GEORGIA SOFTWORKS

SSH Server for Windows 7/8/VISTA/2008/R2/2012 and Windows NT/XP/2000/2003

Keep it Secure – Simply

User's Guide

THIS PAGE INTENTIONALLY LEFT BLANK

GEORGIA SOFTWORKS

SSH Server

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 8.06.0001, January 27, 2015

THIS PROGRAM IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

LICENSOR MAKES NO WARRANTIES OR REPRESENTATIONS, EXPRESS OR IMPLIED, ORAL OR WRITTEN, REGARDING THE PROGRAM OR DOCUMENTATION AND HEREBY EXPRESSLY DISCLAIMS ALL OTHER EXPRESS OR IMPLIED WARRANTIES, INCLUDING MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. LICENSOR DOES NOT WARRANT THE PROGRAM WILL MEET YOUR REQUIREMENTS OR THAT ITS OPERATION WILL BE UNINTERRUPTED OR ERROR FREE.

IN NO EVENT WILL GEORGIA SOFTWORKS BE LIABLE TO YOU FOR ANY DAMAGES, INCLUDING ANY LOST PROFITS, LOST SAVINGS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE SUCH PROGRAMS.

COPYING:

WHILE YOU ARE PERMITTED TO MAKE BACKUP COPIES OF THE SOFTWARE FOR YOU OWN USE AND PROTECTION, YOU ARE NOT PERMITTED TO MAKE COPIES FOR THE USE OF ANYONE ELSE.

LICENSE:

YOU ARE LICENSED TO RUN THIS SOFTWARE ON A SINGLE WINDOWS 7/8/VISTA/2008/R2/2012/R2, NT/XP/2000/2003 SYSTEM. THE GEORGIA SOFTWORKS WINDOWS 7/8/VISTA/2008/R2/2012/R2, NT/XP/2000/2003 SSH SERVER SOFTWARE MAY BE INSTALLED ON A SINGLE WINDOWS 7/8/VISTA/2008/R2/2012/R2, NT/XP/2000/2003 SYSTEM.

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.

Terms/Abbreviations

UTS GSW Universal Terminal Server

SSH Secure Shell Version 2
Always referees to SSH version 2 (SSHv2) except where noted

SSH SHIELD This is the application and interface installer for the GSW SSHv2 Interface

SSH SHIELD Certificate Mapping Tool
This is the GSW GUI tool that is used when configuration and managing the mapping of Digital Certificates, Public Keys and CTL's.
Often called the GSW Mapping Tool or GSW Certificate Mapping Tool.

Telnet Server Unless noted otherwise this referees to the GSW UTS with the default Telnet Protocol

Windows Refers to Microsoft Windows Operating Systems 98/ME/NT 4.0/XP/VISTA/7/8/2000/2003/2008/R2/2012/R2 unless otherwise noted.

Features at a Glance

Offering Secure Remote Logon, Secure Data Exchange, Secure Network Services and Secure Access to your Application on an Insecure Network

Georgia SoftWorks SSH Server

- Complete Data Stream Encryption
  AES-256, 3DES, and other ciphers supported (see below)
- Easy to Install and Use
  Defaults provide strong encryption
  No Certificate provision required (*However, available if you want it*)
- Automatic Generation and installation of RSA, DSA and ECDSA Host Keys
- Host Fingerprints file holds key fingerprints for all host keys offered for server-to-client authentication.
- FIPS 140-2 Compliant Option
- IPv6 Support
- Integrated with GSW UTS feature set including GUI Configuration Tool
- Perfect Support for ALL PC Keys and International Characters
- GSW SSH Clients for Windows Desktops, PPC 2003, Windows CE .Net 4.2+, Windows Mobile (WM5)+ class devices.

Elliptic Curve Cryptography Support for

- Server-to-client authentication
- Key Exchange
- Public key authentication

- **Host Key types**
  - `'ssh-rsa'`
  - `'ssh-dsa'`
  - `'ecdsa-sha2-nistp521'`
- **Key Exchange algorithm**
  - `'ecdh-sha2-nistp256'`
  - `'ecdh-sha2-nistp384'`
  - `'ecdh-sha2-nistp521'`
  - `'diffie-hellman-group1-sha1'`
  - `'diffie-hellman-group14-sha1'`
- **HMAC algorithms**
  - `'hmac-sha2-256'`
  - `'hmac-sha2-512'`
  - `'hmac-sha1'`
  - `'hmac-sha1-96'`

- **Ciphers**
  - `'aes128-cbc'`
  - `'aes128-ctr'`
  - `'3des-cdc'`
  - `'aes192-cbc'`
  - `'aes192-ctr'`
  - `'aes256-cbc'`
  - `'aes256-ctr'`
  - `'rijndael192-cbc'`
  - `'rijndael256-cbc'`

Plus GSW Digital Certificate Based Authentication

- Public Key Authentication with Microsoft IIS like certificate to user account mapping
- **'One-to-one'** and **'Many-to-one'** mapping methods that also support supports certificate trust lists (CTL).
- Certificate mapping tool also supports public key to user account mapping
- Single Sign On through NTLM and Keberos over GSSAPI ('gssapi-with-mic')
- Certificate based authentication through:
  - 'x509v3-sign-rsa' and 'x509-sign-dss' public key authentication standards
  - Integrated with the Microsoft Certificate Stores

Overview

The GSW Secure Shell (SSH) Server provides Secure Remote Access to your Windows Host including Secure Remote Logon, Data Exchange, and Access to your Application on an Insecure Network

Thank you for purchasing the Georgia SoftWorks (GSW) SSH Server for Windows 7/8/VISTA/2008/R2/2012, NT/XP/2000/2003. The GSW SSH Server provides unparalleled performance and includes the powerful features needed to achieve operational objectives in demanding commercial and industrial environments. The growing concern that sensitive data must not be available to unauthorized third parties demands that a client can securely access the remote server. This is especially important for RF access to a server.

Strong "End-to-End" encryption is employed with the GSW SSH Server. No clear text username and passwords are transmitted across the network. No clear text application data is transmitted across the network. All the data is encrypted using the strongest encryption available to provide complete confidentiality.

A Federal Information Processing Standards Publication (FIPS) 140-2 compliant option is available and may be purchased for the GSW SSH Server. This standard specifies the security requirements that will be satisfied by a cryptographic module utilized within a security system protecting sensitive or valuable data. This option is available to Federal agencies, including the US Military. The option is also available for purchase by other organizations such as state governments, educational and research institutions, commercial businesses and other entities with the need or desire to comply with this security requirement for cryptographic modules standard.

The GSW SSH Server is useful in a wide variety of environments that require Secure Remote Access and Strong Encryption that include:

- RF Application, Barcode Scanner, etc. (Warehousing, Inventory, Medical, etc.)
- SAP AG's SAPConsole
- HighJump, QAD and more
- Application Service Providers (ASP), Legacy Applications
- System Administration, Software Development and more!
- The GSW Business Tunnel is an excellent client application for the GSW SSH Server providing secure web browsing, email access, RDP and much more.

The GSW SSH provides SSH (SSH version 2) operation rather than the older iteration SSH1 (SSH version 1) operation. In addition to being faster, smaller and more flexible, SSH provides significant security improvements. Even though SSH1 implementations exist, they are becoming fewer and are usually not recommended. GSW has chosen to provide the strongest, fastest and version of SSH – SSHv2.

An extremely important aspect of the GSW SSH Server is the ease of installation. Complex and lengthy security configuration has been either eliminated or reduced to a minimum in order to get your application up and running fast without forsaking performance or compromising desired security. You do not have the administrative complexity of public/private keys and certificates when using the GSW SSH Server default settings.

Secure Remote Login, Secure Access to the Application and ensuring Data Integrity are the primary areas for concern when securing an application and the GSW SSH Server is optimized to address these needs.

Strong Authentication

The GSW SSH Server offers the Strongest Authentication features available for Windows.

In addition to User Name/Password Authentication, the GSW SSH Server for Windows offers Public Key Authentication with a GUI Internet Information Server (IIS) *like* ***certificate*** to user account mapping. This includes 'One-to-one' and 'Many-to-one' mapping methods and also supports certificate trusts lists (CTL). This mapping works with all user accounts including accounts defined in the Active Directory. Additionally the GSW GUI mapping tool allows ***public key*** to user account mapping.

Please visit the GSW website

http://www.georgiasoftworks.com/products/ssh2/ssh_authentication_x509v3.php

to learn more about GSW Digital Certificate Based Authentication.

Secure Remote Login

The GSW SSH Server only allows connections from SSH clients. This ensures that all user data is encrypted prior to leaving the local client device. The data is decrypted at the remote GSW SSH Server. This includes authentication data such as the *username* and *password* that is required to login to the remote server. The encryption is transparent, and thus the user will not perceive much, if any, variance between operation of a telnet and SSH client.

The SSH connection ensures that the Login and Authentication data is encrypted so that a malicious party can not intercept the sensitive information.

Secure Access to Your Application (Secure Data Exchange)

Since the connection between the SSH client and the GSW SSH Server is encrypted, the data transmitted is not readable by unauthorized parties. When the User is authenticated, a shell is started (cmd.exe), where the user can perform remote command execution or start applications. All data transmitted between the client and the server is encrypted. No one can "snoop" the connection and intercept clear text data because none exists!

Data Integrity

Data Integrity is essential for secure data exchange. The data received must be exactly the same as the data sent; otherwise an unauthorized party may have modified the data during the transmission. The SSH Transport layer ensures that the data received has not been modified from the data sent. This is accomplished by including a message authentication code (MAC) with each packet transmitted. The MAC is determined prior to encryption using the contents of the packet, a "Shared Secret" between the SSH client and SSH server and a packet sequence number.

Ease of Use

Many of the complex and lengthy configurations issues are automatically defined by the GSW SSH Server. It has been observed that an overwhelming majority of customers do not need nor desire to set every possible option available for SSH Security.

Most customers want the strongest security that is practical to implement. Through much dialog with our resellers and customers who use RF environments a main theme emerged. The requirement to "Keep it secure – simply" was paramount.

The installation of the GSW SSH Server is very quick. You will have users connecting with the security of powerful SSH encryption much sooner than expected.

- No Encryption Method has to be specified.
  Many environments must ensure that the Windows Username and Password are encrypted as well as the data. GSW SSH Server provides *complete* confidentiality by defaulting to a very strong encryption method.

  The GSW SSH Server defaults to AES-256.

  AES-256 is the generally accepted strongest encryption standard offered by SSH – it is the Advanced Encryption Standard using a 256 bits cryptographic key. This is also known as the Rijndael algorithm which is a symmetric block cipher capable of using cipher keys that have 128, 192 and 256 bit lengths to process data blocks of 128 bits.

  The GSW SSH server can be configured to refuse a connection if the SSH client can not operate with AES-256. Weaker encryptions only compromise the security of the connection so only the strongest encryption can be configured to ensure the strongest protection - while maintaining exceptional performance. AES-256 encryption is available on almost all SSH clients. Of course other encryptions are supported such as 3DES. The GSW SSH Server will negotiate with the client to agree on the algorithm unless configured otherwise.

- No manual installation of certificates needed
  Additionally, it has been identified that in many cases the administrative requirements for public and private certificate installation are not needed or desired. Using traditional, manual methods the installation of certificates on RF devices can be complex and cumbersome. No public/private key generation or administration is required.

  However, those with the requirements can take full advantage of the security offered by Digital Certificates and Public Keys using the innovative and easy to use SSH Shield Certificate Mapping Tool.

Component Architecture

The GSW SSH is composed of:

- The GSW Universal Terminal Server (UTS)
- The GSW SSH Shield

The GSW UTS is the software module that contains the core software for the GSW Server products, and the majority of the Advanced Features for the GSW Server Products

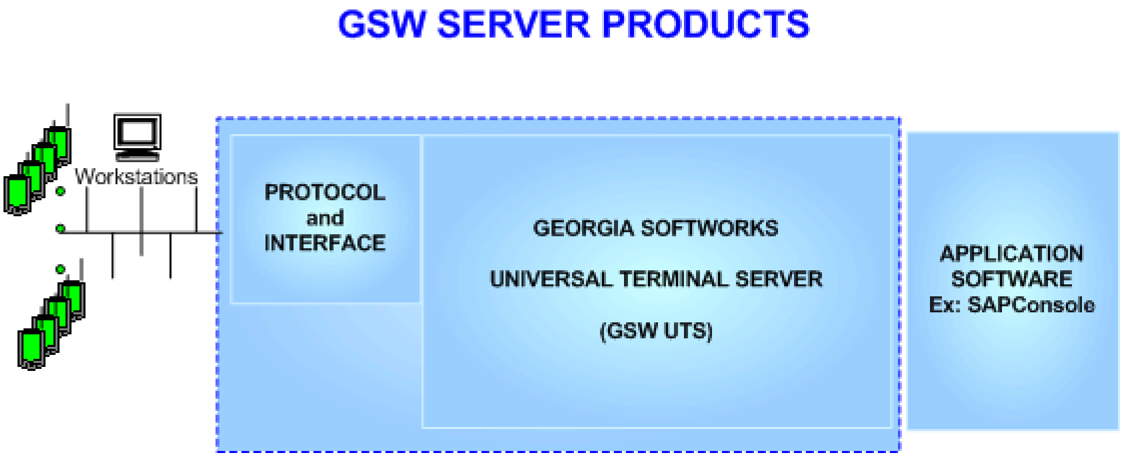


Figure 1: GSW Server Products Block Diagram

The GSW UTS standard option for the Protocol and Interface is the Telnet Interface. This configuration is marketed and sold as the GSW Telnet Server.

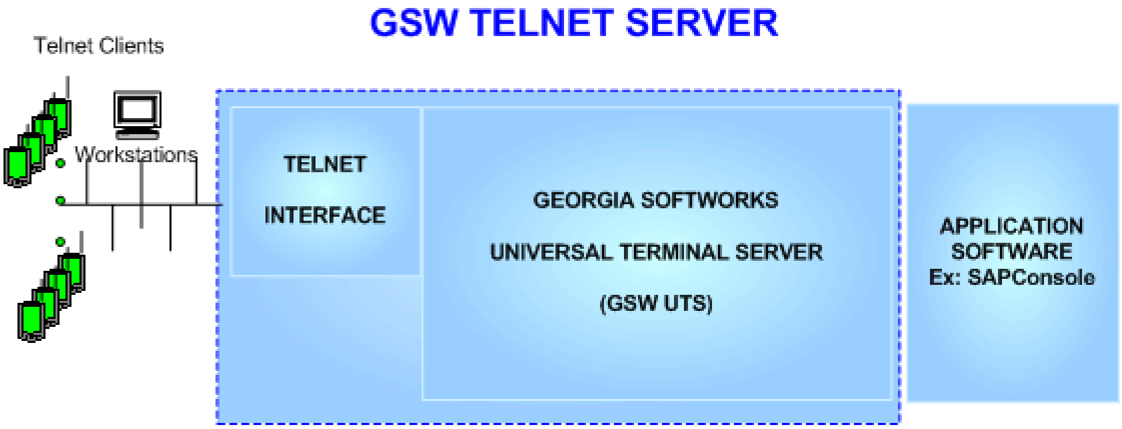


Figure 2: GSW Telnet Server Block Diagram

The GSW UTS SSH interface is installed by applying the GSW SSH Shield to the GSW UTS. The GSW **SSH Shield disconnects the Telnet Protocol Interface** and installs the SSH Interface. This configuration is marketed and sold as the GSW SSH Server

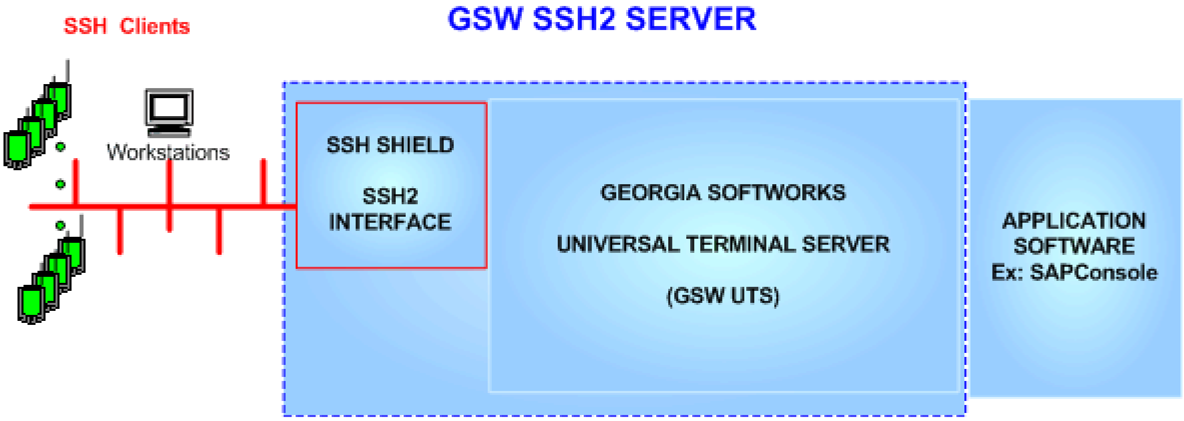


Figure 3: GSW SSH Server Block Diagram

Installation

Overview

When you purchased the GSW SSH Server you either:

a. Own a GSW Telnet Server (UTS) and are upgrading to the SSH Server
   OR
b. Are new customer purchasing the GSW SSH Server[1].

If you own a GSW Telnet Server and are upgrading to the SSH Server then:

a. You must have GSW Telnet Server Version 6.50 or higher to install the SSH Shield. The Telnet Interface becomes disabled when the SSH Shield is installed. If you have an older version then you will need to upgrade to the Version 6.50 or higher before you can apply the SSH Shield.
b. Next install the GSW SSH Shield
c. Register the GSW SSH Server.

If you are purchasing a new GSW SSH Server then:

a. You will receive the current version of the GSW Telnet Server. Install the GSW Telnet Server according to the Installation Instruction in the GSW UTS User Manual. You do not need to register the Telnet Server at this time. Registration takes place after the installation of the GSW SSH Shield.
b. Next install the GSW SSH Shield
c. Register the GSW SSH Server.

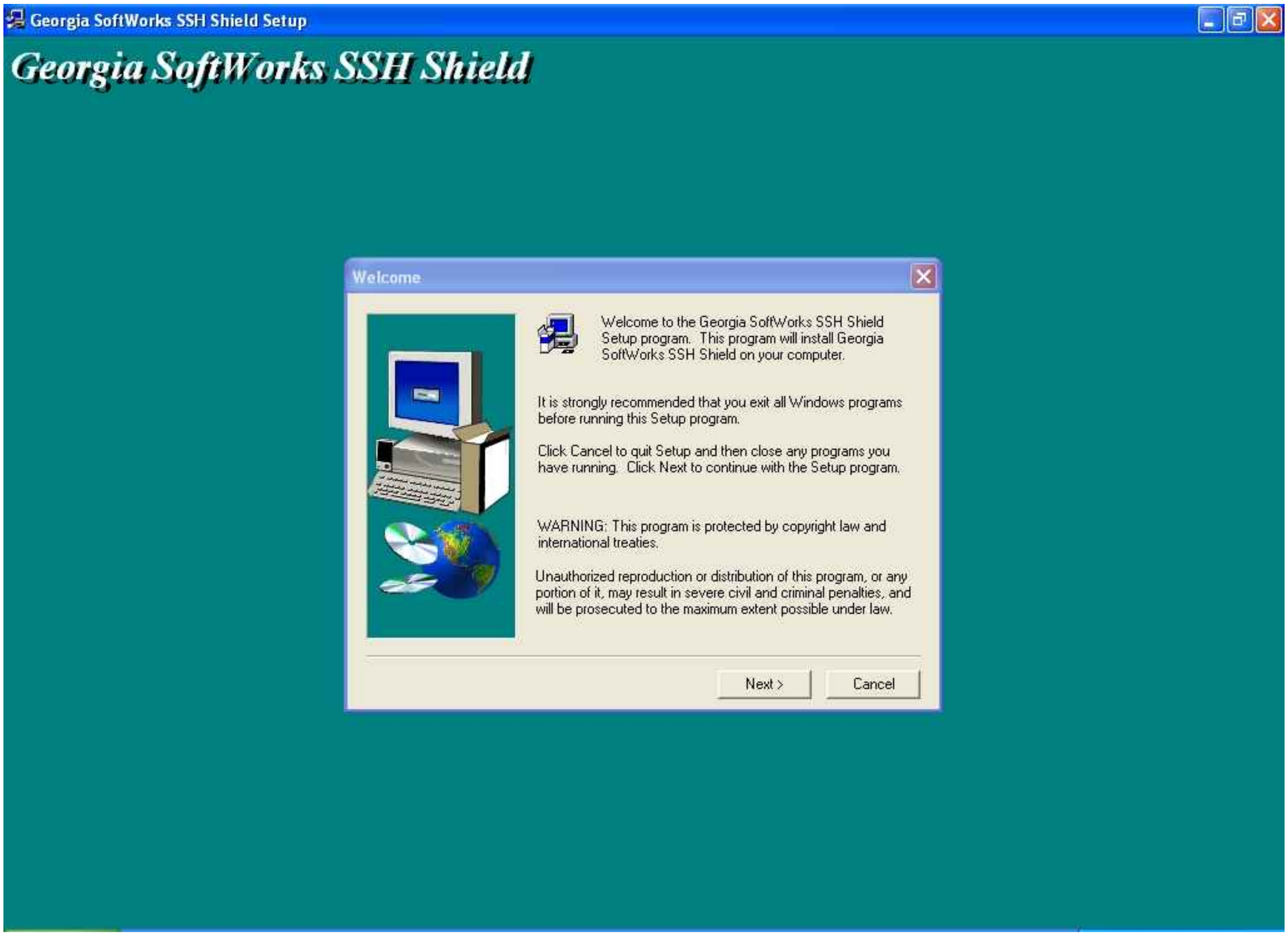
NOTE: The GSW SSH Server requires registration. The registration for the GSW UTS is not sufficient for the GSW SSH Server.

[1] In conjunction with the GSW UTS Server

Procedure

Installation of the GSW SSH Server software is simple and quick. From Windows 7/8/2008/R2/2012/R2, NT/XP/VISTA/2000/2003 perform the following:

1. Run the setup program (sshshld.exe). 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.**


Georgia SoftWorks SSH Shield Setup
Georgia SoftWorks SSH Shield
Welcome
Next >
Cancel

Welcome to the Georgia SoftWorks SSH Shield Setup program. This program will install Georgia SoftWorks SSH Shield on your computer.

It is strongly recommended that you exit all Windows programs before running this Setup program.

Click Cancel to quit Setup and then close any programs you have running. Click Next to continue with the Setup program.

WARNING: This program is protected by copyright law and international treaties.

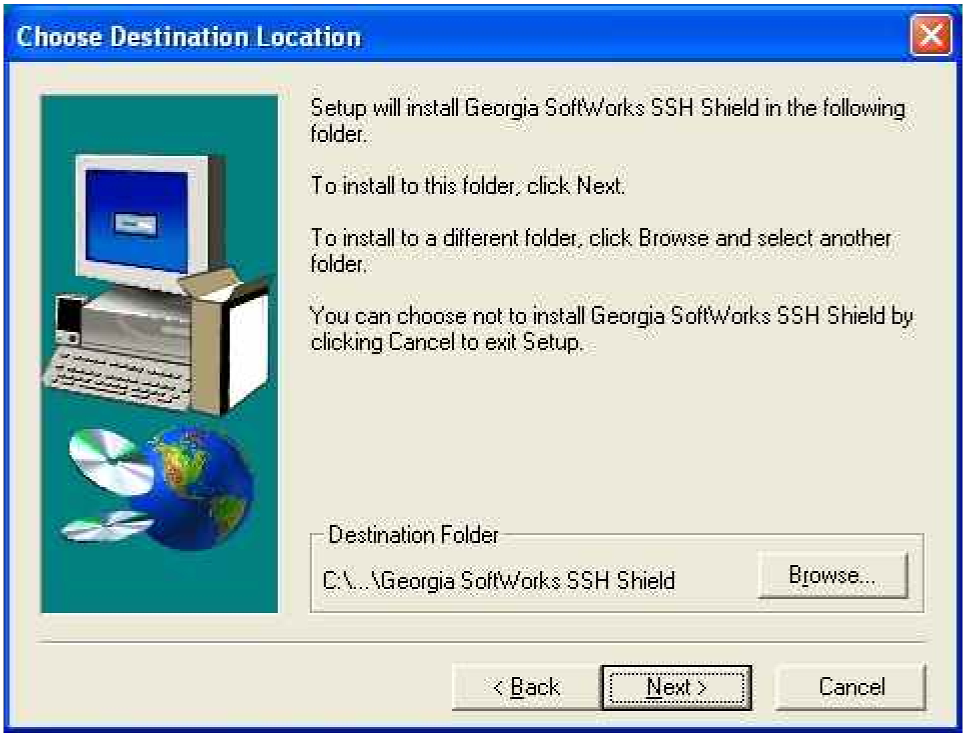
Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.

Figure 4: Installation Welcome Screen

1. A screen is displayed indicating the folder where the GSW SSH Shield will be installed. The default is:

   `C:\Program Files\Georgia SoftWorks\Georgia SoftWorks SSH SHIELD.`

   You may change the installation directory at this time. *Note: Make sure that the users of the SSH Server have full access to the installation directory.*



Choose Destination Location

Setup will install Georgia SoftWorks SSH Shield in the following folder.

To install to this folder, click Next.

To install to a different folder, click Browse and select another folder.

You can choose not to install Georgia SoftWorks SSH Shield by clicking Cancel to exit Setup.

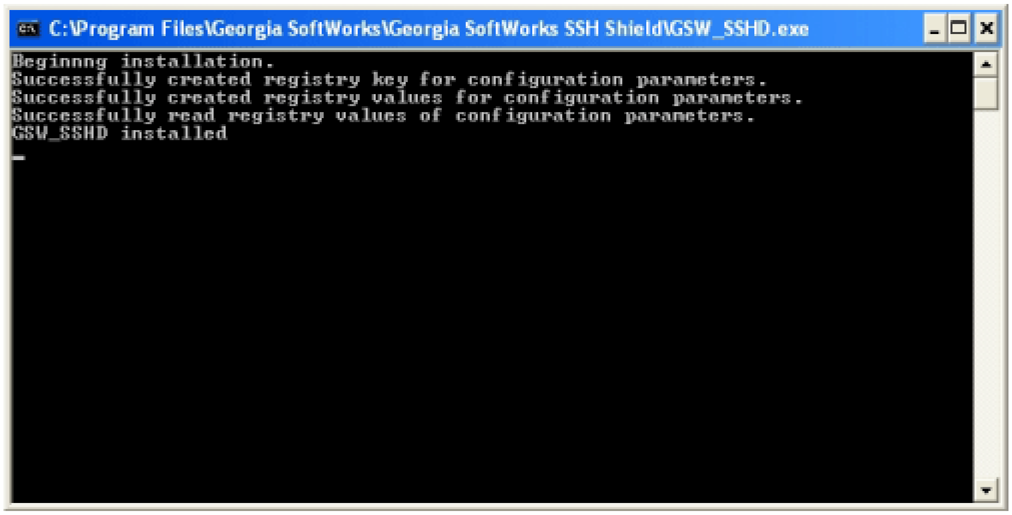
Destination Folder

C:\...\Georgia SoftWorks SSH Shield

Figure 5: Installation – Choose Destination Folder

Select the Program Folder for the SSH Server. **Click Next.**

2. A shell opens a window with installation status lines similar to the figure below.

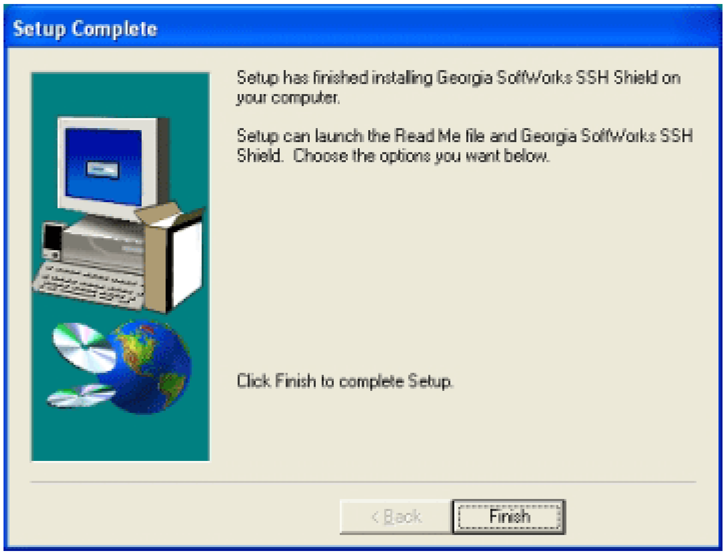


C:\Program Files\Georgia SoftWorks\Georgia SoftWorks SSH Shield\GSW_SSHD.exe

```
Beginnng installation.
Successfully created registry key for configuration parameters.
Successfully created registry values for configuration parameters.
Successfully read registry values of configuration parameters.
GSW_SSHD installed
_
```

Figure 6: Installation – Command Shell Status Lines

3. Now the Setup is complete! Click Finish and *Now its time to register the SSH Server!*



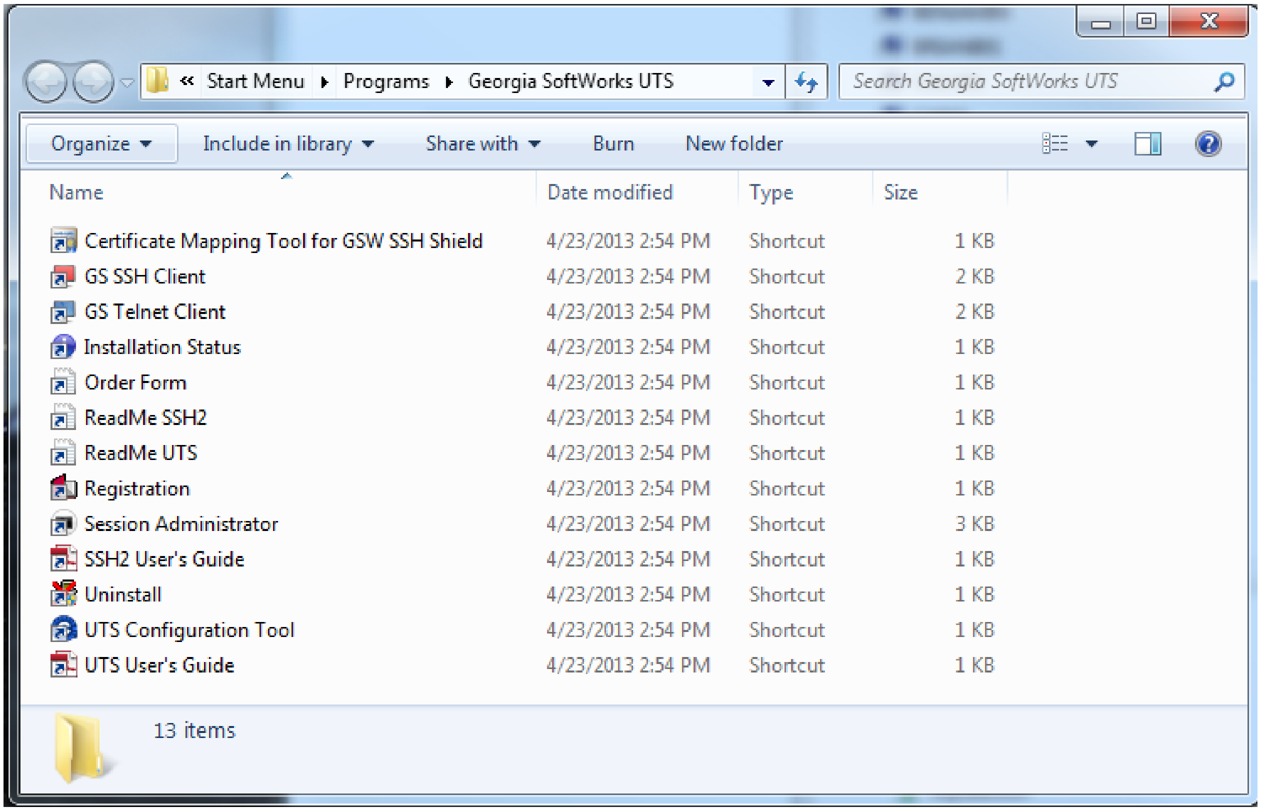
Setup has finished installing Georgia SoftWorks SSH Shield on your computer.

Setup can launch the Read Me file and Georgia SoftWorks SSH Shield. Choose the options you want below.

Click Finish to complete Setup.

Figure 7: Installation Complete

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

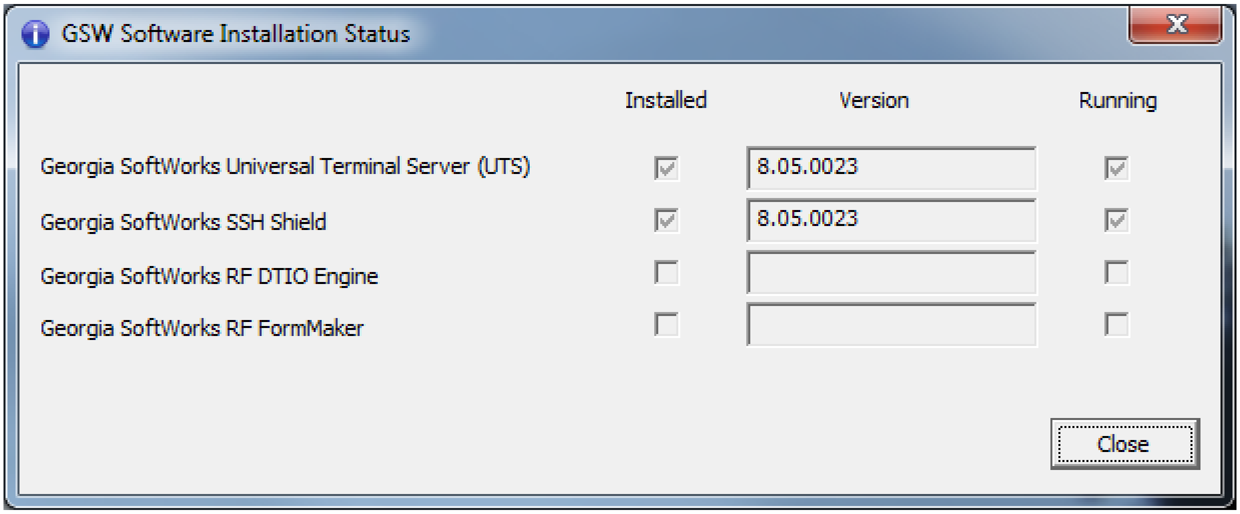

« Start Menu ▸ Programs ▸ Georgia SoftWorks UTS
Search Georgia SoftWorks UTS
Organize
Include in library
Share with
Burn
New folder

Name	Date modified	Type	Size
Certificate Mapping Tool for GSW SSH Shield	4/23/2013 2:54 PM	Shortcut	1 KB
GS SSH Client	4/23/2013 2:54 PM	Shortcut	2 KB
GS Telnet Client	4/23/2013 2:54 PM	Shortcut	2 KB
Installation Status	4/23/2013 2:54 PM	Shortcut	1 KB
Order Form	4/23/2013 2:54 PM	Shortcut	1 KB
ReadMe SSH2	4/23/2013 2:54 PM	Shortcut	1 KB
ReadMe UTS	4/23/2013 2:54 PM	Shortcut	1 KB
Registration	4/23/2013 2:54 PM	Shortcut	1 KB
Session Administrator	4/23/2013 2:54 PM	Shortcut	3 KB
SSH2 User's Guide	4/23/2013 2:54 PM	Shortcut	1 KB
Uninstall	4/23/2013 2:54 PM	Shortcut	1 KB
UTS Configuration Tool	4/23/2013 2:54 PM	Shortcut	1 KB
UTS User's Guide	4/23/2013 2:54 PM	Shortcut	1 KB

13 items

Figure 8: GSW UTS Program Group

Installation will result in the Georgia SoftWorks program group item "Installation Status" showing GSW SSH as installed. Additionally, the version of the GSW SSH Shield is displayed along with the status of the server and other Georgia SoftWorks software that may be installed.



	Installed	Version	Running
Georgia SoftWorks Universal Terminal Server (UTS)	☑	8.05.0023	☑
Georgia SoftWorks SSH Shield	☑	8.05.0023	☑
Georgia SoftWorks RF DTIO Engine	☐		☐
Georgia SoftWorks RF FormMaker	☐		☐

Figure 9: SSH Installation Status

Registration

The GSW SSH Server 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 SSH Server 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
   The Serial Number is pre-programmed into a specific hardware key that came with your purchase. The hardware key connects to a parallel or USB port on the server. See page 22 for details on registration via the Floating License.

2. Registration via Software Serial Number.
   This method exists for environments that do not support Parallel or USB 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 the GSW Ticket System, however is some cases email, fax or telephone. See page 29 for details on Software registration.

Floating License – Overview

The Georgia SoftWorks Floating License provides the flexibility to rapidly move the GSW SSH Server 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 29.*

NOTE: When a SSH Server Pack is purchased (SSH Server and GSW Telnet Server), the same physical Floating License will contain valid Serial Numbers for both products.

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

Common scenarios where the Floating License is useful include:

- **Laboratory usage in a development or test environment** where the SSH Server 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 SSH Servers 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 SSH Server capability**.

The Georgia SoftWorks Floating License is a hardware key that connects to a *female* parallel port connector or USB Port on the server. The parallel port Floating License does not impact functionality of the port for other uses. The parallel hardware key acts as a pass-through allowing normal connections to the other side of the key.

The Georgia SoftWorks Floating License is a hardware key that can be ordered for a Parallel or USB Port.

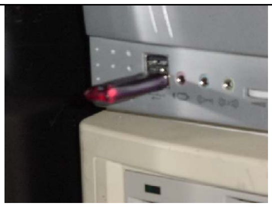
Parallel Port Floating License	USB Floating License
 Figure 10: Floating License – Parallel Port The Parallel Port Floating License is a Pass Through allowing normal function of the port.	 Figure 11: Floating License - USB Port Not attached to a Server
The Parallel Port Floating License connects to a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

Figure 12: Floating License - Hardware Key

The SSH Server will recognize the presence of the key and activate the software with 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 SafeNet, previously Aladdin of the hardware key's setup program. It is described below. The name of the hardware key is HASPHL and you will see it displayed in the setup screens. The best drivers for the HASP4 are the HASP HL drivers.

Floating License – Hardware Key Installation Instructions

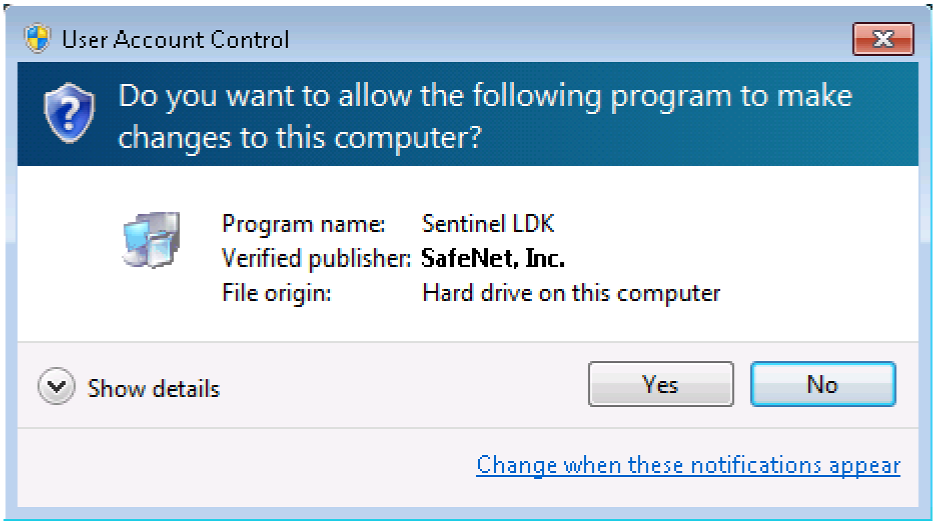
Note: If you are using a *USB Floating License on a Windows NT system* - run the file aksnt4usb.exe prior to the following steps.

Note: Install the Floating License drivers before plugging into the USB port.

1. Copy the files from the Floating License folder (hardkey) on the provided CD to the hard drive on your server.

2. Run the HASPUserSetup.exe program and follow the installation instructions. After installation of the hardware key install the GSW SSH Server as described on page 17 (if it is not already installed).

3. If you have User Account Control enabled you may get a prompt that says "Do you want to allow the following program to make changes to this computer?" Click Yes



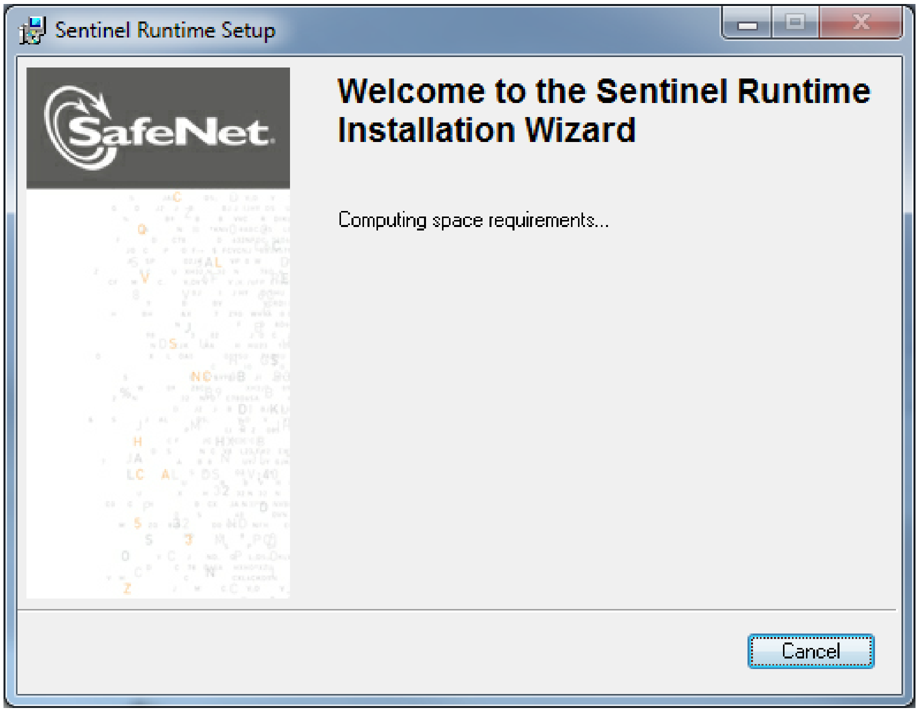
User Account Control

Do you want to allow the following program to make changes to this computer?

Program name: Sentinel LDK
Verified publisher: **SafeNet, Inc.**
File origin: Hard drive on this computer

Figure 13: User Account Control

4. You will first see the SafeNet (formerly Aladdin) initial Welcome Screen.

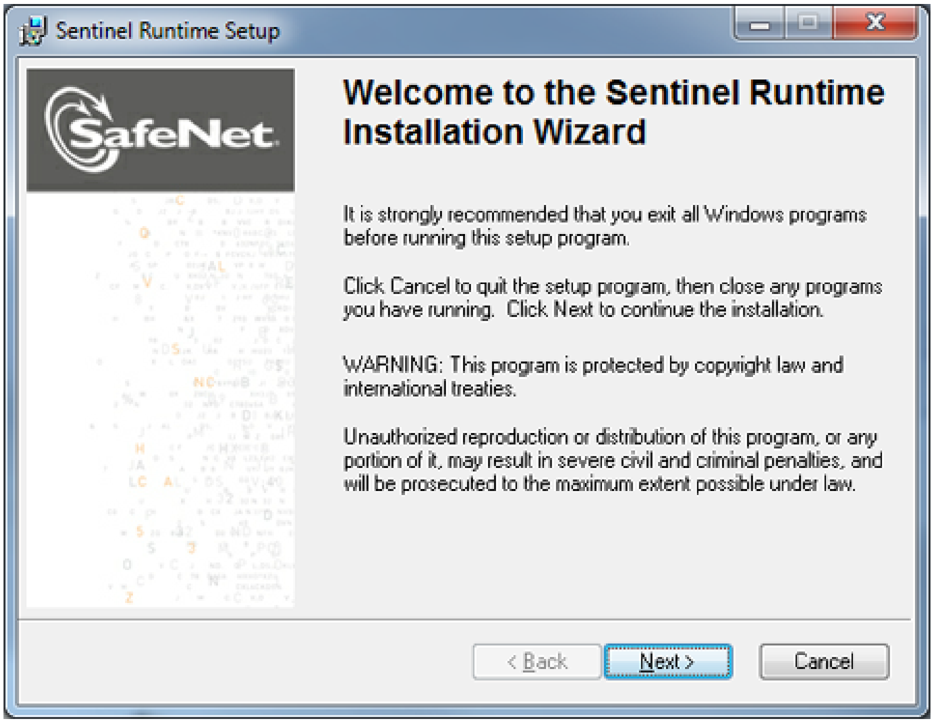


Welcome to the Sentinel Runtime Installation Wizard

Computing space requirements...

Figure 14: SafeNet welcome screen - computing space requirements

5. You will first see the SafeNet complete Welcome Screen, **Click Next**



Welcome to the Sentinel Runtime Installation Wizard

It is strongly recommended that you exit all Windows programs before running this setup program.

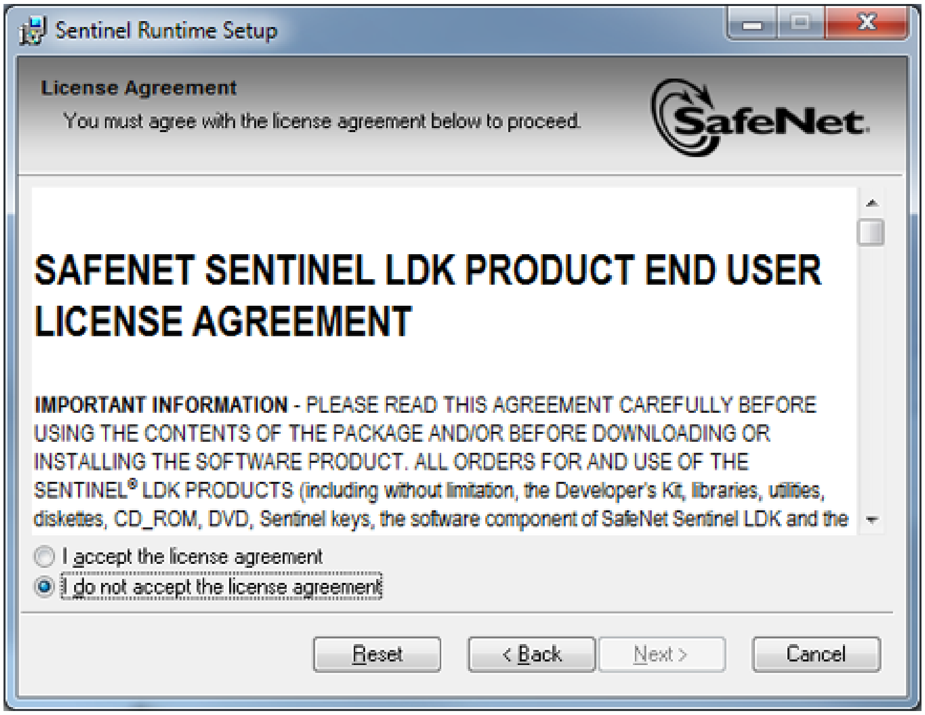
Click Cancel to quit the setup program, then close any programs you have running. Click Next to continue the installation.

WARNING: This program is protected by copyright law and international treaties.

Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.

Figure 15: SafeNet welcome screen - second part

6. The next screen displayed is the SafeNet License Agreement screen.



License Agreement

You must agree with the license agreement below to proceed.

SAFENET SENTINEL LDK PRODUCT END USER LICENSE AGREEMENT

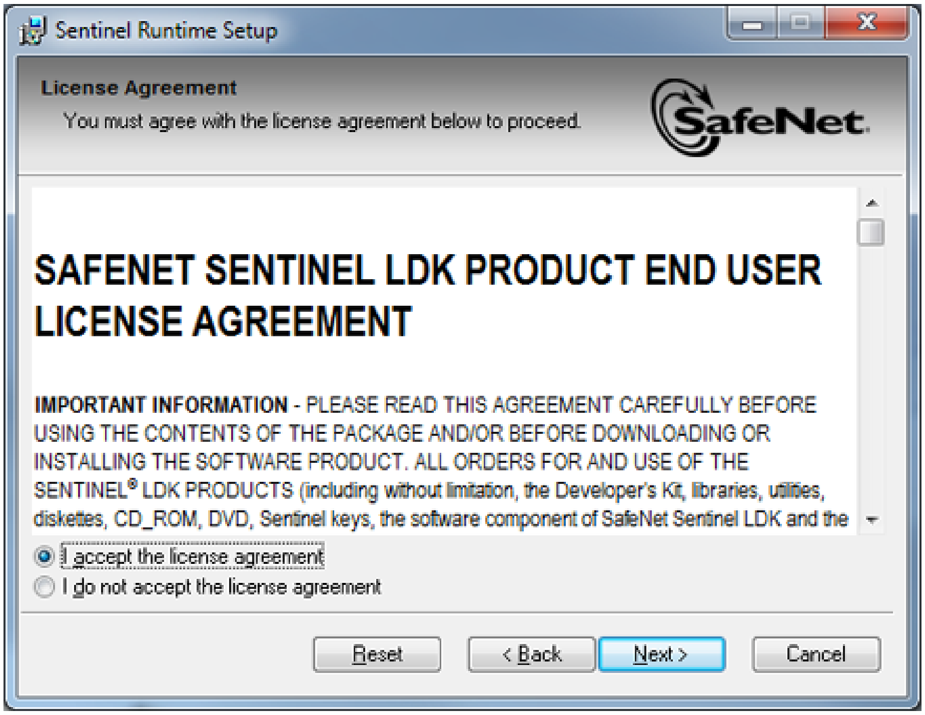
IMPORTANT INFORMATION - PLEASE READ THIS AGREEMENT CAREFULLY BEFORE USING THE CONTENTS OF THE PACKAGE AND/OR BEFORE DOWNLOADING OR INSTALLING THE SOFTWARE PRODUCT. ALL ORDERS FOR AND USE OF THE SENTINEL® LDK PRODUCTS (including without limitation, the Developer's Kit, libraries, utilities, diskettes, CD_ROM, DVD, Sentinel keys, the software component of SafeNet Sentinel LDK and the

○ I accept the license agreement

● I do not accept the license agreement

Figure 16: SafeNet License Agreement

7. Read the license agreement and select “I accept the license agreement”, and then **Click Install**.



License Agreement

You must agree with the license agreement below to proceed.

SAFENET SENTINEL LDK PRODUCT END USER LICENSE AGREEMENT

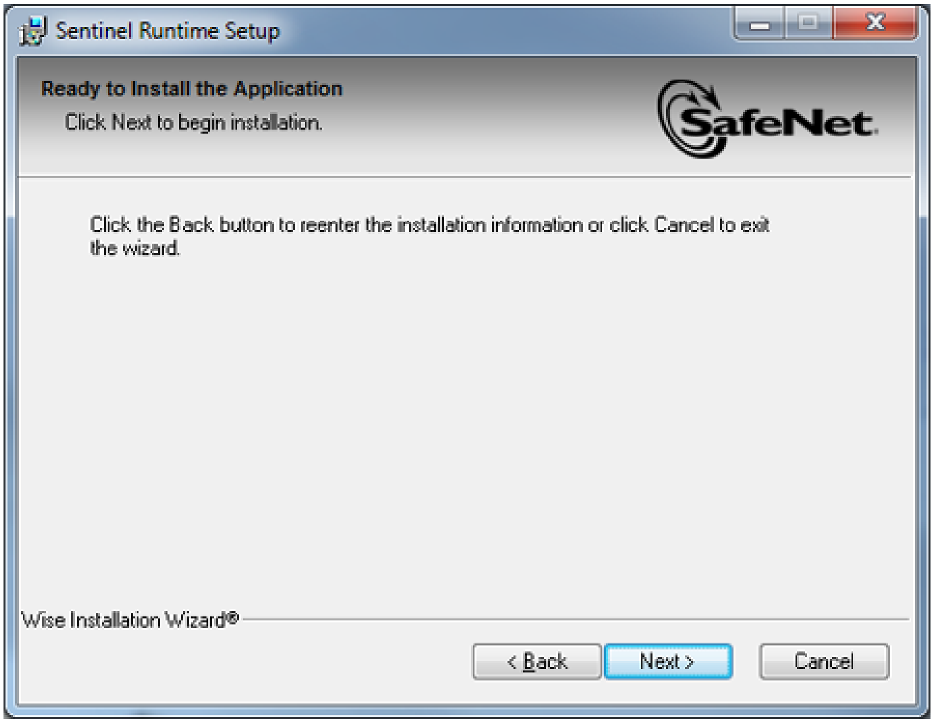
IMPORTANT INFORMATION - PLEASE READ THIS AGREEMENT CAREFULLY BEFORE USING THE CONTENTS OF THE PACKAGE AND/OR BEFORE DOWNLOADING OR INSTALLING THE SOFTWARE PRODUCT. ALL ORDERS FOR AND USE OF THE SENTINEL® LDK PRODUCTS (including without limitation, the Developer's Kit, libraries, utilities, diskettes, CD_ROM, DVD, Sentinel keys, the software component of SafeNet Sentinel LDK and the

● I accept the license agreement

○ I do not accept the license agreement

Figure 17: SafeNet License Agreement - Read and Accept

8. The SafeNet Ready to install screen is displayed. **Click Next**.



Sentinel Runtime Setup

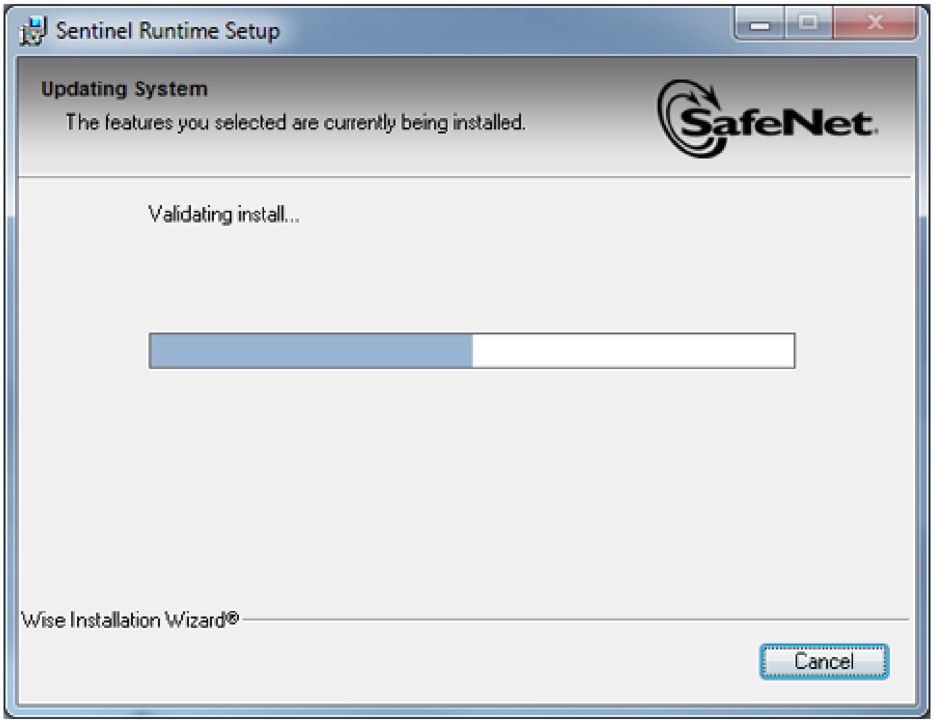
Ready to Install the Application

Click Next to begin installation.

Click the Back button to reenter the installation information or click Cancel to exit the wizard.

Figure 18: SafeNet – Ready to Install

9. The SafeNet Updating System screen is displayed.



Sentinel Runtime Setup

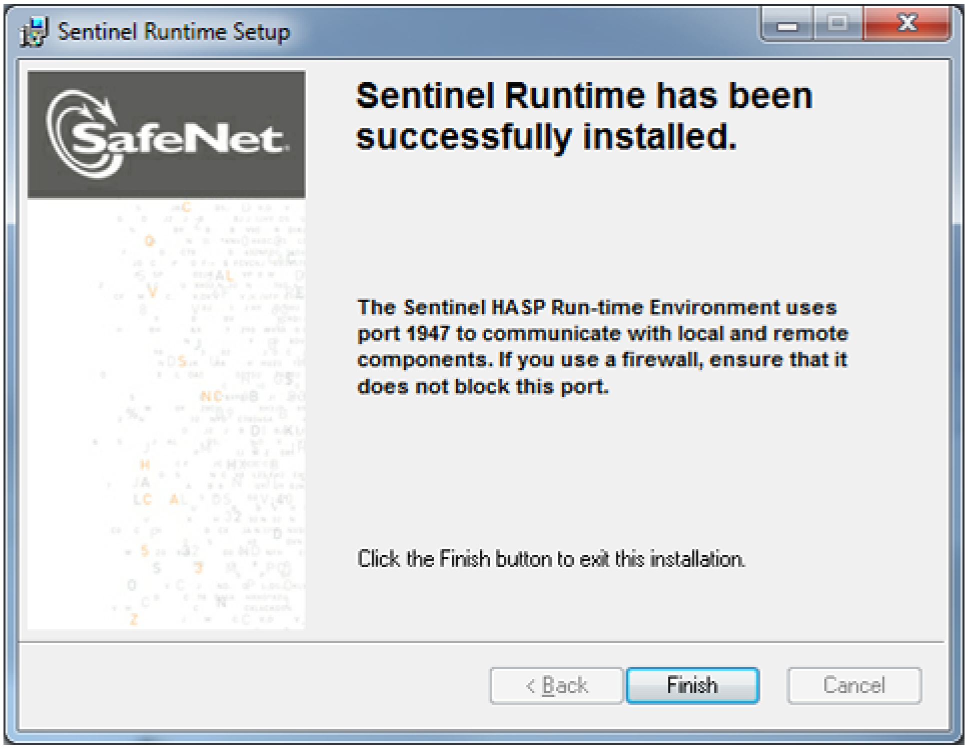
Updating System

The features you selected are currently being installed.

Validating install...

Figure 19: SafeNet Validating Install

10. The SafeNet Successfully Installed Screen is displayed. **Click Finish**.



Sentinel Runtime has been successfully installed.

The Sentinel HASP Run-time Environment uses port 1947 to communicate with local and remote components. If you use a firewall, ensure that it does not block this port.

Click the Finish button to exit this installation.

Figure 20: SafeNet Successful Installation

11. 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 UTS) after installing the driver, please reboot the server.

Uninstall Floating License – (Hardware Key)

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

NOTE: Removing or uninstalling the Floating License will disable the GSW UTS Server.

Registration via Software Serial Number

To run the GSW SSH Server you must first register the software. (*This registration is **NOT** required if you installed the Floating License, Page 22*) 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. Georgia SoftWorks will provide you with the Serial Number based on the Product ID. When you enter the Serial Number into the Registration Tool, click Register.

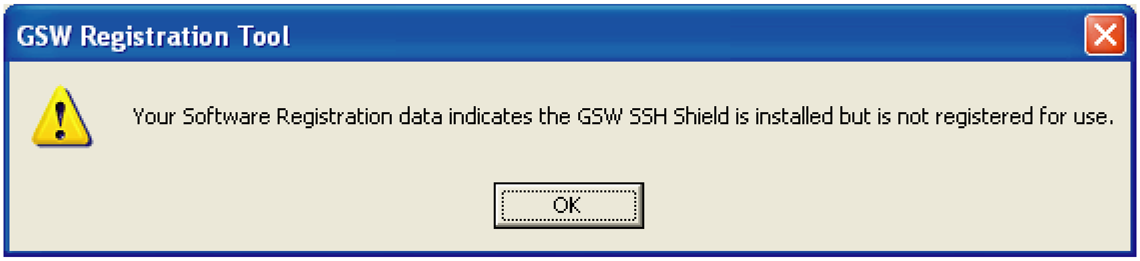
NOTE: Read System Signature chapter at the end of manual (page 73).

How to Register the Software

To run the registration software -

- Select the *Start* button on the task bar; select *Programs*, then *Georgia SoftWorks UTS Server and* right click on *Registration* and Run as Administrator.

Prior to registering the SSH Server, a reminder dialog is presented indicating that the SSH Shield is not registered.



Your Software Registration data indicates the GSW SSH Shield is installed but is not registered for use.

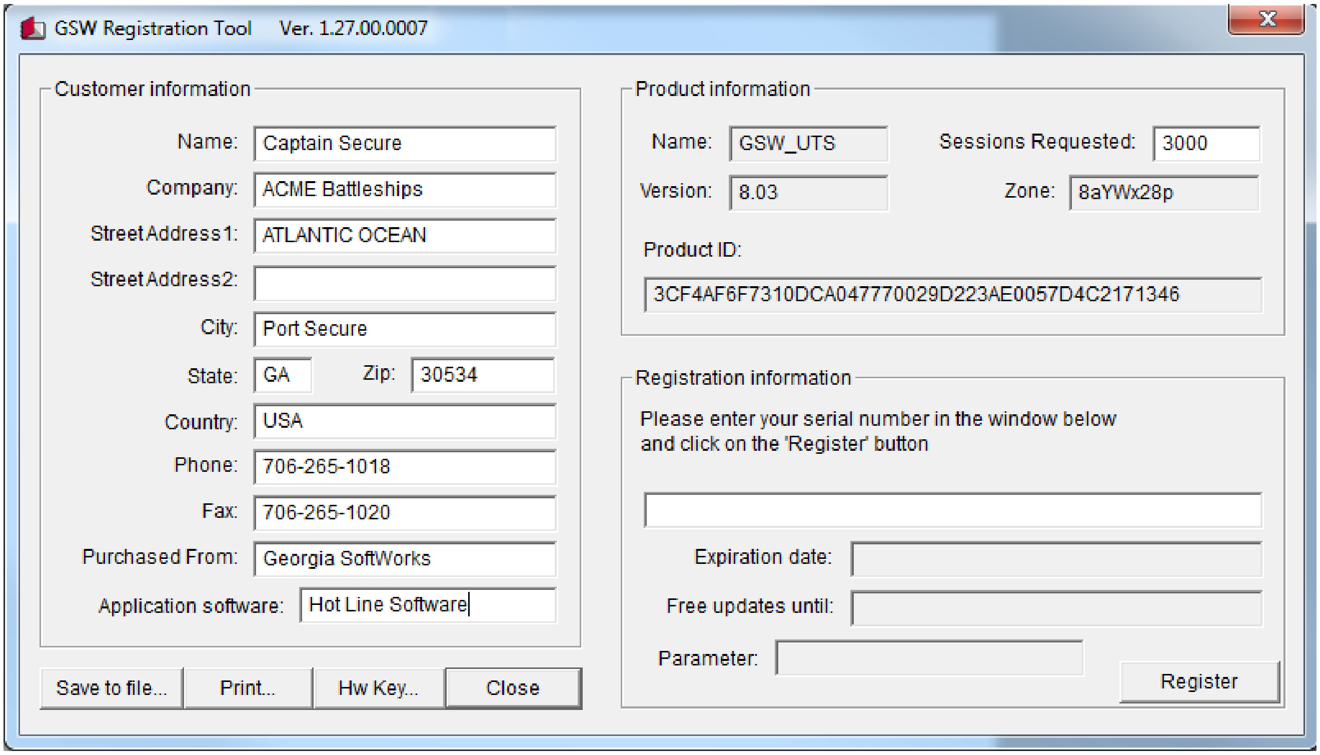
Figure 21: Registration – SSH Shield is not registered for use

The GSW SSH Server will be fully functional for a Trial Period of 30 days without requiring registering when installed for the first time on a system. ***Click OK***

IMPORTANT NOTE: If you already own a GSW Telnet Server and you want to run a 30 day trial of the GSW SSH Server then you will need to request a 30 day trial serial number from Georgia SoftWorks. Please save a copy of the current SERIAL NUMBER for your telnet server prior to installing a 30 day trial GSW SSH Server. In the event that you do not purchase the GSW SSH Server prior to the expiration of the trial, you will need to apply your original serial number to re-activate the original GSW Telnet Server.

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

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



GSW Registration Tool Ver. 1.27.00.0007

Customer information

Name: Captain Secure
Company: ACME Battleships
Street Address1: ATLANTIC OCEAN
Street Address2:
City: Port Secure
State: GA Zip: 30534
Country: USA
Phone: 706-265-1018
Fax: 706-265-1020
Purchased From: Georgia SoftWorks
Application software: Hot Line Software

Product information

Name: GSW_UTS Sessions Requested: 3000
Version: 8.03 Zone: 8aYWx28p
Product ID: 3CF4AF6F7310DCA047770029D223AE0057D4C2171346

Registration information

Please enter your serial number in the window below and click on the 'Register' button

Expiration date:
Free updates until:
Parameter:

Figure 22: GSW Registration - Initial Screen

Note that the Customer Information and Serial Number in the Registration Information may be already filled. This will be the case if the GSW UTS has previously been registered and operating as the GSW Telnet Server.

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

1. Please complete the *Customer Information*, including the *Purchased From and the Application software* fields in the Registration Screen.

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

2. Go to: http://www.georgiasoftworks.com/support_ost/open.php to submit a ticket for Registration. Complete necessary fields and attach the file you saved in the previous step. - *Preferred method*.

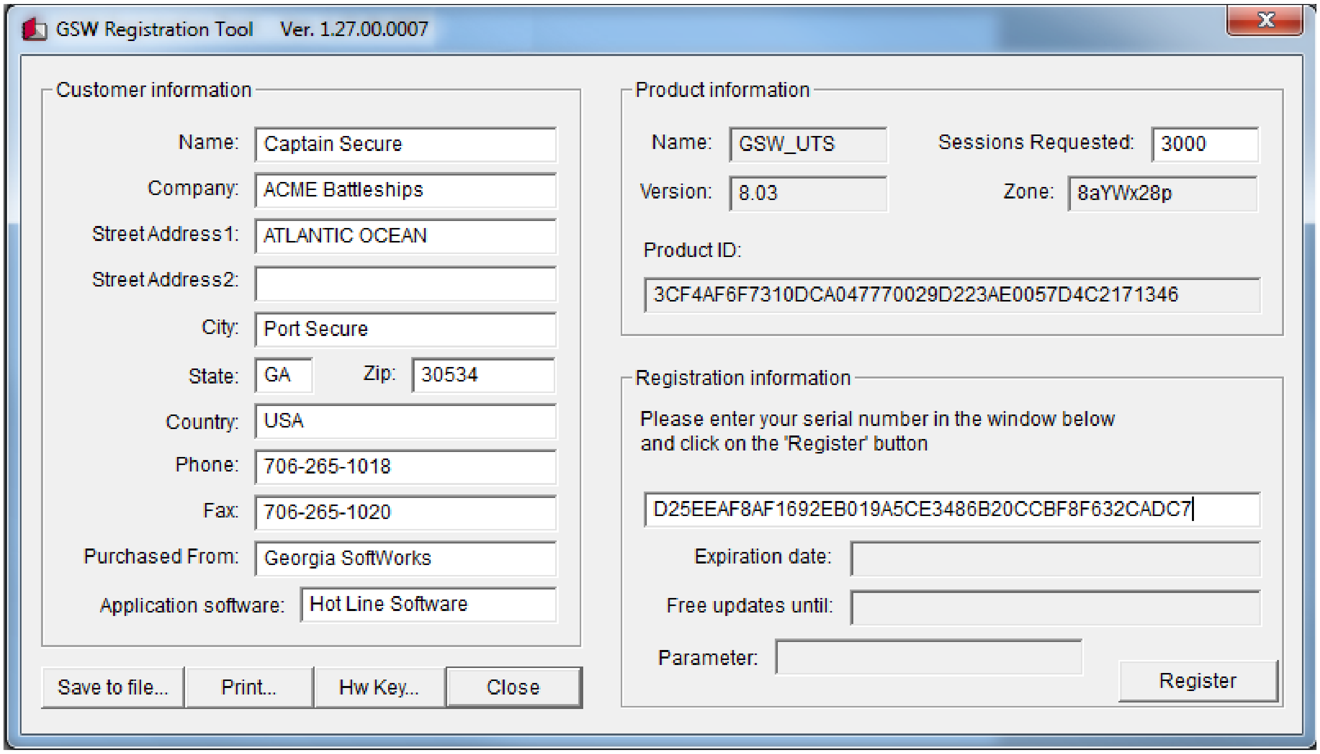
   OR

   1. Email the file to registration@georgiasoftworks.com

   2. Print the information and Fax it to Georgia SoftWorks- 706.265.1020

Once Georgia SoftWorks receives the information, we can generate a Serial Number on demand and will send it to you. You may close the registration program at this time.

3. When the Serial Number is provided run the Registration Program (see page 29) 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`).



GSW Registration Tool Ver. 1.27.00.0007

Customer information

Name: Captain Secure
Company: ACME Battleships
Street Address1: ATLANTIC OCEAN
Street Address2:
City: Port Secure
State: GA Zip: 30534
Country: USA
Phone: 706-265-1018
Fax: 706-265-1020
Purchased From: Georgia SoftWorks
Application software: Hot Line Software

Product information

Name: GSW_UTS Sessions Requested: 3000
Version: 8.03 Zone: 8aYWx28p
Product ID:
3CF4AF6F7310DCA047770029D223AE0057D4C2171346

Registration information

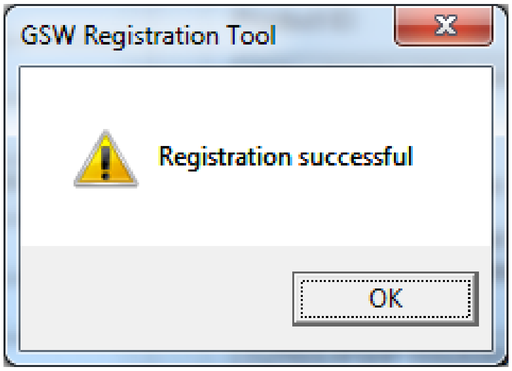
Please enter your serial number in the window below
and click on the 'Register' button

D25EEAF8AF1692EB019A5CE3486B20CCBF8F632CADC7

Expiration date:
Free updates until:
Parameter:

Figure 23: Registration - Serial Number Applied

4. **Click Register**.



GSW Registration Tool

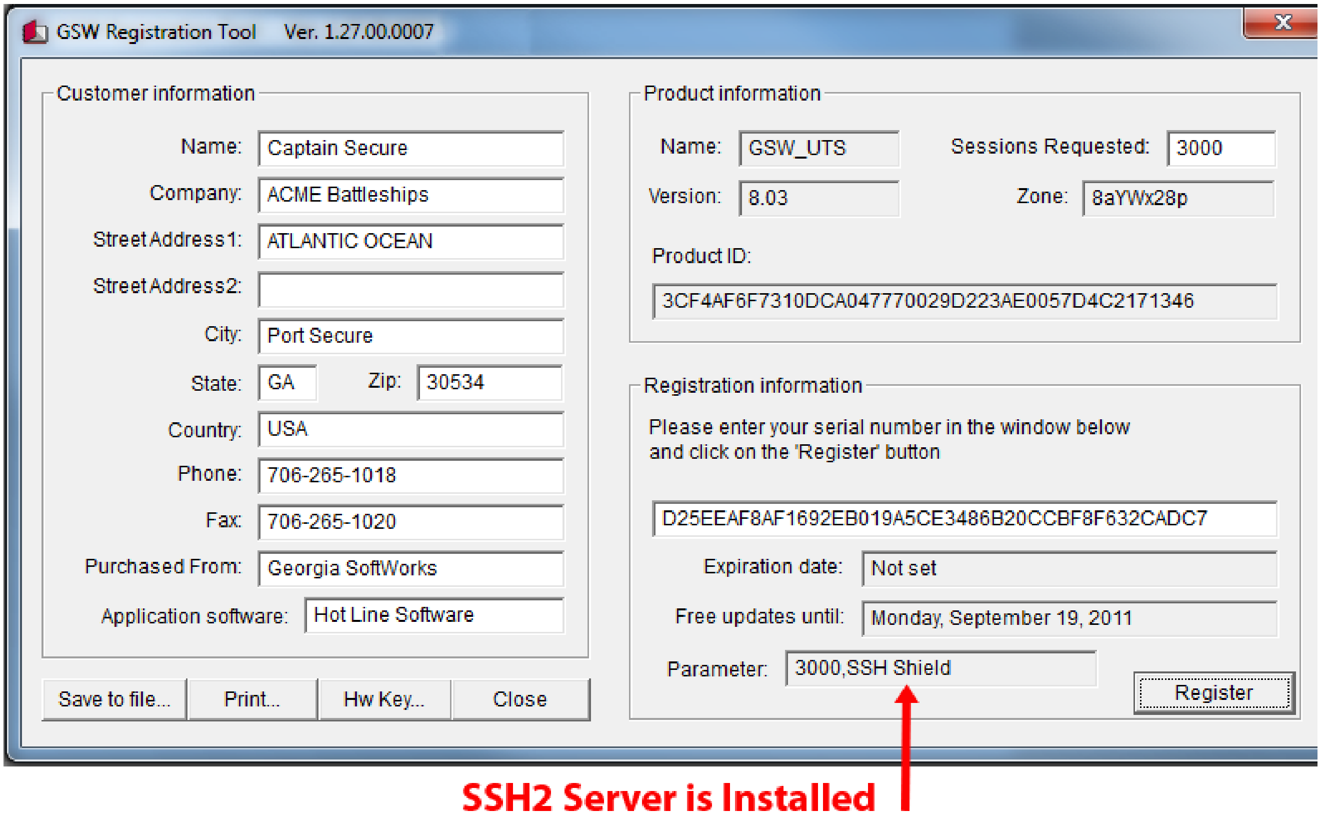
Registration successful

Figure 24: Registration Successful Screen

5. **Click OK**.

Now the software is registered.

You will notice that in this case the Parameter field in the registration form is set to 3000, SSH Shield. This indicates that the SSH Server is installed and registered and is enabled for 3000 sessions.



GSW Registration Tool Ver. 1.27.00.0007

Customer information

Name: Captain Secure
Company: ACME Battleships
Street Address1: ATLANTIC OCEAN
Street Address2:
City: Port Secure
State: GA Zip: 30534
Country: USA
Phone: 706-265-1018
Fax: 706-265-1020
Purchased From: Georgia SoftWorks
Application software: Hot Line Software

Product information

Name: GSW_UTS Sessions Requested: 3000
Version: 8.03 Zone: 8aYWx28p
Product ID:
3CF4AF6F7310DCA047770029D223AE0057D4C2171346

Registration information

Please enter your serial number in the window below
and click on the 'Register' button

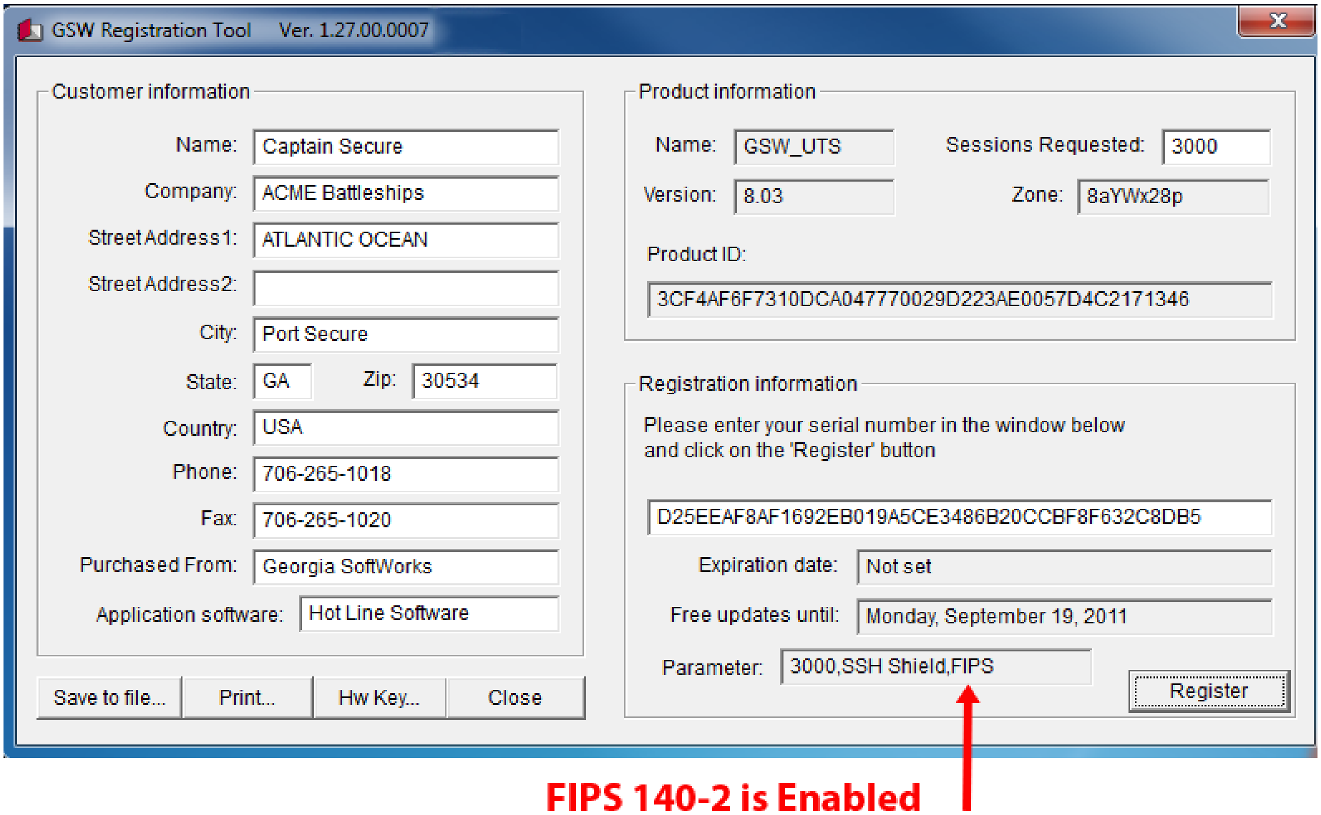
D25EEAF8AF1692EB019A5CE3486B20CCBF8F632CADC7

Expiration date: Not set
Free updates until: Monday, September 19, 2011
Parameter: 3000,SSH Shield

SSH2 Server is Installed

Figure 25: Registration Verification

If you have purchased the Federal Information Processing Standards Publications (FIPS 140-2) option, you can verify that it is enabled by viewing the registration screen as shown below in Figure 26. Please note that the GSW SSH Server must be installed for the FIPS option to be available. GSW True FIPS 140-2 compliant connections can be identified using the GSW Session Administrator in the GSW UTS Server. Please see the GSW UTS Users Guide for further details.



GSW Registration Tool Ver. 1.27.00.0007

Customer information

Name: Captain Secure
Company: ACME Battleships
Street Address1: ATLANTIC OCEAN
Street Address2:
City: Port Secure
State: GA Zip: 30534
Country: USA
Phone: 706-265-1018
Fax: 706-265-1020
Purchased From: Georgia SoftWorks
Application software: Hot Line Software

Product information

Name: GSW_UTS Sessions Requested: 3000
Version: 8.03 Zone: 8aYWx28p
Product ID: 3CF4AF6F7310DCA047770029D223AE0057D4C2171346

Registration information

Please enter your serial number in the window below
and click on the 'Register' button

D25EEAF8AF1692EB019A5CE3486B20CCBF8F632C8DB5

Expiration date: Not set
Free updates until: Monday, September 19, 2011
Parameter: 3000,SSH Shield,FIPS

FIPS 140-2 is Enabled

Figure 26: Registration - Verify that FIPS 140-2 is Enabled

IMPORTANT: READ SYSTEM SIGNATURE CHAPTER AT END OF MANUAL (page 73).

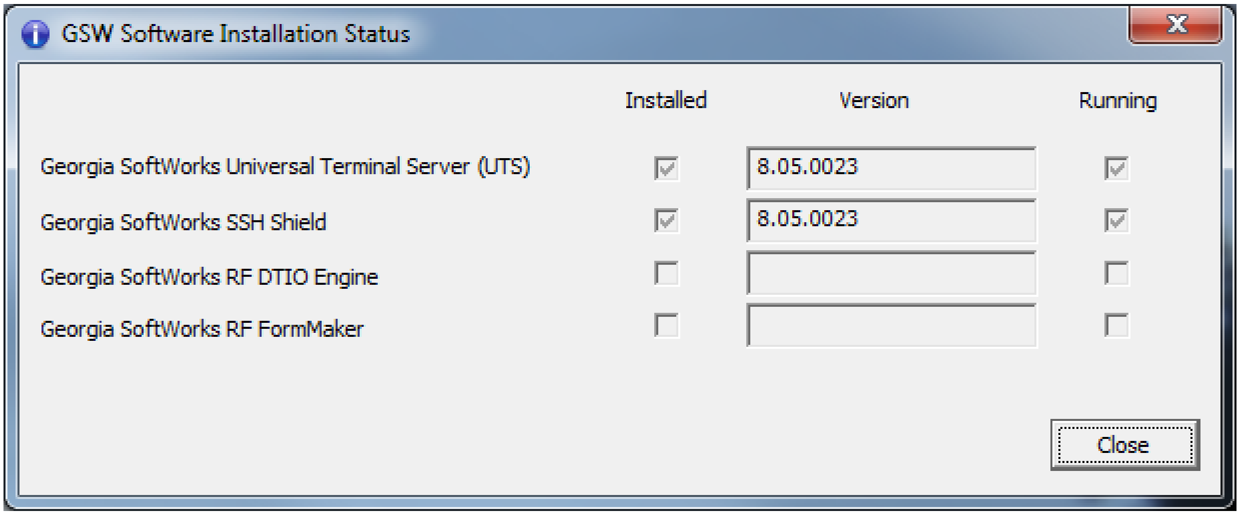
You may now run the Georgia SoftWorks SSH Server. Note that you will be able to obtain Free Updates until the date specified.

GSW SSH Server

After Installation and Registration the GSW SSH Server is ready to use.

You can further configure the SSH Server to use more advanced features as needed. See page 42. Power configuration options for the SSH Server are implemented as common Universal Terminal Server configuration parameters. See User Manual for the GSW Universal Terminal Server for information on the powerful features available to the GSW SSH Server.

Using the Installation Status Program Item within Georgia SoftWorks UTS program group, you can view the Installation Status of the GSW UTS and SSH Server.

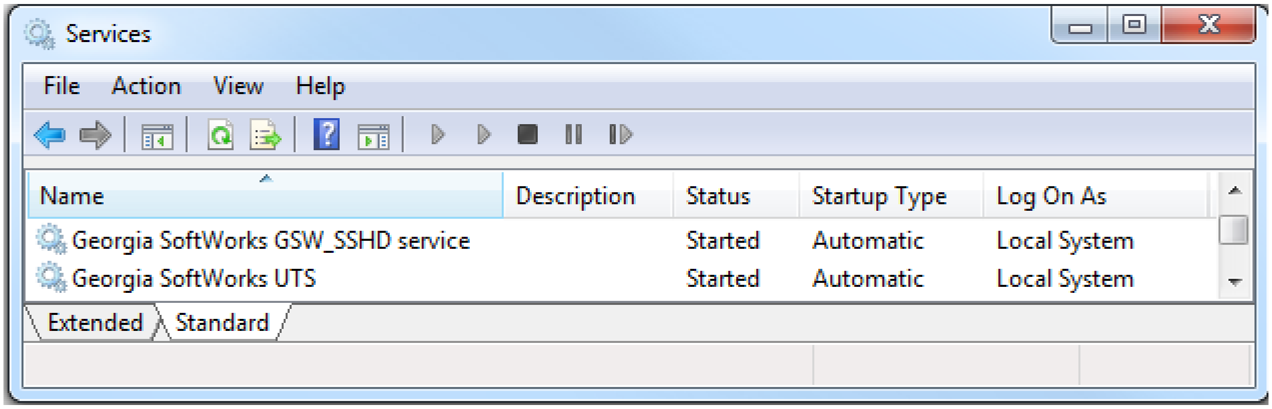


GSW Software Installation Status

	Installed	Version	Running
Georgia SoftWorks Universal Terminal Server (UTS)	☑	8.05.0023	☑
Georgia SoftWorks SSH Shield	☑	8.05.0023	☑
Georgia SoftWorks RF DTIO Engine	□		□
Georgia SoftWorks RF FormMaker	□		□

Figure 27 - GSW Software Installation Status Tool

The Windows Control Panel can be used to view and alter the status of the GSW SSH and the GSW UTS services.



Services

Name	Description	Status	Startup Type	Log On As
Georgia SoftWorks GSW_SSHD service		Started	Automatic	Local System
Georgia SoftWorks UTS		Started	Automatic	Local System

Figure 28: Control Panel - GSW SSH Services Started

The Georgia SoftWorks GSW_SSHD service and the Georgia SoftWorks Universal Terminal Server should both have a status of Started and a Startup Type of Automatic.

Using the Windows Services utility is the recommended method to start and stop the GSW services when required.

GSW FIPS 140-2 Compliant Option

GSW provides a Federal Information Processing Standards Publication (FIPS) 140-2 compliant option for those entities with requirements to meet cryptographic module security standards to protect sensitive and valuable data. FIPS standards are either mandated or recommended for use in federal government information technology (IT) systems.

Georgia SoftWorks undertook a purposed and specific development effort in order to provide required FIPS 140-2 compliant SSH server and client software to the United States Military. Having completed this task, GSW is able to make this software available to other branches of the Federal government as well as State governments and other institutions including research, educational and commercial.

Software Requirements

In addition to the development required for FIPS 140-2 compliance of the GSW server and client software, the GSW mobile clients must run on an operating system that is FIPS 140-2 certified or provides a cryptographic module that has been certified.

In order that your SSH connections are FIPS 140-2 compliant you must ensure that you have the minimum GSW software versions as well as the proper Windows Mobile/CE operating system version.

Software Requirements for FIPS Compliancy

GSW Software	Version			Certificate
GSW UTS Server	7.50+			#918
GSW SSH Server	7.50+			#918
GSW Desktop Clients	7.50+			#918
GSW CE/Mobile Clients	7.50+			#560,# 825

Table 1: GSW Software versions required for FIPS 140-2

Required Device Operating System for Mobile/CE Clients				Certificate
Windows CE 5.0 Depends on Vendor - *Made available to OEMs via Windows Update 061211_KB911762*				#560
Windows Mobile 5.0				#560
Windows CE 6.0				#825
Windows Mobile 6.0+				#825

Table 2: Device Operating System Versions Required for FIPS 140-2

The significant aspect of the client device operating system is that the version of the cryptographic module rsaenh.dll must be NIST (National Institute of Standards and Technology) certified, which begins with build 14343.0.0. With Windows CE 5.0 extra attention should be taken to ensure the version of rsaenh.dll. This may require contacting the device vendor to determine the correct version number of that cryptographic module.

Enable Option

FIPS 140-2 must be enabled on both the GSW SSH server and the GSW clients to complete a FIPS 140-2 compliant connection.

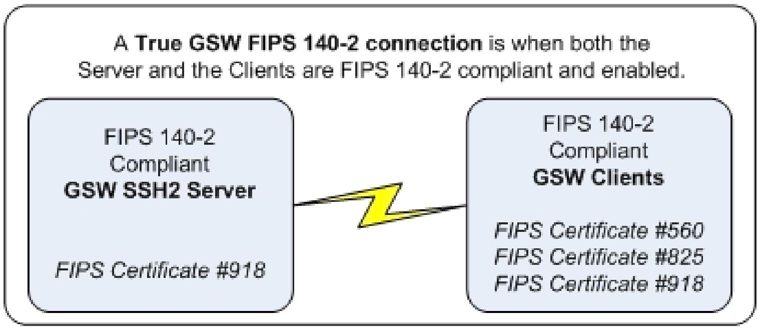
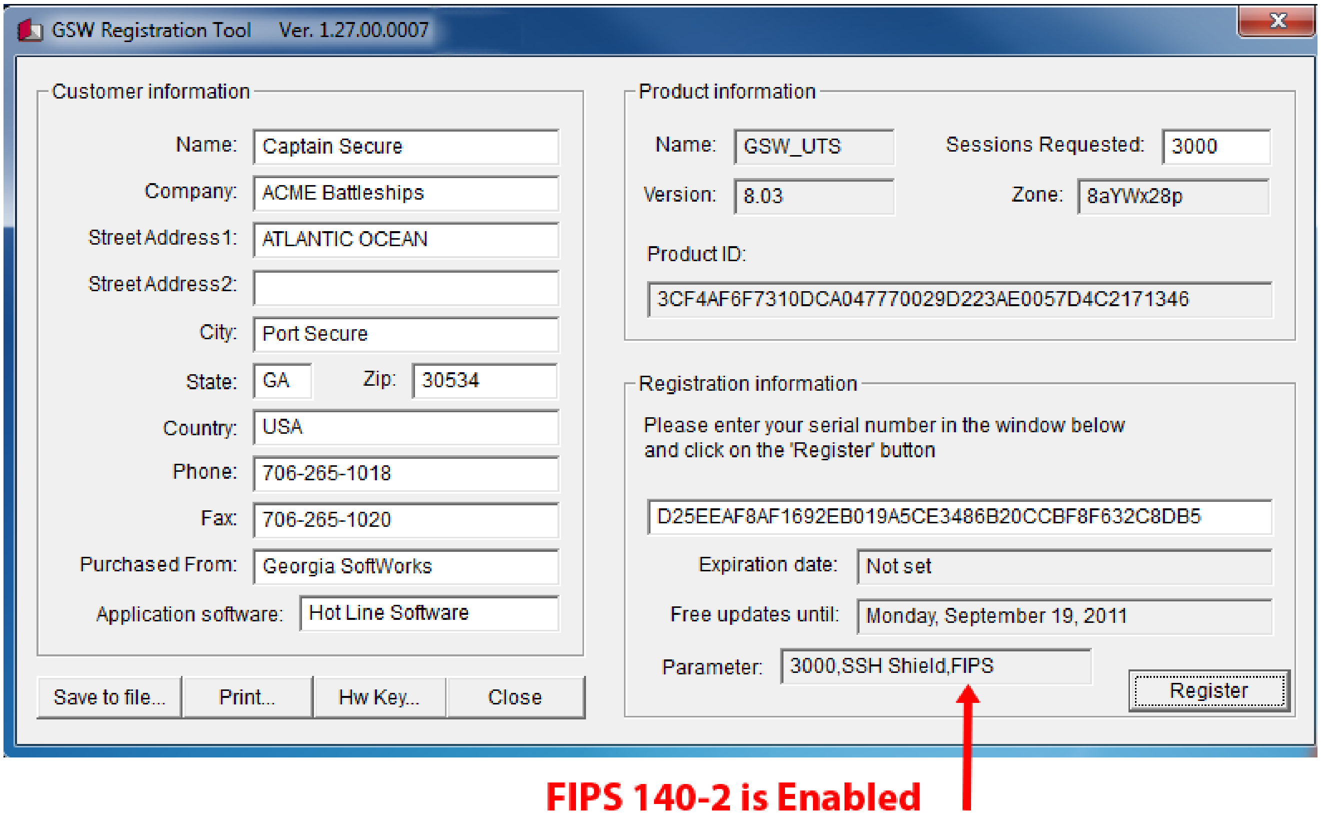

A **True GSW FIPS 140-2 connection** is when both the Server and the Clients are FIPS 140-2 compliant and enabled.
FIPS 140-2 Compliant **GSW SSH2 Server**
FIPS Certificate #918
FIPS 140-2 Compliant **GSW Clients**
FIPS Certificate #560
FIPS Certificate #825
FIPS Certificate #918

Figure 29: GSW True FIPS 140-2 Connection – Server and Client

ENABLE FIPS 140-2 ON SSH SERVER

Proper registration will enable the FIPS option on the SSH Server. View the registration tool to ensure the GSW SSH Server is registered with the FIPS option enabled.

Select the Start button on the task bar; select Programs, then Georgia SoftWorks UTS and then Registration. The current registration information is displayed.



Customer information

Name: Captain Secure
Company: ACME Battleships
Street Address1: ATLANTIC OCEAN
Street Address2:
City: Port Secure
State: GA Zip: 30534
Country: USA
Phone: 706-265-1018
Fax: 706-265-1020
Purchased From: Georgia SoftWorks
Application software: Hot Line Software

Product information

Name: GSW_UTS Sessions Requested: 3000
Version: 8.03 Zone: 8aYWx28p
Product ID:
3CF4AF6F7310DCA047770029D223AE0057D4C2171346

Registration information

Please enter your serial number in the window below
and click on the 'Register' button

D25EEAF8AF1692EB019A5CE3486B20CCBF8F632C8DB5
Expiration date: Not set
Free updates until: Monday, September 19, 2011
Parameter: 3000,SSH Shield,FIPS

FIPS 140-2 is Enabled

Figure 30: FIPS 140-2 Option Enabled

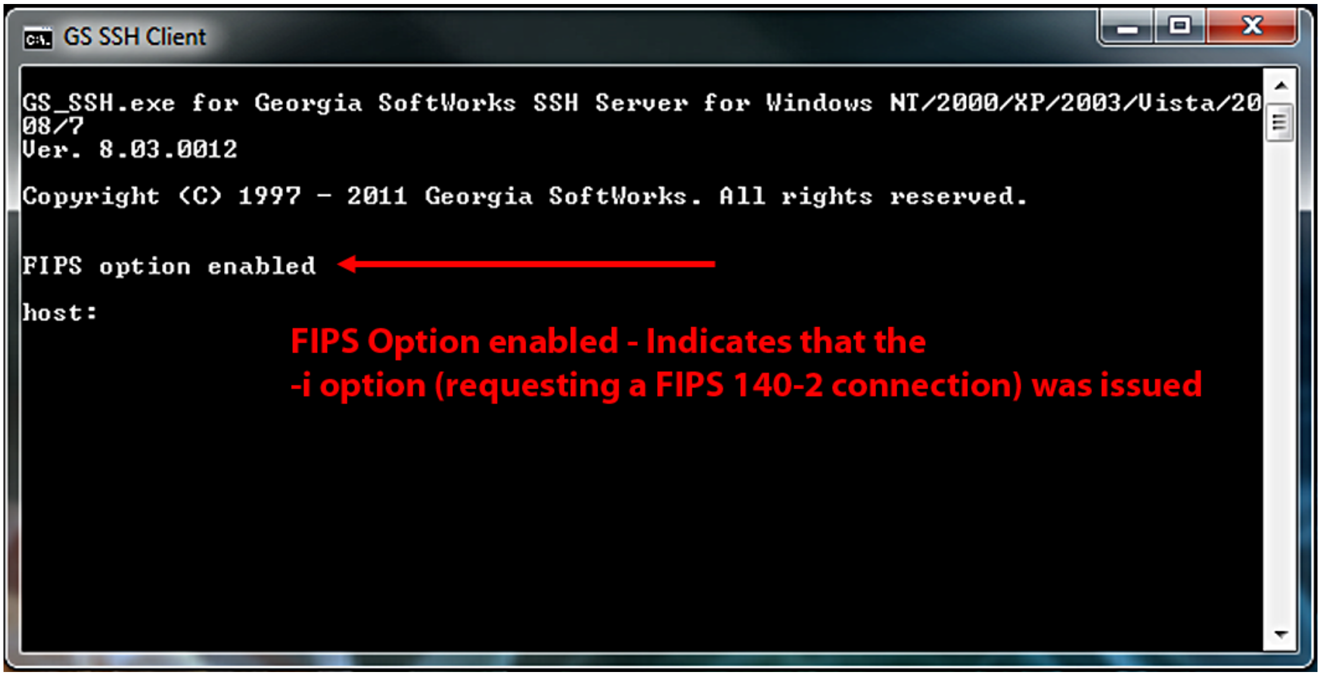
In the `Parameter` field you will observe the number of concurrent sessions allowed followed by the text "SSH Shield" indicating that the GSW SSH server is licensed and FIPS indicating that the FIPS 140-2 option is enabled.

ENABLE FIPS 140-2 ON GSW MOBILE/CE and DESKTOP CLIENTS

Desktop Client

Use the "-i" command line parameter when launching on GSW Desktop clients to enable FIPS 140-2 option. Please see the UTS user's guide for a description and examples of desktop client command line options.

When FIPS 140-2 enabled GSW desktop clients are launched you will receive a banner indicating that the "-i" command line parameter was issued by the client.



```
GS_SSH.exe for Georgia SoftWorks SSH Server for Windows NT/2000/XP/2003/Vista/20
08/7
Ver. 8.03.0012

Copyright (C) 1997 - 2011 Georgia SoftWorks. All rights reserved.

FIPS option enabled

host:
```

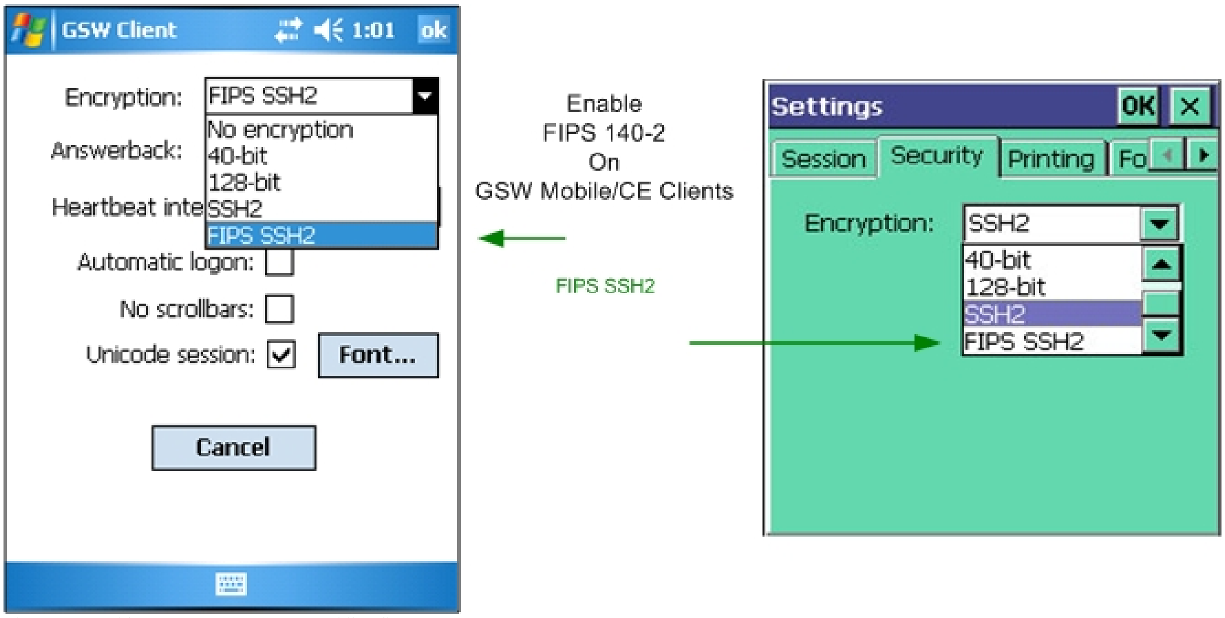
FIPS Option enabled - Indicates that the -i option (requesting a FIPS 140-2 connection) was issued

Figure 31: Desktop Client "-i" option issued

Please note that to have a both ends (client and server) FIPS 140-2 compliant, FIPS 140-2 must be enabled on the GSW SSH Server too.

Mobile/CE Clients

Enable FIPS140-2 on GSW Mobile/CE clients via the Encryption list box. The Mobile/CE device screen that you see will be similar to the ones below.



Encryption: FIPS SSH2

Unicode session: ☑

Encryption: SSH2

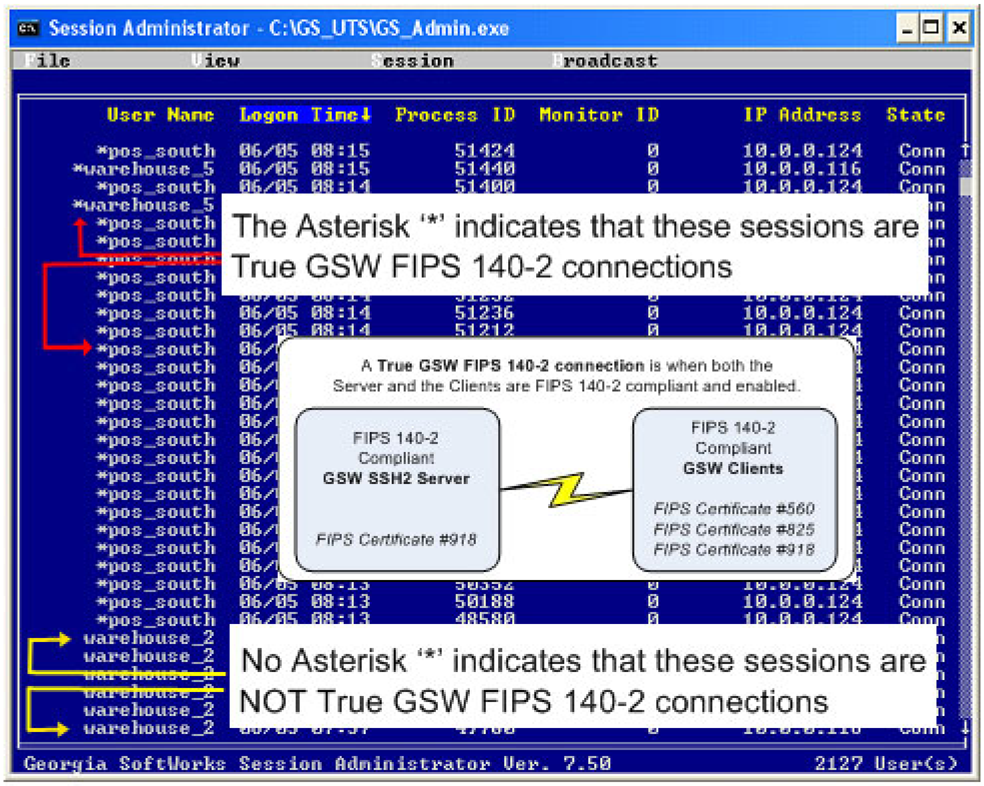
Figure 32: Enable FIPS 140-2 on GSW Mobile Clients

Please note that to have a both ends (client and server) FIPS 140-2 compliant, FIPS 140-2 must be enabled on the GSW SSH Server too.

FIPS 140-2 Connections

Using the UTS Session Administrator you can verify True GSW FIPS 140-2 compliant connections. An asterisk "*" will be prepended to the user name for connections that are FIPS 140-2 compliant for both the client and the server.

The possibility exists that a third party client may be FIPS 140-2 compliant but it cannot be verified unless it is a GSW client.



```
       User Name  Logon Time↓  Process ID  Monitor ID     IP Address  State

      *pos_south  06/05 08:15       51424           0     10.0.0.124   Conn
    *warehouse_5  06/05 08:15       51440           0     10.0.0.116   Conn
      *pos_south  06/05 08:14       51400           0     10.0.0.124   Conn
    *warehouse_5                                                         n
      *pos_south                                                         n
      *pos_south                                                         n
                                                                         n
      *pos_south                                                         n
      *pos_south                                                       Conn
      *pos_south  06/05 08:14       51236           0     10.0.0.124   Conn
      *pos_south  06/05 08:14       51212           0     10.0.0.124   Conn
      *pos_south  06/                                              1   Conn
      *pos_south  06/                                              1   Conn
      *pos_south  06/                                              1   Conn
      *pos_south  06/                                              1   Conn
      *pos_south  06/                                              1   Conn
      *pos_south  06/                                              1   Conn
      *pos_south  06/                                              1   Conn
      *pos_south  06/                                              1   Conn
      *pos_south  06/                                              1   Conn
      *pos_south  06/                                              1   Conn
      *pos_south  06/                                              1   Conn
      *pos_south  06/                                              1   Conn
      *pos_south  06/                                              1   Conn
      *pos_south                                                       Conn
      *pos_south  06/05 08:13       50188           0     10.0.0.124   Conn
      *pos_south  06/05 08:13       48580           0     10.0.0.124   Conn
     warehouse_2                                                         n
     warehouse_2                                                         n
     warehouse_2                                                         n
     warehouse_2                                                         n
     warehouse_2                                                         n
     warehouse_2                                                       Conn
Georgia SoftWorks Session Administrator Ver. 7.50             2127 User(s)
```

The Asterisk '*' indicates that these sessions are True GSW FIPS 140-2 connections

A **True GSW FIPS 140-2 connection** is when both the Server and the Clients are FIPS 140-2 compliant and enabled.

No Asterisk '*' indicates that these sessions are NOT True GSW FIPS 140-2 connections

Figure 33: Verify FIPS 140-2 Compliant Connections

.

Configuration

No configuration is required beyond installation in order for the GSW SSH Server to operate providing secure logon, strong encryption and data integrity on an insecure network. Optional SSH Configuration is provided to implement advanced features. The GSW SSH Server reads configuration values each time the GSW_SSHD service is started.

Please consider the optional GSW UTS GUI Configuration tool for SSH provisioning or use the methods described below.

Registry Key Locations

Registry keys referenced in this User's Guide are located here on 32 bit operating systems

```
HKEY_LOCAL_MACHINE\SOFTWARE\Georgia SoftWorks\GSW_SSHD\Parameters
```

Registry keys referenced in this User's Guide are located here on 64 bit operating systems

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Georgia SoftWorks\GSW_SSHD\Parameters
```

Allow only AES-256 Encryption

The default configuration restricts connections to those clients offering only the strongest encryption AES-256. In the event you do not want to require the strongest encryption then the GSW SSH Server can be configured to allow the client to negotiate the encryption.

This configuration is contained in the registry key `bAES256Only` which is a flag. The key is:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Georgia SoftWorks\GSW_SSHD\Parameters\bAES256Only
```

The default value is 1. (Only allow clients with AES-256 to connect)

You may allow the SSH client to negotiate the encryption strength by setting it to `0x0`.

The following is a procedure to change the registry key for the AES-256 Encryption Only flag.

1. Click the **Start** button at the bottom left corner of your screen.
2. Click **RUN**
3. Type REGEDIT
4. Click **OK**
5. Select Windows item **HKEY_LOCAL_MACHINE**
6. Select the menu item **Edit**

7. Move the mouse pointer and click **Find**

8. Type **bAES256Only**

9. Click on **Find Next**

10. Select the menu item **Edit** and then click on **Modify**

11. Enter the new value for the Allow AES-256 Only flag and click **OK**

The new value will take effect when the GSW SSHD service is restarted.

Change the SSH Port Number.

The default port number is port 22. You can change the port number to the port of your choice. **Important:** Be sure that you also change the port number on the SSH clients to the same port number configured on the SSH Server.

In the event you want to change the SSH port on the server you can do so by changing the following registry key.

This configuration is contained in the registry key `usGSWSSHDPort` which is a number. The key is:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Georgia SoftWorks\GSW_SSHD\Parameters\usGSWSSHDPort
```

The default value is 22.

This following is a procedure to change the registry key for the SSH port number.

1. Click the **Start** button at the bottom left corner of your screen.

2. Click **RUN**

3. Type `REGEDIT`

4. Click **OK**

5. Select Windows item **HKEY_LOCAL_MACHINE**

6. Select the menu item **Edit**

7. Move the mouse pointer and click **Find**

8. Type **`usGSWSSHDPort`**

9. Click on **Find Next**

10. Select the menu item **Edit** and then click on **Modify**

11. Enter the new value for the SSH Port number and click **OK**

The new value will take effect when the GSW SSHD service is restarted.

Location of SSH Server RSA Private Key.

The SSH Server RSA Private Key is in an encrypted file and is in the PEM format.

This configuration is contained in the registry key `szServerRSAKeyFile` which is a text string. You can change the location by modifying the registry key.

The key is:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Georgia SoftWorks\GSW_SSHD\Parameters\szServerRSAKeyFile
```

The default value is the installation folder for the GSW SSH Shield.

```
C:\Program Files\Georgia SoftWorks\Georgia SoftWorks SSH Shield\sshd_rsa.key
```

The following is a procedure to change the Location of SSH Server RSA Private Key.

1. Click the **Start** button at the bottom left corner of your screen.
2. Click **RUN**
3. Type `REGEDIT`
4. Click **OK**
5. Select Windows item **HKEY_LOCAL_MACHINE**
6. Select the menu item **Edit**
7. Move the mouse pointer and click **Find**
8. Type **`szServerRSAKeyFile`**
9. Click on **Find Next**
10. Select the menu item **Edit** and then click on **Modify**
11. Enter the new value for the Server RSA Key Location and click **OK**

The new value will take effect when the GSW SSHD service is restarted.

Location of SSH Server DSA Private Key.

The SSH Server DSA Private Key is in an encrypted file and is in the PEM format.

This configuration is contained in the registry key `szServerDSAKeyFile` which is a text string. You can change the location by modifying the registry key.

The key is:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Georgia SoftWorks\GSW_SSHD\Parameters\szServerDSAKeyFile
```

The default value is the installation folder for the GSW SSH Shield.

```
C:\Program Files\Georgia SoftWorks\Georgia SoftWorks SSH Shield\sshd_dsa.key
```

1. Click the **Start** button at the bottom left corner of your screen.
2. Click **RUN**
3. Type `REGEDIT`
4. Click **OK**
5. Select Windows item **HKEY_LOCAL_MACHINE**
6. Select the menu item **Edit**
7. Move the mouse pointer and click **Find**
8. Type **`szServerDSAKeyFile`**
9. Click on **Find Next**
10. Select the menu item **Edit** and then click on **Modify**
11. Enter the new value for the Server DSA Key Location and click **OK**

The new value will take effect when the GSW SSHD service is restarted.

Location of SSH Server ECDSA Private Key.

The SSH Server Elliptic Curve Cryptography DSA Private Key is in an encrypted file and is in the PEM format.

This configuration is contained in the registry key `szServerECDSAKeyFile` which is a text string. You can change the location by modifying the registry key.

The key is:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Georgia SoftWorks\GSW_SSHD\Parameters\szServerECDSAKeyFile
```

The default value is the installation folder for the GSW SSH Shield.

```
   C:\Program Files\Georgia SoftWorks\Georgia SoftWorks SSH Shield\sshd_ecdsa.key
```

1. Click the **Start** button at the bottom left corner of your screen.

2. Click **RUN**

3. Type `REGEDIT`

4. Click **OK**

5. Select Windows item **HKEY_LOCAL_MACHINE**

6. Select the menu item **Edit**

7. Move the mouse pointer and click **Find**

8. Type **`szServerECDSAKeyFile`**

9. Click on **Find Next**

10. Select the menu item **Edit** and then click on **Modify**

11. Enter the new value for the Server ECDSA Key Location and click **OK**

The new value will take effect when the GSW SSHD service is restarted.

Location of Fingerprints for all Host Keys.

The file HostFingerPrints.txt in the Georgia SoftWorks SSH Shield installation folder[2] contains key fingerprints for all host keys offered for server-to-client authentication. These key fingerprints may be entered for host fingerprint configuration of the Georgia SoftWorks Business Tunnel.

The file is formatted as shown below:

```
RSA key fingerprint ..... f7:4f:8e:2f:ae:12:05:8a:50:5b:02:e0:89:bc:e1:7f

DSA key fingerprint ..... d4:62:8d:5s:b3:b8:43:b3:5c:1e:ac:3c:b6:3a:f7:bb

ECDSA key fingerprint ... f1:93:63:15:89:0c:6d:73:32:8e:b2:6e:82:6d:d7:c1
```

Internal SSH Activity Logging FLAG for Debugging.

In the event that GSW Technical Support requires additional information, you may need to turn on SSH internal activity logging.

You can activate the internal SSH activity logging by modifying the following registry key.

This configuration is contained in the registry key `bEnableWODLog` which is a flag. The key is:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Georgia SoftWorks\GSW_SSHD\Parameters\bEnableWODLog
```

The default value is **0.**

1. Click the **Start** button at the bottom left corner of your screen.
2. Click **RUN**
3. Type `REGEDIT`
4. Click **OK**
5. Select Windows item **HKEY_LOCAL_MACHINE**
6. Select the menu item **Edit**
7. Move the mouse pointer and click **Find**
8. Type **`bEnableWODLog`**
9. Click on **Find Next**
10. Select the menu item **Edit** and then click on **Modify**

[2] Usually 'C:\Program Files\Georgia SoftWorks\Georgia SoftWorks SSH Shield

11. Enter the new value for the Enable Activity Logging and click **OK**

The new value will take effect when the GSW SSHD service is restarted.

Internal SSH Activity Log file location for Debugging.

In the event that GSW Technical Support requires additional information, you may need change the SSH internal activity log file location.

You can modify the internal SSH activity log file name and location by modifying the following registry key.

This configuration is contained in the registry key `szWODLogFile` which is a text string. The key is:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Georgia SoftWorks\GSW_SSHD\Parameters\szWODLogFile
```

The default value is the log folder in the GSW UTS Installation directory. Usually this is:

```
C:\GS_UTS\log
```

NOTE: bEnableWODLog must be set to 1 for the log file to operate.

Note: (you must be on the Windows NT/XP/VISTA/2000+ system that the Georgia SoftWorks SSH Server is installed. However, you may connect to the SSH Registry from a remote location).

1. Click the **Start** button at the bottom left corner of your screen.
2. Click **RUN**
3. Type `REGEDIT`
4. Click **OK**
5. Select Windows item **HKEY_LOCAL_MACHINE**
6. Select the menu item **Edit**
7. Move the mouse pointer and click **Find**
8. Type **`szWODLogFile`**
9. Click on **Find Next**
10. Select the menu item **Edit** and then click on **Modify**
11. Enter the new value for the Activity Log File Name and Location and click **OK**

The new value will take effect when the GSW SSHD service is restarted.

SSH Server Mapping Tool for Certificates and Public Keys

Georgia SoftWorks researched and developed an innovative, easy to use, and secure implementation of Digital Certificates[3]. The result of this effort is the GSW SSH SHIELD Certificate Mapping Tool.

The entire configuration is done through a GUI with wizard style dialogs reminiscent of IIS certificate-to-user account mapping. The solution preserves all of the cryptographic strength of the public key solution, adds convenient, well scaling, certificate-to-user account mapping options while eliminating the time consuming, error-prone, and potentially insecure setup.

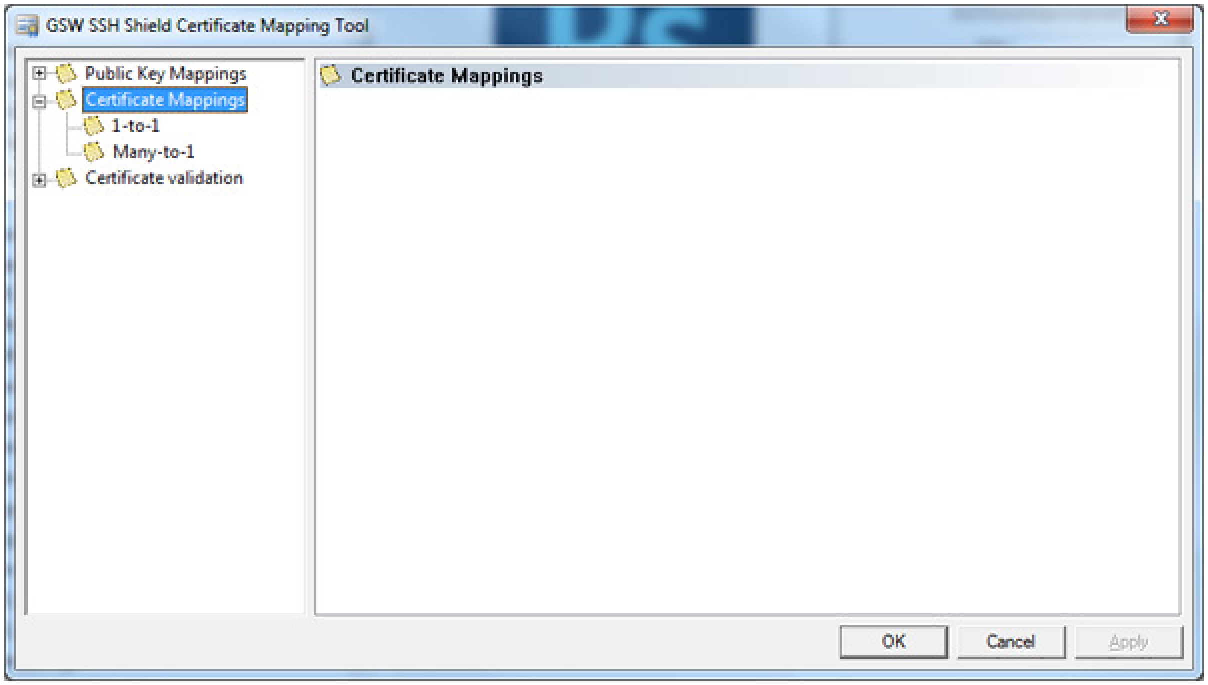


Figure 34 - SSH Certificate Mapping Tool

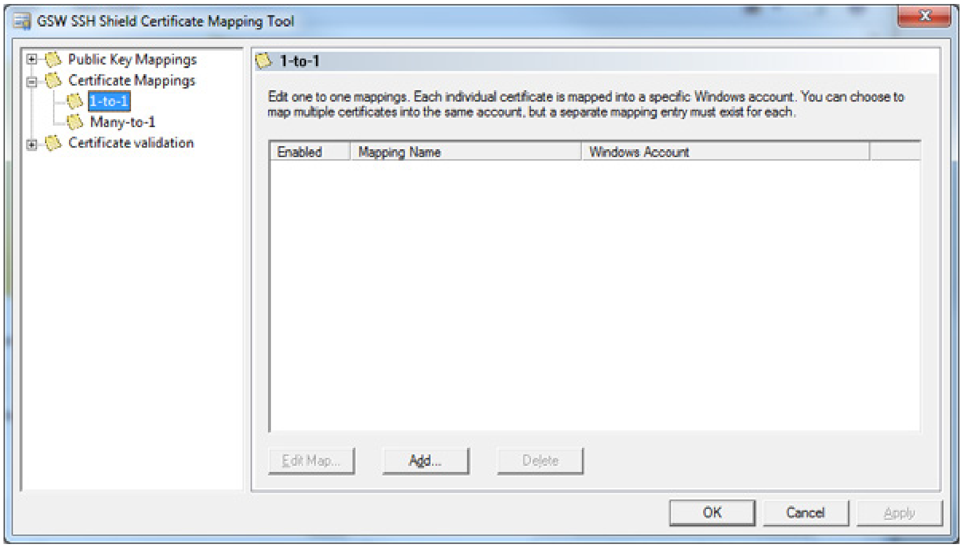
The overall solution allows authenticating SSH users who log on with a client certificate by mapping the certificates to Windows user accounts. The client certificates are analyzed and used to either deny or grant host access to a connecting session.

There are two methods in which one can map certificates.

[3] A Digital Certificate binds a name (or identity) to a public key value and is used in verifying the identity of the certificates owner.

Certificate One-to-one mapping

'**One-to-one**' mapping maps a individual client certificate to a individual Windows user account. The SSH-2 server compares certificates from a pre-configured list with the client certificate that is sent by the SSH-2 client. An identical match must occur for the mapping to proceed.

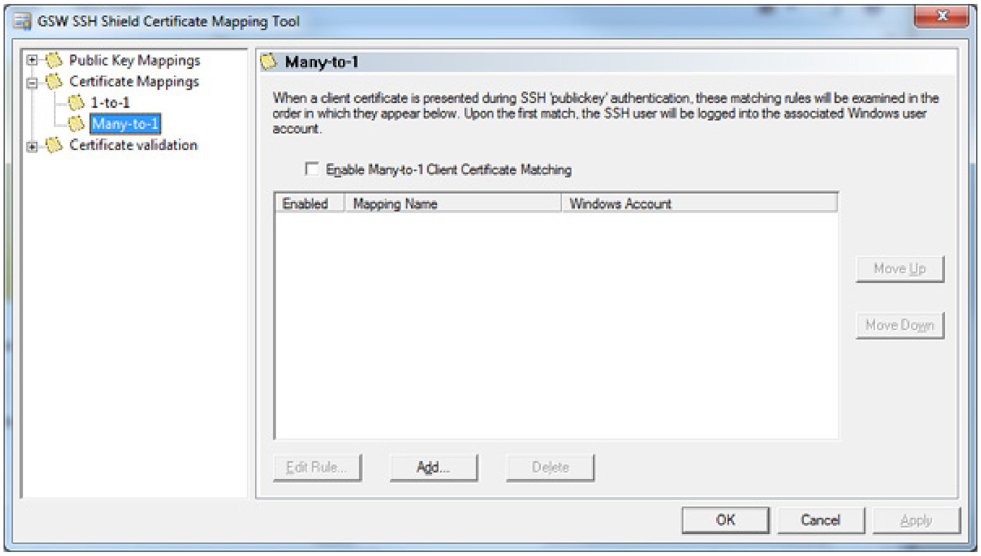


Edit one to one mappings. Each individual certificate is mapped into a specific Windows account. You can choose to map multiple certificates into the same account, but a separate mapping entry must exist for each.

Figure 35 - One-to-one certificate mapping

Certificate Many-to-one mapping

'**Many-to-one**' mapping maps multiple certificates to an individual Windows user account. It uses wildcard matching rules to define the certificate criteria for mapping. This type of mapping does not compare the actual client certificate. Instead, it accepts all client certificates that meet specific criteria. If a certificate matches the rules, it is mapped to the indicated user account. Typically one would also select a Certificate Trust List (CTL) to assure the client certificates are truly trustworthy. CTLs make it possible to limit the number of acceptable root CAs which are able to issue certificates to users.



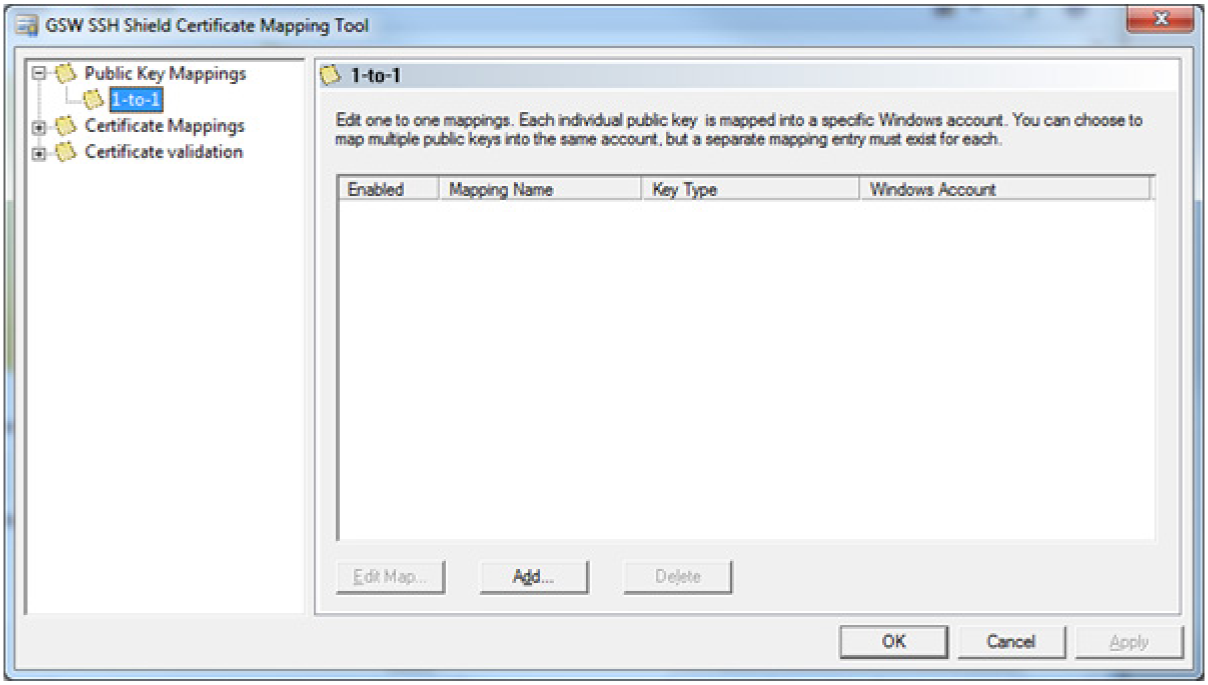
When a client certificate is presented during SSH 'publickey' authentication, these matching rules will be examined in the order in which they appear below. Upon the first match, the SSH user will be logged into the associated Windows user account.

☐ Enable Many-to-1 Client Certificate Matching

Figure 36 - Many-to-one certificate mapping

Public Key 1-to-1 mapping

Public Key '1to1' mapping provides a very nice method to allow public key to user account mapping.

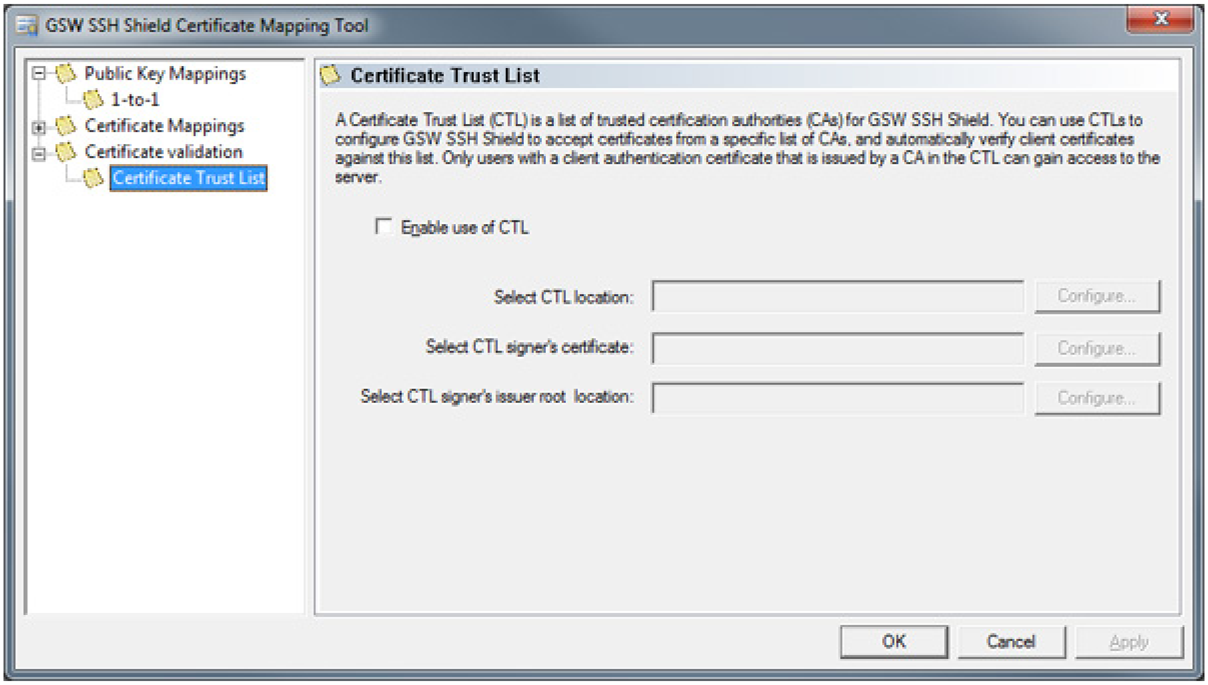


Edit one to one mappings. Each individual public key is mapped into a specific Windows account. You can choose to map multiple public keys into the same account, but a separate mapping entry must exist for each.

Figure 37 - Public Key Mappings - 1-to-1

Certification Validation – Certificate Trust List

You can also configure Certificate Trust List (CTL) with the GSW Mapping Tool.



A Certificate Trust List (CTL) is a list of trusted certification authorities (CAs) for GSW SSH Shield. You can use CTLs to configure GSW SSH Shield to accept certificates from a specific list of CAs, and automatically verify client certificates against this list. Only users with a client authentication certificate that is issued by a CA in the CTL can gain access to the server.

☐ Enable use of CTL

Select CTL location:

Select CTL signer's certificate:

Select CTL signer's issuer root location:

Figure 38 - Certificate Validation Certificate Trust List

SSH Clients

In addition to the GSW SSH clients, the Georgia SoftWorks SSH Server is compatible with all SSH compliant third party clients.

GSW SSH CLIENTS

All the powerful and popular GSW Client options and features described in the GSW UTS are available for the GSW SSH server except where specifically noted. Georgia SoftWorks offers SSH Clients for the following platforms:

Operating System	GSW SSH Client	Method to Launch Client
Window 98/ME	Yes	Program Group Shortcut
Windows NT 4.0	Yes	Program Group Shortcut
Windows 2000	Yes	Program Group Shortcut
Windows XP	Yes	Program Group Shortcut
Windows VISTA	Yes	Program Group Shortcut
Windows 2003	Yes	Program Group Shortcut
Windows 7	Yes	Program Group Shortcut
Windows 8	Yes	Program Group Shortcut
Windows 2008/R2	Yes	Program Group Shortcut
Windows 2012/R2	Yes	Program Group Shortcut
Windows CE .NET 4.2+	Yes	Device Desktop Shortcut
Windows Mobile	Yes	Device: Start|Programs|GSW Telnet and SSH
Pocket PC 2002	No	
Pocket PC 2003	Yes	Device: Start|Programs|GSW Telnet and SSH
Java Client	No	
Java Applet	No	

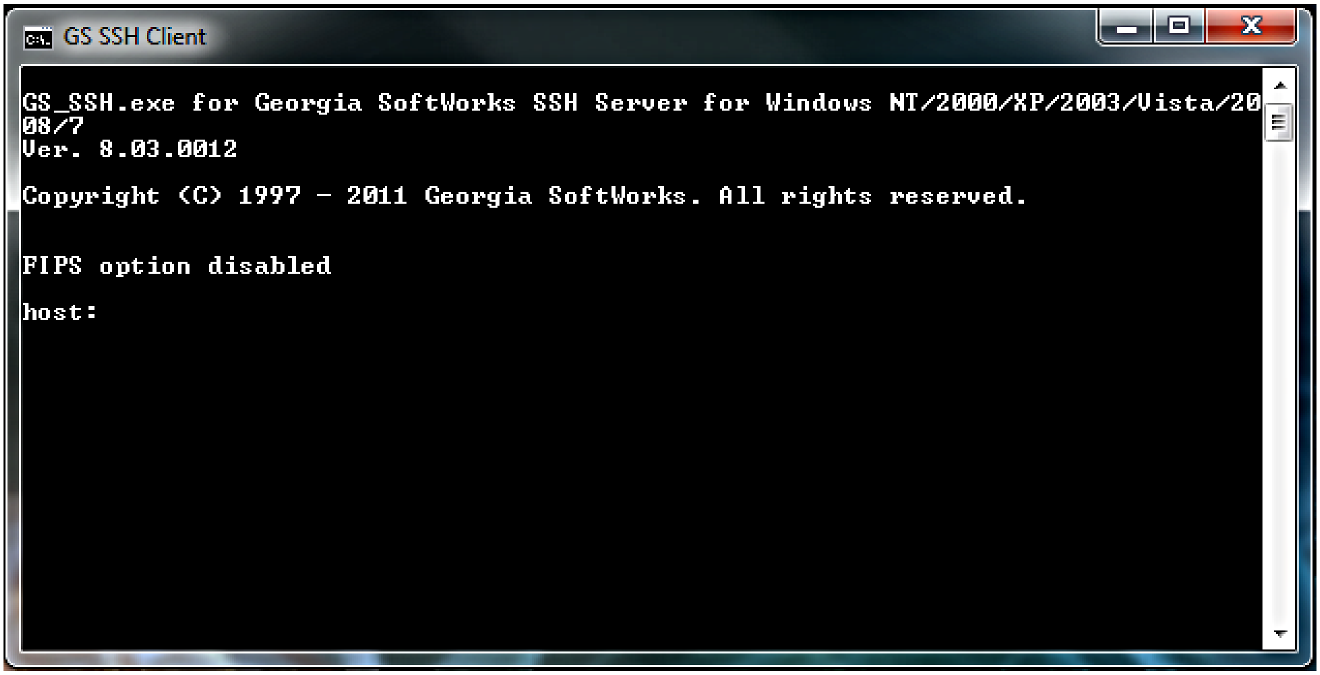
Table 3: GSW SSH Client Platforms

Please see the Georgia SoftWorks UTS User Guide for detailed description of client features and options.

GSW DESKTOP CLIENT

In general, the GSW client installation procedures and features described in the GSW UTS User Manual are applicable to the GSW SSH Clients. The strongest AES-256 Encryption is automatically selected.

To invoke the GSW SSH Client, use the GS SSH Client shortcut in the GSW UTS program group. When connecting with the GSW SSH desktop client, you will get a logon banner similar to the one displayed below. The Host, Username, Password, and domain prompts are presented.



```
GS_SSH.exe for Georgia SoftWorks SSH Server for Windows NT/2000/XP/2003/Vista/20
08/7
Ver. 8.03.0012

Copyright (C) 1997 - 2011 Georgia SoftWorks. All rights reserved.


FIPS option disabled

host:
```

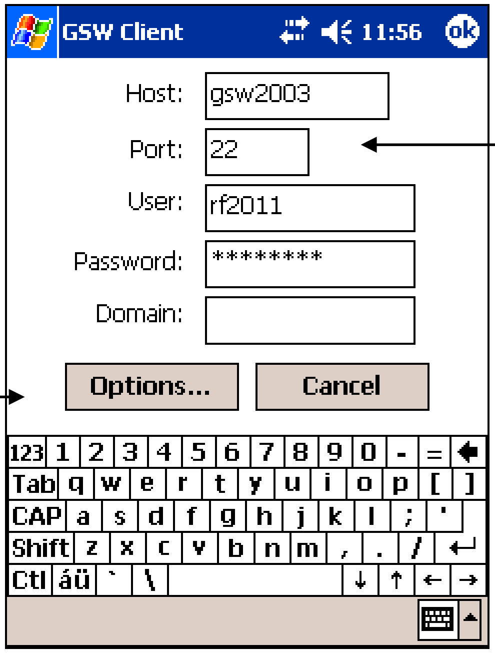
Figure 39: GSW SSH Desktop Client

Windows Mobile Clients

GSW provides SSH clients for Pocket PC/Windows Mobile class devices. Installation is as described in the GSW UTS User Manual. Items specific to the GSW SSH Pocket PC clients are noted below.

Windows Mobile

Upon installation of the GSW UTS Windows Mobile client, you have the connection configuration similar as pictured below. The main item of interest is the Port selected to use for the SSH connection. The normal port used for SSH connections is port 22. Please configure as identified.



Host: gsw2003
Port: 22
User: rf2011
Password: ********
Domain:

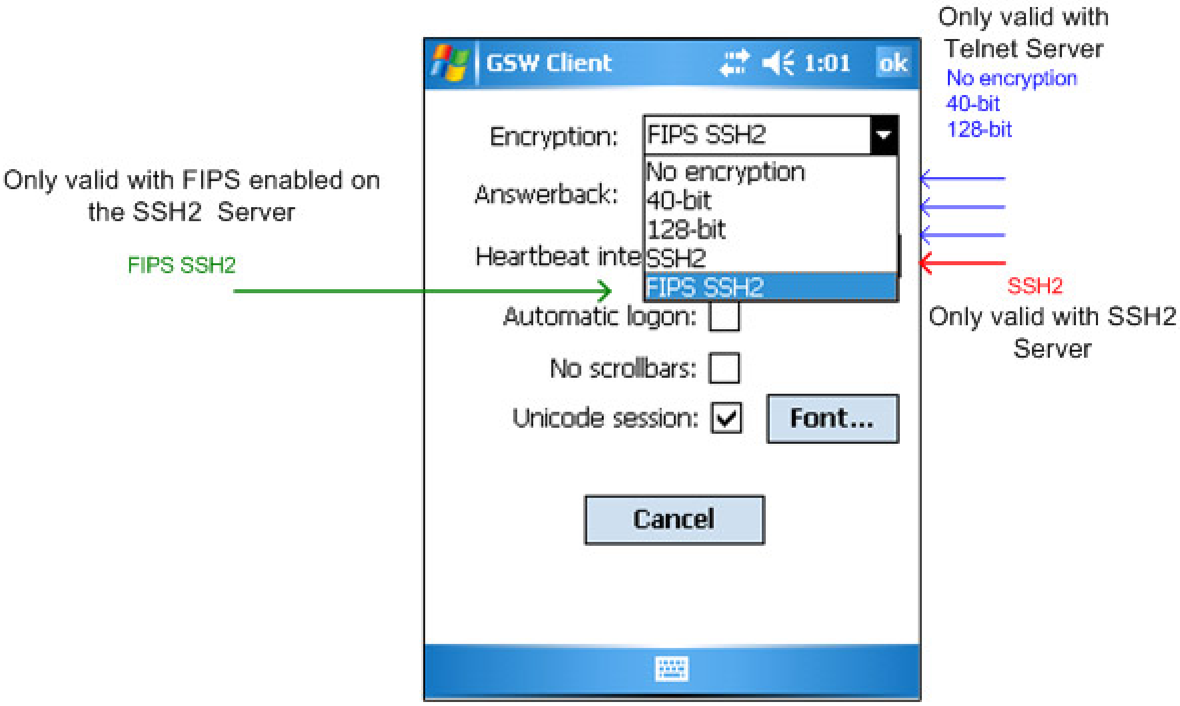
Port 22 is used for SSH connections

Options Button

Figure 40: GSW PPC 2003 Client

To enable SSH encryption click on the Options button.

After clicking on the Options Button the following screen is displayed. The encryption combo box allows the options No encryption, 40-bit, 128-bit, SSH and FIPS SSH. Options selected that do not fit into the context of the GSW Server will result in a failed connection. For example, selecting FIPS SSH encryption when the GSW SSH server does not have FIPS enabled.



Encryption: FIPS SSH2

No encryption
40-bit
128-bit
SSH2
FIPS SSH2

Answerback:

Heartbeat inte

Automatic logon: □

No scrollbars: □

Unicode session: ☑

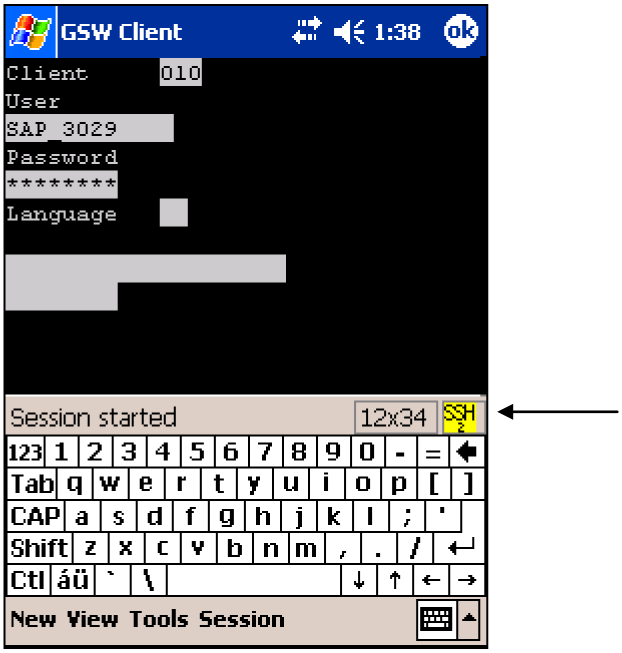
Only valid with Telnet Server
No encryption
40-bit
128-bit

Only valid with FIPS enabled on the SSH2 Server
FIPS SSH2

SSH2
Only valid with SSH2 Server

Figure 41: GSW PPC 2003 Client – Options

This is a screen shot of a PPC2003 connection to SAP via SAPConsole.



```
Client      010
User
SAP_3029
Password
********
Language
```

Session started 12x34 SSH

123 1 2 3 4 5 6 7 8 9 0 - =
Tab q w e r t y u i o p [ ]
CAP a s d f g h j k l ; '
Shift z x c v b n m , . /
Ctl áü ` \ ↓ ↑ ← →
New View Tools Session

Note: The Yellow SSH symbol confirms that the SSH protocol is in use.

Figure 42: GSW PPC 2003 Client - SAPConsole - SSH

Windows CE 4.2+ Devices

Georgia SoftWorks provides a Windows CE .NET 4.2+ SSH client. Below are some screen images of the GSW SSH Client in action on a Psion-Teklogix device.

Upon launching from the shortcut on the device desktop the initial screen (Figure 43) is displayed. From the Initial Screen you have the menu options File, View, Session and Help.

The Session menu (Figure 44) item provides the mechanism to Connect, Disconnect and to configure your session configuration settings.

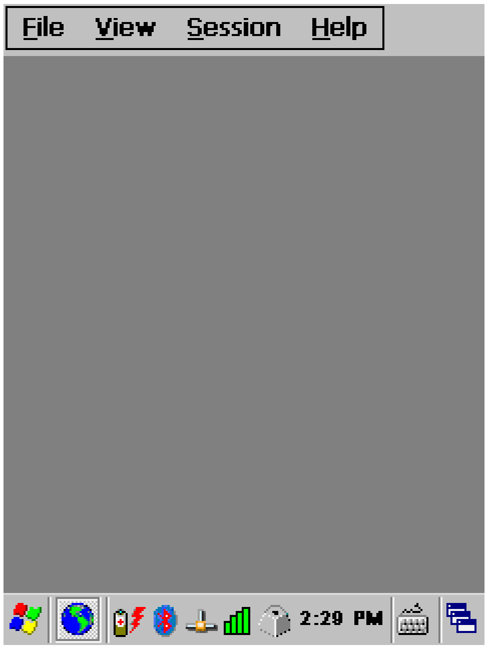


Figure 43: Psion-Teklogix Initial Screen

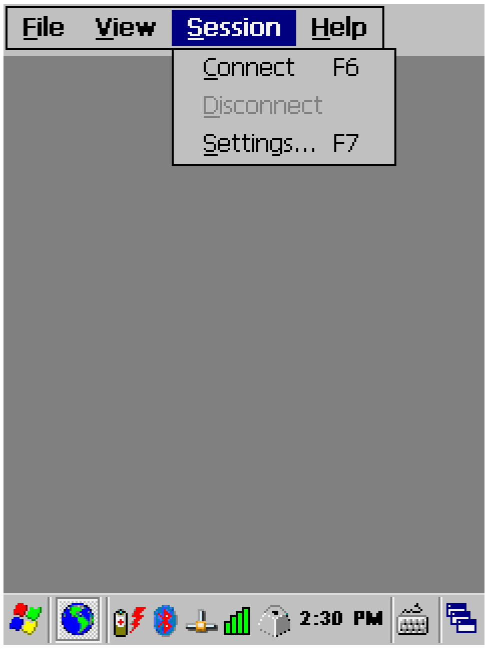
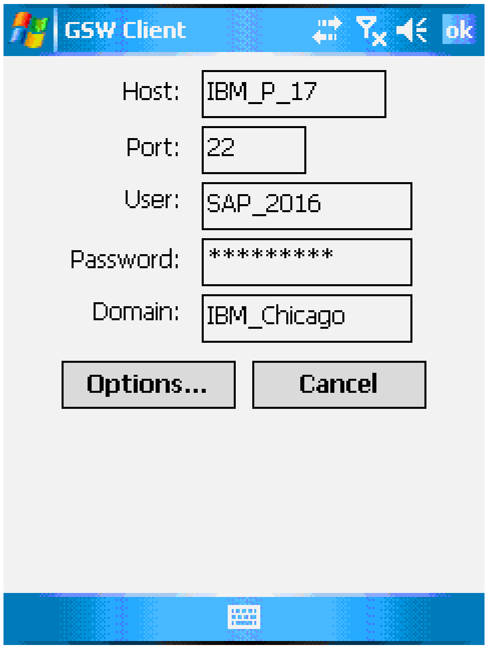


Figure 44: Psion-Teklogix – Session Menu Items

By selecting the Session -> Settings the screen below (Figure 45) is presented allowing configuration of the Host, Port, User, Password and Domain. Selecting the Options button provides similar options as presented in the GSW Windows Mobile client (Figure 41).



Host: IBM_P_17

Port: 22

User: SAP_2016

Password: *********

Domain: IBM_Chicago

Figure 45: Psion-Teklogix Connection Settings

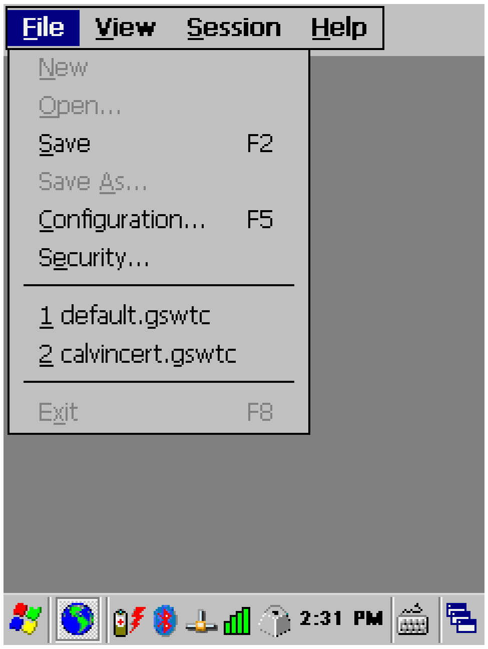
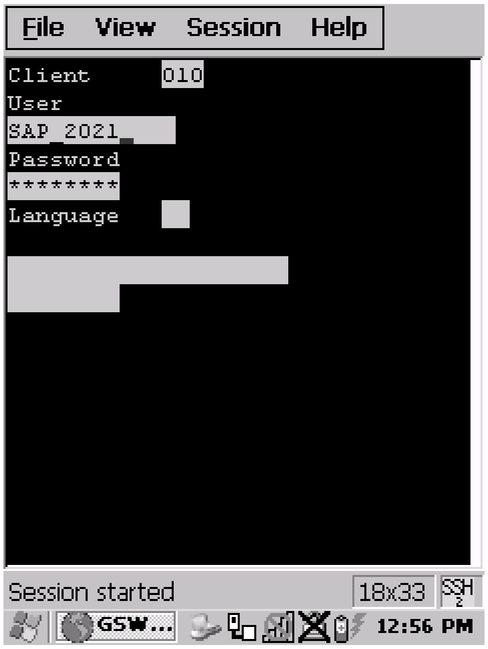


Figure 46: Psion-Teklogix – Save Settings

When the configuration is complete you can save the session configuration information by using the File menu item (Figure 46). You may recall the configuration and minimize the amount of data typed to connect. It also provides the flexibility to save several profiles if needed.

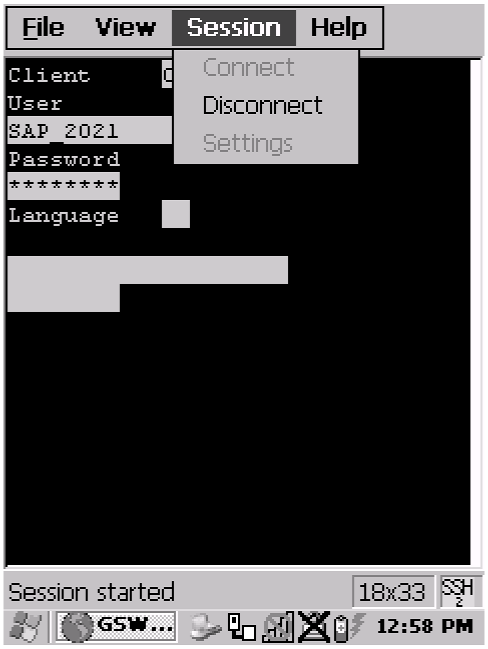
Using the Menu item Session->Connect, the connection is established and Figure 47 is an example of a connection to SAP via SAPConsole.



```
Client    010
User
SAP_2021
Password
********
Language
```

Session started 18x33 12:56 PM

Figure 47: Psion-Teklogix running SAP via SAPConsole



```
Client    0
User
SAP_2021
Password
********
Language
```

Session started 18x33 12:58 PM

Figure 48: Psion-Teklogix Save Client Settings Menu

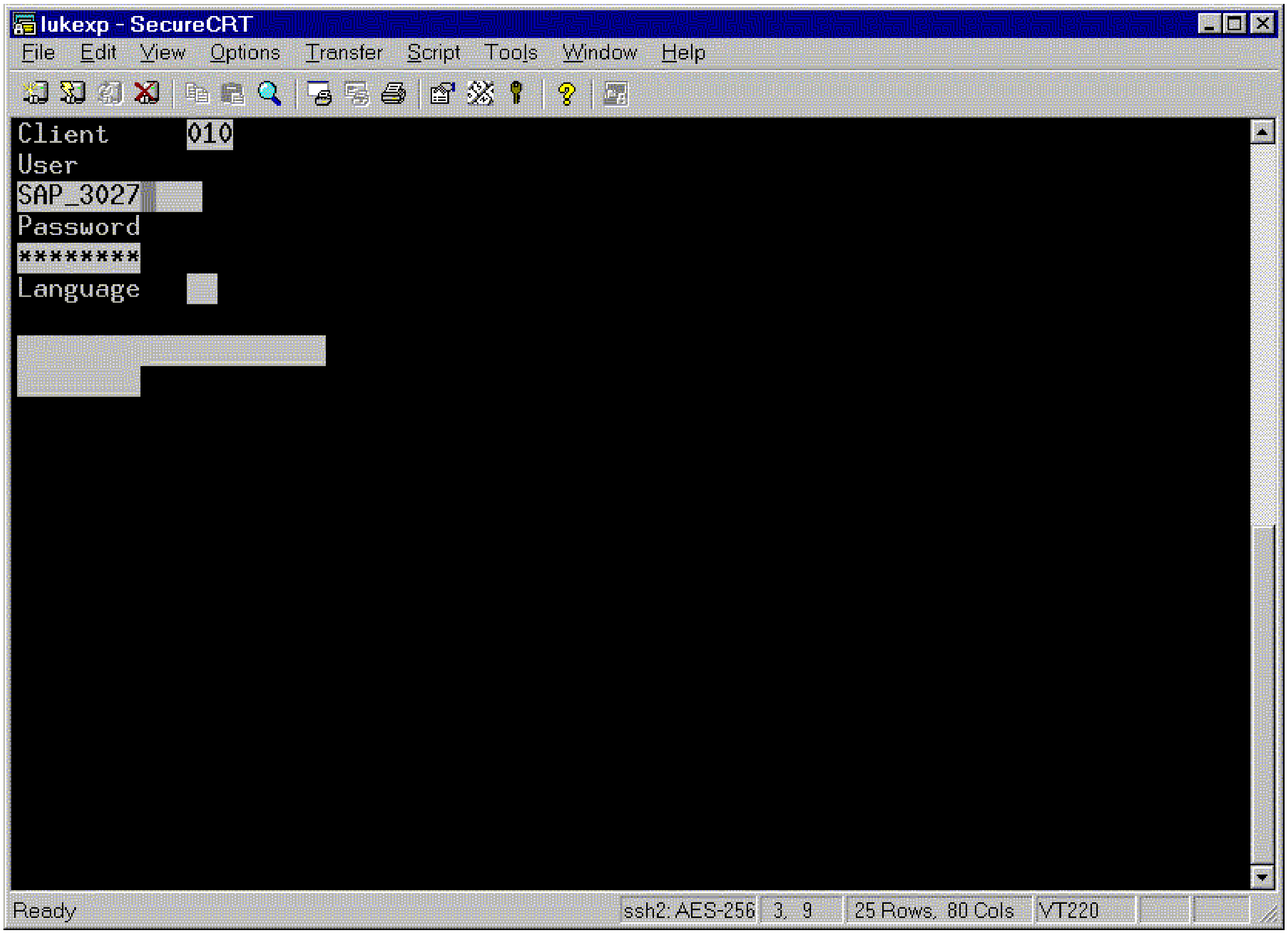
After the work is complete the session is disconnected by using the Menu item Session->Disconnect.

Third Party SSH Clients

The GSW SSH Server allows connections from 3rd Party SSH Clients.

Please see the User's Manual of the 3rd party SSH client of interest for operations of that client. We have included screen shots from three popular SSH clients operating with the GSW SSH Server.

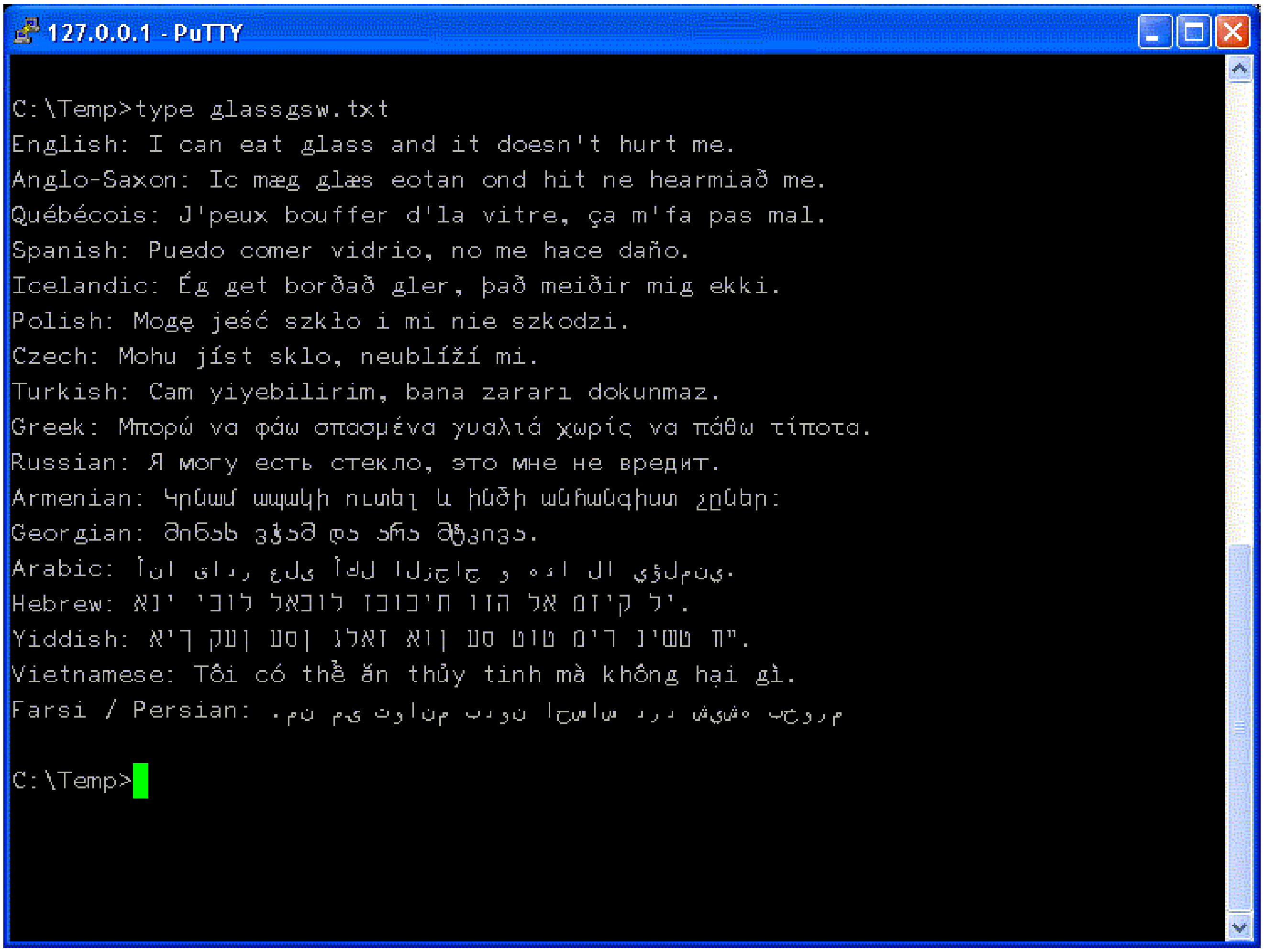
Below is a screen shot of the SecureCRT SSH Client connected to the GSW SSH Server and running SAP via SAPConsole.



```
Client      010
User
SAP_3027
Password
********
Language
```

Figure 49: 3rd Party Client – SecureCRT – SAPConsole

Below is a screen shot of the PuTTY SSH Client displaying some of the GSW International character support.

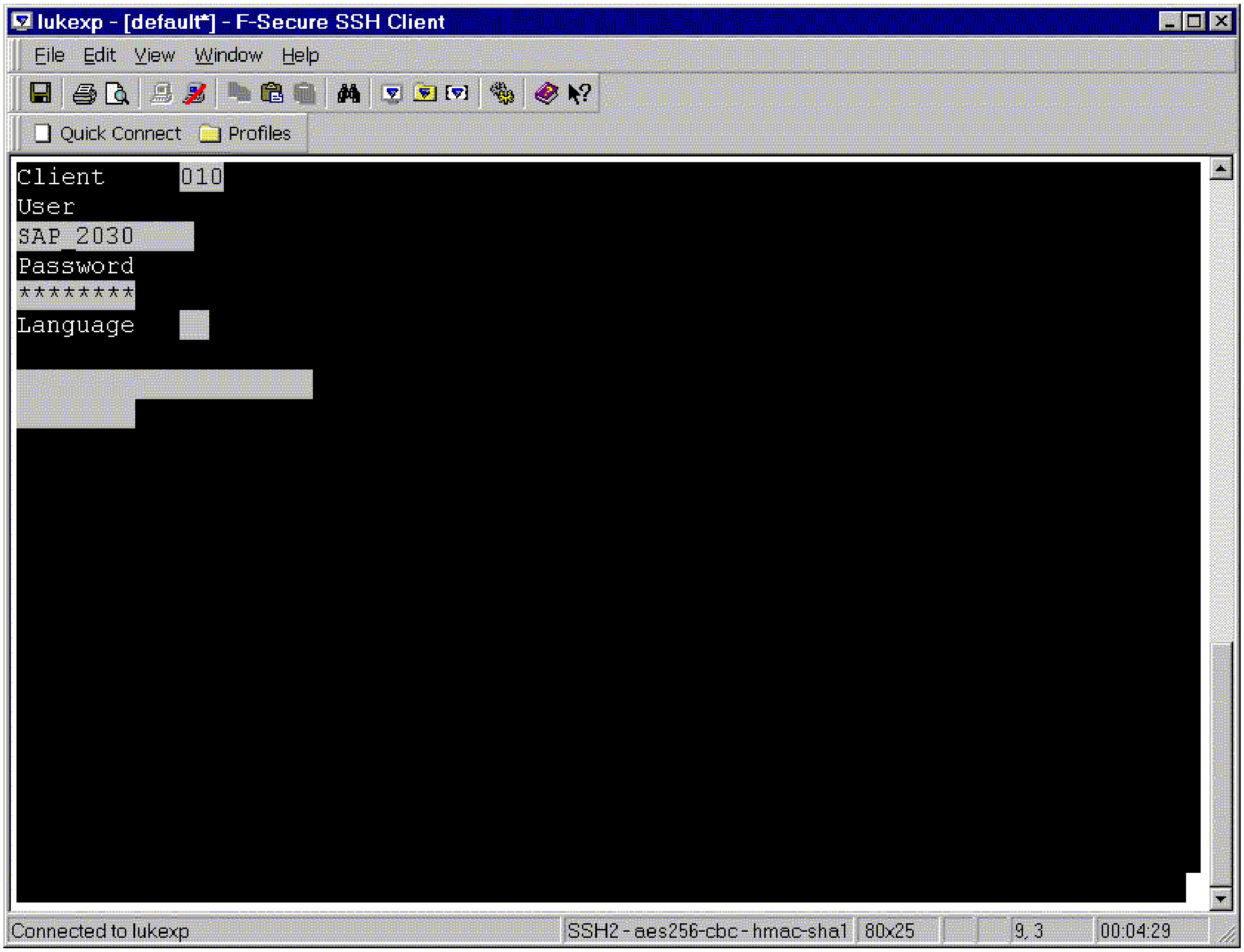


```
C:\Temp>type glassgsw.txt
English: I can eat glass and it doesn't hurt me.
Anglo-Saxon: Ic mæg glæs eotan ond hit ne hearmiað me.
Québécois: J'peux bouffer d'la vitre, ça m'fa pas mal.
Spanish: Puedo comer vidrio, no me hace daño.
Icelandic: Ég get borðað gler, það meiðir mig ekki.
Polish: Mogę jeść szkło i mi nie szkodzi.
Czech: Mohu jíst sklo, neublíží mi.
Turkish: Cam yiyebilirim, bana zararı dokunmaz.
Greek: Μπορώ να φάω σπασμένα γυαλιά χωρίς να πάθω τίποτα.
Russian: Я могу есть стекло, это мне не вредит.
Armenian: Կրնամ ապակի ուտել և ինծի անհանգիստ չըներ:
Georgian: მინას ვჭამ და არა მტკივა.
Arabic: أنا قادر على أكل الزجاج و هذا لا يؤلمني.
Hebrew: אני יכול לאכול זכוכית וזה לא מזיק לי.
Yiddish: איך קען עסן גלאז און עס טוט מיר נישט װײ.
Vietnamese: Tôi có thể ăn thủy tinh mà không hại gì.
Farsi / Persian: .من می توانم بدون احساس درد شیشه بخورم

C:\Temp>
```

Figure 50: 3rd Party Client - PuTTY - Unicode

Below is a screen shot of the F-Secure SSH Client connected to the GSW SSH Server and running SAP via SAPConsole.


lukexp - [default*] - F-Secure SSH Client
File Edit View Window Help
Quick Connect
Profiles

```
Client       010
User
SAP_2030
Password
********
Language
```

Connected to lukexp
SSH2 - aes256-cbc - hmac-sha1
80x25
9, 3
00:04:29

Figure 51: 3rd Party Client - F-Secure SSH Client

Specify Domain with a 3rd Party Client

A user account's domain can be specified in the SSH client's user name field. If a domain is not specified then the GSW UTS will use the default domain configured in the UTS registry. If a UTS default domain is not configured and a domain is not specified in the SSH client's user name field then the system will attempt to validate the user account logon using the local account database.

Use the following syntax to specify the domain in the SSH client's user name field:

```
username@domainname
```

where `username` is the name of the user and `domainname` is the name of the domain.

If a default domain is specified in the UTS registry then the domain entered above will take precedence. Please see the GSW UTS User Manual for more information.

Registry Variables

Many registry variables exist for provisioning the system. Registry variables are an excellent method to configure software while utilizing skills already learned by the system administrator. There is no need to learn yet another interface to provision the software. Here is a list of the registry variables and a brief description of their use. Please see the appropriate section in this User Manual for complete descriptions.

All Registry values used by the Georgia SoftWorks SSH Server are stored in the following Registry path.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Georgia SoftWorks\GSW_SSHD\Parameters
```

- `bAES256Only` – Allow for AES-256 connections only. Default = 1. (Page 42)
- `bEnableWODLog` – Turn Logging ON for SSH internals activity. Default = 0 (Page 47)
- `dwInactivityTimeout` – Reserved, do not change
- `szServerAddress` – Reserved, do not change
- `szServerDSAKeyFile` – Location of SSH Servers DSA private key file in PEM format. The file is encrypted. (Page 46)
- `szServerECDSAKeyFile` – Location of SSH Servers ECDSA private key file in PEM format. The file is encrypted. (Page 47)
- `szServerRSAKeyFile` – Location of SSH Servers RSA private key file in PEM format. The file is encrypted. (Page 45)
- `szWODLogFile` – Path and File Name of the SSH internal activity log file. To enable the log bEnableWODLog must be set to 1. (Page 50)
- `usGSWSSHDPort` – The port number clients will be connecting to. Default = 22(decimal) is the standard port assigned to SSH. (Page 43)

HMACs - Hash Message Authentication Code

A Hash Message Authentication Code is method for message authentication using cryptographic hash functions combined with a secret key that is shared.

HMACs
hmac-sha2-256
hmac-sha2-512
hmac-sha1
hmac-sha1-96

Table 4: Hash Message Authentication Codes (HMACs) supported

Ciphers

Ciphers are algorithms used for performing encryption or decryption.

Ciphers	
aes128-cbc	aes256-cbc
aes128-ctr	aes256-ctr
3des-cbc	rijndael128-cbc
aes192-cbc	rijndael192-cbc
aes192-ctr	rijndael256-cbc

Table 5: Ciphers supported

Key Exchange Algorithms

Key exchange algorithms are used to exchange cryptographic keys between the SSH Server and the SSH client.

Key Exchange Algorithms
ecdh-sha2-nistp256
ecdh-sha2-nistp384
ecdh-sha2-nistp521
diffie-hellman-group1-sha1
diffie-hellman-group14-sha1

Table 6: Key Exchange Algorithms supported

Host Key Types

The purpose of a Host Key is to ensure that when you connect to a remote host, it is actually the host you want to connect. It is the SSH Server's public key and is used by the SSH client to decrypt the authentication message sent from the server when establishing a connection.

The public key / certificate formats supported by the GSW SSH Server are shown below.

Host Key Types
ssh-rsa
ssh-dss
ecdsa-sha2-nistp521

Table 7: Host Key types supported

FIPS 140-2 Resources

Additional information about FIPS and NIST can be found using the following links.

http://csrc.nist.gov/publications/PubsFIPS.html

Certificate numbers

Certificate Numbers	Descriptions
#560	Certificate #560 Windows CE and Windows Mobile Enhanced Cryptographic Provider (RSAENH) (Software Versions: 5.01.01603 [1], 5.00.911762 [1], 5.04.17228 [2] and 5.05.19202 [2]) http://csrc.nist.gov/publications/PubsFIPS.html
#825	Certificate #825 Windows CE and Windows Mobile Enhanced Cryptographic Provider (RSAENH) (Software Version: 6.00.1937) http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140crt/140crt825.pdf
#918	Certificate #918 OpenSSL FIPS Object Module) http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140crt/140crt918.pdf

Table 8: FIPS 140-2 certificate links

GSW SSH Server 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 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 features or defect resolutions are Alpha and Beta tested we generate a release. This provides our customers with features much quicker than the "*grouping*" or "scheduling" method used by other companies.

The GSW SSH Server (and Rocket Pack, RF DTIO) Subscription grants 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 you 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 9: Version Upgrade Pricing **with** GSW Subscription Plan

The pricing for version upgrades without the Subscription is based on the period of time since 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 10: Version Upgrade Pricing **Without** Subscription Plan

HOW TO UPDATE THE SOFTWARE

1. Download the software or use the supplied CD.

2. Make sure the SSH Server is not in use.

3. Run the 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

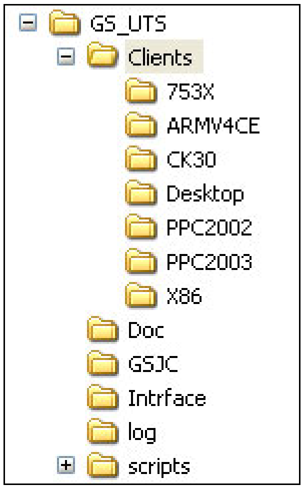
Please use the following procedure when renewing the GSW SSH Server or Rocket Pack Subscription.

Step	Who		Action
1.	GSW		Send notice to customer 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 (if applicable)
5.		Customer	Install new Floating License (and software if desired)
6.		Customer	Ships OLD Floating License back to GSW

Table 11: Steps to Renew the GSW Subscription Plan

SSH Server Folder Layout

The Installation folder of the GSW UTS is as follows



```
⊟ GS_UTS
    ⊟ Clients
        753X
        ARMV4CE
        CK30
        Desktop
        PPC2002
        PPC2003
        X86
      Doc
      GSJC
      Intrface
      log
    ⊞ scripts
```

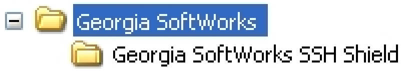
Figure 52: Installation Folder Layout of the GSW UTS

The folders of interest are:

- ○ Clients: Contains all the GSW clients for the SSH Server and the Telnet Server. These files are needed for automatic update of our client software.
- ○ 753x Contains the GSW Client for Teklogix 753x devices.
- ○ ARMV4CE Contains the GSW Client for ARM devices
- ○ CK30 Contains the GSW Client for Intermec CK30 devices
- ○ Desktop Contains the GSW clients that run on Windows Desktops.
- ○ PPC2002 GSW Clients for Windows Pocket PC 2002 class devices
- ○ PPC2003 GSW Clients for Windows Pocket PC 2003 class devices.
- ○ X86 Contains the GSW Client for x86 based devices

- Doc: Contains the documentation for your viewing or printing.
- GSJC Contain the files for the GS Java Client and Applet
- Log Contains the GSW UTS Log files to provide to the GSW Technical Support Group in the event of a problem. See page 74 for more information.
- Scripts This is where your logon scripts will reside. See GSW UTS User Manual.

The installation folder layout of the GSW SSH Shield is as follows under the Windows\Program Files folder.



Georgia SoftWorks
Georgia SoftWorks SSH Shield

Figure 53: Installation Folder Layout of the GSW SSH Shield

The Georgia SoftWorks UTS logs folder contains the GSW SSH Server log files to provide to the GSW Technical Support Group in the event of a technical problem.

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 SSH Server.

The signature is comprised of hardware and software identifiers that exist on your system that make the target system unique. These identifies 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 SSH Server. 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 and environment information.
- Write your question down. This not only helps us but also helps you in articulating the question.

Provide Log Files To GSW Technical Support

A typical sequence when GSW Technical Support needs the logs files are to delete the log files, reproduce the behavior in question and email the log files, which are recreated during the test, to GSW Support.

Email Support Tips:

To expedite support for suspected problems please perform the following test steps below to help us diagnose the issue.

1. Disconnect all users. Make sure that no other user connects at the time of the test.
2. Wait 5 minutes
3. Delete the Log files

   Delete all log files from the GSW UTS Server installation 'Log' subdirectory on the computer running the GSW Universal Terminal Server. (Usually `c:\GS_UTS\Log`)
4. To expedite resolution, reboot the Server if possible
5. Duplicate the problem.
6. The log files are automatically re-created. Send us the files using the GSW Ticket System
7. Please also include
   a. A description of the problem including User ID's, Domain and IP Addresses
   b. The logon script associated with the user experiencing the problem. (That is the `c_start.bat` or the `k_start.bat` file that resides in the scripts folder in the GSW UTS directory
   c. And of course your contact information.

Again, send us the files using the GSW Ticket System. 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**