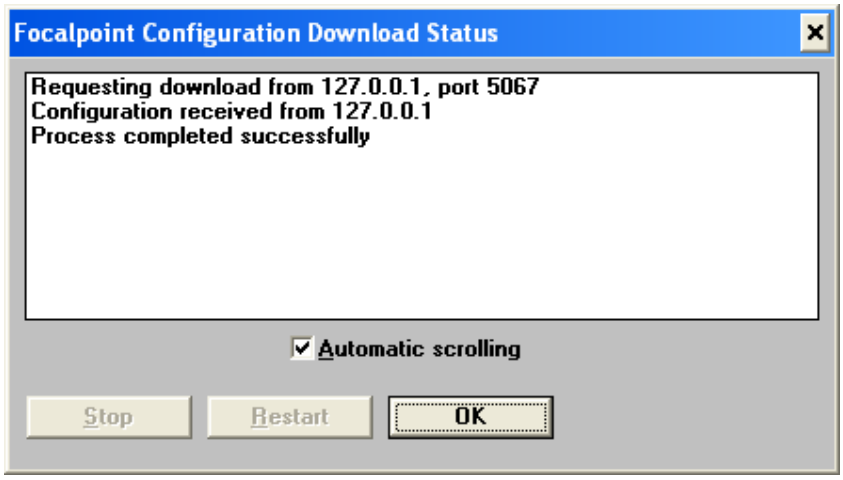
Use these steps to install Galileo SSL over an existing Focalpoint 3.5 workstation.

Close Focalpoint	
Double Click GALILEOSSL.EXE	
The installation will check for the presence of Microsoft.NET version 2.0. If this is already installed the installation will continue.	If Microsoft.NET version 2.0 is not found the download will start automatically. The download is approx 23 MB. d. After the download if prompted with a security message to run or not run, click Run. e. Follow the Microsoft.NET install prompts to install. f. After the install the SSL software installation will automatically continue.
The Welcome Screen displays.	Click Next.
The Terms and Conditions Screen displays.	Click I acknowledge to accept.



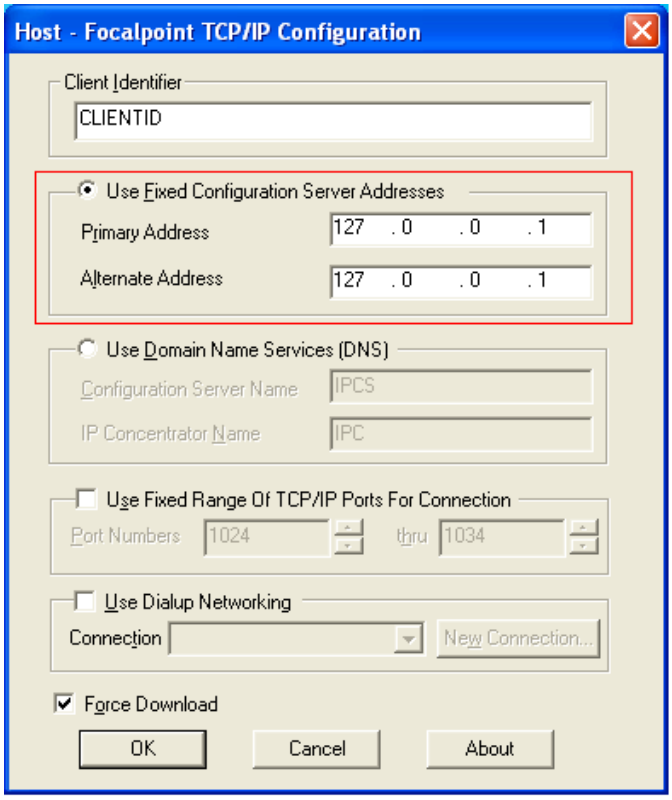
The Finish Screen displays.	Click Finish.

Launch Focalpoint, the Focalpoint Configuration Download Status will display.
Click OK when the Process completes successfully.



4. Configuration of Focalpoint 3.5 on a workstation that has Galileo SSL Software already installed.

Use these steps to Configure Focalpoint 3.5 on a Galileo SSL workstation.

Close Focalpoint	
To verify that Galileo SSL is installed.	a. Access Control Panel b. Double Click Add/Remove Programs If the Galileo SSL Software has been installed it will display on the list as “Galileo SSL”
Access the Galileo TCP/IP configuration	a. In Control Panel, click on the Galileo TCP/IP Icon. b. Select your connection and click Edit. c. Verify your Client ID is correct d. Change the Fixed Primary and Alternate Configuration Server Addresses to 127.0.0.1 e. Click the force download checkbox f. Click OK. 

Galileo Print Manager (GPM)

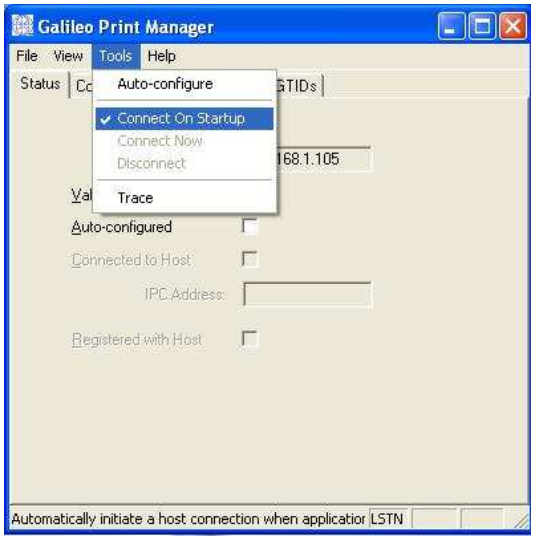
5. Configuration of Galileo Print Manager (or Focalpoint Print Manager) on a workstation that has Galileo SSL Software already installed.

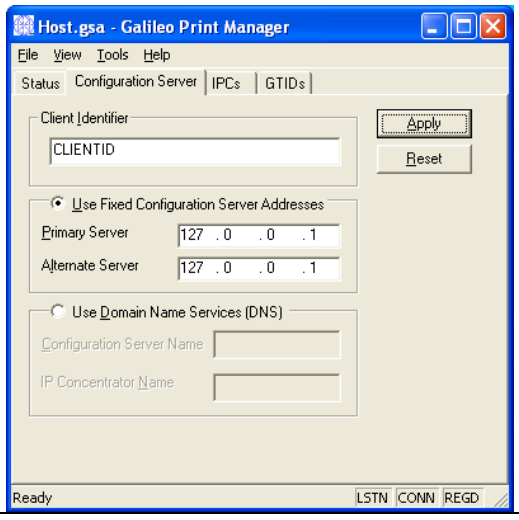
Use these steps to Configure Galileo Print Manager on a Galileo SSL workstation.

<table>
<tr><td>Close Galileo Print Manager</td><td></td></tr>
<tr><td>To verify that Galileo SSL is installed.</td><td>a. Access Control Panel
b. Double Click Add/Remove Programs
If the Galileo SSL Software has been installed it will display on the list as “Galileo SSL”</td></tr>
<tr><td>Configure GPM for SSL access:

1. Click Start, Programs, Galileo Print Manager, Print Manager
2. Click the Tools Menu.
3. Select “Connect on Startup” option.

Note: Galileo Print Manager does not automatically wake up so must be configured to “Connect on Startup”. Once connected GPM will always stay connected.

4. Click the Configuration Server Tab.
5. Type your GPM Client ID.
6. Change the Primary and Alternate Server addresses to 127.0.0.1
7. Click Apply.
8. From the File Menu, select Save.</td><td> 


</td></tr>
</table>

TS, Citrix and Thin Client Configuration

Install Desktop & SSL software, configure SSL using (Step 1)	Create users, create or modify **win.ini** for each user	Point **win.ini**'s to each users machine dir location (Step 2)	Modify **dat32com.ini** per user in machine folder (Step 3)	Set ForceDownload=1 in **dat32com.ini** file if required, test (Step 4)

Follow the instructions below if you require a single installation of the SSL Client.

Step 1

- **Modifiying the SSLClientservices.exe.config file in Notepad**

Navigate to C:\Program Files\Galileo\SSL
Open **SSLClientservices.exe.config**

```
appSettings>
    <add key="SSL Server Address" value="gdssl.galileo.com"/>
    <add key="SSL Server Port" value="443"/>
    <add key="Keepalive Seconds" value="120"/>
    <add key="Trace Level Override" value="Warning" />
    <add key="Server Mode" value="Enabled" />
    <add key="Server Mode Local IP Address" value="192.168.1.111" />
    <add key="SSL Server Address" value="sslfpemea.galileo.com" />
  </appSettings>
  <CustomTCPConnectionSettings>
    <!-- The format of entries in this section is:-
    <add key="unique-name" value="listen port, endpoint-server, endpoint-port,
userid"/> -->
  </CustomTCPConnectionSettings>
</configuration>
```

Add the following lines

- Server Mode Value must be set to = **Enabled**
- Server Mode Local IP Address Value = **IP of machine running the SSL Client**
- SSL Server Address Value = **SSL Client ID URL** (Diag1)

Enter one of the SSL Server Address Value from the table below

Diag1

DNS Name	IP Address	TCP Port
gdssl-atl.galileo.com	216.113.159.226	443
gdssl.galileo.com	216.113.159.225	443
sslfpemea.galileo.com	216.113.159.227	443

Step 2

Follow the instructions below to setup a unique SSL Client ID for each down line workstation

- Modify **Win.ini** to point the **Machine** directory to a unique location per user. The highlighted line indicates the change required, you may use a different mapping or keep it local. e.g. MACHINEDIR=C:\FOLDERNAME\USER\MACHINE

[Focalpoint]
SWDIR=C:\fp\swdir\
DATADIR=C:\fp\datadir\
MACHINEDIR=G:\ssl server\user1\machine\ (Note: MUST have training backslash!)
SingleFrame=VP
CommandWindow=True
LogonEnabled=2
GDVersion=2.1
Host=Galileo
Language=ENU
TestKey=
username=

Step 3

The Machine directory contains a file called **dat32com.ini**

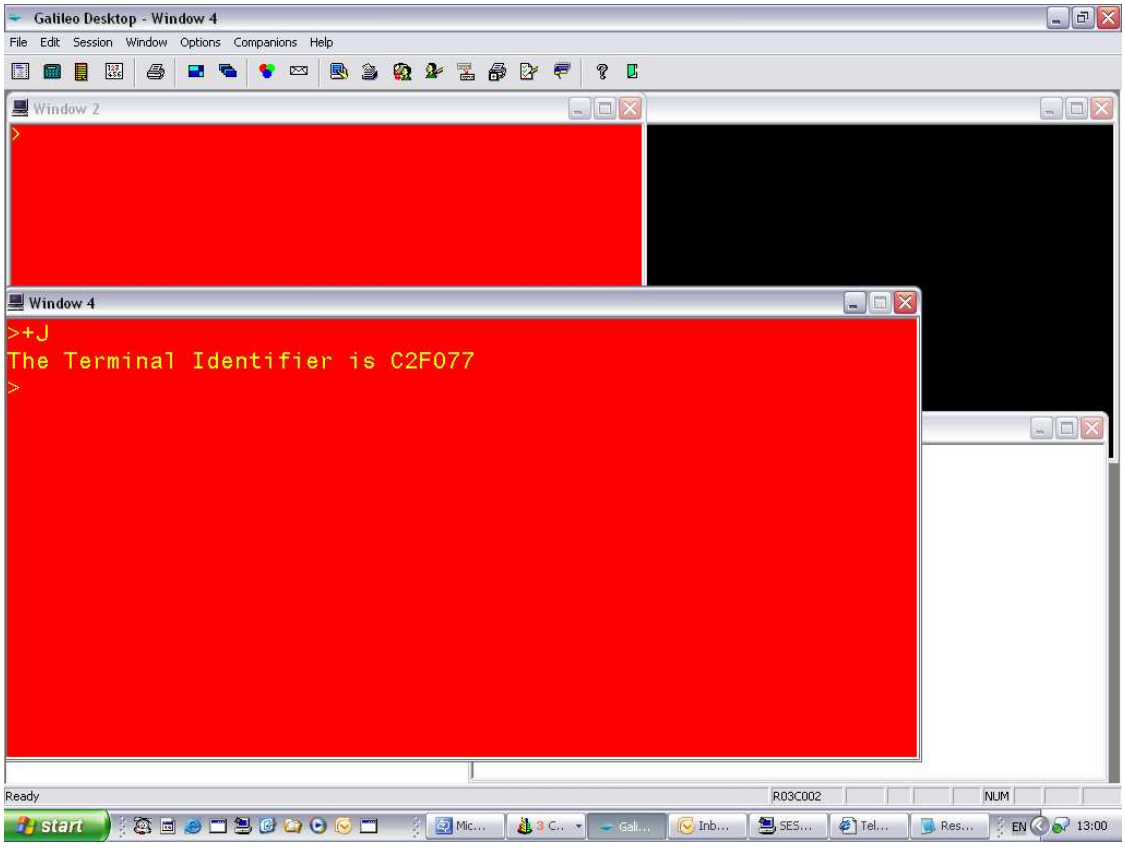
- Modify the \user\dat32com.ini file with the appropriate **Client ID**

[MyConnection]
type=HCM
SupportsSpecialCharacters=1
Client Identifier=Gxxxxxxx
ConfigServerName=localhost
IPCName=
PrimaryIPCS=SSL Server IP Address
SecondaryIPCS= SSL Server IP Address
DerivedFrom=
Use DNS=0
UsesSpecialCharacters=0
TerminalCharacterMapOut=TerminalCharacterMapOutHCM.txt
TerminalCharacterMapIn=TerminalCharacterMapInHCM.txt
StructuredCharacterMapOut=StructuredCharacterMapOutHCM.txt
StructuredCharacterMapIn=StructuredCharacterMapInHCM.txt
ForceDownload=1
[DefaultConnection]
type=HCM
SupportsSpecialCharacters=1
Client Identifier=Gxxxxxxx
ConfigServerName=localhost
IPCName=
PrimaryIPCS=SSL Server IP Address
SecondaryIPCS=SSL Server IP Address

Step 4

Check each downline workstation has a unique Client ID / GTID.

Enter **+J** in Focalpoint, this should display the Terminal GTID

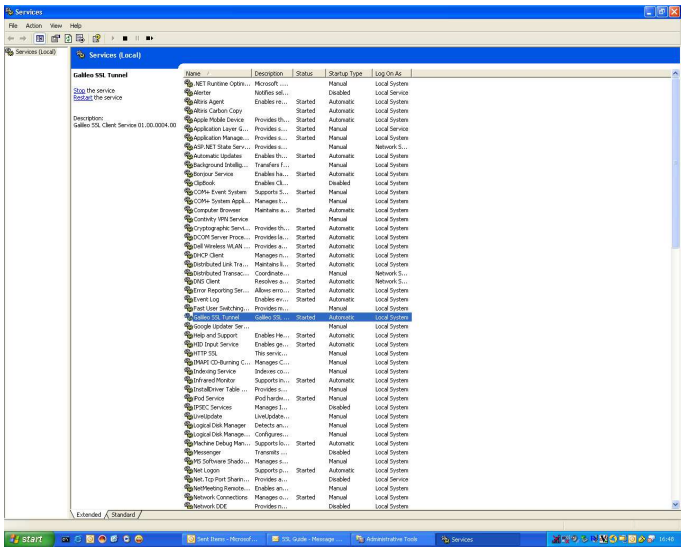


Resolving SSL connectivity issues

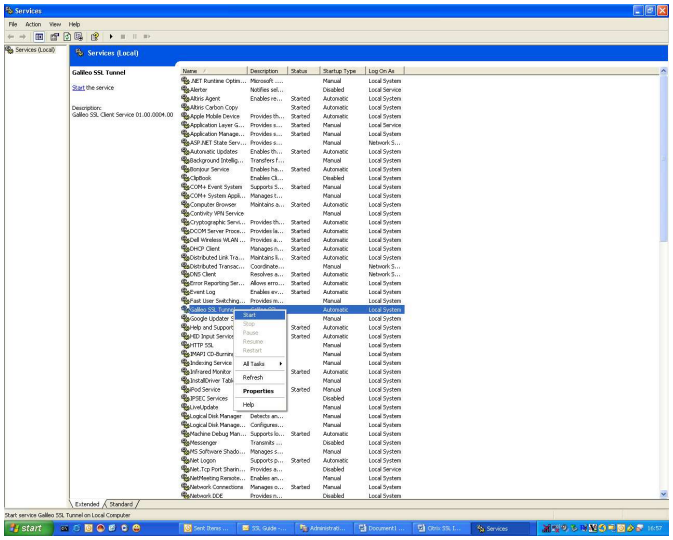
- **Check the SSL client service status is started**

Navigate to Control Panel / Administrative Tools / Services

Check the Galileo SSL Tunnel status is started.



If the SSL Tunnel status is blank, right click on the SSL service; from the drop down menu select **Start**.



- **Ping Test**

From the Command Prompt screen Ping the SSL DNS names

DNS Name	IP Address	TCP Port
gdssl-atl.galileo.com	216.113.159.226	443
gdssl.galileo.com	216.113.159.225	443
sslfpemea.galileo.com	216.113.159.227	443

- **Telnet Test**

Launch your telnet application.
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 note:

Could not open connection to the host, on port 443: Connect failed.
This note indicates there is a connectivity issue between the workstation and the Galileo SSL farm. This should be investigated by the agency network personnel, and is likely a firewall rule issue.

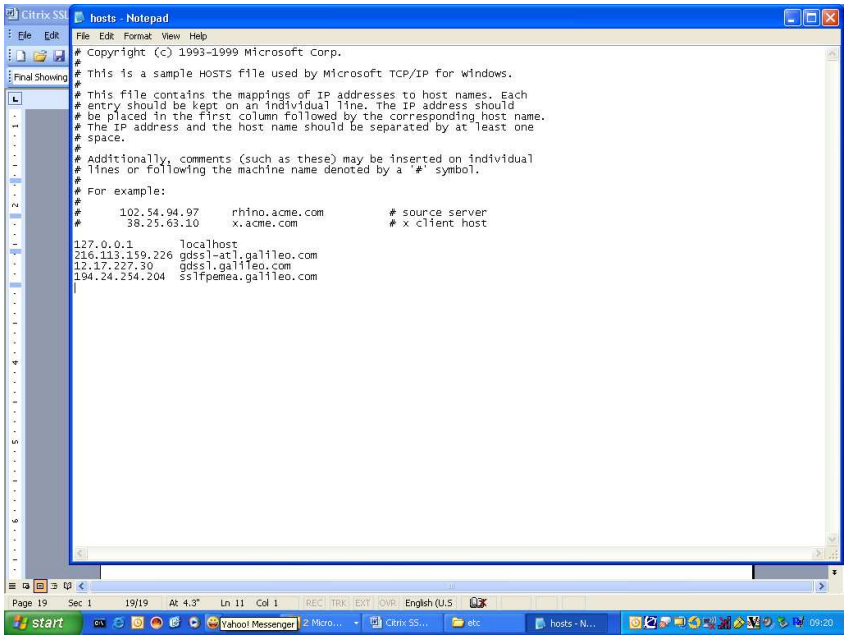
Ping the SSL DNS Names, check first that it resolves the name and returns an IP address, if not your issue is with DNS (host file) Does the ping reach its destination? If not it's a routing or firewall issue ASSUMING ICMP is open, try pinging google.com.

Host File

Navigate to C:\windows or winnt\system32\drivers\etc

Open the host file with Notepad

Add the TCP/IP Addresses and SSL DNS Names (as above) from Diag 1



- **Turn on the Logging in the SSL client.**

Navigate to C:\Program Files\Galileo\SSL

Open SSLClientService.exe.config in notepad.

Change value = "Warning" to value ="ALL" for

<add name="sourceSwitch" value="ALL"/>

<add key="Trace Level Override" value="ALL" />

Save the file Delete the existing Log (c:\ SSLClientService.log) Restart the service.

Check the log file.

You will see the service start and all the ports that are listening

e.g.

SSLClient Information: 114 : Galileo SSL Tunnel Client Service is starting...
ProcessId=760
DateTime=2008-05-15T09:39:23.5564450Z
SSLClient Information: 115 : Starting IPC traffic handler on port 2748
ProcessId=760
DateTime=2008-05-15T09:39:23.5691395Z

You will also see connection errors , such as:
SSLClient Error: 304 : ServerConnection.Connect() - SocketException thrown: A connection attempt failed because the connected party did not properly respond after a period of time, or established connection failed because connected host has failed to respond 12.17.227.30:443
ProcessId=760
DateTime=2008-05-15T09:40:07.7127985Z

Note the client throws the error "connected party did not properly respond" for a number of reasons one of which is that the fingerprint doesn't match! It is done this way at infosec's request so as not to help any "hackers".

To reset the fingerprint contact the Galileo Service Desk

Don't forget to turn Logging back off when you are done!

- **SSL Client ID and TCP/IP Address**

Navigate to the Control Panel and select the Galileo TCP/IP Icon

Check the SSL Client ID is correct

Check the Primary & Secondary TCP/IP addresses are correct – 127.0.0.1