GEORGIA SOFTWORKS
SSH2 FIPS 140-2 Option Quick View for Windows

Keep it Secure - Period

Quick View
Table of Contents

QUICK VIEW ..................................................................................................................................................... 1
SOFTWARE REQUIREMENTS .......................................................................................................................... 2
ENABLE FIPS 140-2 OPTION ....................................................................................................................... 3
  ENABLE FIPS 140-2 ON SSH2 SERVER .................................................................................................. 3
  ENABLE FIPS 140-2 ON GSW MOBILE/CE and DESKTOP CLIENTS .................................................. 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
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.

<table>
<thead>
<tr>
<th>GSW Software</th>
<th>Version</th>
<th>Certificate</th>
</tr>
</thead>
<tbody>
<tr>
<td>GSW UTS Server</td>
<td>7.50+</td>
<td>#918</td>
</tr>
<tr>
<td>GSW SSH2 Server</td>
<td>7.50+</td>
<td>#918</td>
</tr>
<tr>
<td>GSW Desktop Clients</td>
<td>7.50+</td>
<td>#918</td>
</tr>
<tr>
<td>GSW CE/Mobile Clients</td>
<td>7.50+</td>
<td>#560, #825</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Required Device Operating System for Mobile/CE Clients</th>
<th>Certificate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows CE 5.0</td>
<td>#560</td>
</tr>
<tr>
<td>Depends on Vendor</td>
<td></td>
</tr>
<tr>
<td>- Made available to OEMs via Windows Update 061211_KB911762</td>
<td></td>
</tr>
<tr>
<td>Windows Mobile 5.0</td>
<td>#560</td>
</tr>
<tr>
<td>Windows CE 6.0</td>
<td>#825</td>
</tr>
<tr>
<td>Windows Mobile 6.0</td>
<td>#825</td>
</tr>
<tr>
<td>Windows Mobile 7.0</td>
<td></td>
</tr>
</tbody>
</table>

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.

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

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.

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.

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.
Identify 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. Only GSW clients can be verified as FIPS 140-2 compliant.

![Diagram showing FIPS 140-2 connections verification]

Figure 7: Verify FIPS 140-2 Compliant Connections
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

<table>
<thead>
<tr>
<th>Certificate Numbers</th>
<th>Descriptions</th>
</tr>
</thead>
</table>
| **#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])  
| **#825**            | Certificate #825  
|                     | Windows CE and Windows Mobile Enhanced Cryptographic Provider (RSAENH)  
|                     | (Software Version: 6.00.1937)  
| **#918**            | Certificate #918  
|                     | OpenSSL FIPS Object Module)  

Table 3: FIPS 140-2 certificate links