

GEORGIA SOFTWAREWORKS

SSH2 FIPS 140-2 Option Quick View for Windows
NT/XP/VISTA/2000/2003/2008

Keep it Secure -Period

Quick View

THIS PAGE INTENTIONALLY LEFT BLANK

GEORGIA SOFTWORKS

SSH2 FIPS 140-2 Option Quick View

Copyright © 1997-2008, Georgia SoftWorks, All Rights Reserved
Public Square
17 Hwy 9 South • PO Box 729
Dawsonville Georgia 30534
Telephone 706.265.1018 • Fax 706.265.1020
<http://www.georgiasoftworks.com>

Table of Contents

QUICK VIEW	1
SOFTWARE REQUIREMENTS	2
ENABLE FIPS 140-2 OPTION	3
<i>ENABLE FIPS 140-2 ON SSH2 SERVER</i>	3
<i>ENABLE FIPS 140-2 ON GSW MOBILE/CE and DESKTOP CLIENTS</i>	4
IDENTIFY FIPS 140-2 CONNECTIONS	6
FIPS 140-2 RESOURCES	7

TABLE OF FIGURES

Figure 1: EVERY client and the Server running FIPS 140-2 compliant software.....	1
Figure 2: GSW True FIPS 140-2 Connection – Server and Client	3
Figure 3: FIPS 104-2 Option Enabled.....	3
Figure 4: Desktop Client "-i" option issued.....	4
Figure 5: Enable FIPS 140-2 on GSW Mobile Clients	5
Figure 6: GSW Encryption Options for Windows Mobile 5+.....	5
Figure 7: Verify FIPS 140-2 Compliant Connections	6

Table of Tables

Table 1: GSW Software versions required for FIPS 140-2	2
Table 2: Device Operating System Versions Required for FIPS 140-2.....	2
Table 3: FIPS 140-2 certificate links	7

Copyright © Georgia SoftWorks, 1997-2008 All Rights Reserved.

Quick View, Version 7.50, July 18, 2008

Microsoft, Windows, Windows VISTA, Windows XP, Windows 2000 Windows NT, Windows 98, Windows 95 are trademarks of Microsoft Corporation. SAP, SAPConsole is trademarks of SAP AG. SecureCRT, F-Secure, PuTTY are trademarks of their respective companies.

Quick View

“FIPS 140-2 specifies the security requirements that will be satisfied by a cryptographic module utilized within a security system protecting sensitive or valuable data”

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 SSH2 server and client software to the United States Military. Having completed this task, GSW is able to make this software commercially available to other Federal and State agencies.

This option is also available for purchase by other organizations such as educational and research institutions, commercial businesses and other entities with the need or desire to comply with this security requirement for cryptographic modules standard.

What are you doing to combat the onslaught of new and growing security threats? The GSW SSH2 Server with the FIPS 140-2 option may be a crucial element in your enterprise access compliance strategy. GSW SSH2 server with the FIPS 140-2 option increases security while speeding the time to compliance.

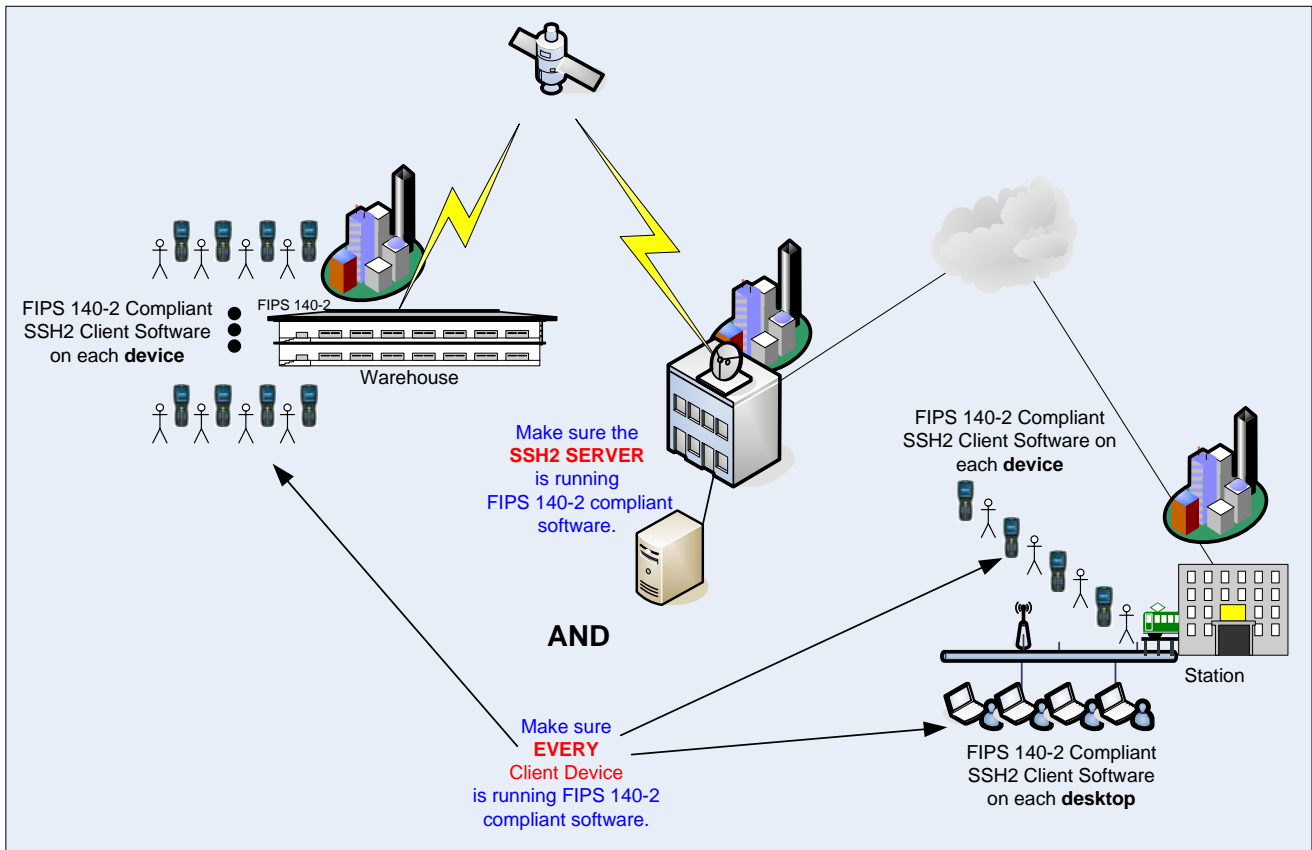


Figure 1: EVERY client and the Server running FIPS 140-2 compliant software

Software Requirements

The GSW FIPS option is available for purchase to owners of the GSW SSH2 Server version 7.50 and higher. The GSW FIPS 140-2 option can be purchased at the same time as the SSH2 Server or it can be obtained later.

The GSW mobile clients must run on an operating system that is FIPS 140-2 certified or provides a cryptographic module that has been FIPS 140-2 certified.

In order that your SSH2 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.

GSW Software	Version			Certificate
GSW UTS Server	7.50+			#918
GSW SSH2 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 <i>- Made available to OEMs via Windows Update 061211_KB911762</i>				#560
Windows Mobile 5.0				#560
Windows CE 6.0				#825
Windows Mobile 6.0				#825
Windows Mobile 7.0				

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 14343.0.0.0 With Windows CE 5.0 extra attention should be taken to ensure the correct version of rsaenh.dll is present. Per information from Microsoft support, early versions of Windows CE 5.0 did not come with a FIPS 140-2 certified version of rsaenh.dll. This may require contacting the device vendor to determine the correct version number of that cryptographic module.

Enable FIPS 140-2 Option

FIPS 140-2 must be enabled on both the GSW SSH2 server and the GSW clients to ensure a FIPS 140-2 compliant connection.

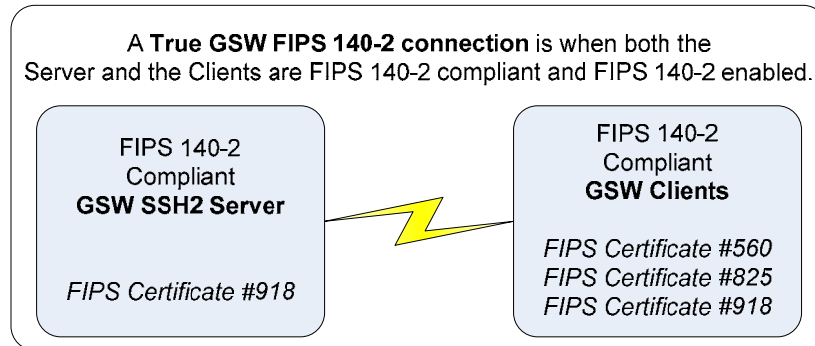


Figure 2: GSW True FIPS 140-2 Connection – Server and Client

ENABLE FIPS 140-2 ON SSH2 SERVER

Proper registration will enable the FIPS option on the SSH2 Server. View the registration tool to ensure the GSW SSH2 Server is registered with the FIPS option enabled.

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

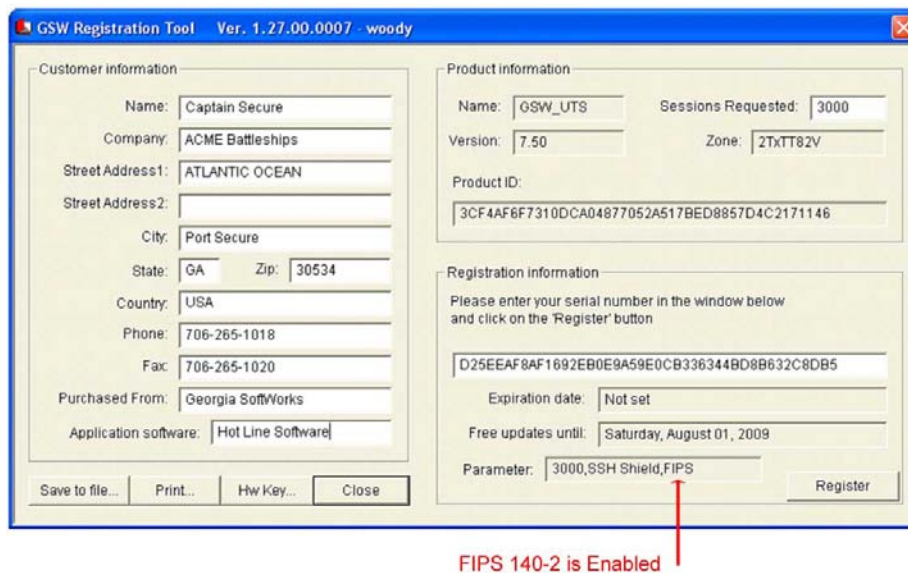


Figure 3: FIPS 104-2 Option Enabled

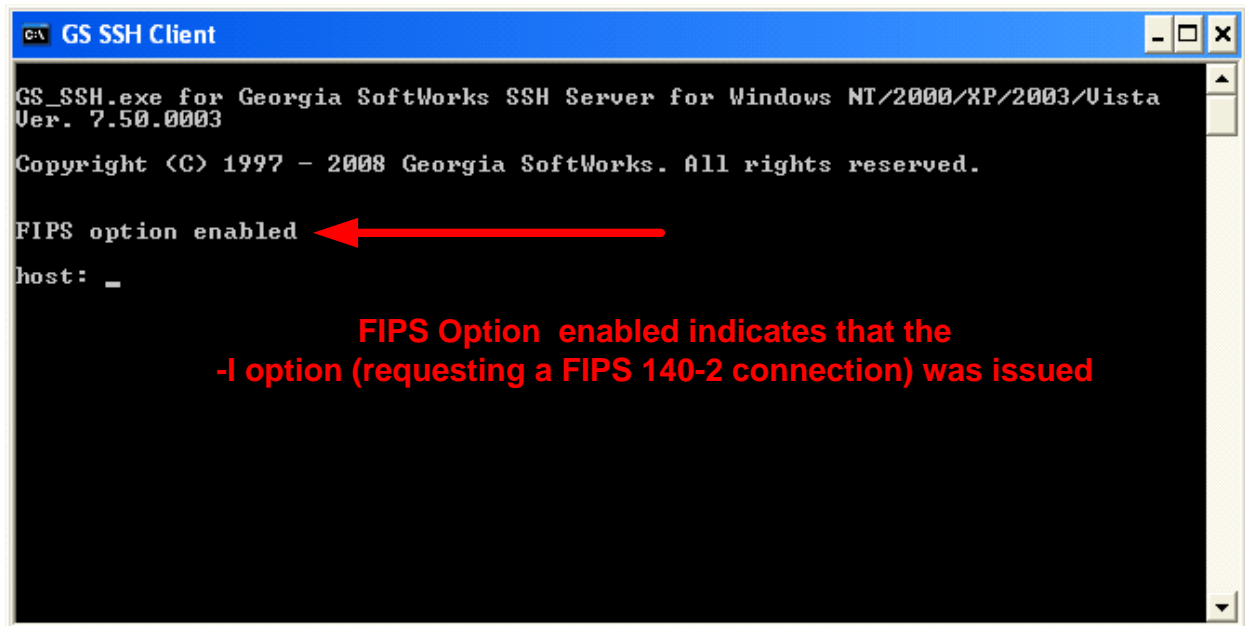
In the Parameter field you will observe the number of concurrent sessions allowed followed by the text "SSH Shield" indicating that the GSW SSH2 server is installed and FIPS indicating that the FIPS 140-2 option is enabled.

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 users manual 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 Client
GS_SSH.exe for Georgia SoftWorks SSH Server for Windows NT/2000/XP/2003/Vista
Ver. 7.50.0003
Copyright (C) 1997 - 2008 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 4: Desktop Client "-i" option issued

Please note that to have both ends (client and server) FIPS 140-2 compliant, FIPS 140-2 must be enabled on the GSW SSH2 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. The diagram on the left is a Windows Mobile screen and the one on the right is a Windows CE screen.

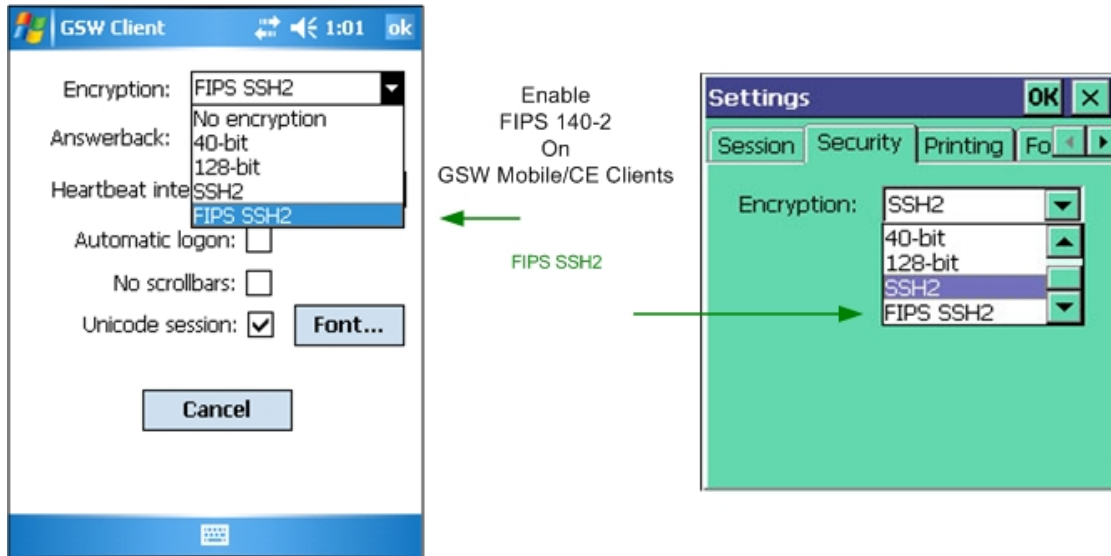


Figure 5: Enable FIPS 140-2 on GSW Mobile Clients

The encryption combo box allows the options No encryption, 40-bit, 128-bit, SSH2 and FIPS SSH2. Options selected that do not fit into the context of the GSW Server will result in a failed connection. For example, selecting FIPS SSH2 encryption when the GSW SSH2 server does not have FIPS enabled.

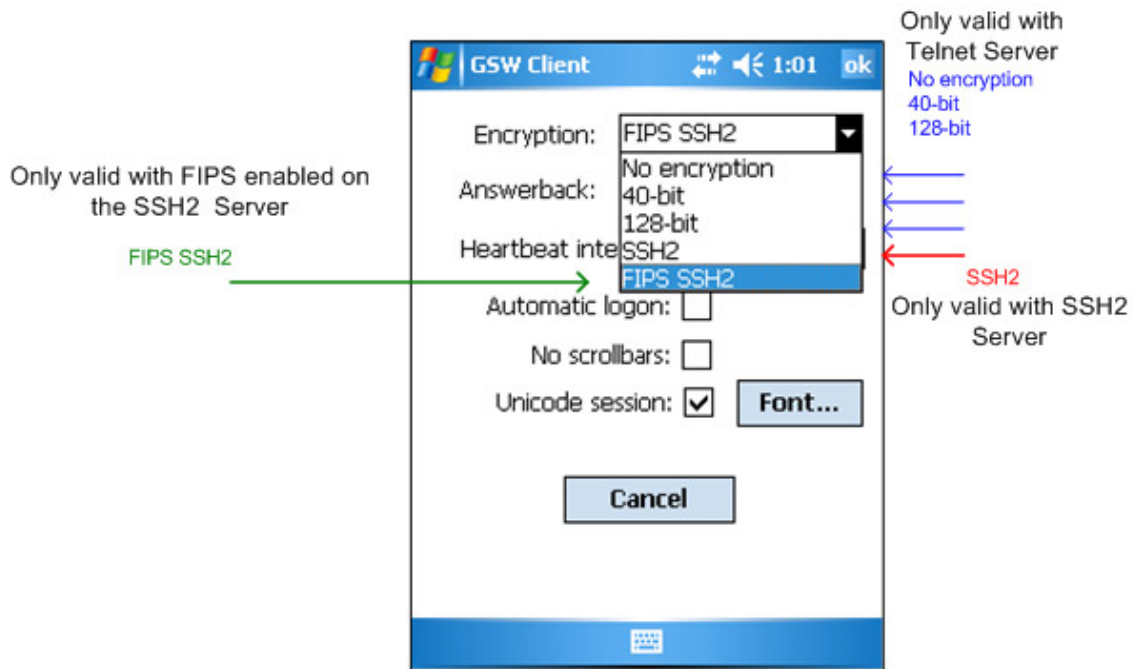


Figure 6: GSW Encryption Options for Windows Mobile 5+

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/groups/STM/cmvp/documents/140-1/140crt/140crt560.pdf
#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 3: FIPS 140-2 certificate links