GEORGIA SOFTWORKS

SuperSSL for Windows NT/XP/2000/2003+

User Manual

THIS PAGE INTENTIONALLY LEFT BLANK

GEORGIA SOFTWORKS

SuperSSL

Public Square
17 Hwy 9 South • PO Box 729
Dawsonville Georgia 30534
Telephone 706.265.1018 • Fax 706.265.1020
http://www.georgiasoftworks.com

User's Manual, Version 1.31, Oct 16, 2006

This Page Left Intentionally Blank

Table of Contents

Table of Figures

Table of Tables

Typographic Conventions

Italics:	are used to emphasize certain words, especially new terms or phrases when they are introduced.
Initial Caps Bold:	Words that appear in initial caps boldface represent menu options, buttons, icons or any object that you may click.
`Courier`:	This font represents anything you must type.
"<**enter**>"	This represents the enter key.

This Page Left Intentionally Blank

Features at a Glance

Very Secure Connection Alternative

Georgia SoftWorks SuperSSL
• Very Strong Encryption • Optionally require client software to present specific certificates • Import your own certificates for the SuperSSL • Configure Certificate Revocation Lists • Flexible port assignment. Use a different port than 992 • Optionally instruct SuperSSL not to expect the client to use Telnet • Specify SSL/TLS re-negotiations for increased security
Compatibility - Works GREAT with:
• Georgia SoftWorks (UTS) Telnet Server • Georgia SoftWorks Pocket 2002 PC Telnet Clients • Compatible with SSL Enabled Telnet Clients ex: Kermit 95 Cryptographic Version 2.0, Naurtech, etc.

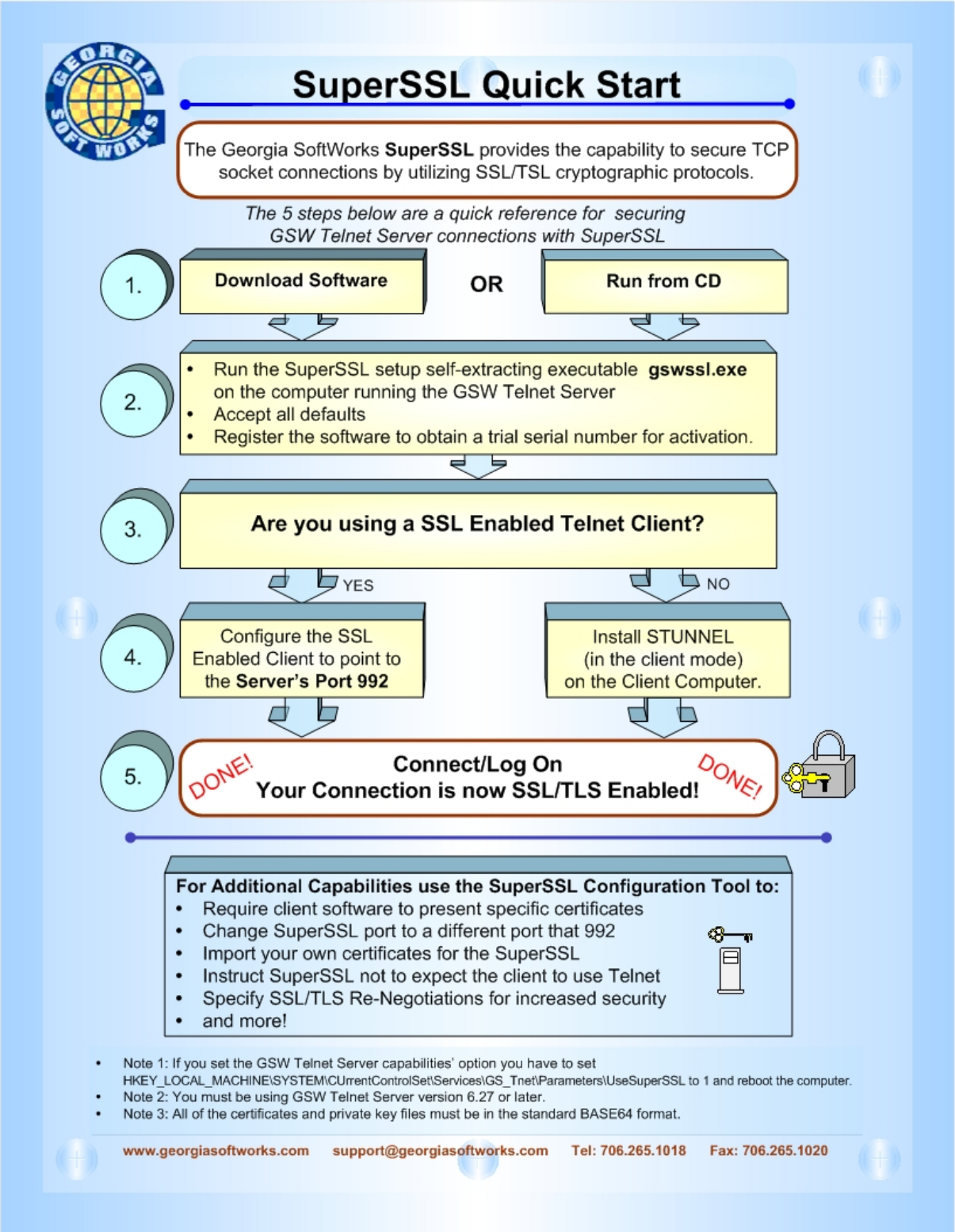

Figure 1: GSW SuperSSL Quickstart

Overview

The GSW SuperSSL is a SSL/TLS Tunneling Proxy and provides the capability to secure TCP socket connections by utilizing SSL/TLS cryptographic protocols.

Thank you for purchasing the Georgia SoftWorks SuperSSL for Windows NT/XP//2000/2003+.

Have confidence knowing that your connection is secure using one of the best cryptographic protocols available, in addition to potentially the strongest authentication mechanisms recognized.

GSW SuperSSL is a service which receives Secure Socket Layer (SSL) encrypted data (usually from client software), decrypts it, and sends the decrypted data to an arbitrary port on a local or remote machine (server). Additionally, SuperSSL receives data from the mentioned port, SSL encrypts it, and sends it back to the client.

SuperSSL is RFC2941 compliant. RFC2941 describes the SSL authentication option and provides a generic method for negotiation authentication type and mode for the telnet protocol.

SuperSSL works great with the GSW UTS (Telnet) Server but it is not limited to the GSW UTS Server. SuperSSL will work with third party telnet servers, yet is not limited to telnet. SuperSSL provides a secure transparent channel to which SSL-enabled clients may connect. The convenience of having a transparent channel allows nearly any protocol that can run over TCP to run over SuperSSL.

This extends SSL security to server software that is not natively SSL-enabled to communicate with a SSL-enabled client. Examples of server software includes but is not limited to POP3, HTTP and IMAP.

The SuperSSL is designed for use with the GSW UTS Telnet Server. You will be pleased with the innovative yet seamless integration between the GSW SuperSSL and the GSW Telnet Server. Together they facilitate secure telnet connectivity.

SSL is a secure and sophisticated protocol that requires prerequisite skills and knowledge by the administrator for proper configuration. This document does not attempt to explain the details of the SSL protocol but rather how to install and configure GSW SuperSSL by the knowledgeable administrator.

Installation

Installation of the GSW SuperSSL software is simple and quick. From Windows NT/XP/2000/2003+ perform the following:

1. Run the `gswssl.exe` self-extracting program.

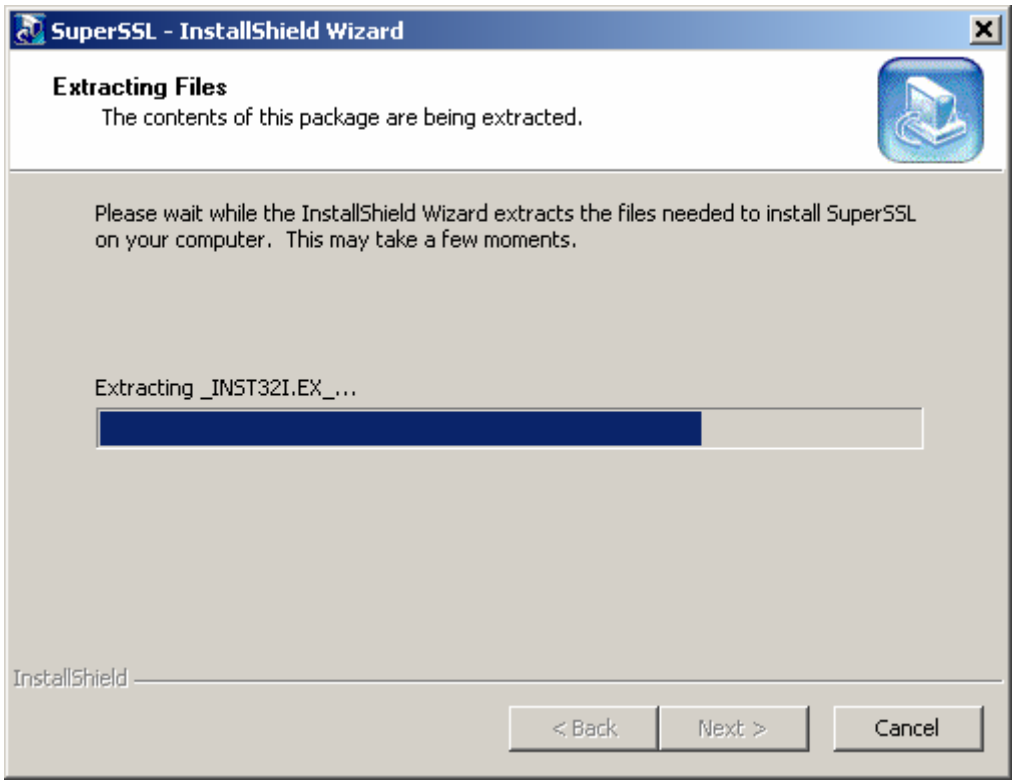

Figure 2 - Self extracting installation file gswssl.exe

2. Immediately following the self-extraction you will observe the launch of the setup program.

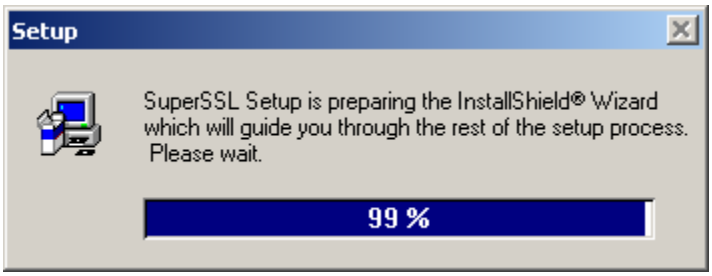

Figure 3: Initial Setup Screen

3. The Welcome screen of the setup program is displayed and you are reminded and urged to exit all Windows programs before continuing. You are also reminded that you must have administrative privileges to install this program. Click **Next.**

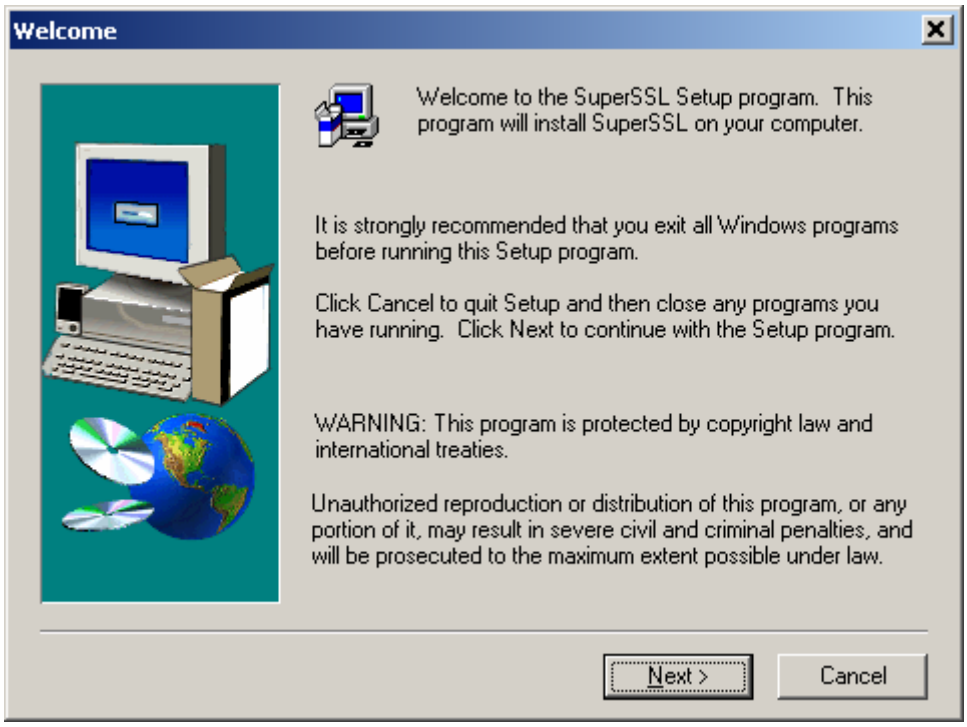

Figure 4: Installation Welcome Screen

4. A screen is displayed indicating the folder that the GSW SuperSSL will be installed. The default is:

   `C:\Program Files\Georgia SoftWorks\Georgia SoftWorks SuperSSL`

   Click **Next**.

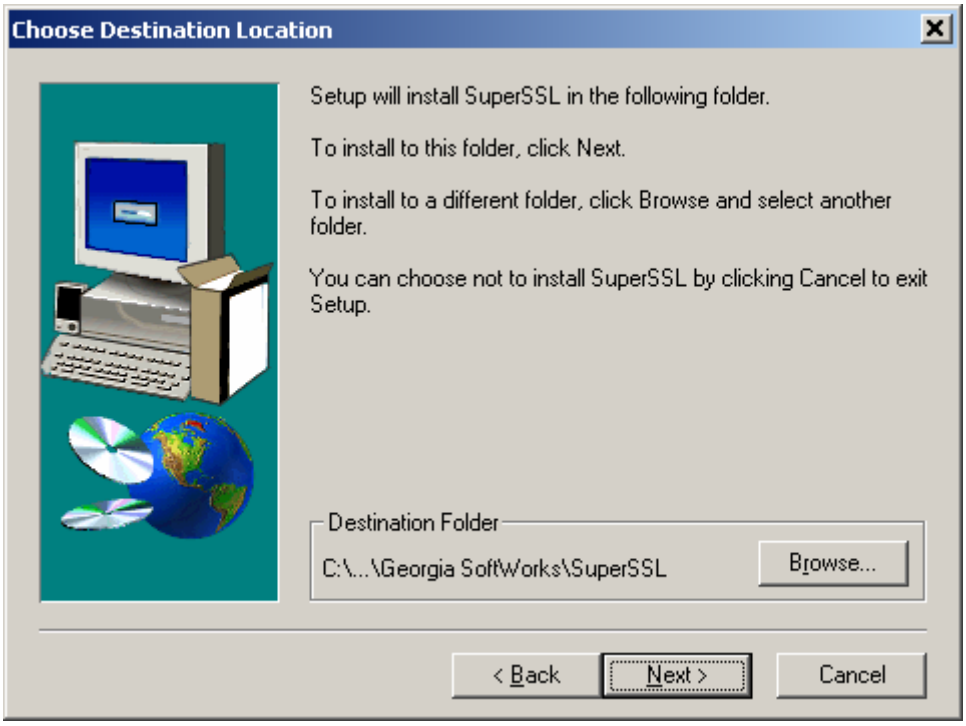

Figure 5: Installation - Choose Destination Folder

5. Select the Program Folder for the SuperSSL. Click **Next.**

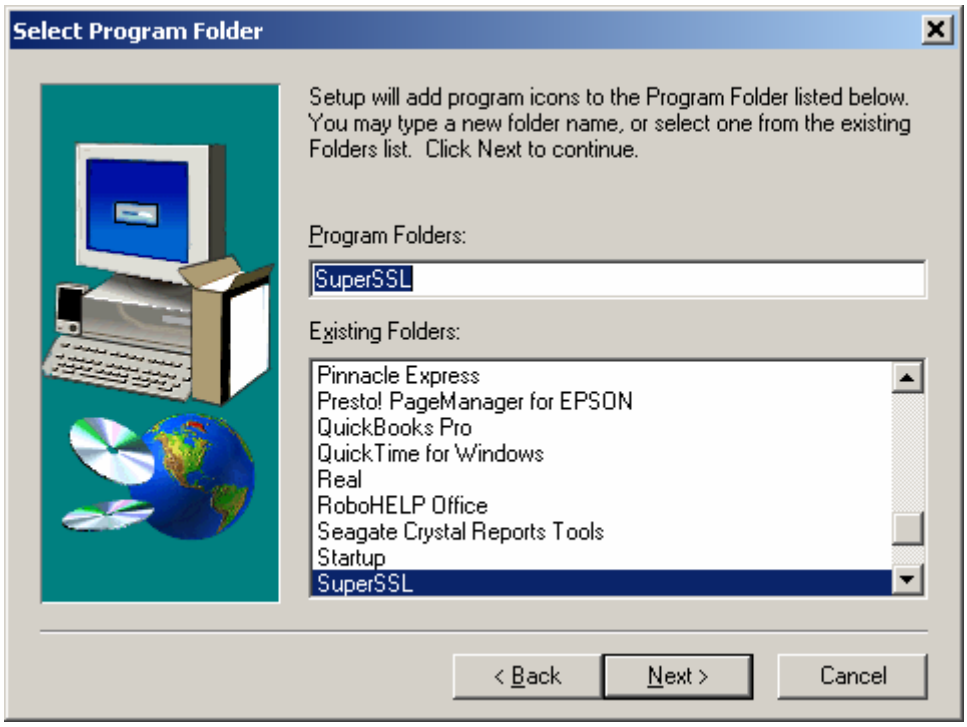

Figure 6: Installation - Select Program Folder

A few installation progress screens will be momentarily displayed.

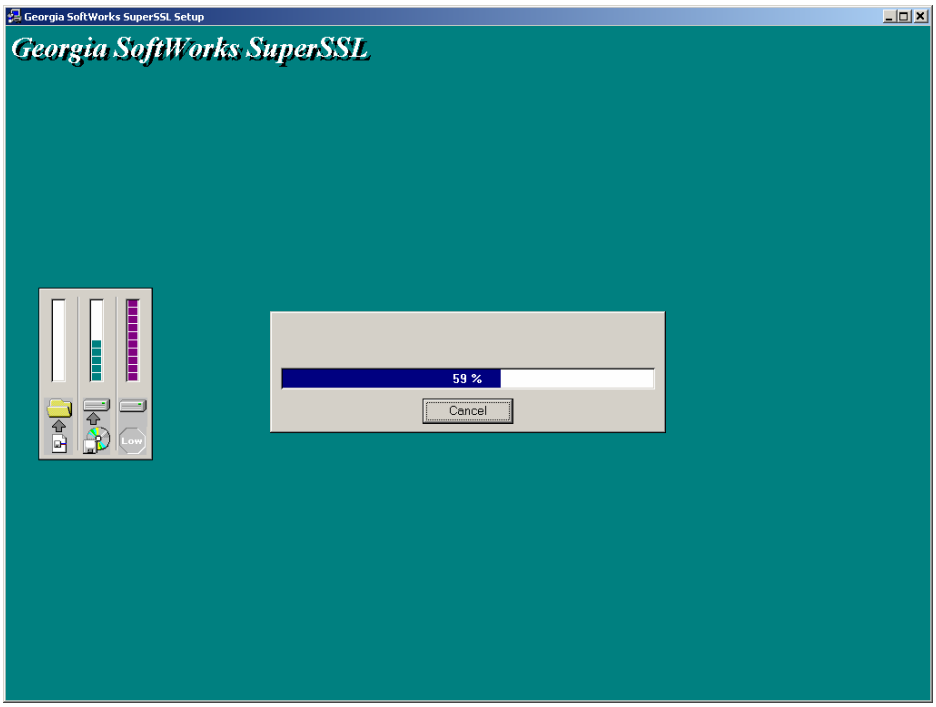

Figure 7: Installation - Progress Screen

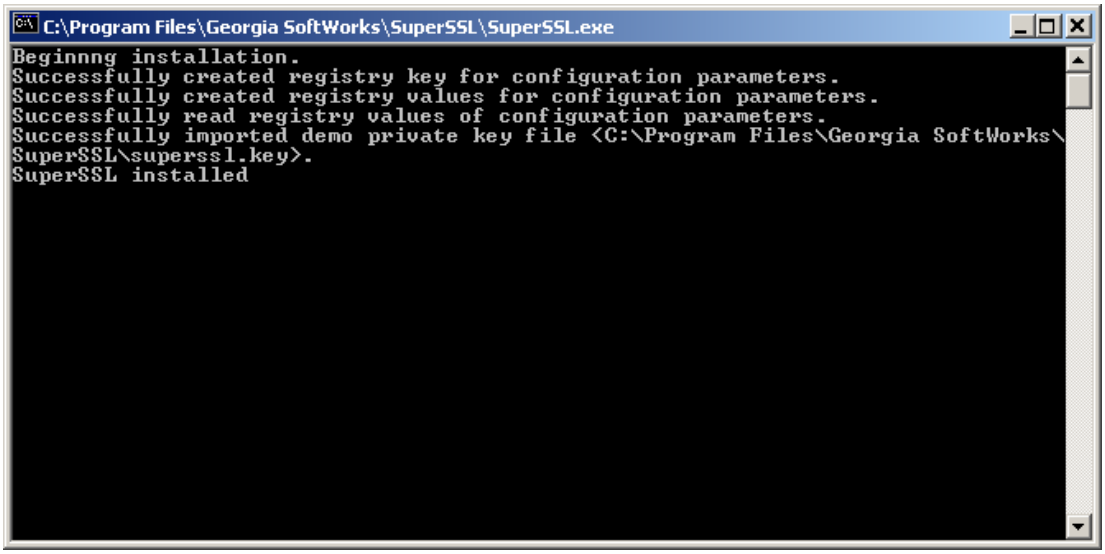

Figure 8: Installation - Progress Screen 2

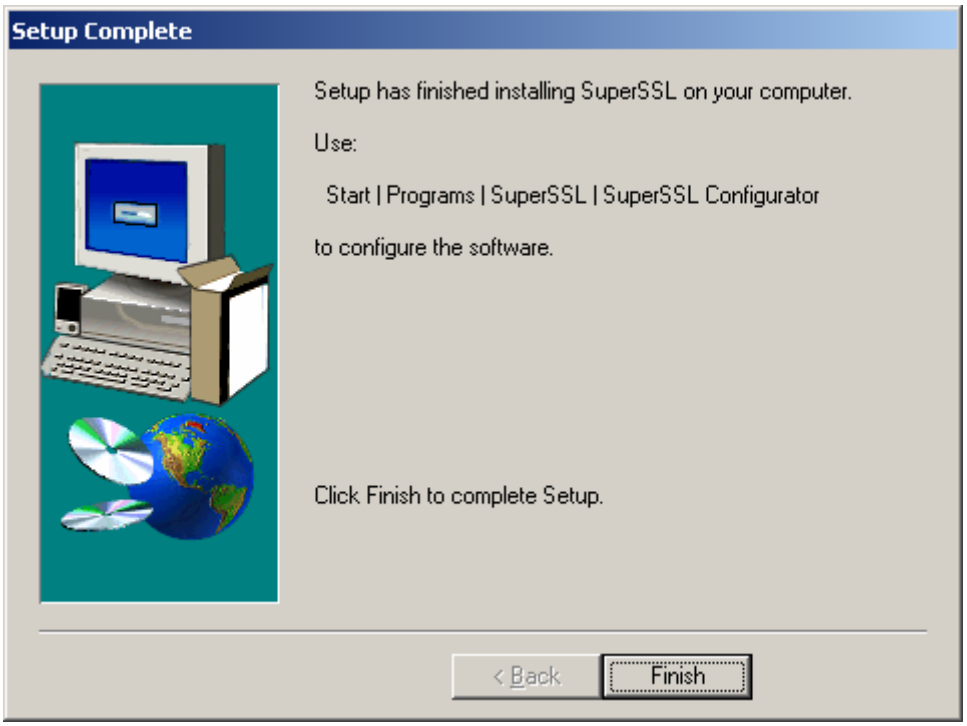

Figure 9: Installation - Setup Complete

6. Now the Setup is complete! *Now its time to register SuperSSL.*

Please view the `readme.txt` file as it may contain late breaking information about SuperSSL that has not yet made it into the user guide. Release notes are also contained in the `readme.txt` file.

Registration

The GSW SuperSSL is licensed for a single server. The license must be *activated* for the software to operate. To activate the license a valid *Serial Number* is required and is examined periodically by the SuperSSL software. The Serial Number also allows new versions to be downloaded and installed for the duration of your subscription plan.

Two methods exist to obtain a valid Serial Number.

1. Registration via Floating License (default method)
   The Serial Number is pre-programmed into a specific hardware key that came with your purchase. The hardware key connects to a USB or parallel port on the server. See page 12 for details on registration via the Floating License.

2. Registration via Software Serial Number
   This method exists for environments that do not support USB or parallel ports. In brief, this entails providing GSW with a machine specific Product ID. A Serial Number is generated based on the Product ID. This is usually performed via email, fax or telephone.

Floating License – Overview

The Georgia SoftWorks Floating License provides the flexibility to rapidly move the GSW SuperSSL from one machine to another. *If you are unable to use the Floating License - skip this section and go to the section on Registration via Software Serial Number on page 18.*

With the Floating License **NO** software registration is required for the SuperSSL to operate.

Common scenarios where the Floating License is useful include:

- **Laboratory usage in a development or test environment** where the SuperSSL is required for short periods of time on any particular machine and then moved to a new machine.
- **Backup Servers in a production environment**. Typically multiple SuperSSLs are purchased for backup systems, however with a Floating License the Hardware Key can be quickly moved from the primary machine to the backup without any other registration requirements.
- **Environments where a failed server must be replaced or rebuilt and immediately restored to operation with full SuperSSL capability**.

The Georgia SoftWorks floating license is a hardware key that can be ordered for a USB Port or a Parallel port.

Parallel Port Floating License	USB Floating License
 Figure 10: Floating License – Parallel Port The Parallel Port Floating License is a Pass Through allowing normal function of the port.	 Figure 11: Floating License - USB Port Not attached to a Server
The Parallel Port Floating License connects to a female parallel port on the server and does not impact functionality of the port for other uses. It acts pass though allowing normal connections to the other side of the key.	 USB LED Lights when Installed

Table 1: Floating Licenses - Parallel and USB Ports

SuperSSL will recognize the presence of the key and activate the software and the proper date for which free version upgrades can be obtained. It does not matter which parallel or USB port on the server the Hardware Key is installed, as all ports will be scanned for the installation of the key.

The Floating License currently is installed using the manufacturer (Aladdin) of the hardware key's setup program. It is described below. The name of the hardware key is HASP4 and you will see it displayed in the setup screens

Note: If you are using a *USB Floating License on a Windows NT system* run the file `aksnt4usb.exe` prior to the following steps.

1. Install the GSW SuperSSL software as described on page 5 (if it is not already installed).
2. Copy the files from the Floating License folder (hardkey) on the provided CD to the hard drive on your server.
3. Run the `hinstall.exe` program and follow the installation instructions.

   You will first see the Aladdin Splash Screen. The Aladdin Splash Screen will display for about 5 seconds.

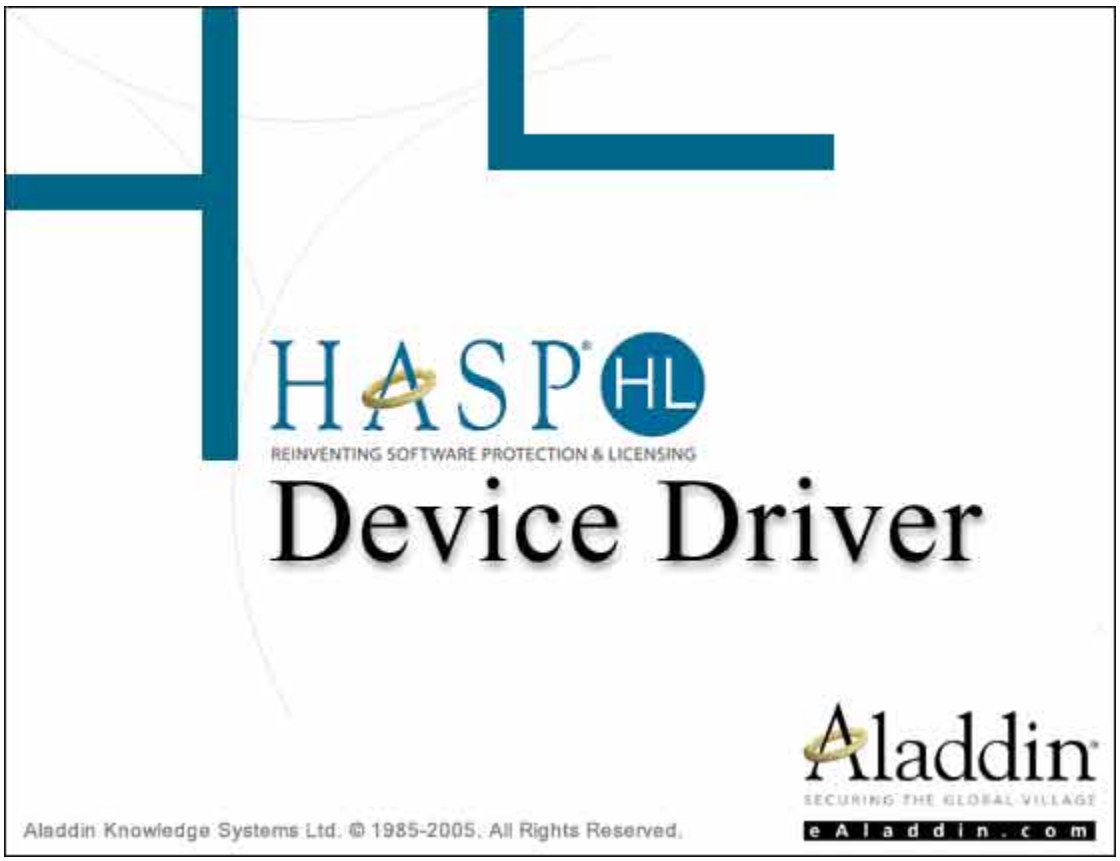

Figure 12: Floating License – HW Key Initial Splash Screen

4. The next screen displayed is the Aladdin Welcome Screen.

Figure 13: Floating License – Welcome Screen

As the dialog indicates, if you have any running application please close them now. **Click Next**.

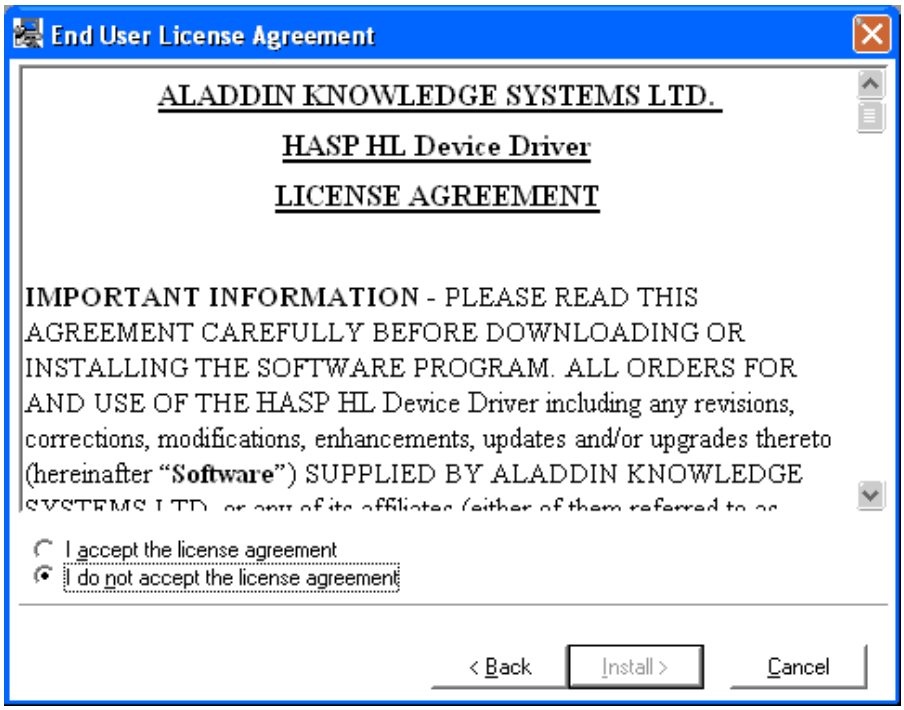

Figure 14: Floating License - License Agreement

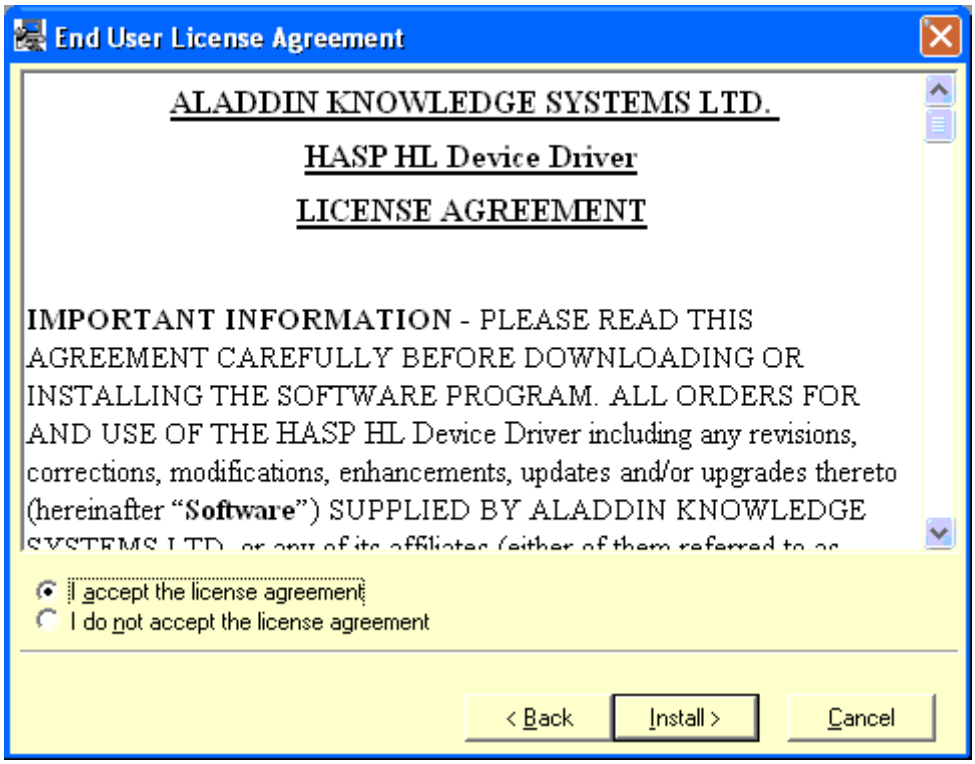

Figure 15: Floating License - Accept License Agreement

Read the license agreement and select "I accept the license agreement", and then **Click Install**.

5. An installation status progress meter is quickly displayed and when the status gathered is completed the screen below is displayed.

Figure 16: Floating License - HW Key - Installation Status

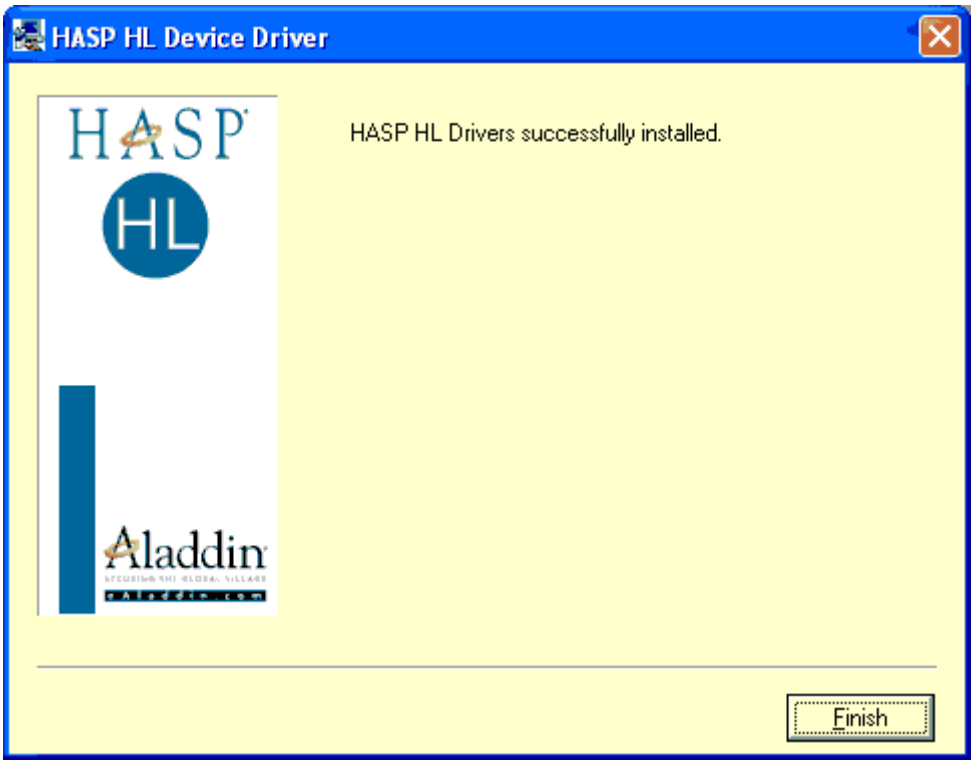

Figure 17: Floating License Drivers Successful Installation

6. When the installation of the Aladdin Hasp Device driver is complete the screen below is displayed. **Click Finish**.

7. Plug the hardware key onto the parallel or USB port on the server.

   NOTE: On some systems you may have to reboot the server after installation. If the Floating License is not recognized (by the GSW SuperSSL) after installing the driver, please reboot the server.

Uninstall Floating License – (Hardware Key)

In the event that you need to uninstall the Floating License (Aladdin HaspHL) please use the Windows Control Panel Add/Remove Programs administrative utilities.

NOTE: Removing or uninstalling the Floating License will disable the GSW SuperSSL Software.

Registration via Software Serial Number

To run the GSW SuperSSL you must first register the software. (*This registration is **NOT** required if you installed the Floating License. Page 11*) Registration via Software Serial Number entails just a few steps that involve obtaining the Product ID and providing this Identification to Georgia SoftWorks so a Serial Number can be generated. - **NOTE:** Read System Signature chapter at the end of manual.

How to Register the Software

To run the registration software -

- Select the *Start* button on the task bar; select *Programs*, then *Georgia SoftWorks SuperSSL* and then *Registration.*

Note: The Product Information *Name* and *Version* must contain valid data or it will not generate a correct Product ID.

The registration screen is displayed. The Registration software automatically fills in the Product Information fields as show in the figure below. Complete the Customer Information fields as shown in the figure below.

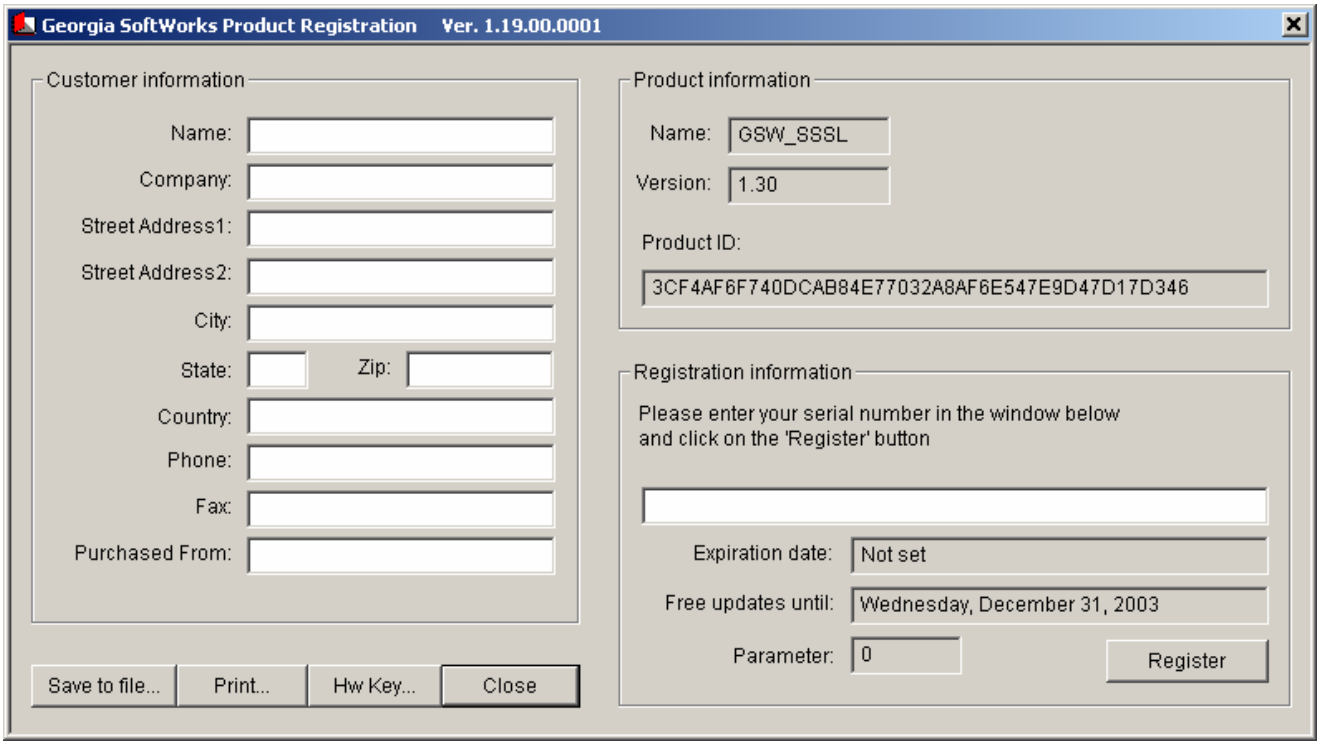

Figure 18: Registration with Serial Number - Initial Screen

1. Please complete the *Customer Information*, the *Purchased From* and the *Sessions Requested* fields in the Registration Screen. Enter the name of the software that will be your primary application to use with Telnet/SSH2 in the *Application software* field. Examples could be SAP, QAD, Catalyst, System Administration, etc

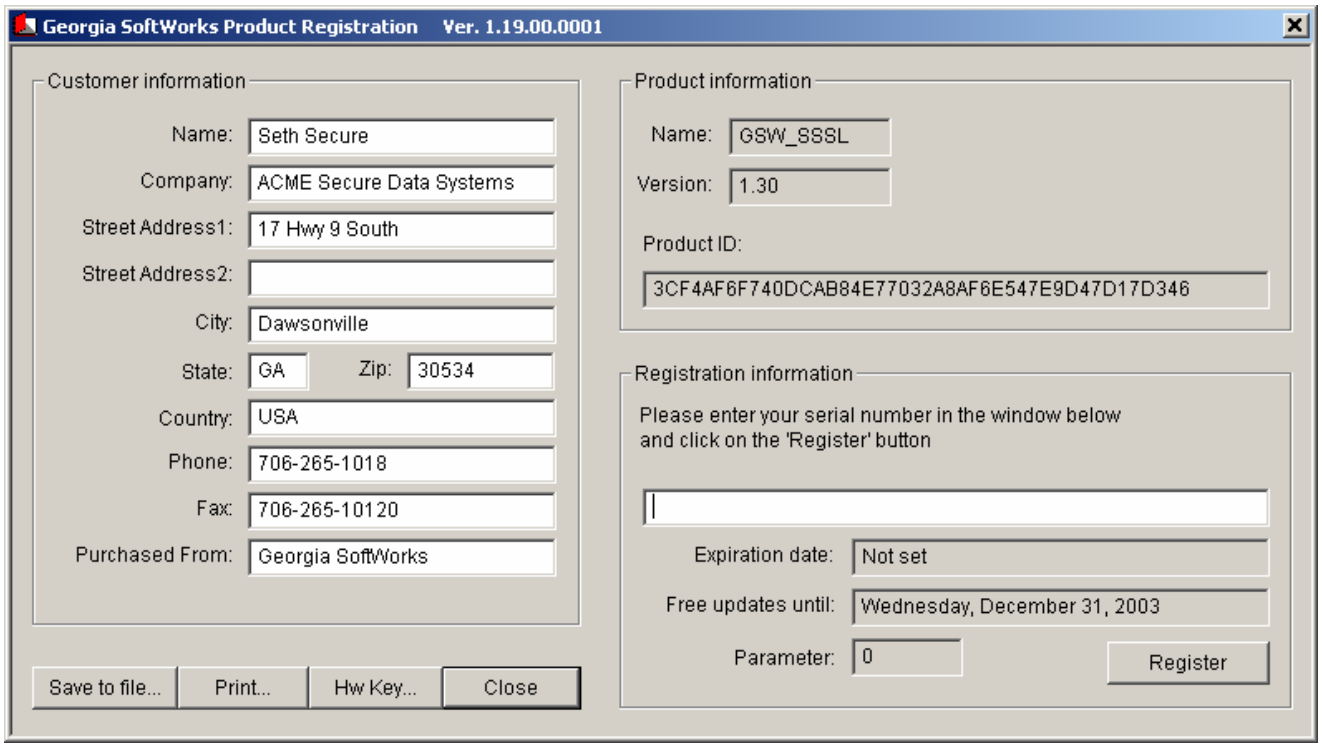

Figure 19: Registration - User Information

2. The registration information must be provided to Georgia SoftWorks to obtain the Serial Number. Several methods are available for your convenience.

    a. Save the information to a file and email it to Georgia SoftWorks - *Preferred method*.

    OR

    b. Print the information and Fax it to Georgia SoftWorks

    Please save (using the **Save to file** button on the registration screen) this information to a file and email to Georgia SoftWorks registration@georgiasoftworks.com

    OR

    Please print (using the **Print** button on the registration screen) this information and fax to Georgia SoftWorks - 706.265.1020

Once Georgia SoftWorks receives the information, we can generate a Serial Number on demand[1]. We will reply back via Fax or email. You may close the registration program at this time.

3. When the Serial Number is provided Run the Registration Program again and enter the Serial Number. The easiest method to get the serial number is to highlight the returned Serial Number and copy (ctrl-c). Then position the mouse in the Serial Number field in the Registration Information box and paste (ctrl-v).

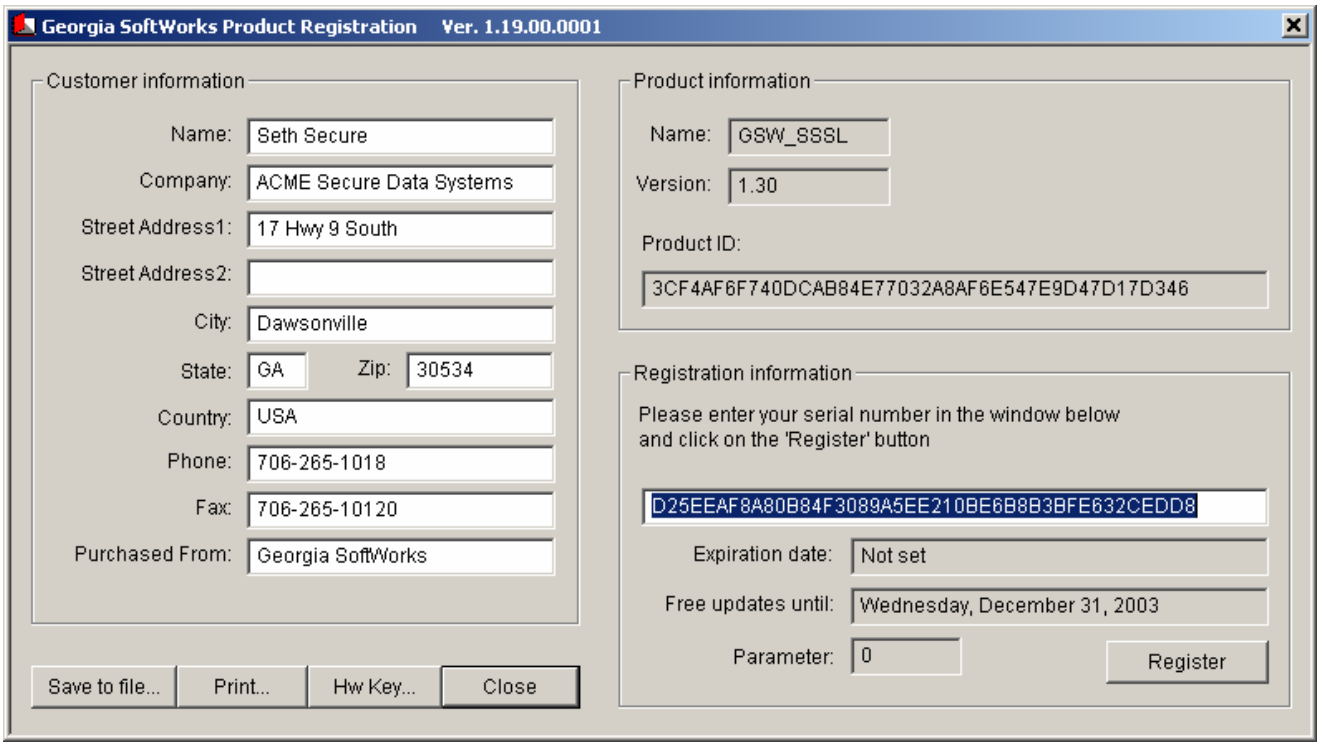

Figure 20: Registration - Serial Number Applied

4. **Click Register**.

Figure 21: Registration Successful Screen

Now the software is registered. You may now run the Georgia SoftWorks SuperSSL. Note that you will be able to obtain Free Updates until the date specified.

IMPORTANT: READ SYSTEM SIGNATURE CHAPTER AT END OF MANUAL (PAGE 35).

[1] This is during normal business hours Eastern Standard Time. Emails registrations are checked periodically on weekends.

Configuration

Once the GSW SuperSSL is installed and registered it is ready to use. However, you may want to take advantage of the flexibility or increase security by using the SuperSSL configuration utility. You will need to restart the SuperSSL service after any configuration values described in this section are modified.

General Tab

Open the SuperSSL Configuration utility. Your screen will be similar to the figure below.

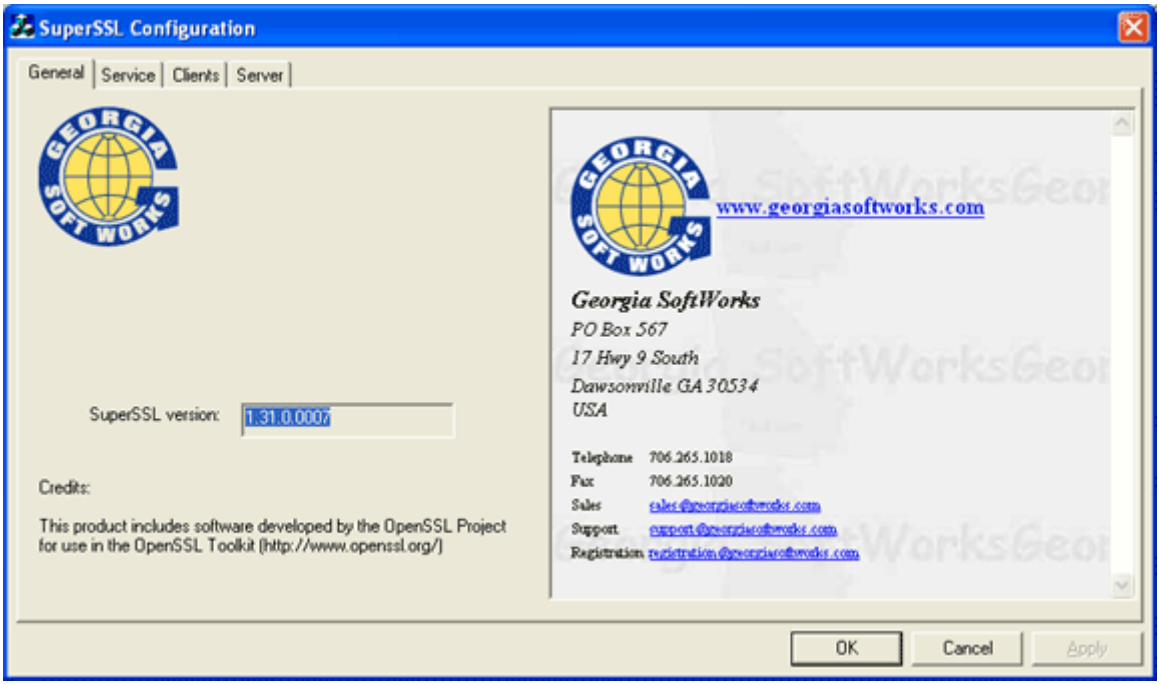

Figure 22: Configuration - General Tab

The General Tab provides information such as the SuperSSL version that you have installed as well as contact information for Georgia SoftWorks. You can initiate an email to sales, support or registration from the general tab as well as visit the Georgia SoftWorks web site. You should visit the GSW web site for new versions of SuperSSL that you can download free for the duration of your subscription.

Service Tab

The Service Tab provides configuration associated with the SuperSSL service. The configuration areas associated with the service are:

- TCP/IP Port Number – Specifies the Port Number to use for SuperSSL
- SSL Renegotiate – Enables and configures or Disables SSL renegotiation capability
- Identity – Specifies the path to the GSW Certificate and private key.

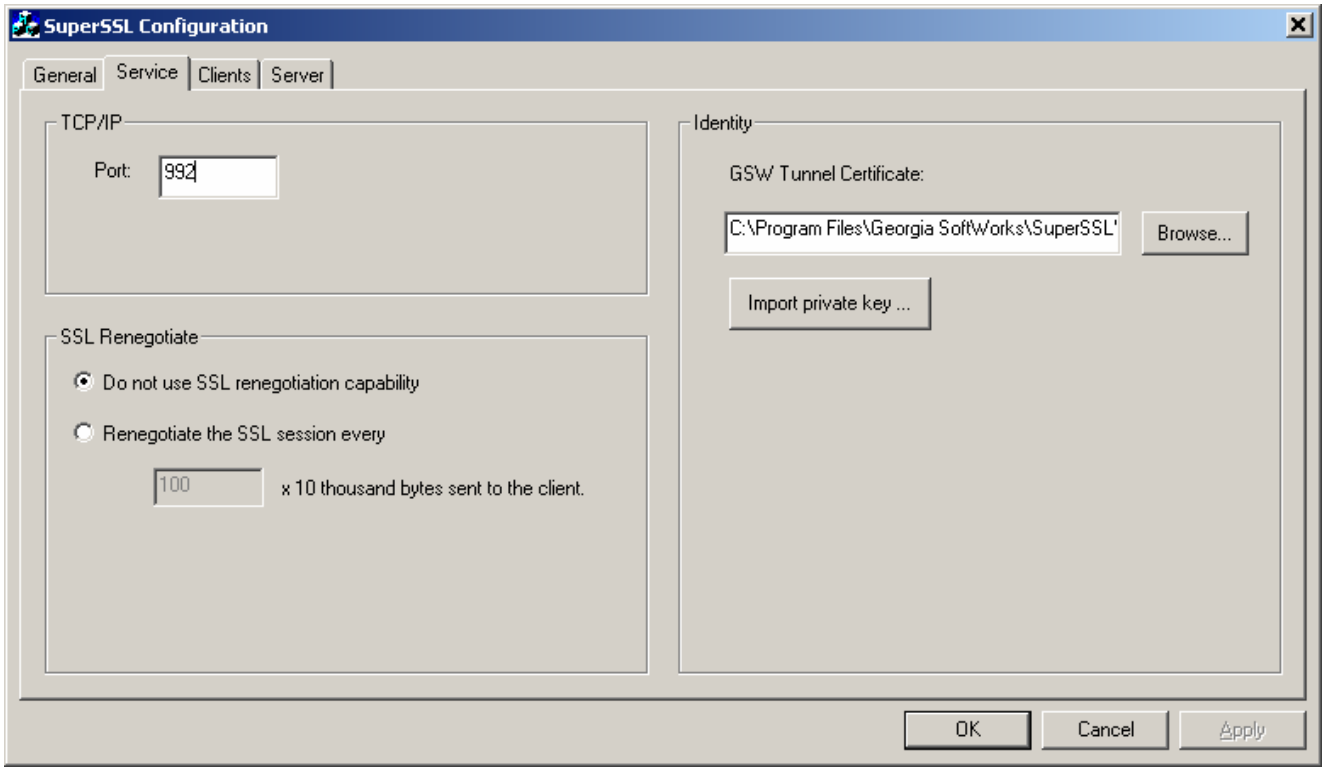

Figure 23: Configuration – Service Tab

TCP/IP Port

The TCP/IP Port number specifies the port on which SuperSSL will listen . Typically the default port for SSL is 443. The default port for GSW SuperSSL is port 992. However you may specify any port[2]. This is the standard port number for SSL telnet assigned by the Internet Assigned Number Authority (IANA).

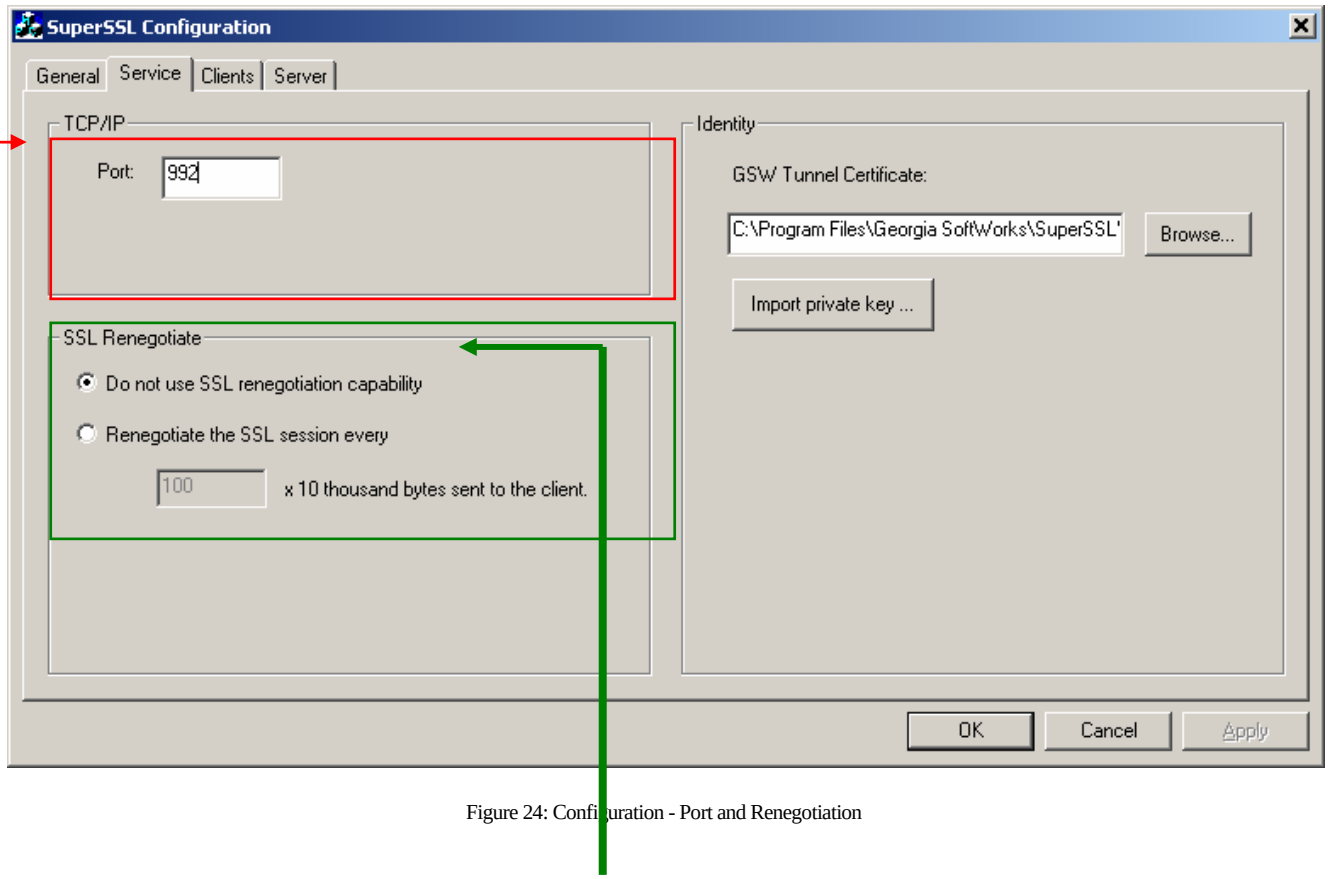

Figure 24: Configuration - Port and Renegotiation

SSL Renegotiate

The SSL Renegotiate configuration specifies if the server is allowed to re-negotiate the set of session security parameters. The renegotiation can be configured to re-negotiate periodically based on the number of bytes sent to the client.

[2] Of course, you should take care not to create a conflict on the port.

The SSL Handshake Protocol allows the server and client to authenticate each other and to negotiate an encryption algorithm and cryptographic keys; before the application protocol transmits or receives its first byte of data, or periodically during the session.

SuperSSL Identity

Server Authentication is performed using the GSW Certificate and the corresponding private key. GSW SuperSSL comes with a default demo certificate to allow you to get up and running fast, however you should obtain an official certificate (examples: Thawte, Verisign, and Entrust) so your client software can authenticate the server without having to install additional certificates on the client. If you have the expertise you may also generate your own certificate. Windows Servers come with tools for this purpose. The demo GSW Certificate is automatically installed in a default location – C:\Program Files\Georgia SoftWorks\SuperSSL\superssl.pem.

You can specify the location of your Server Certificate by clicking the Browse button.

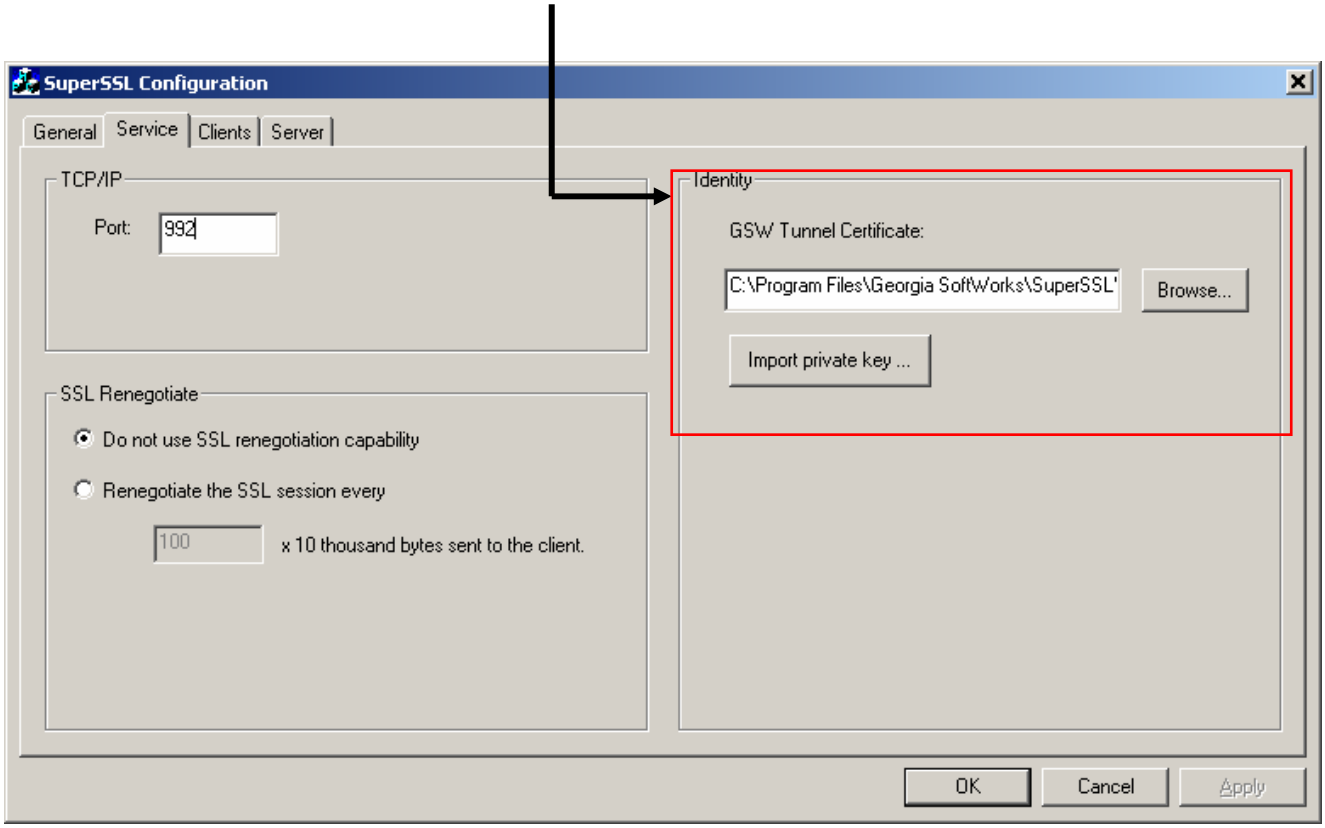

Figure 25: Configuration – GSW Identity

Private Key

Additionally the private key associated with the server certificate must be imported. Click on the Import Private Key button and you will get prompted for the location of the private key file and the password associated with it.

The location of the private key file is specified by clicking on the browse button.

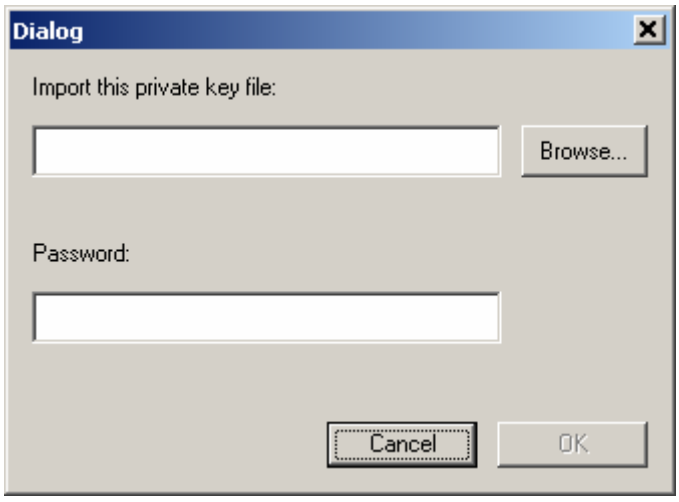

Figure 26: GSW Certificate - Import Private Key

The Password associated with the private key file is entered next.

Clients Tab

The Client Tab provides configuration associated with the Clients that connect to the server. The configuration areas associated with the clients are:

- Security Policy – Client Certificate Requirements and folder locations
- Certificate Revocation List (CRL) – Enable/Disable and file location of CRL
- Trusted Certificate Authorities (CAs) – Enable/Disable and file Location
  - CA Hash Directory – Enable/Disable and folder locations

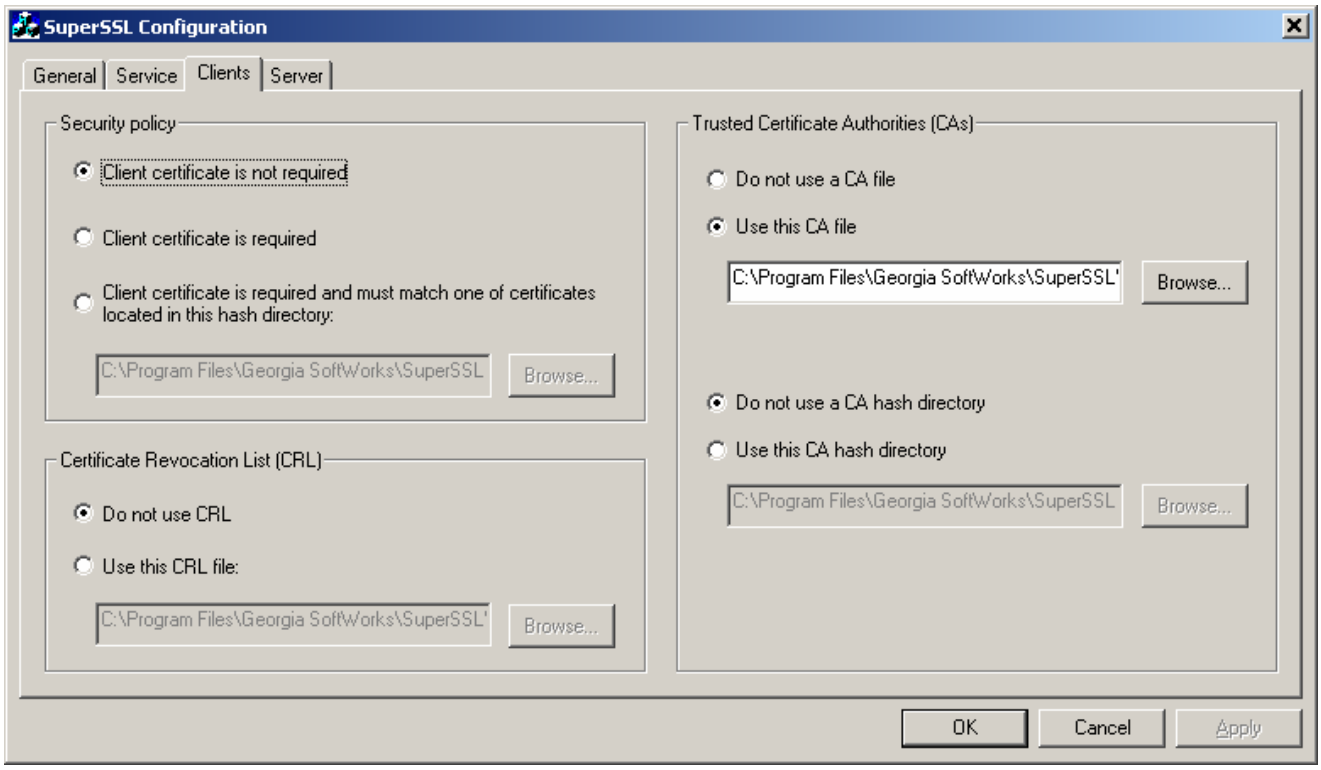

Figure 27: Configuration - Clients Tab

Security Policy

By default the client certificate is not required. This is how SSL security works with browsers by default. You connect to sites but you are not required to have your own certificate.

Client certificates allow the creation of usage scenarios where the server can identify (accepts or rejects) a client connection based on the identity embedded in the client certificate. Having or not having a client certificate does not change the cryptographic security of the protocol.

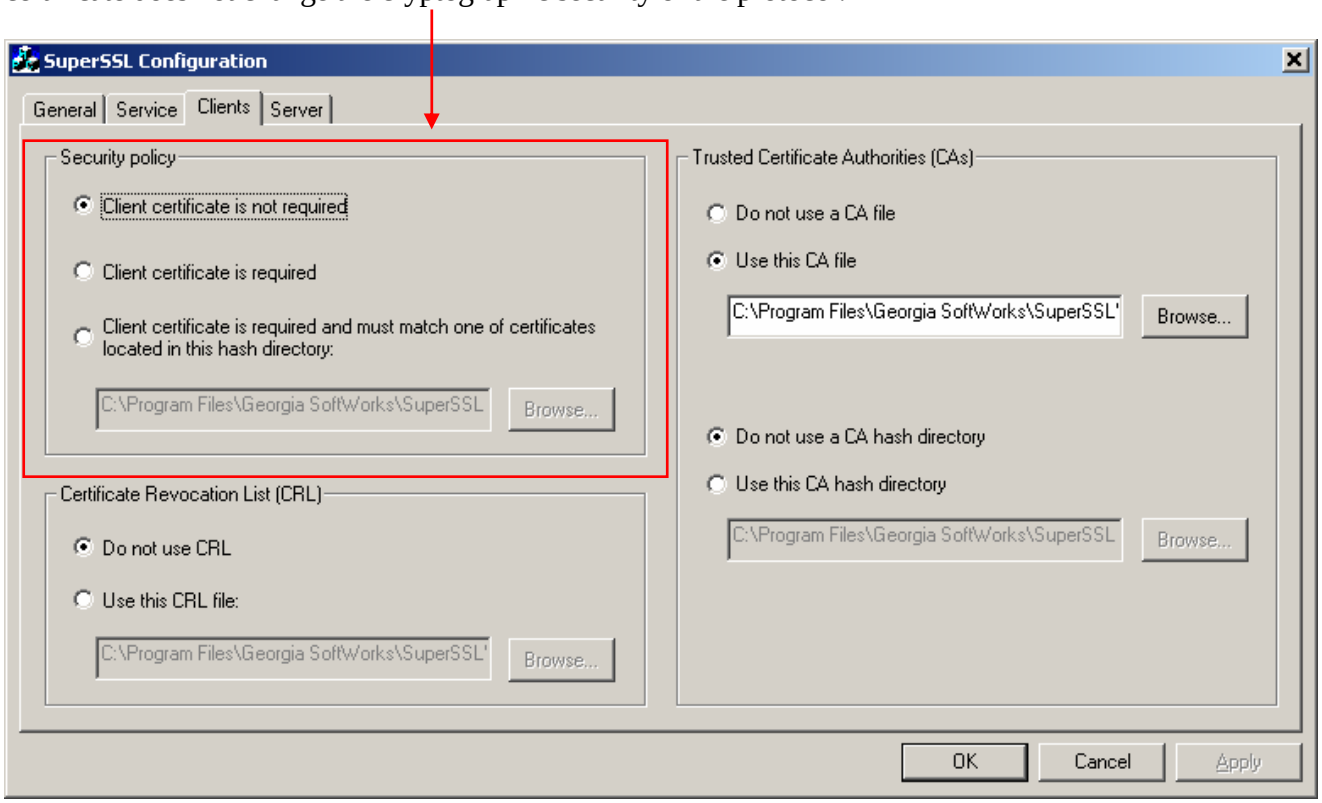

Figure 28: Configuration - Clients Tab - Security Policy

Additional security may be added by requiring identification of the client by the server. The options available allow the administrator to specify that the client must have a certificate OR the client must have a certificate and it must match one of the certificates know to the server.

Selecting the option “Client certificate is required” requires that the Client have a certificate.

You can also specify that the client certificate is required and it must match one or more certificates stored in a hash directory. Selecting the corresponding option enables the directory navigation button, allowing you to specify the hash directory that contains the certificates that the client certificate must match.

Certificate Revocation List

Specify the certificate revocation list.

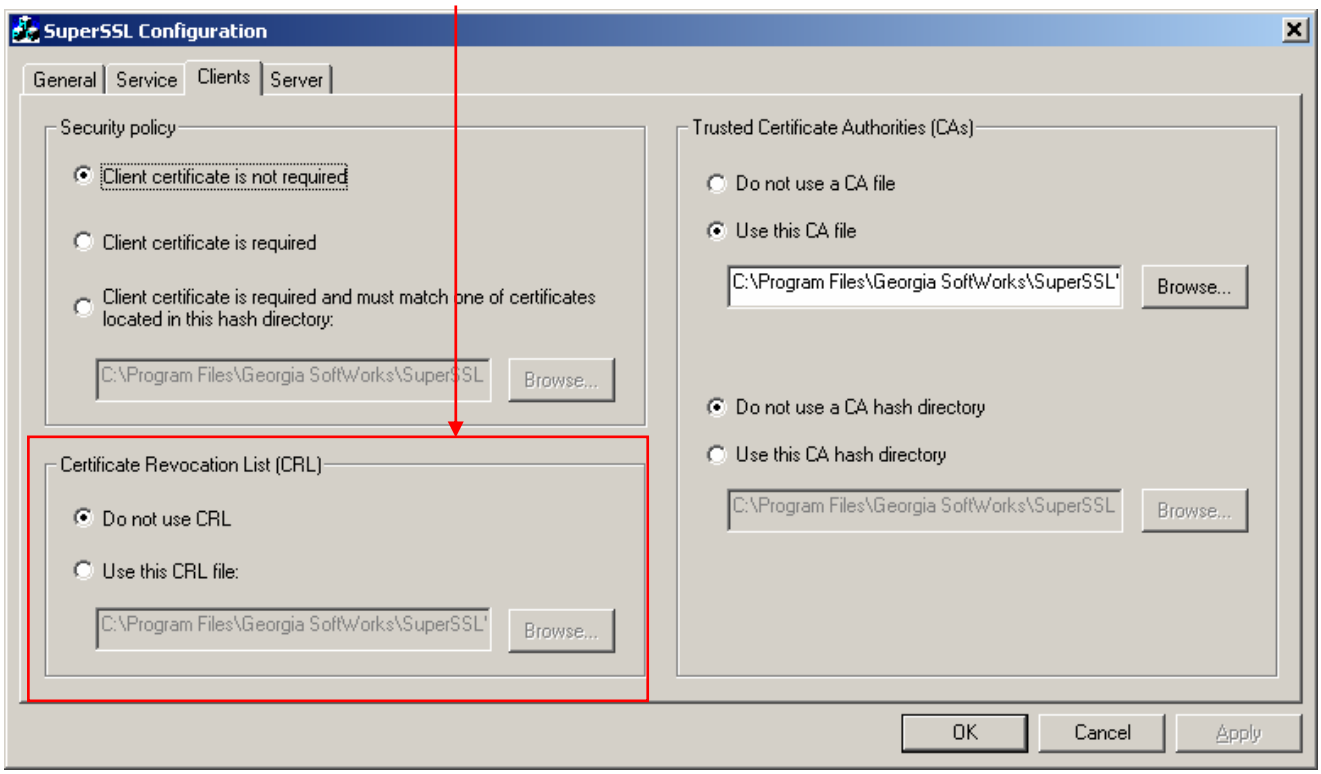

Figure 29: Configuration - Clients Tab - Certificate Revocation List

The Certificate Revocation List is a list of previously issued certificates that the authority no longer considers valid.

To configure the Certificate Revocation List (CRL), select the option

"Use this CRL file:"

And browse to and select the file that contains the CRL.

Click "OK"

Trusted Certificate Authorities (CAs)

When looking up CA certificates, SuperSSL will first search the certificates in CA file, then those in CA hash directory. Certificate matching is done based on the subject name, the key identifier (if present), and the serial number as taken from the certificate to be verified.

If these data do not match, the next certificate will be tried. If a first certificate matching the parameters is found, the verification process will be performed; no other certificates for the same parameters will be searched in case of failure.

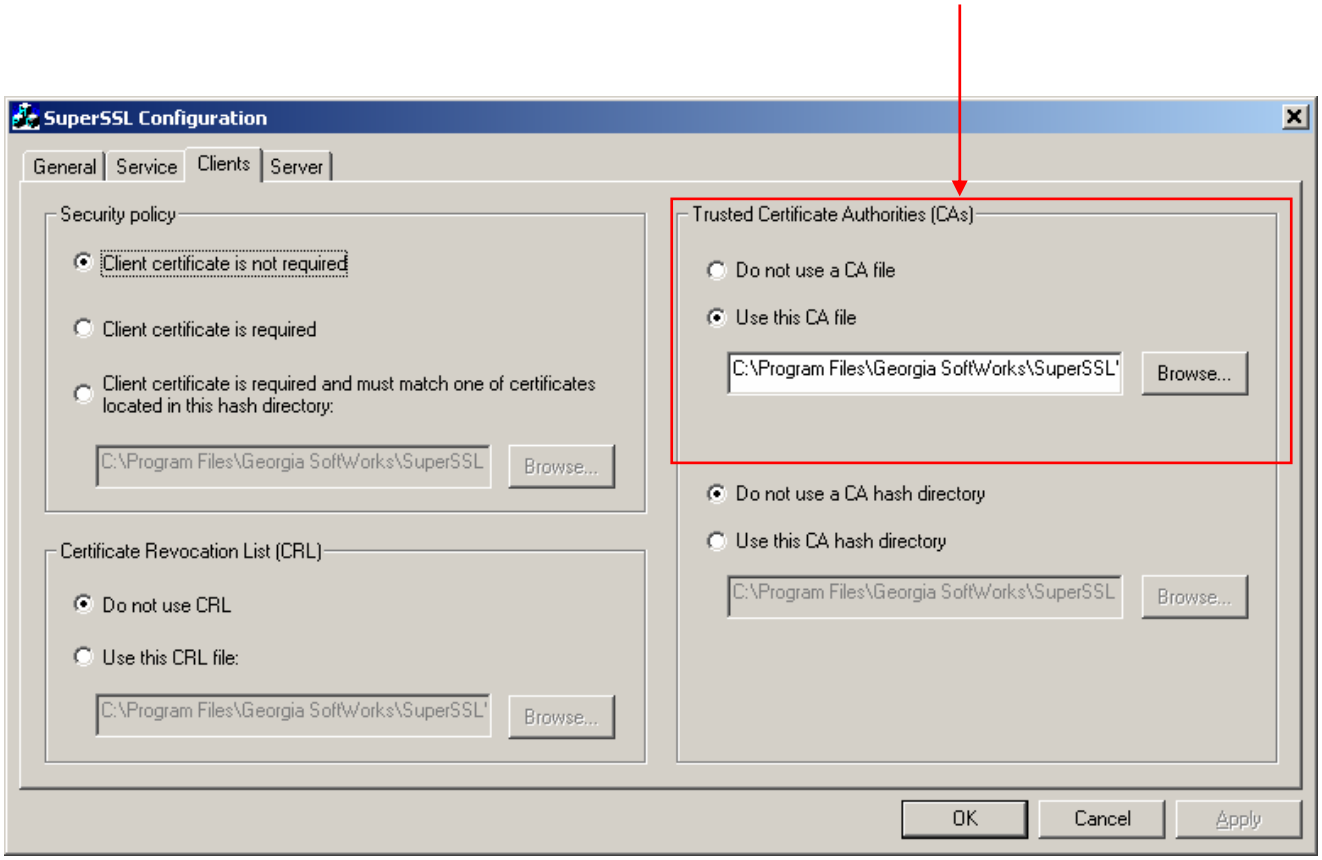

Figure 30: Configuration - Clients Tab - Trusted Certificate Authorities

Trusted Certificate Authorities is the list of certificate issuers that you want SSL to trust.

The options available are

- Not use Trusted Certificate Authority file.
    - Select this option when you do not want to use a Trusted Certificate Authorities file.
- Use Trusted Certificate Authorities file
    - If this option is selected then the path to the file should be identified and entered.

If CA file is specified, it points to a file of CA certificates in PEM format. The file can contain several CA certificates identified by sequences such as:

```
-----BEGIN CERTIFICATE-----CERTIFICATE----...
    ... (CA certificate in base64 encoding) ...
-----END CERTIFICATE-------CERTIFICATE----
```

Before, between, and after the certificates, text is allowed which can be used e.g. for descriptions of the certificates.

Trusted Certificates Hash Directory

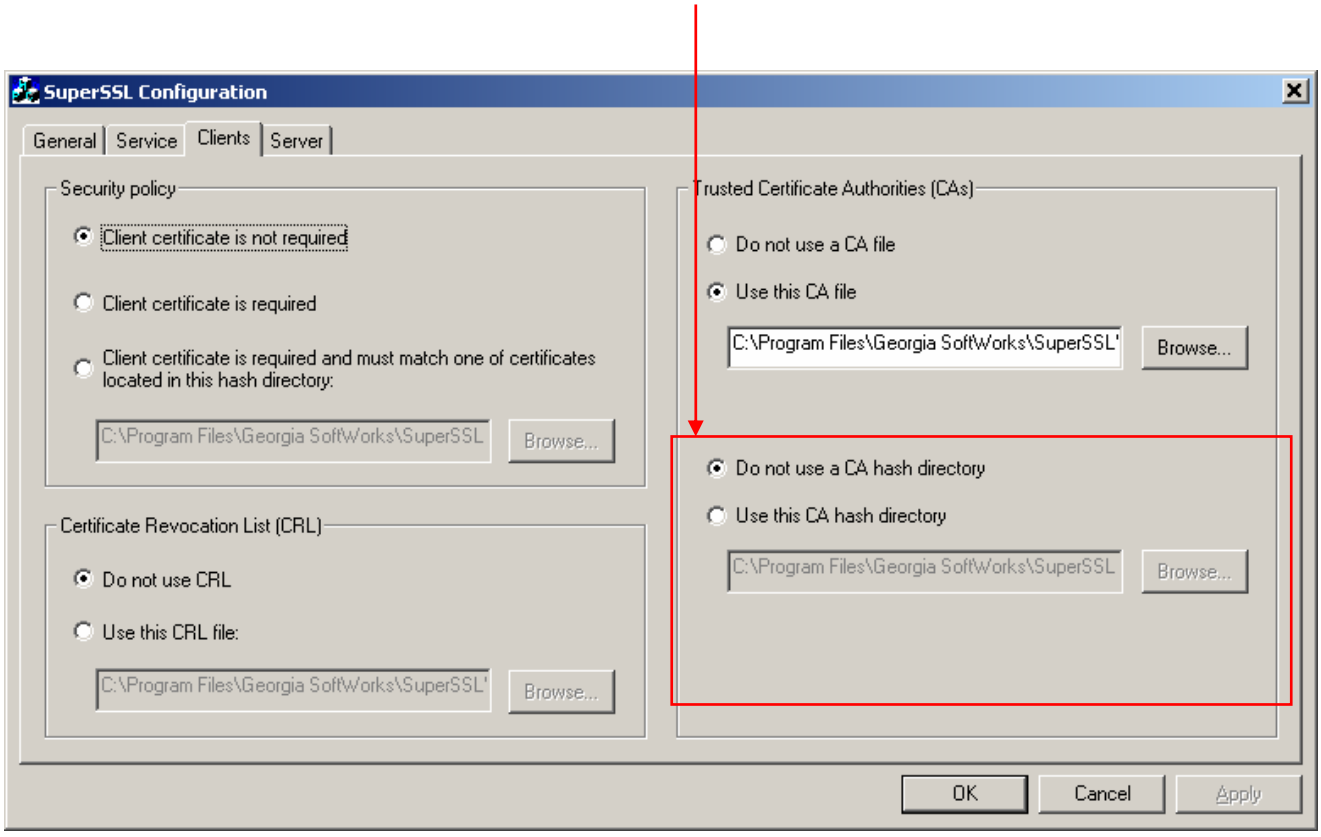

Figure 31: Configuration - Clients Tab - Trusted Certificate Authorities – Hash directory

You may specify the hash directory for your trusted certificate authorities.

The options available are

- Do not use Trusted Certificate Authorities hash directory.
    - Select this option when you do not want to use a Trusted Certificate Authority hash directory.
- Use Trusted Certificate Authorities hash directory.
    - If this option is selected then the path to the hash directory should be identified and entered.

If CA hash directory is specified, it points to a directory containing CA certificates in PEM format. The files each contain one CA certificate. The files are looked up by the CA subject name hash value, which must thus be available. If several CA certificates exist with the same name hash value, the extension must be different (e.g. 9d66eef0.0, 9d66eef0.1 etc). The search is performed in the order of the extension number, regardless of other properties of the certificates. Use the OpenSSL utilities to generate the hash values.

Server Tab

The Server Tab provides configuration associated with the Server. The configuration areas associated with the Server are:

- Connection Parameters: The IP Address and the Port Number for the Telnet Server
- Server Type:
  - Fully Utilize the GSW Telnet Server capabilities when used with SuperSSL
  - AUTH (RFC2941) Option – Enable/Disable option

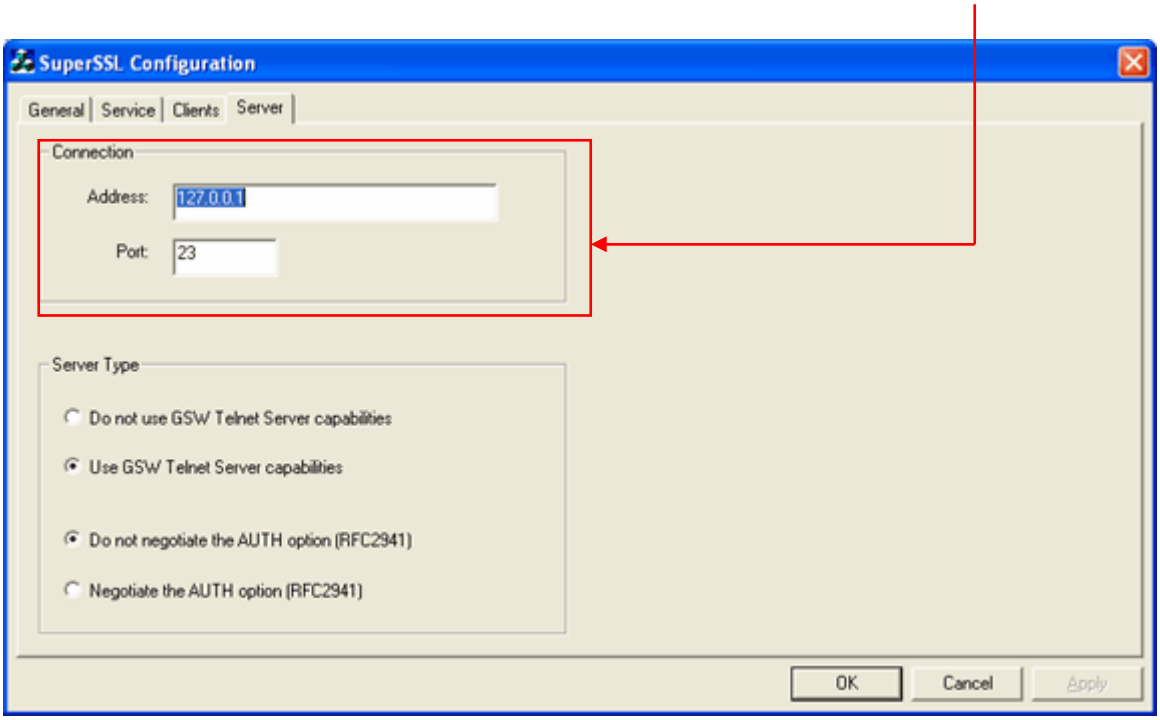

Figure 32: Configuration - Server Tab

Connection

This is where the IP Address of the Server and the Port Number is specified. Please note that the default settings point to the local telnet server port.

Server Type

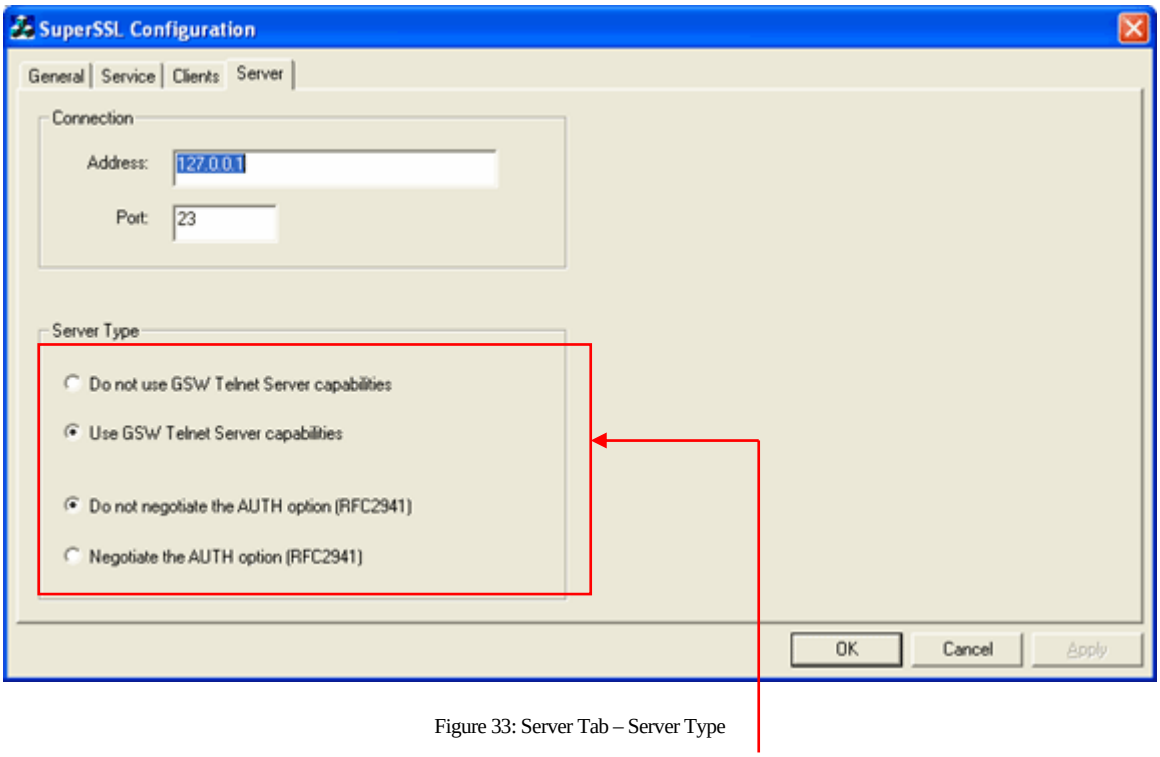

Figure 33: Server Tab – Server Type

The Server Type has two sets of options for configuration. The first is the GSW Telnet Server Capabilities.

- GSW Telnet Server Capabilities

  Typically when a telnet server is used with SSL, all the telnet management, report and display capabilities do not show the correct incoming client IP Address. The IP address of the machine on which SSL is installed is shown as the IP address of the client.

  However, if you are using the GSW Telnet Server then SuperSSL is able to pass the correct Client IP address to the Telnet Server. In many environments this is not an option and is critical for administrative features such as monitoring, shadowing etc.

  If you are using the GSW UTS (Telnet) Server then you should check the option to Use GSW Telnet Server capabilities. Be sure to set the UseSuperSSL parameter in the GSW UTS to 1 to enable this feature on the GSW UTS(Telnet) Server. This is a registry value in the GSW UTS as identified below. You will need to Stop and Start the GSW Telnet Server after this change is made.

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\GS_Tnet\Parameters\UseSuperSSL

If you are not using the GSW Telnet Server then you should leave the default option “Do not use GSW Telnet Server capabilities” checked.

The second set of options for the Server Type is the Negotiation of RFC2941 option.

- Negotiation of the RFC2941 Authentication

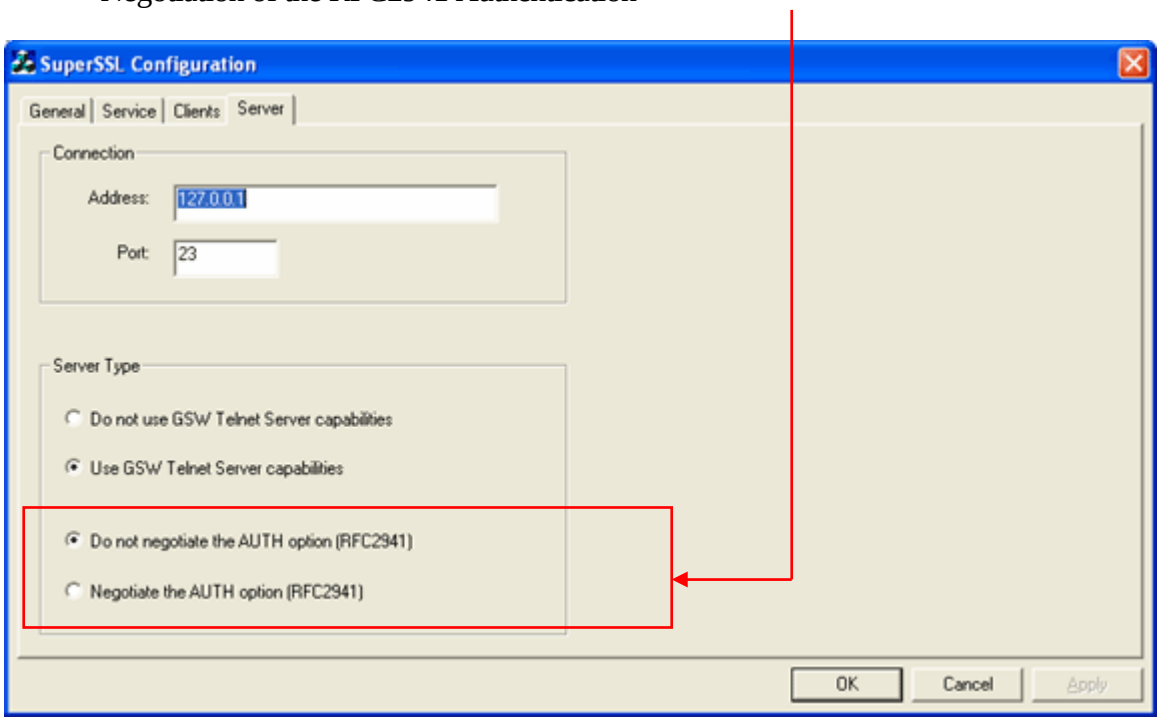

Figure 34: Configuration - RFC2941 Negotiation

If you are not using telnet (either GSW Telnet or a Third Party) then this option must be set to “Do not negotiate the AUTH option”. This is the default setting.

Some SSL telnet clients require this option to be on (example Kermit V2.0 and later) and other telnet clients require this option to be off (example Naurtech CETERM VT220 V5.1).

The setting of the Negotiation option is based on the client requirements.

GSW SuperSSL Subscription

The GSW Subscription plan provides access to the most current versions of the software as well as priority support.

In general, Georgia SoftWorks releases a new version as soon as new features are ready rather than waiting for scheduled quarterly or annual releases. Due to our development and release generation methods, and JIT User Manual production, we can release software on a much more frequent basis than other organizations. As soon as the features or defect resolutions are Alpha and Beta tested we can generate a release. This provides our customers with features much quicker than the "*grouping*" method used by other companies.

The GSW SuperSSL subscription provides access to free version upgrades for the duration of the subscription. The duration is either 1, 2 or 3 years. This is good as you can obtain new versions of the software at your convenience obtaining all new features and defect resolutions.

NOTE: New versions can be downloaded from our web site at your convenience.

The GSW Subscription plan is an excellent value. Even if you upgrade the software once every few years you will save with the subscription.

Version Upgrade Pricing with Subscription Plan	
Time from date of purchase	**Price**
For the Duration of Plan (1, 2 and 3 year plans are available).	**Free**

Table 2: Version Upgrade Pricing with GSW Subscription Plan

The pricing for version upgrades without the Subscription is based on the time from the date of the original purchase or last version upgrade.

Version Upgrade Pricing without Subscription Plan	
Time from date of purchase	**Price**
Less than 60 days	Free
Greater than 60 days but less than 1 year	50% of the current list
Greater than 1 year	90% of the current list

Table 3: Version Upgrade Pricing Without Subscription Plan

HOW TO UPDATE THE SOFTWARE

1. Download the software or use the supplied CD
2. Make sure the SuperSSL is not in use.
3. Run the new Setup Program for the Update as done in the original installation.
4. You may specify the same or different installation folder.

HOW TO RENEW THE GSW Subscription

Please use the following procedure when renewing the GSW SuperSSL Subscription.

Step	Who		Action
1.	GSW		Send notice to customer giving indicating that the subscription is about to expire. The notice is sent approximately 4 to 8 weeks prior to the expiration of the plan.
2.		Customer	Places order for new subscription
3.	GSW		Confirms Order
4.	GSW		Ships current software, documentation and new Floating License
5.		Customer	Install new Floating License (and software if desired)
6.		Customer	Ships OLD Floating License back to GSW

Table 4: Steps to Renew the GSW Subscription Plan

System Signature - IMPORTANT PLEASE READ

NOTE: This section only applies to Software Registration

The registration software obtains a system signature that is unique to your system. This signature is an added security measure to inhibit unauthorized personnel to obtain working copies of the GSW SuperSSL.

The signature is comprised of hardware and software identifiers that exist on your system that make the target system unique. These identities are hashed into a Product ID and a Serial Number can be generated from this Product id.

If major hardware components of your system are removed, replaced or modified your **Serial Number** may discontinue to work and you may need a new **Serial Number** to obtain access to the SuperSSL. Please contact Georgia SoftWorks Technical Support if needed.

Technical Support

In order to keep Technical Support Free please help keep our cost down.

- Gather all relevant system information.
- Write your question down. This not only helps us but also helps you in articulating the question.

If the question is not an emergency, please use e-mail at support@georgiasoftworks.com. We try to respond within 24 hours.

Or Call 706.265.1018 EST, M-F 9:00 a.m. to 5:00 p.m. and have your Product ID ready