High Security Supplement

User Manual Supplement
for Digi XPress Wireless Radios
with FIPS 140-2 Security

(XPress Series)

90002005_A
January 4, 2011

Information in this document is subject to change without notice and does not represent a commitment on the part of Digi International.

Digi provides this document “as is,” without warranty of any kind, either expressed or implied, including, but not limited to, the implied warranties of, fitness or merchantability for a particular purpose. Digi may make improvements and/or changes in this manual or in the product(s) and/or the program(s) described in this manual at any time.

This product could include technical inaccuracies or typographical errors. Changes are made periodically to the information herein; these changes may be incorporated in new editions of the publication.

To contact Digi International for more information about your Digi products, or for customer service and technical support, use the following contact information:

To Contact Digi International by:	**Use:**
Mail	Digi International 11001 Bren Road East Minnetonka, MN 55343 U.S.A.
World Wide Web:	http://www.digi.com/support/
email	http://www.digi.com/support/eservice
Telephone (U.S.)	(952) 912-3444 or (877) 912-3444
Telephone (other locations)	+1 (952) 912-3444 or (877) 912-3444

High Security Supplement

If you have a Digi radio with FIPS 140-2 Security, this supplement to the User Manual provides instructions for setting up the encryption. Please disregard the AES Encryption instructions in the regular manual: this superceded them. A feature of the level of security provided is that there is no way to change the encryption method or key through the radio's interface. A separate port must be used.

To program the encryption characteristics of your Digi radio, the radio must be powered off and the cover opened. A PC must be connected to the USB port on the XEB-AW140 Security Module inside (a small piggy-back board with a tamper-evident conforming coating). The necessary portion of the electronics for managing the setup is powered from the module's USB connection.

The PC must have two critical pieces of software installed:

1. A driver that provides a virtual COM port through the USB connection. This driver can be downloaded from the Future Technology Devices International website, http://www.ftdichip.com. Follow their menu to the webpage for VCP drivers and choose the one that matches your operating system. Installation guides are also available in the documents section of the website.
2. A terminal emulator that will provide the user interface to the XEB-AW140. Windows XP and earlier included a program known as HyperTerminal that would work fine, but Microsoft has not included it in newer versions. Customers using post-XP versions of Windows can use Digi's XCTU for this same function: www.digi.com/xctu. Customers using non-Windows OS can use a suitable tool such as minicom for Linux Ubuntu or ZTerm for Mac.

There are two roles defined for those having access to the programming interface, Crypto Officer and User. Each has a different password. Only the Crypto Officer is allowed to set the encryption method and encryption key. The user may examine self test results and firmware version only.

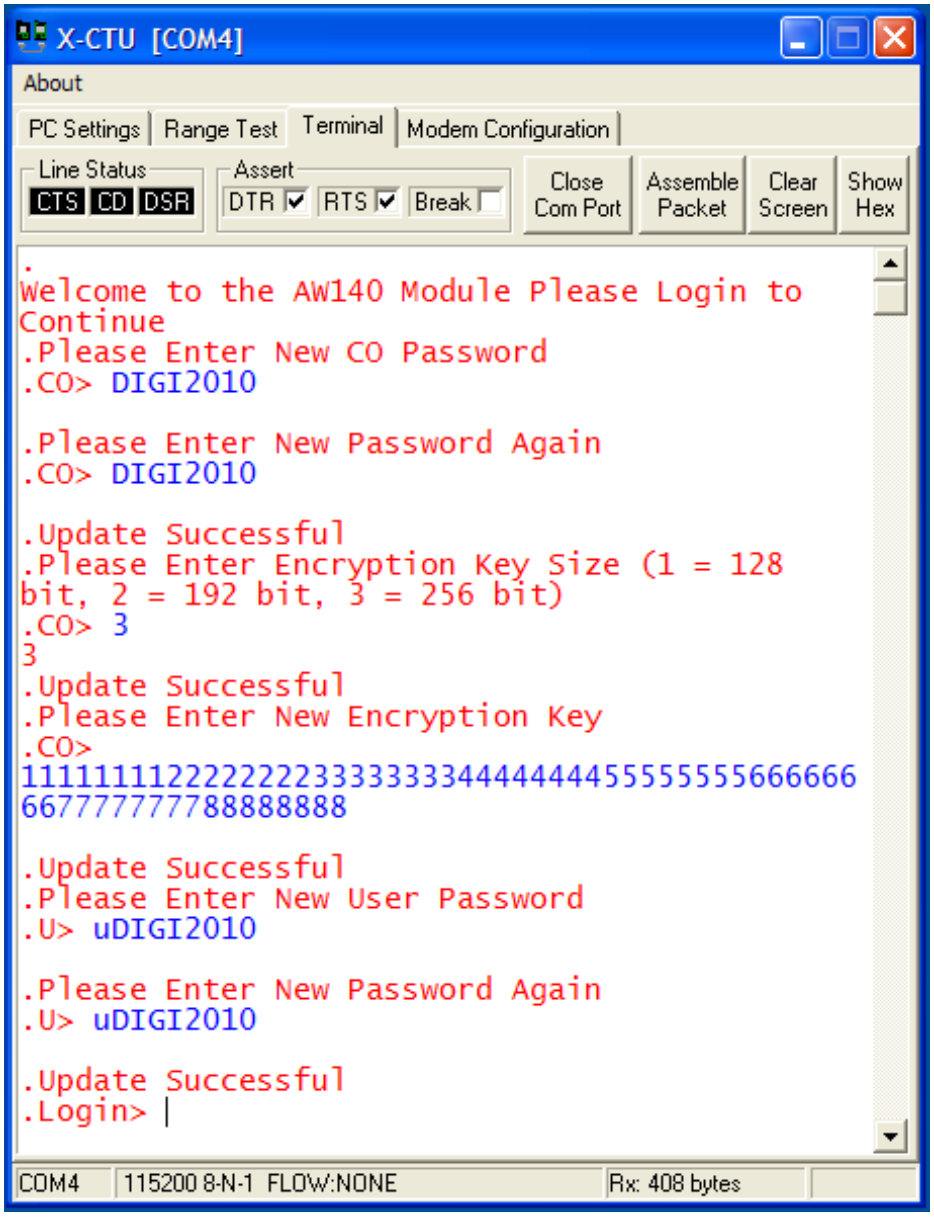
Step by step programming procedure:

1. Make sure the main power for the radio is off and connect the XEB-AW140 module's USB port to your computer using a USB mini B cable.
2. Open your terminal emulator program and set the COM port settings as follows:

Data bits:	8
Baud rate:	115200
Parity:	none
Stop bits:	1
Flow control:	none

3. Press any key to activate the XEB-AW140. If the module has never been programmed, setup prompts will occur as shown in the example screen shot below. If you see only a login prompt, then the module has previously been initialized. If you know the password, enter it. If no, type "init" to erase all keys and passwords and return the module to its uninitialized state.

4. Initial setup commands:



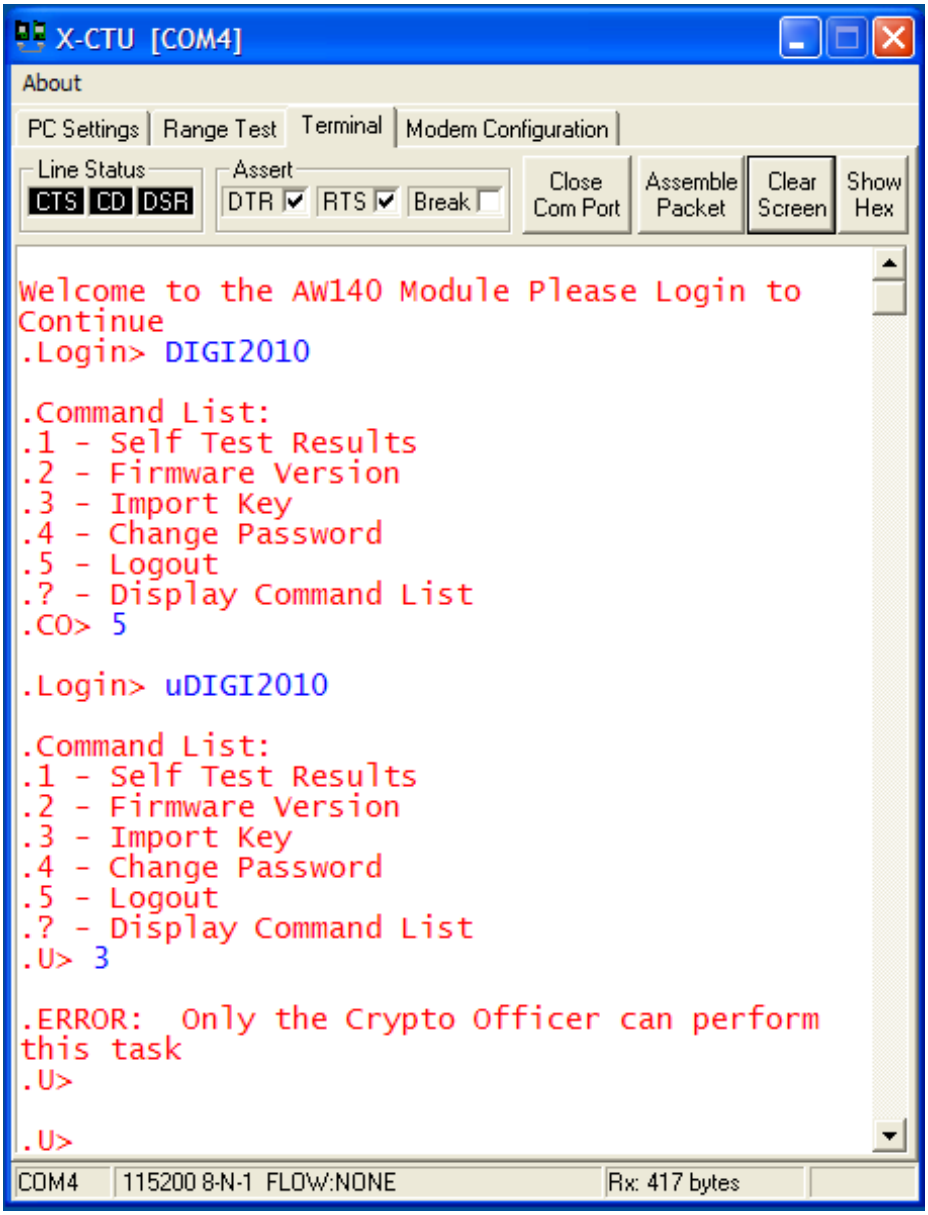
Passwords must be supplied for both the Crypto Officer and User Roles.

Passwords must be between 8 and 32 characters. Case matters and any symbols may be used (ASCII characters allowed).

The Encryption Choice may be 128, 192, or 256 bits as shown in the prompt.

The Encryption Key must be entered as a 32, 48, or 64 digit hexadecimal number (0-9, a-f), corresponding to the Encryption Choice. Here, case does not matter - A-F or a-f may be used. It is possible to enter less than the full number of digits; the XEB-AW140 will pad the rest with zeros.

5. After completing the initial setup, disconnect the USB cable and power up the Digi radio to begin normal cryptographic operation.
6. It may become necessary to change the programming or test the module at some later time. In order to do so turn off the power for the radio, then open its cover and connect the USB cable to the XEB-AW140 and set up the COM port parameters and terminal emulator program as described in step 2. A screen similar to the one below will appear:



Self Test Results displays the results of the power up self test. At power up, the XEB-AW140 runs a known answer test for all encryption/ decryption algorithms.

Firmware Version displays the revision number of the firmware running in the XEB-AW140 module.

Change Algorithm and **Change Key** can only be used by the Crypto Officer Role. If the User Role attempts to run these commands, an error occurs as shown in the above screen shot.

Change Password allows a new choice for the Crypto Officer or User password, depending on which Role is logged in.

Logout and **Display Command List** are self-explanatory.

Note: If an incorrect password is entered at the login prompt, two more tries are allowed and then the XEB-AW140 enters a lockout state for 5 minutes.

7. After completing the setup or testing, log out and disconnect the USB cable. Next, power up the Digi radio to resume normal cryptographic operation.