

No. : TDUM02- TE002-EN	Name: Secure Starter Kit User Manual	Version : V2.0
------------------------	--------------------------------------	----------------

Secure Starter Kit User Manual V2.0

Content

1	INTRODUCTION TO STARTER KIT.....	8
1.1	HARDWARE APPEARANCE.....	8
1.2	BLOCK DIAGRAM.....	9
2	STARTER KIT SOFTWARE.....	10
2.1	SOFTWARE INSTALLER	10
2.2	STARTER KIT FIRMWARE UPDATE.....	13
2.3	SOFTWARE REMOVAL.....	14
2.4	SOFTWARE STARTUP.....	16
2.5	STARTER KIT LAUNCHER	16
3	SYSTEM REQUIREMENT	19
4	STARTER KIT SOFTWARE FUNCTION DESCRIPTION (SQ7101/SQ7103/SQ7515).....	19
4.1	SOFTWARE INTRODUCTION.....	19
4.2	STARTER KIT MAIN SCREEN.....	19
4.2.1	Build Command.....	20
4.2.2	Main Menu	22
4.2.3	Status Bar.....	25
4.2.4	Log.....	27
4.2.5	AES-256 Support	28
4.3	MEMORY	30
4.3.1	Memory Configuration	32
4.3.2	Configuration Menu.....	33
4.3.2.1	Configuration Update	33
4.3.2.2	Other Zones Update.....	34
4.3.3	Menu Bar	35
4.3.3.1	File sub-Menu.....	36
4.4	PROGRAM DEVICE	40
4.4.1	Memory Configuration	41
4.4.1.1	Configuration	41
4.4.1.2	User Zone	43
4.4.1.3	Small Zone.....	44
4.4.1.4	Counter Zone.....	45
4.4.1.5	Key	46
4.4.2	Function Options	47
4.4.3	Menu Bar	52
4.4.4	Log Window	57
5	STARTER KIT SOFTWARE FUNCTION DESCRIPTION (SQ713X).....	58

5.1	SOFTWARE INTRODUCTION.....	58
5.2	STARTER KIT MAIN SCREEN.....	58
5.2.1	Main Menu.....	58
5.2.1.1	File.....	59
5.2.1.2	Tools	59
5.2.1.3	Macro.....	60
5.2.1.4	Writer Configuration.....	61
5.2.1.5	Setting	63
5.2.1.6	View.....	64
5.2.1.7	Help	65
5.2.2	Main Windows.....	65
5.2.2.1	Zone Navigator Window.....	65
5.2.2.2	Zone View Window.....	66
5.2.2.3	Configuration Label View	67
5.2.2.4	Configuration Data Grid View.....	67
5.2.2.5	Zone Configuration Window.....	68
5.2.2.6	System Information Window.....	69
5.2.2.7	Log Window	70
6	STARTER KIT SOFTWARE FUNCTION DESCRIPTION (HQS600X).....	71
6.1	SOFTWARE INTRODUCTION.....	71
6.2	STARTER KIT MAIN SCREEN.....	71
6.2.1	Main Menu.....	71
6.2.1.1	File.....	72
6.2.1.2	Tools	72
6.2.1.3	Macro.....	73
6.2.1.4	Setting	73
6.2.1.5	Help	74
6.2.2	Main Windows.....	74
6.2.2.1	Log Window	74
6.2.2.2	Log Window	75
APPENDIX A: HARDWARE SETTINGS PRECAUTIONS FOR PROTOTYPING SQ7515.....		76
CHANGE HISTORY		78

Figure 1 iMQ Secure Starter Kit appearance (with Socket version).....	8
Figure 2 iMQ Secure Starter Kit appearance (no Socket version, used with EVB, for SQ75 series) .8	
Figure 3 iMQ Starter Kit Block Diagram	9
Figure 4 Example: iMQ_StarterKit_Setup_V3.3.....	10
Figure 5 Installation path, the default path is C:\iMQ_StarterKit.....	10

No. : TDUM02- TE002-EN	Name: Secure Starter Kit User Manual	Version : V2.0
------------------------	--------------------------------------	----------------

Figure 6 Checkbox to create a desktop shortcut.....	11
Figure 7 Reconfirm the installation data	11
Figure 8 Checkbox to launch iMO StarterKit Tool	12
Figure 9 Cannot find Secure StarterKit warning message	12
Figure 10 firmware update message	13
Figure 11 firmware successfully update message	14
Figure 12 Installation directory	14
Figure 13 Confirm to uninstall StarterKit.....	15
Figure 14 Uninstall successful message	15
Figure 15 iMO StarterKit Tool shortcut icon	16
Figure 16 Using the Secure Starter Kit, and Socket is SQ7101 (I2C) device.....	16
Figure 17 Using the Secure Starter Kit, and Socket is SQ7103 (SPI) device.	16
Figure 18 Use the Secure Starter Kit to configure or read the Security Processor with SQ7515 EVB.....	17
Figure 19 Using the Secure Starter Kit, and Socket is SQ7131 (I2C) device.....	17
Figure 20 Using the Secure Starter Kit, and Socket is SQ7133 (SPI) device.	17
Figure 21 Using the Secure Starter Kit, and Socket is SQ7135 (SWI) device.....	18
Figure 22 Using the Secure Starter Kit, and Socket is HOS6004 (SPI) device.....	18
Figure 23 Cannot find Secure StarterKit message	18
Figure 24 SQ710x Starter Kit main screen	20
Figure 25 SQ710x Build Command area	21
Figure 26 SQ710x Main menu	22
Figure 27 SQ710x File sub menu.....	22
Figure 28 SQ710x Memory sub menu	23
Figure 29 SQ710x Tool sub menu/XOR.....	23
Figure 30 SQ710x Tool sub menu/Program Device	24
Figure 31 SQ710x: SQ710x About sub menu	24
Figure 32 SQ710x SQ710x About dialog	24
Figure 33 SQ710x Status bar	25
Figure 34 SQ710x Status bar (SPI device)	26
Figure 35 SQ710x Log area	27
Figure 36 SQ710x Enable AES-256	28
Figure 37 SQ710x Memory: AES256 field selected as "Yes"	29
Figure 38 SQ710x Click Memory on the main menu	30
Figure 39 SQ710x Memory window	31
Figure 40 SQ710x Memory: Memory configuration block.....	32
Figure 41 SQ710x Memory: Configuration update.....	33

No. : TDUM02- TE002-EN	Name: Secure Starter Kit User Manual	Version : V2.0
------------------------	--------------------------------------	----------------

Figure 42 SQ710x Memory: User Zone update	34
Figure 43 SQ710x Memory: Menu bar.....	35
Figure 44 SQ710x Memory: File sub menu/Export file.....	36
Figure 45 SQ710x Memory: Export file dialog	36
Figure 46 SQ710x Memory: Export finish message	37
Figure 47 SQ710x Memory: File sub menu/Import file.....	37
Figure 48 SQ710x Memory: Import file dialog.....	37
Figure 49 SQ710x Memory: Select import data dialog	38
Figure 50 SQ710x Memory: Import data finish message	38
Figure 51 SQ710x Memory: Reload Data sub menu item.....	39
Figure 52 SQ710x Memory: Reloading memory dialog	39
Figure 53 SQ710x Starter Kit Tool sub menu/Program Device	40
Figure 54 SQ710x Program Device window.....	41
Figure 55 SQ710x Program Device: Configuration Zone	42
Figure 56 SQ710x Program Device: User Zone	43
Figure 57 SQ710x Program Device: Small Zone	44
Figure 58 SQ710x Program Device: Counter Zone.....	45
Figure 59 SQ710x Program Device: Key Zone.....	46
Figure 60 SQ710x Program Device: Function Options	47
Figure 61 SQ710x Program Device: Program confirm message box	48
Figure 62 SQ710x Program Device: Socket device not detected message box.....	48
Figure 63 SQ710x Program Device: Communication mode not match message box	49
Figure 64 SQ710x Program Device: Zone Locked message box	49
Figure 65 SQ710x Program Device: Small zone locked, continue dialog.	49
Figure 66 SQ710x Program Device: AES mode not match message box.....	50
Figure 67 SQ710x Program Device: Program Done message box	50
Figure 68 SQ710x Program Device:Export log	51
Figure 69 SQ710x Program Device: Export log dialog	51
Figure 70 SQ710x Program Device: Clear Log.....	51
Figure 71 SQ710x Program Device: Menu bar	52
Figure 72 SQ710x Program Device: File menu/Export Data	53
Figure 73 SQ710x Program Device: Export Data dialog	53
Figure 74 SQ710x Program Device: Export data done message box.....	53
Figure 75 SQ710x Program Device: File menu/Import Data/Socket Device	54
Figure 76 SQ710x Program Device: File menu/Import Data/On Board Device	54
Figure 77 SQ710x Program Device: File menu/Import Data/File	54
Figure 78 SQ710x Program Device: Import file dialog	55

No. : TDUM02- TE002-EN	Name: Secure Starter Kit User Manual	Version : V2.0
------------------------	--------------------------------------	----------------

Figure 79 SQ710x Program Device: Import file done message.....	55
Figure 80 SQ710x Program Device: Import Data: Block Read Error message box.....	56
Figure 81 SQ710x Program Device: Log Window	57
Figure 82 SQ710x Program Device: Copy contents of Log Window	57
Figure 83 SQ713x Main screen	58
Figure 84 SQ713x Main menu	58
Figure 85 SQ713x File sub menu.....	59
Figure 86 SQ713x Tools sub menu	59
Figure 87 SQ713x Cryptor Calculator	59
Figure 88 SQ713x Command Builder	60
Figure 89 SQ713x Macro sub menu.....	60
Figure 90 SQ713x Writer Configuration sub menu	61
Figure 91 SQ713x Writer Configuration Utility/Configuration Zone	61
Figure 92 SQ713x Writer Configuration Utility/SlotKey Configuration.....	62
Figure 93 SQ713x Writer Configuration Utility/Data Slot EditWrite.....	63
Figure 94 SQ713x Programming device twice inhibition message.....	63
Figure 95 SQ713x Setting sub menu	64
Figure 96 SQ713x I2C I/O Setting	64
Figure 97 SQ713x SPI I/O Setting	64
Figure 98 SQ713x SWI does not support I/O Setting	64
Figure 99 SQ713x View sub menu.....	64
Figure 100 SQ713x Help sub menu	65
Figure 101 SQ713x About dialog	65
Figure 102 SQ713x Zone navigator window	65
Figure 103 SQ713x Editable and savable data grid view	66
Figure 104 SQ713x Non-editable and non-savable data grid view.....	66
Figure 105 SQ713x Configuration label view	67
Figure 106 SQ713x Configuration data grid view	67
Figure 107 SQ713x Zone configuration window (Configuration zone)	68
Figure 108 SQ713x Zone configuration window (Slot zone).....	68
Figure 109 SQ713x Zone description of Data/Key Slot Zone.....	69
Figure 110 SQ713x System information window/Device state	69
Figure 111 SQ713x System information window/Lock state	69
Figure 112 SQ713x System information window/System status	70
Figure 113 SQ713x Log window.....	70
Figure 114 HQS600x Main screen.....	71
Figure 115 HQS600x Main menu	71

No. : TDUM02- TE002-EN	Name: Secure Starter Kit User Manual	Version : V2.0
------------------------	--------------------------------------	----------------

Figure 1 16 HOS600x File sub-menu.....	72
Figure 1 17 HOS600x Tools sub-menu	72
Figure 1 18 HOS600x Crypto calculator	72
Figure 1 19 HOS600x Command builder	73
Figure 120 HOS600x Macro sub-menu	73
Figure 121 HOS600x Setting sub-menu	73
Figure 122 HOS600x I2C I/O Setting	74
Figure 123 HOS600x SPI I/O Setting	74
Figure 124 HOS600x Help sub-menu	74
Figure 125 HOS600x About dialog	74
Figure 126 HOS600x System information/System status	75
Figure 127 HOS600x Log window	75
Figure 128 SQ7515 hardware settings	76
Figure 129 EVBV 1.1 Add a Reset grounding jumper	76

1 Introduction to Starter Kit

1.1 Hardware Appearance

The Secure Starter Kit is powered by the USB port. Plug the Starter Kit into the USB port and turn the PWR switch to ON position. When the connection to the computer is successful, the power indicator light will be on (green light). After the software starts, it will scan the currently connected IC devices.



Figure 1 iMO Secure Starter Kit appearance (with Socket version)

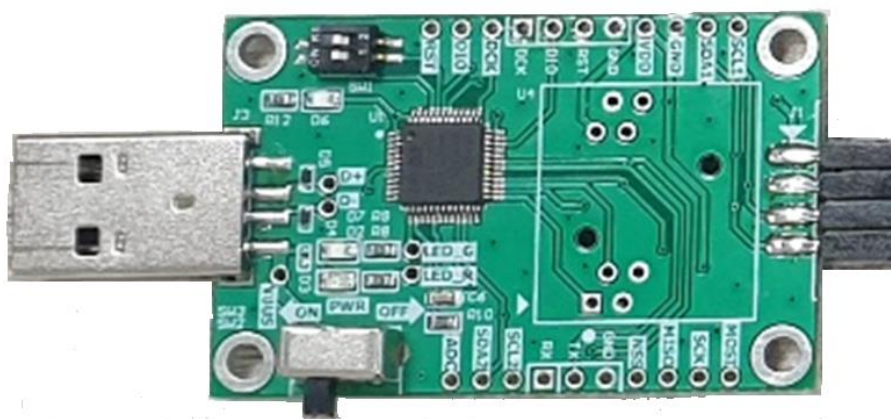


Figure 2 iMO Secure Starter Kit appearance (no Socket version, used with EVB, for SQ75 series)

Note: Developed for SQ75 series. Please refer to the hardware setting precautions [Appendix A](#).

If developing the IC placed on the Socket, the PWR power switch should be switch to OFF position before replacing the IC. After the IC is replace, turn the PWR power switch to ON position again to avoid IC failure caused by live wire operation.

The IC replacement process placed in the socket is as follows

1. Turn the PWR power switch to OFF position to turn off the power.
2. Replace the next IC.
3. Turn the PWR power switch to ON position to turn on the power.

1.2 Block Diagram

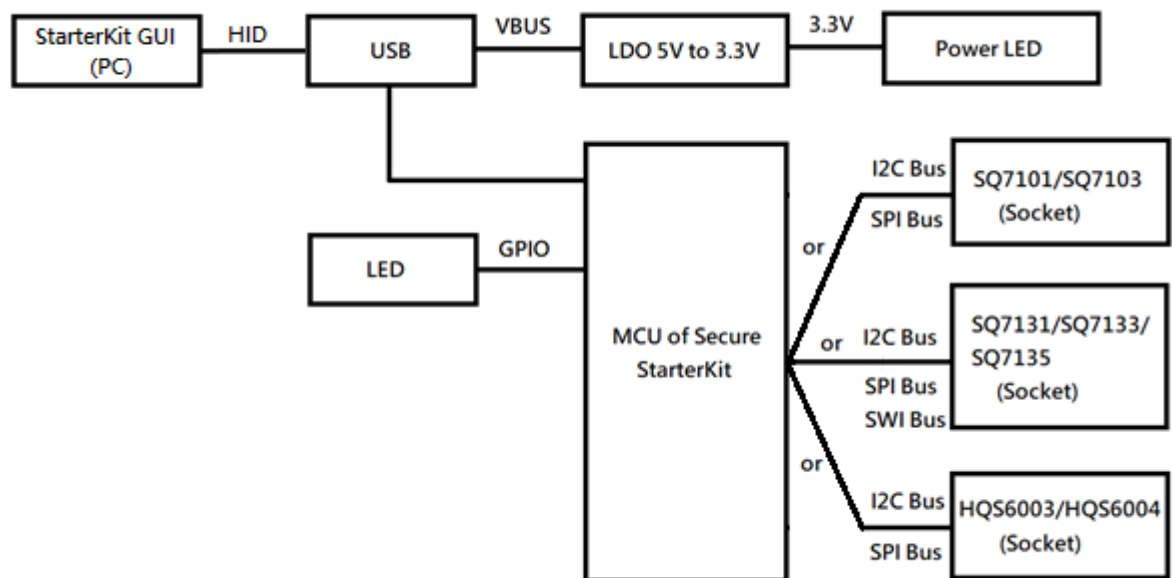


Figure 3 iMO Starter Kit Block Diagram

2 Starter Kit Software

2.1 Software Installer

Step 1. Click the iMQ StarterKit Setup installation program to execute the installation.

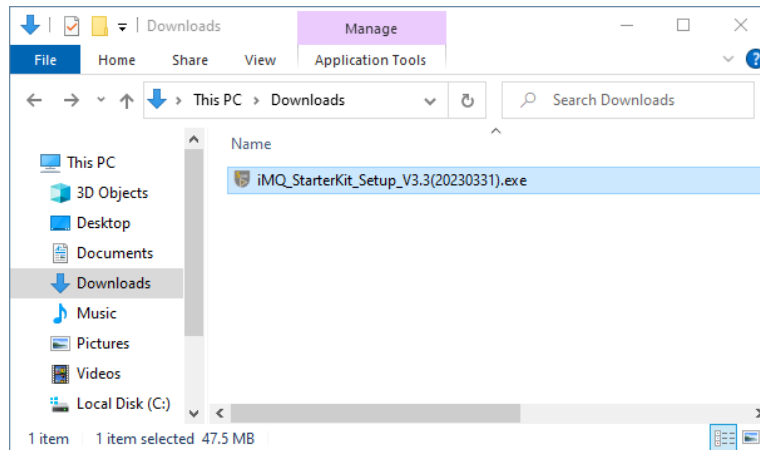


Figure 4 Example: iMQ_StarterKit_Setup_V3.3

Step 2. Select the iMQ StarterKit installation path, Press "Next".

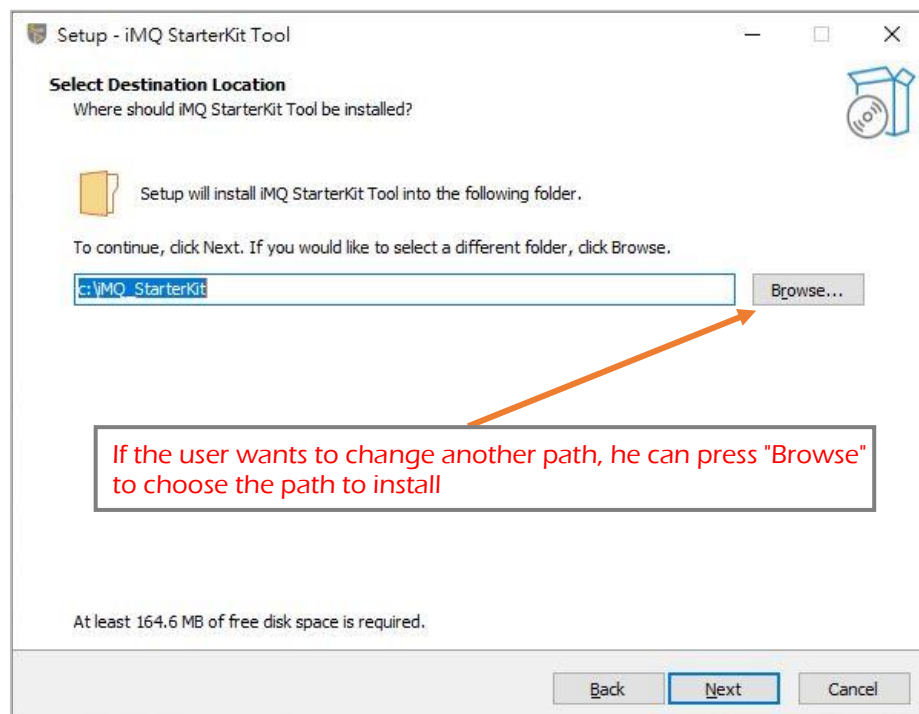


Figure 5 Installation path, the default path is C:\iMQ_StarterKit

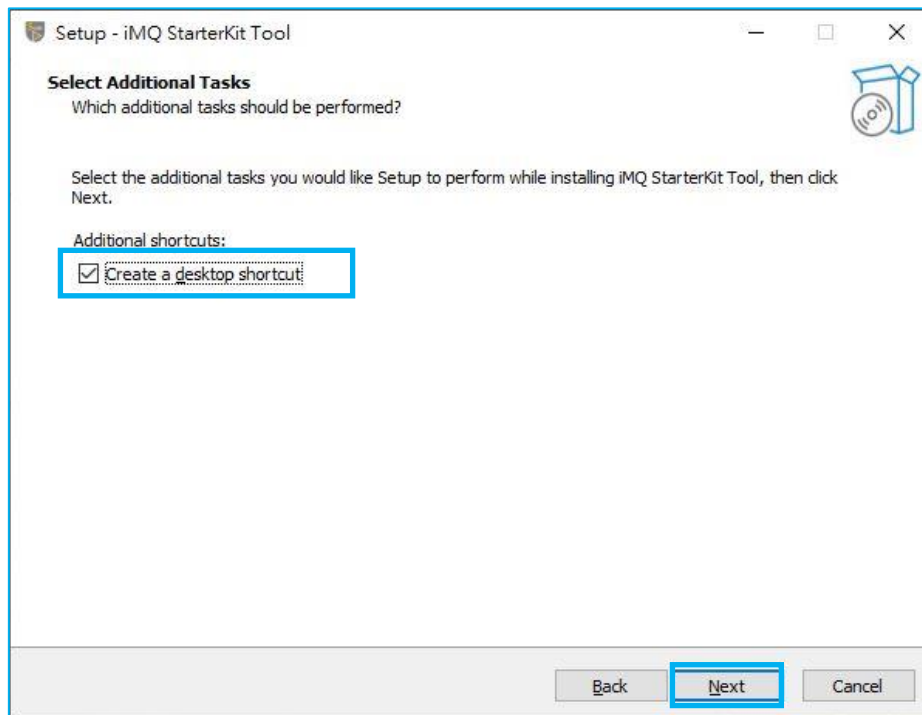
Step 3. After ticking Create a desktop shortcut, Press "Next".

Figure 6 Checkbox to create a desktop shortcut

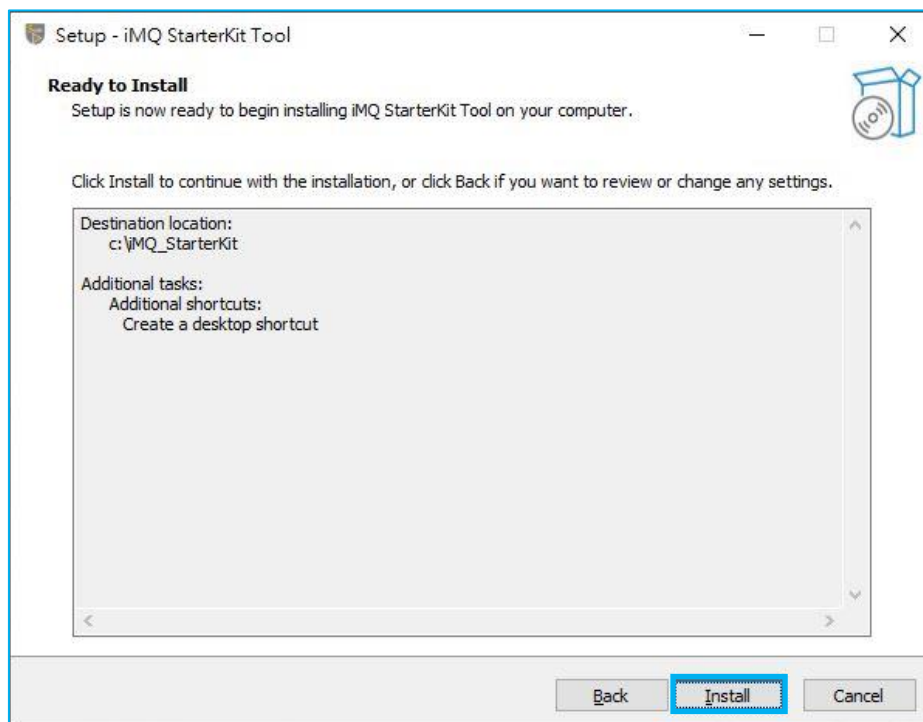
Step 4. This page will reconfirm the installation path and whether to create a shortcut icon. If there is no problem, press "Install" to install.

Figure 7 Reconfirm the installation data

Step 5. Press "Finish" to complete the installation.

Figure 8 Checkbox to launch iMQ StarterKit Tool

Note: If the Secure Starter Kit is not connected to the computer when the Starter Kit software is executed, you will not be able to enter the main screen for use, and a "Device not connected" warning window will pop up.

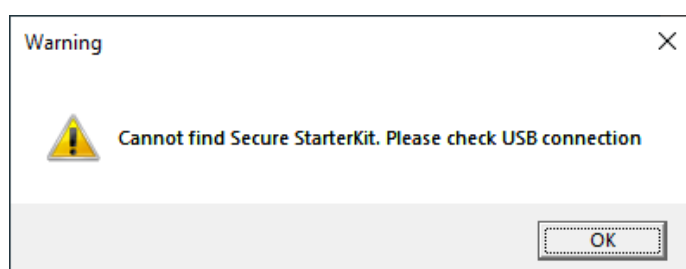


Figure 9 Cannot find Secure StarterKit warning message

2.2 Starter Kit Firmware Update

The update of firmware is not always necessary. It is only necessary to update firmware when firmware version is updated (Updated information will be described in the release note).

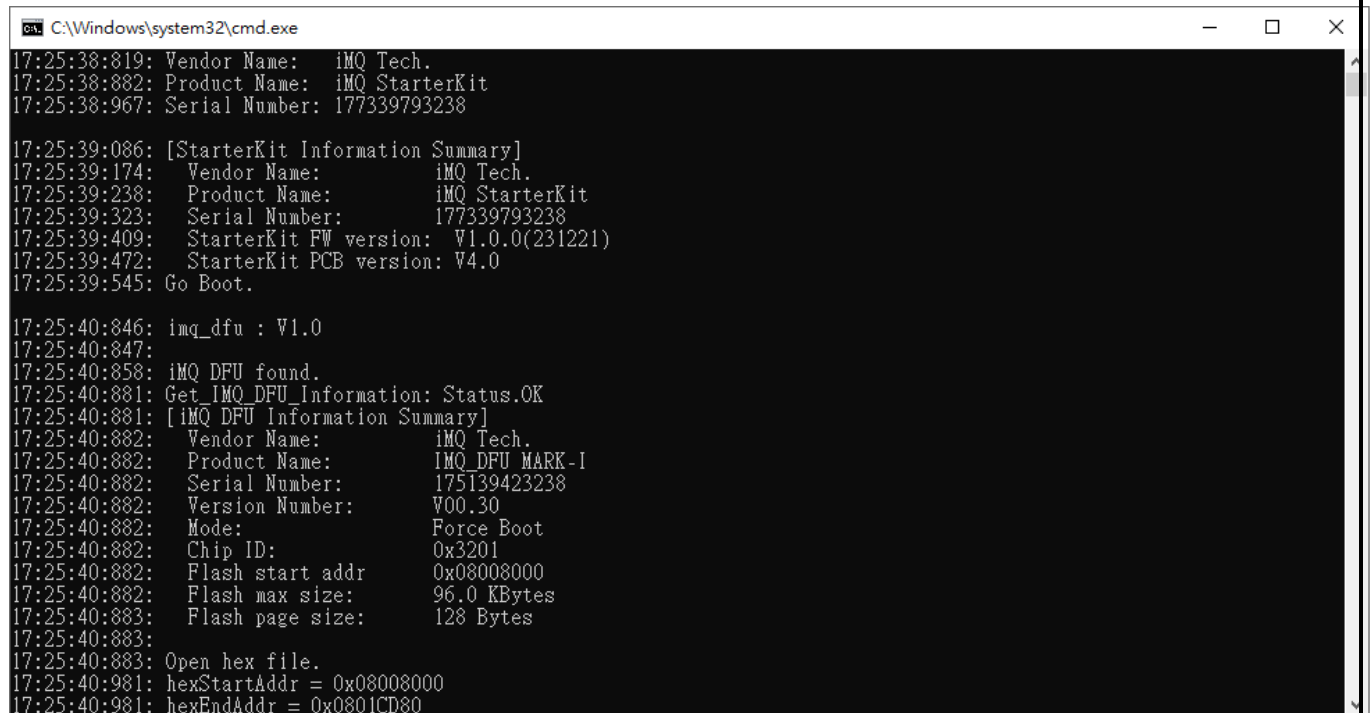
The installation steps are as follows:

Step1. Connect your PC to the StarterKit using a USB cable

Step2. Power on StarterKit

Step3. Change Windows directory to c:\iMQ\Firmware

Step4. Execute update.bat



```

C:\Windows\system32\cmd.exe
17:25:38:819: Vendor Name: iMQ Tech.
17:25:38:882: Product Name: iMQ StarterKit
17:25:38:967: Serial Number: 177339793238

17:25:39:086: [StarterKit Information Summary]
17:25:39:174: Vendor Name: iMQ Tech.
17:25:39:238: Product Name: iMQ StarterKit
17:25:39:323: Serial Number: 177339793238
17:25:39:409: StarterKit FW version: V1.0.0(231221)
17:25:39:472: StarterKit PCB version: V4.0
17:25:39:545: Go Boot.

17:25:40:846: imq_dfu : V1.0
17:25:40:847:
17:25:40:858: iMQ DFU found.
17:25:40:881: Get_IMQ_DFU_Information: Status.OK
17:25:40:881: [iMQ DFU Information Summary]
17:25:40:882: Vendor Name: iMQ Tech.
17:25:40:882: Product Name: IMQ DFU MARK-I
17:25:40:882: Serial Number: 175139423238
17:25:40:882: Version Number: V00.30
17:25:40:882: Mode: Force Boot
17:25:40:882: Chip ID: 0x3201
17:25:40:882: Flash start addr 0x08008000
17:25:40:882: Flash max size: 96.0 KBytes
17:25:40:883: Flash page size: 128 Bytes
17:25:40:883:
17:25:40:883: Open hex file.
17:25:40:981: hexStartAddr = 0x08008000
17:25:40:981: hexEndAddr = 0x0801CD80
  
```

Figure 10 firmware update message

Step5. Update successfully

```

C:\Windows\system32\cmd.exe
17:25:48:149: DFU_Flash_Erase: Status.OK
17:25:48:152: DFU_Flash_Write: ADDR = 0x0801B000, Size = 0x1000
17:25:48:387: DFU_Flash_Write: Status.OK
17:25:48:387: DFU_Flash_Erase: ADDR = 0x0801C000, Size = 0x0D80
17:25:48:496: DFU_Flash_Erase: Status.OK
17:25:48:497: DFU_Flash_Write: ADDR = 0x0801C000, Size = 0x0D80
17:25:48:698: DFU_Flash_Write: Status.OK
17:25:48:698: Programing finish.
17:25:48:762: DFU_Get_CRC: Status.OK
17:25:48:762: DFU_Get_CRC: APP FW CRC = 0xABE7
17:25:48:764: Verify CRC Success.
17:25:48:824: DFU_Go_APP: Status.OK
17:25:48:824: Go APP Success.
17:25:48:825: Elapsed time: 7 seconds 978 ms
17:25:48:826:
17:25:50:013: Vendor Name: iMQ Tech.
17:25:50:117: Product Name: iMQ StarterKit
17:25:50:289: Serial Number: 177339793238

17:25:50:445: [StarterKit Information Summary]
17:25:50:563: Vendor Name: iMQ Tech.
17:25:50:663: Product Name: iMQ StarterKit
17:25:50:803: Serial Number: 177339793238
17:25:50:930: StarterKit FW version: V1.0.0(231221)
17:25:51:030: StarterKit PCB version: V4.0
17:25:51:123: Total 0 device detected.

Press any key to continue . . .

```

Figure 11 firmware successfully update message

2.3 Software Removal

Completely remove the installed iMQ StarterKit, you can remove it according to the normal removal process or follow the steps below:

Step 1. Click to execute unin000.exe from the installation directory

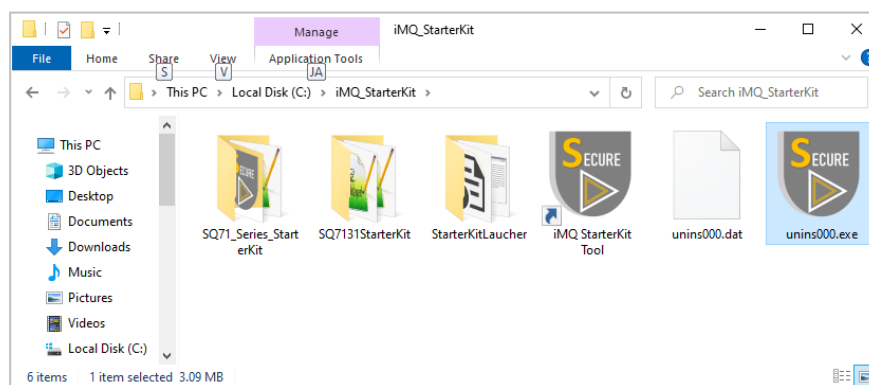


Figure 12 Installation directory

Step 2. Confirm whether you want to remove the StarterKit software

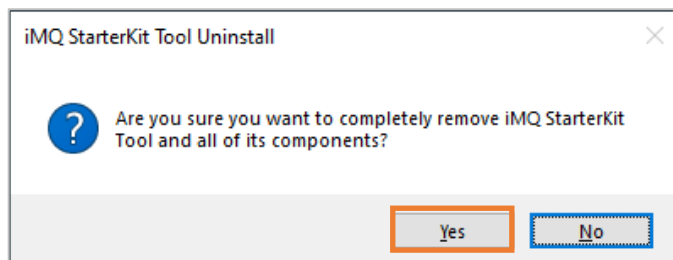


Figure 13 Confirm to uninstall StarterKit

Step 3. Successful removal

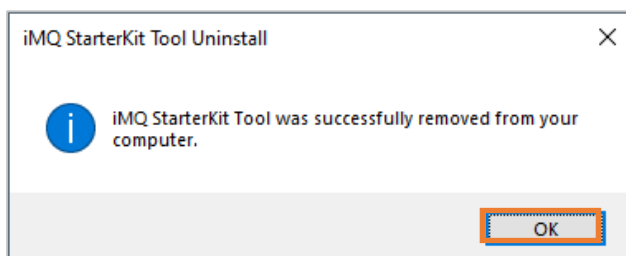


Figure 14 Uninstall successful message

2.4 Software Startup

Step 1. Connect the Secure Starter Kit to the computer via USB.

Step 2. Execute iMQ StarterKit software program

Double-click the iMQ StarterKit Tool shortcut icon to start software.



Figure 15 iMQ StarterKit Tool shortcut icon

2.5 Starter Kit Launcher

When different devices on the Starter Kit Socket are equipped with different interfaces, the launcher will detect and display the currently connected device and interface information in the list. The user selects the device and clicks "Select Device" to enter the main screen.



Figure 16 Using the Secure Starter Kit, and Socket is SQ7101 (I2C) device.



Figure 17 Using the Secure Starter Kit, and Socket is SQ7103 (SPI) device.



Figure 18 Use the Secure Starter Kit to configure or read the Security Processor with SQ7515 EVB

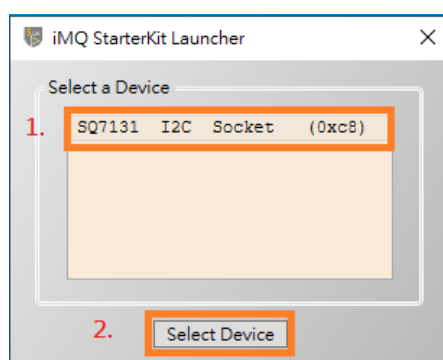


Figure 19 Using the Secure Starter Kit, and Socket is SQ7131 (I2C) device.

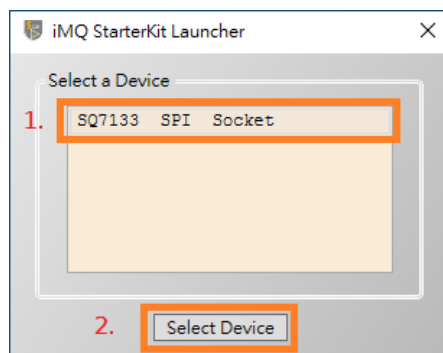


Figure 20 Using the Secure Starter Kit, and Socket is SQ7133 (SPI) device.

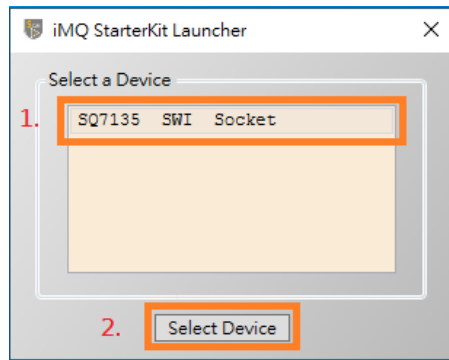


Figure 21 Using the Secure Starter Kit, and Socket is SQ7135 (SWI) device.

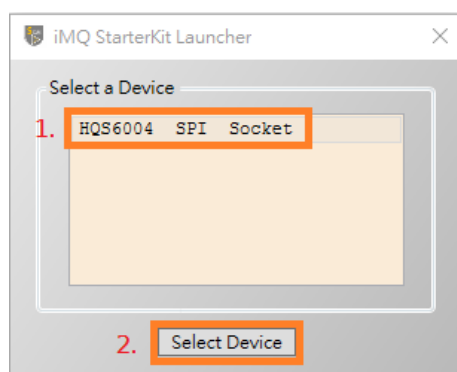


Figure 22 Using the Secure Starter Kit, and Socket is HQS6004 (SPI) device.

Note: When replacing the IC on the Socket, please make sure that the PWR switch on the Starter Kit is turn off. Please refer to [1.1 Hardware Appearance](#)

If the device is not scanned, a prompt screen as shown in the figure below will pop up, and the user can check whether the Secure Starter Kit is connected to the computer.

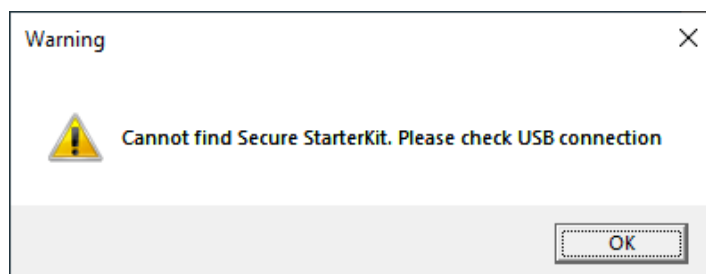


Figure 23 Cannot find Secure StarterKit message

3 System Requirement

Before using the Security Starter Kit, prepare the following items and confirm your computer's system specifications.

- Windows 10 OS, Microsoft.NET Framework 4.8 (inclusive) or above.
- Secure Starter Kit (Hardware)
- iMQ Starter Kit Setup Software installation package

Note : [Microsoft.NET Framework 4.8 Official Download](#)

4 Starter Kit Software Function Description (SQ7101/SQ7103/SQ7515)

The function description in this chapter applies to support symmetric encryption algorithm products. (e.g. SQ7101, SQ7103, SQ7515)

4.1 Software Introduction

The user interface is divided into two windows. The first is the main screen, all build command, sending commands, opening the Memory window, toolbox (Tool), transfer records, etc. are all executed and displayed in this window; The second is the memory window, it must be opened from the main screen to be displayed, and its function is to configure the memory.

4.2 Starter Kit Main Screen

The main screen is divided into four parts, namely:

1. **Build Command:** Including command packet block, send packet information block, receive return packet information block and execute command button.
2. **Menu Bar:** Menus for File, Memory, Tool, and About.
3. **Status Bar:** Displays the connected device, its communication protocols and device addresses.
4. **Log:** Record the time and content of command transmission and received messages.

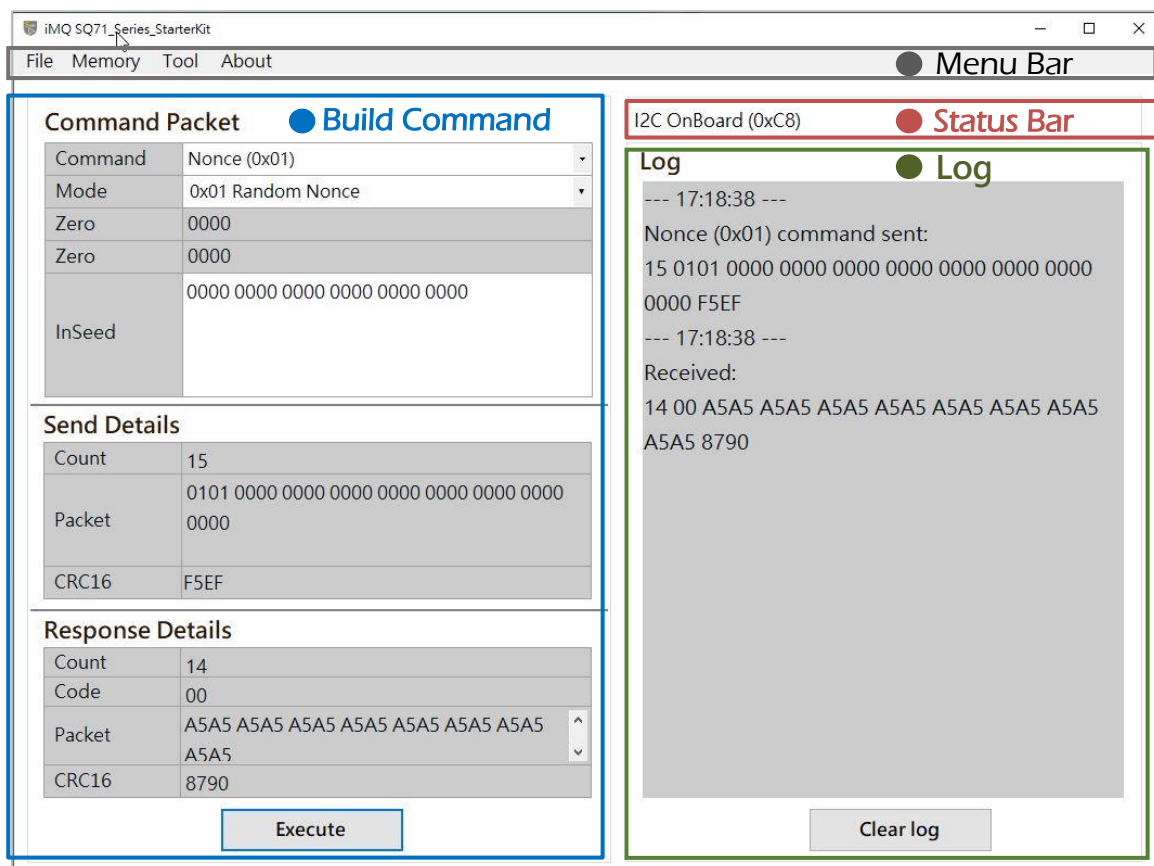


Figure 24 SQ710x Starter Kit main screen

4.2.1 Build Command

The Build Command area is divided into three blocks, namely: command packet block, send detail block, response details block and execute button.

- 1. Command packet block:** It is used to select commands, modes, parameters and other settings. Commands are drop-down menus, and there are many commands to choose. The parameters will change according to the command selected by the user.
- 2. Execute button:** After pressing "Execute", the command and parameter in the command packet block will be executed.
- 3. Send details block:** Display the data length, content and CRC check code of the transmitted packet.
- 4. Response details block:** Display the data length, return code, content and CRC check code of the received packet.

Note 1 : All fields are expressed in hexadecimal

Note 2 : The gray background field is read-only information, user cannot modify it; The white background field, it means user can input or select it.

Note 3 : If the IC is in deep sleep mode and has not been woken up, it will ignore any command received through I2C or SPI and return NAK, and the IC will return to the operation mode. When the Host receives the NAK, it has to resend the command to execute.

The diagram illustrates the 'Build Command area' for the SQ710x device, organized into three main sections: Command Packet, Send Details, and Response Details. Each section has a title and a corresponding icon (a blue circle with a dot).

Command Packet (Command packet block):

- Command:** A dropdown menu currently showing 'Encrypt (0x06)'.
- Mode:** A dropdown menu currently showing '0x00'.
- EKeyID:** A text field containing '0000'.
- Count:** A text field containing '0010'.
- Data:** A large text area containing '0000 0000 0000 0000 0000 0000 0000 0000'.

Send Details (Send details block):

- Count:** A text field containing '19'.
- Packet:** A text area containing '0600 0000 0010 0000 0000 0000 0000 0000' and '0000 0000 0000'.
- CRC16:** A text field containing 'E9E0'.

Response Details (Response details block):

- Count:** A text field.
- Code:** A text field.
- Packet:** A text area.
- CRC16:** A text field.

Execute button: A button labeled 'Execute'.

Labels on the left side of the diagram point to specific fields:

- Command:** Points to the Command dropdown.
- Change fields by command:** Points to the EKeyID field.
- Send packet:** Points to the Count field in the Send Details section.
- Length:** Points to the Count field in the Send Details section.
- Content:** Points to the Packet field in the Send Details section.
- CRC check code:** Points to the CRC16 field in the Send Details section.
- Response packet:** Points to the Count field in the Response Details section.
- Length:** Points to the Count field in the Response Details section.
- Return code:** Points to the Code field in the Response Details section.
- Content:** Points to the Packet field in the Response Details section.
- CRC check code:** Points to the CRC16 field in the Response Details section.

Figure 25 SQ710x Build Command area

4.2.2 Main Menu

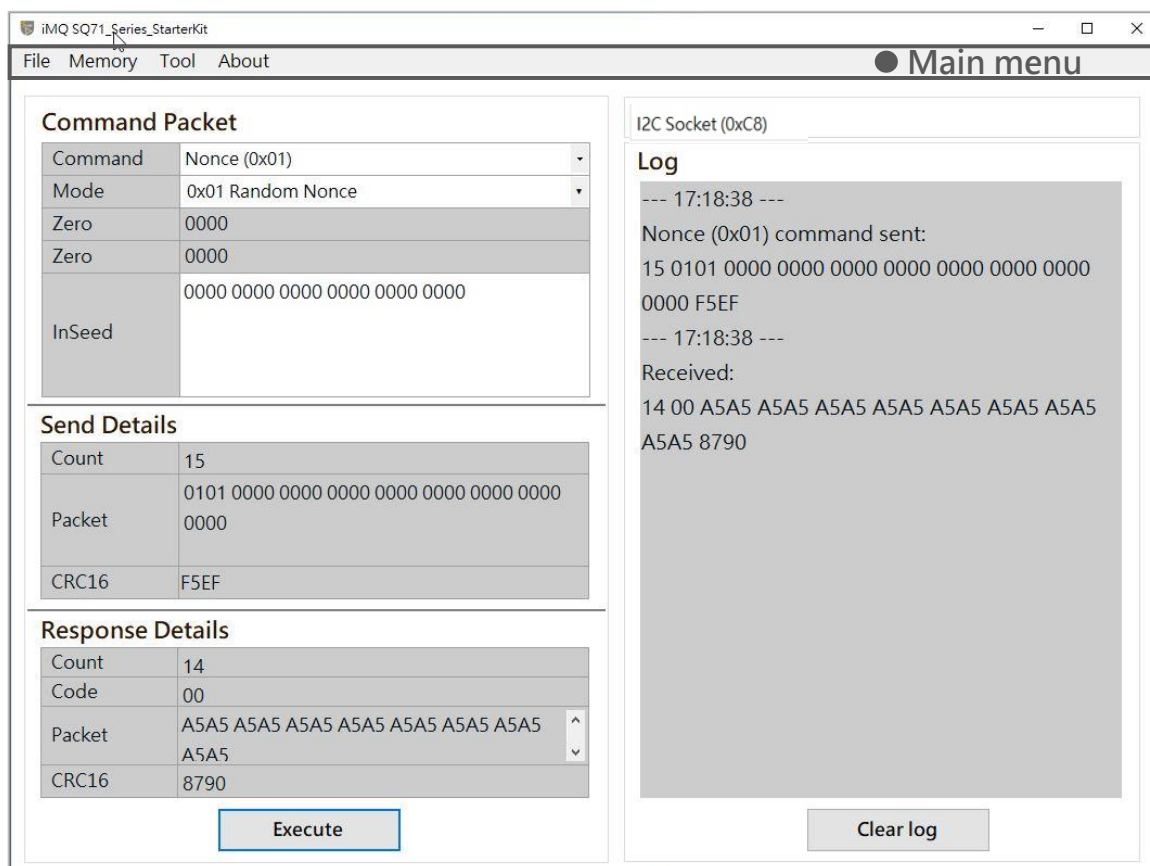


Figure 26 SQ710x Main menu

There are menus for File, Memory, Tool, and about on the menu bar, as shown in the figure below:

1. **File sub menu:** Click File, press Exit to close the main screen and memory window.
File\Exit



Figure 27 SQ710x File sub menu

2. Memory sub-menu: Click Memory, it will pop up memory window after the reading is completed.

Note 1: **Do not remove the Secure Starter Kit from the computer while the reading is in progress.**

Note 2: The memory window will be explained in the following chapter 「[4.1.3 Memory](#)」

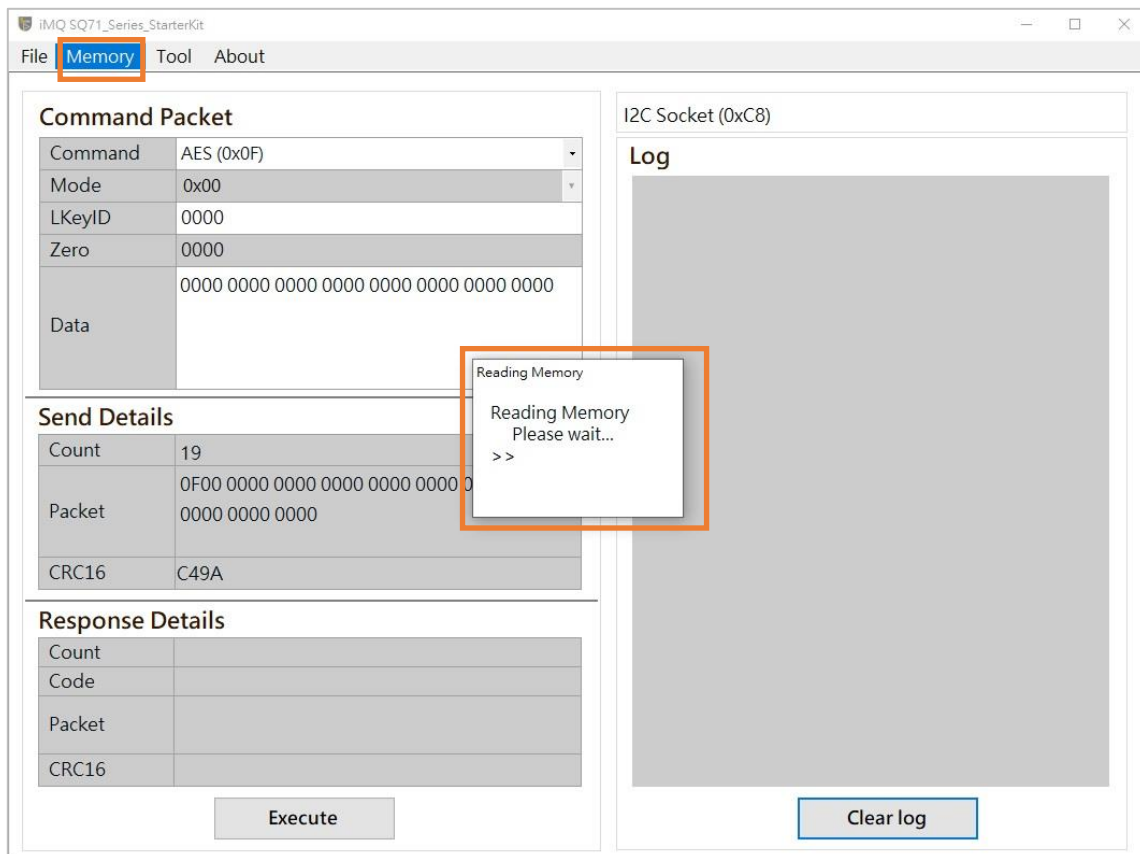


Figure 28 SQ710x Memory sub menu

3. Tool sub-menu: Click Tool, and then select XOR to open the XOR calculation.

Tool\XOR



Figure 29 SQ710x Tool sub menu/XOR

Note 1: When Data1 and Data2 have different lengths, the effective calculation length will be based on the shorter Data length.

Note 2: XOR calculation tool for hexadecimal calculation.

Click Tool, and then select Program Device to open the Program Device window.

Tool\Program



Figure 30 SQ710x Tool sub menu/Program Device

Note 3: The program device window will be explained in the following chapter 「[4.1.4 Program Device](#)」

4. About sub-menu: Click About to view software, firmware, and Secure Starter Kit hardware versions information.



Figure 31 SQ710x: SQ710x About sub menu

Note 1: **Do not remove the Security Starter Kit from your computer while viewing the version.**

Note 2: When a new version of iMQ StarterKit is released, it will be released on the following website:

<http://www.imqtech.com/>

<http://www.imqtech.com.cn/>

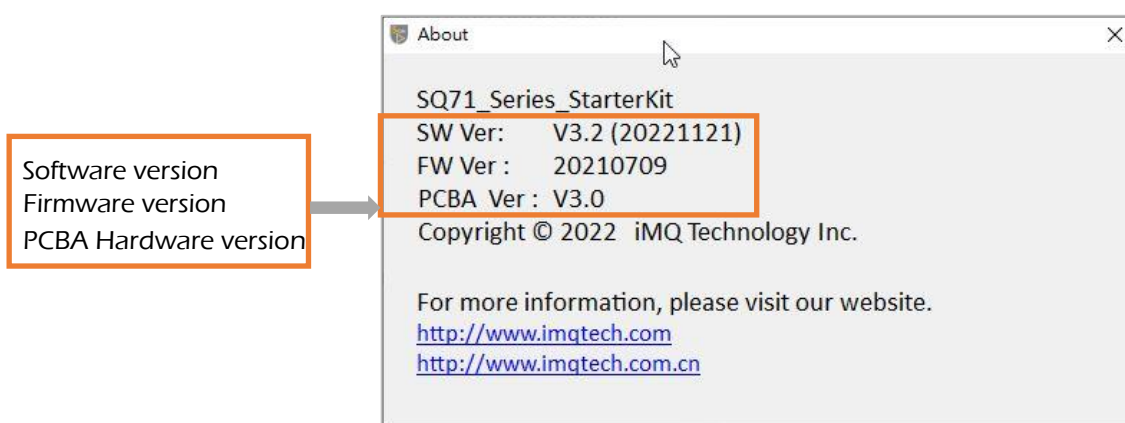


Figure 32 SQ710x SQ710x About dialog

4.2.3 Status Bar

The communication protocol and device address of the device connected to Starter Kit will be displayed on the status bar. As shown in the figure below, the communication protocol is I2C, and the device I2C address is 0xC8.

Note 1: The communication protocol and device address displayed on the status bar are the same as the slave device selected by the user before entering the main screen.

Note 2: After entering the main screen, if you change the communication address of the device, you must re-plug the Secure Starter Kit and restart the Starter Kit program, the new device address will take effect.

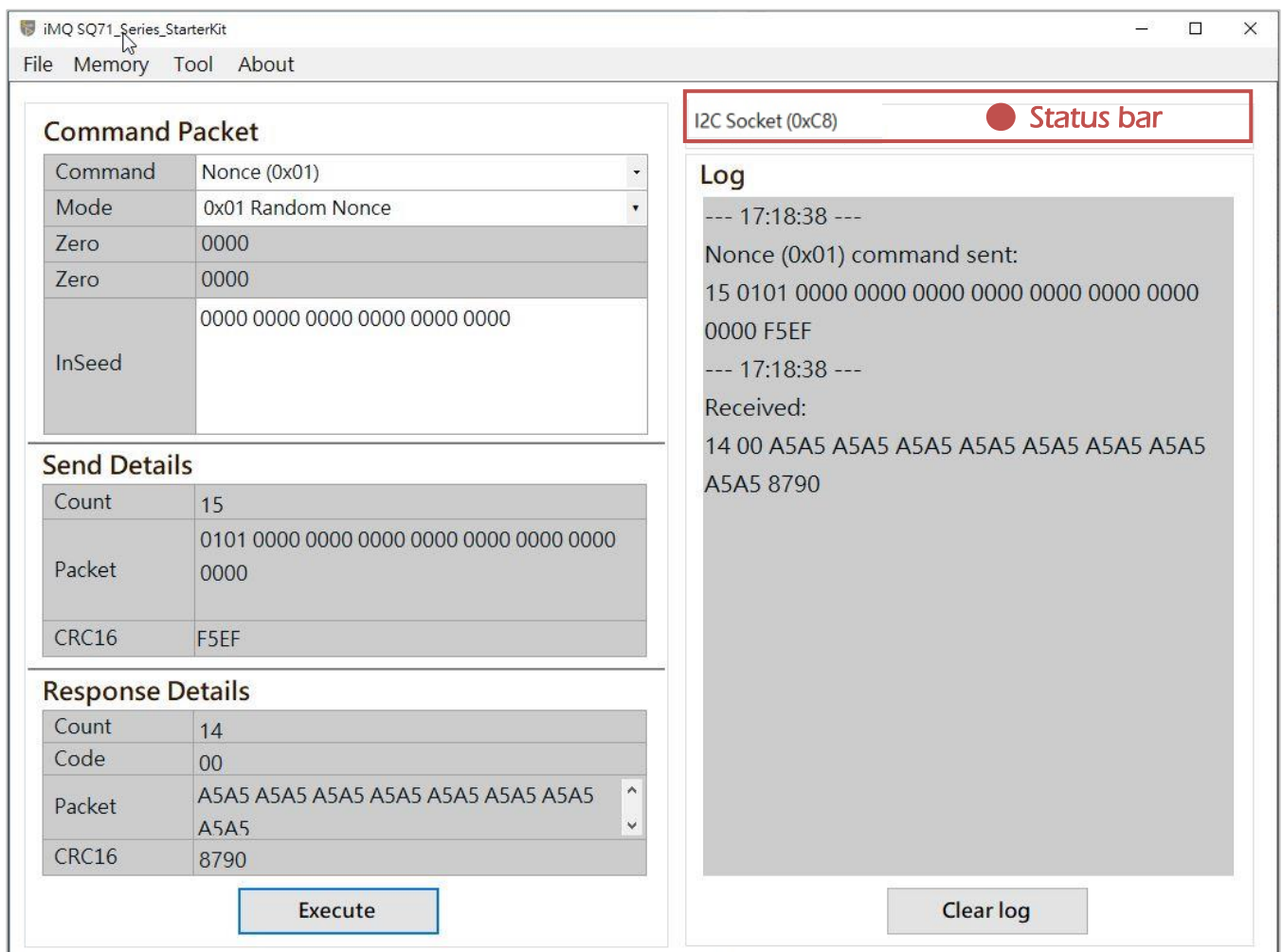


Figure 33 SQ710x Status bar

If the slave device is a SPI device (such as SQ7103), the status bar will display "SPI Socket".

The screenshot shows the iMQ SQ71_Series_StarterKit application window. The interface is divided into several sections:

- Command Packet:** A table with fields for Command (AES (0x0F)), Mode (0x00), LKeyID (0000), Zero (0000), and Data (0000 0000 0000 0000 0000 0000 0000 0000).
- Send Details:** A table with fields for Count (19), Packet (0F00 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000), and CRC16 (C49A).
- Response Details:** A table with fields for Count, Code, Packet, and CRC16.
- Status bar:** Located at the top right, it displays "SPI Socket" next to a red dot icon.
- Log:** A large text area for logging, currently empty.
- Buttons:** "Execute" and "Clear log" buttons are located at the bottom of the Command Packet and Log sections, respectively.

Figure 34 SQ710x Status bar (SPI device)

4.2.4 Log

This area records the time and content of command sending and receiving packet messages.

The screenshot shows the iMQ SQ71_Series_StarterKit application window. It has a menu bar with 'File', 'Memory', 'Tool', and 'About'. The main area is divided into several sections:

- Command Packet:** A table with fields: Command (Nonce (0x01)), Mode (0x01 Random Nonce), Zero (0000), Zero (0000), and InSeed (0000 0000 0000 0000 0000 0000).
- Send Details:** A table with fields: Count (15), Packet (0101 0000 0000 0000 0000 0000 0000 0000 0000), and CRC16 (F5EF).
- Response Details:** A table with fields: Count (14), Code (00), Packet (A5A5 A5A5 A5A5 A5A5 A5A5 A5A5 A5A5 A5A5), and CRC16 (8790).
- Log:** A large text area showing the log of commands and responses. It includes a timestamp '--- 17:18:38 ---' and the following text:


```
Nonce (0x01) command sent:
15 0101 0000 0000 0000 0000 0000 0000 0000
0000 F5EF
--- 17:18:38 ---
Received:
14 00 A5A5 A5A5 A5A5 A5A5 A5A5 A5A5 A5A5
A5A5 8790
```

At the bottom of the Command Packet, Send Details, and Response Details sections are buttons labeled 'Execute' and 'Clear log' respectively. A green dot and the text 'Log area' are also present in the Log section.

Figure 35 SQ710x Log area

Note 1: If there are too many logs, users can click the "Clear Logs" button to clear the logs.

Note: After the log is cleared, it cannot be restored!

4.2.5 AES-256 Support

Support AES-256 key, AES-256 option appears on some Command windows item, check to enable/disable the support for AES-256 key.

iMQ SQ71_Series_StarterKit

File Memory Tool About

Command Packet ☒ AES-256

Command	EncWrite (0x05)
Mode	0x00
Address	0000
Count	0020
Data	0000 0000

Send Details

Count	39
Packet	0500 0000 0020 0000
CRC16	C105

Response Details

Count	
Code	
Packet	
CRC16	

Execute

Figure 36 SQ710x Enable AES-256

To enable AES-256, you must first set Byte-4 of the key configuration in the Memory page, and select "Yes" for the AES256 field.

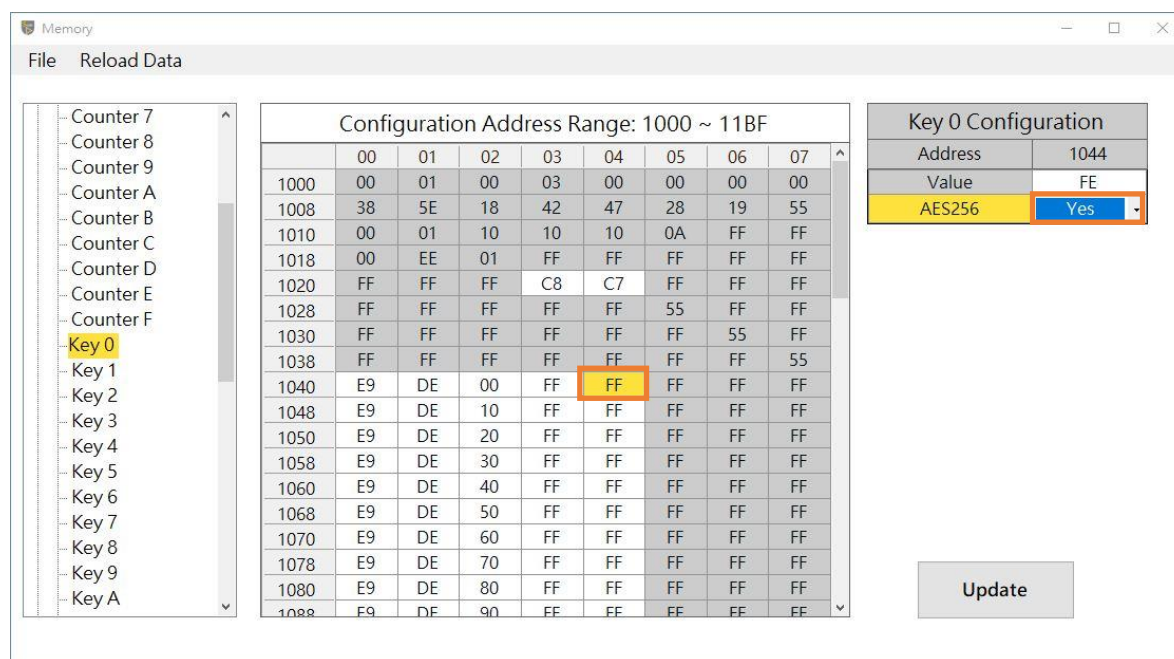


Figure 37 SQ710x Memory: AES256 field selected as "Yes"

4.3 Memory

Click “Memory”, and the memory window will pop up after the reading is completed.

Note: Do not remove the Secure Starter Kit from the computer while the reading is in progress.

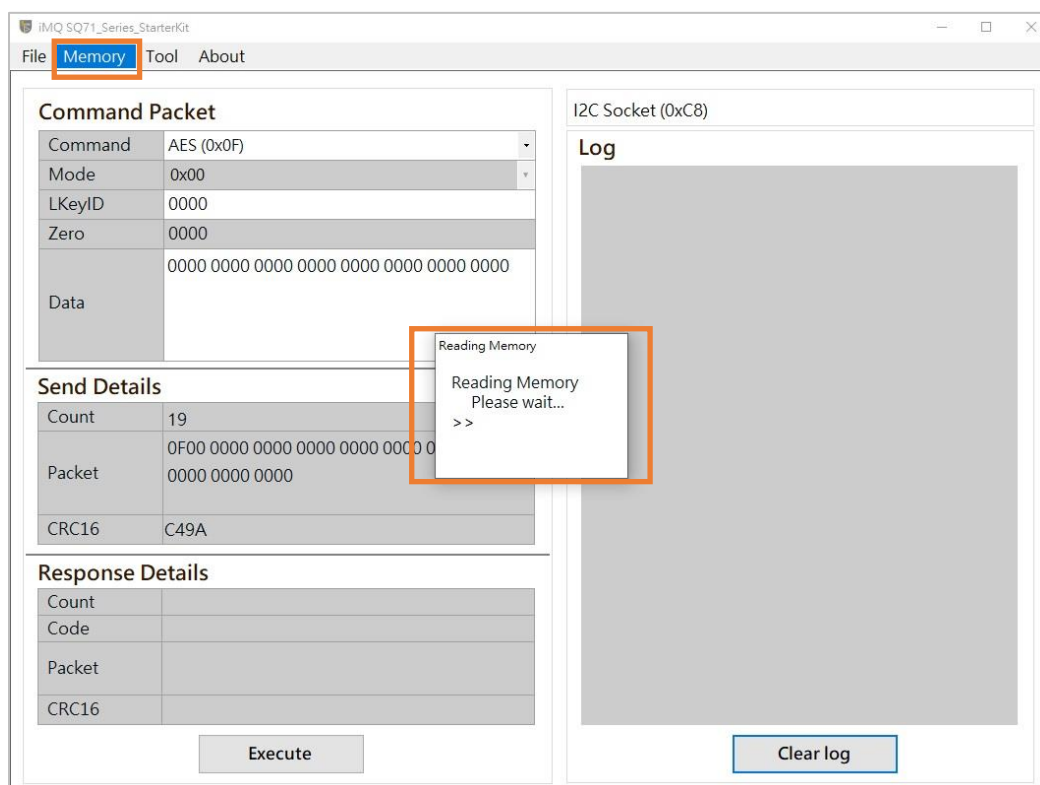


Figure 38 SQ710x Click Memory on the main menu

The memory window can be divided into memory configuration block, configuration menu block and menu bar, which will be explained in the following chapters.

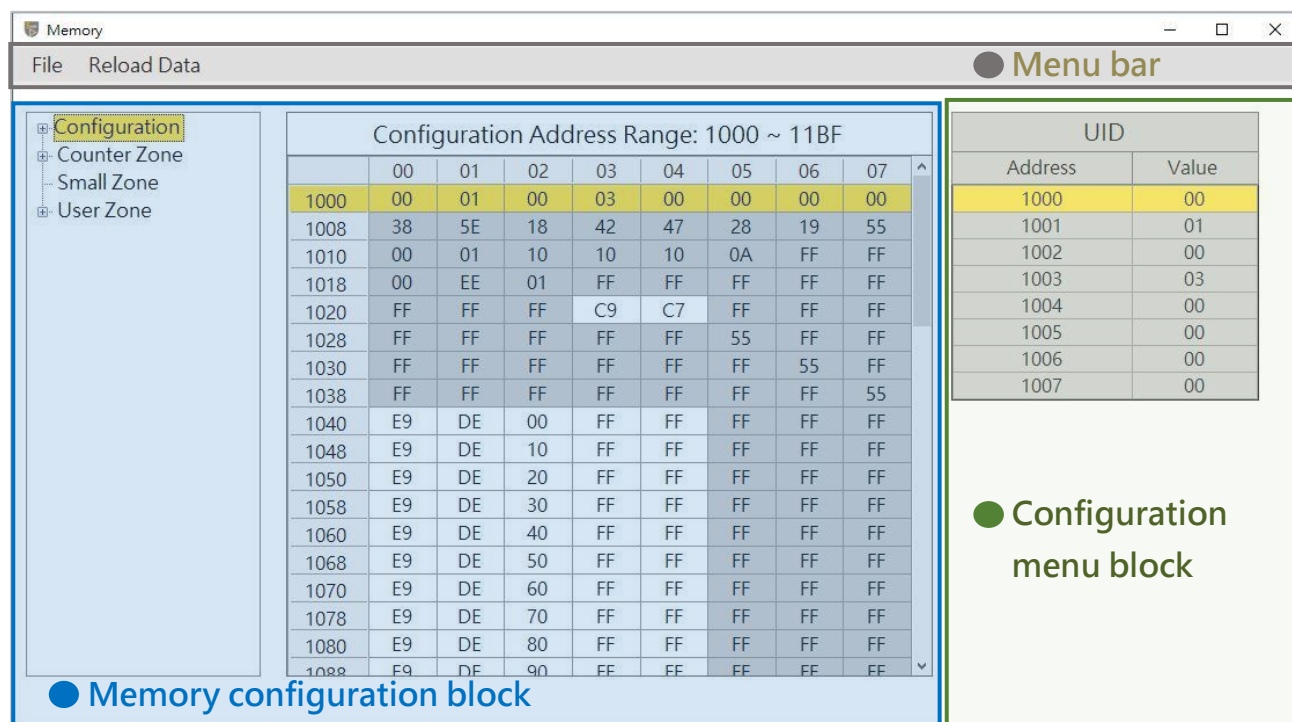


Figure 39 SQ710x Memory window

4.3.1 Memory Configuration

The left side displays each memory zone that can be viewed and the user can select to view. The memory data of the zone is displayed in the middle field (expressed in hexadecimal).

Note 1: If the user wants to modify the configuration, first select the memory address to be modified and then modify it in the configuration menu displayed on the far right.

Note 2: If the field has a gray background, it means read-only (Read-only) information, and the user cannot change its settings.

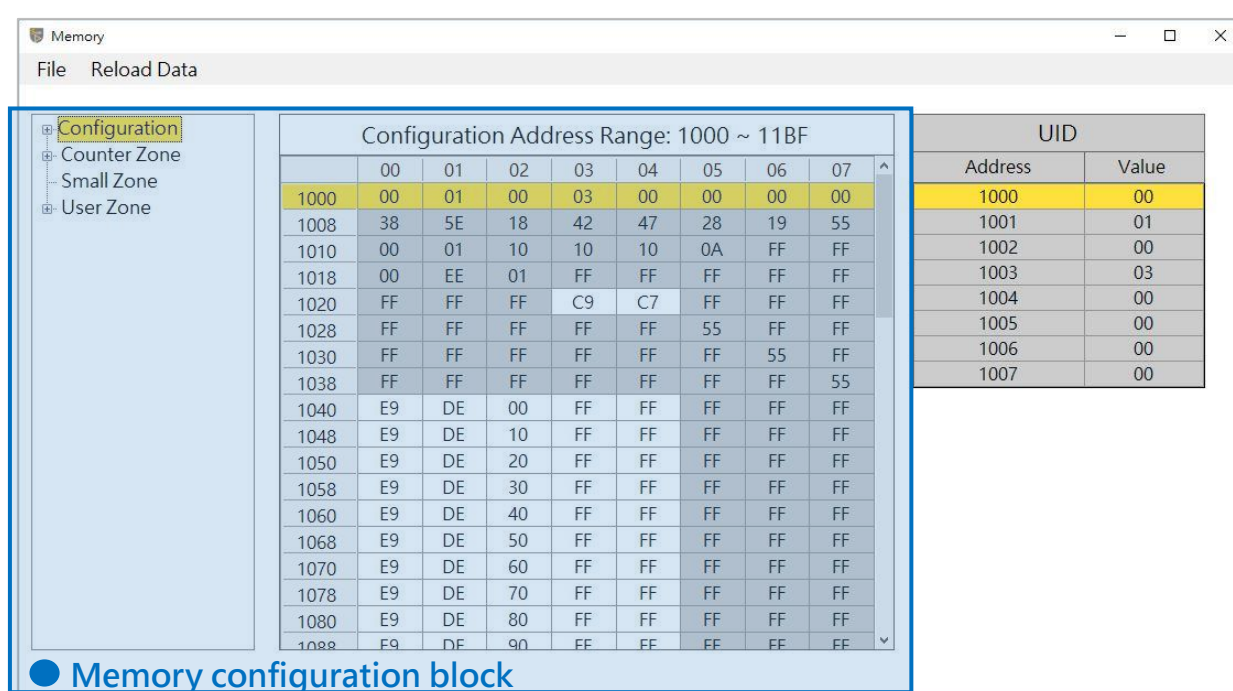


Figure 40 SQ710x Memory: Memory configuration block

4.3.2 Configuration Menu

The configuration menu is divided into configuration zone and other zones.

- Configuration: Set the configuration of chip, key, user area and counter.
- Other zones: User Zone, Counter Zone and Small Zone.

4.3.2.1 Configuration Update

After selecting the address to be modified in the memory configuration block, the configuration menu corresponding to the address will be displayed. The following steps take configuring Key 0 as an example.

Step 1. At memory configuration block (the leftmost field) select Configuration\Key 0.

Step 2. At memory configuration block (middle field) select the address to modify the configuration.

Key 0 configuration address is 0x1040.

Step 3. Configure in the configuration menu

Click the configuration field, and the options available for configuration will be listed and user can configure according to your needs.

Step 4. Confirm update configuration

After pressing "Update", the newly configured options will be written to Device and the new configuration values will be displayed on Value.

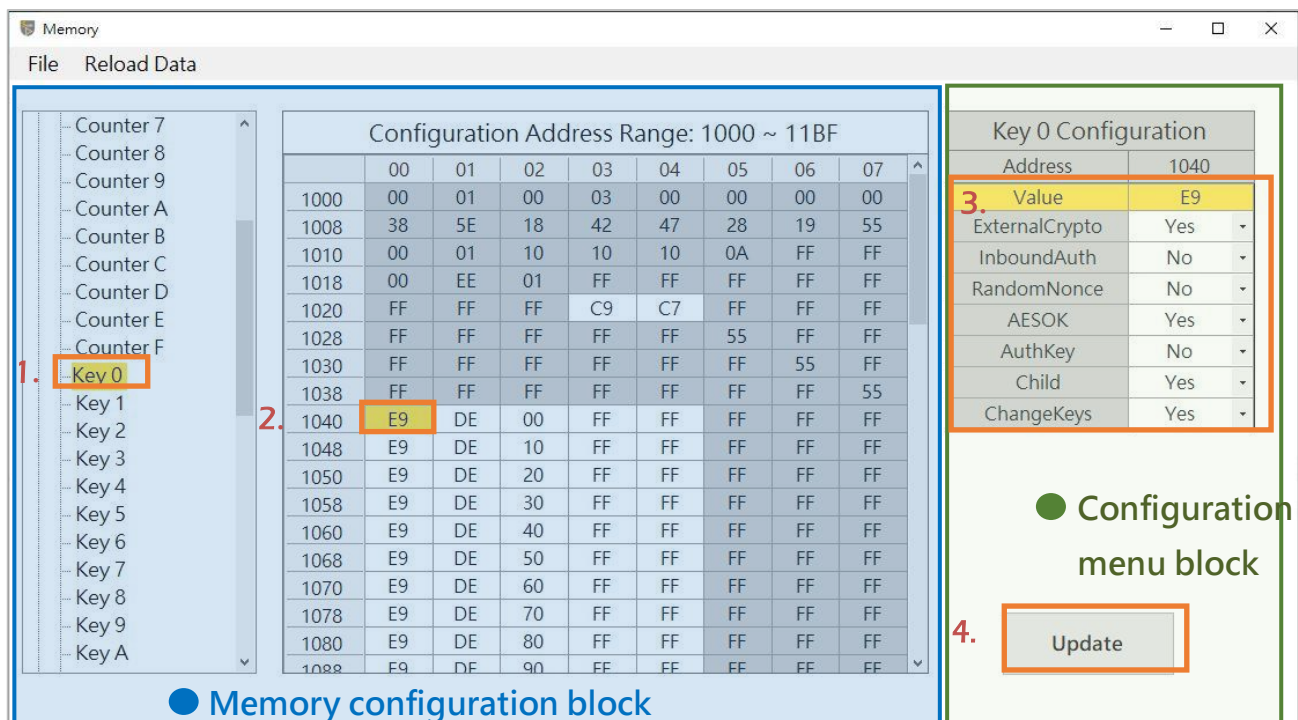


Figure 41 SQ710x Memory: Configuration update

4.3.2.2 Other Zones Update

After selecting the address to be modified in the memory configuration block, a continuous section will be automatically selected, and the value of the continuous section will be displayed on the right configuration menu. The user double-clicks the Value field in the configuration menu, and the window for updating the value will pop up. The window shows the starting address of the continuous zone and all the values of the zone, and the value can be modified directly. After modification, click the "Update" button to write to the device. The following steps take modifying the data of User Zone00 as an example.

Step 1. At memory configuration block (the leftmost field) select User Zone\User Zone 00.

Step 2. At memory configuration block (middle field) select the address to modify the configuration.

User Zone address is 0x0000~0x00FF, a total of 256 bytes.

Step 3. Double-click the Value field to be modified in the configuration menu.

Click the Value field to modify the configuration, and the window for updating the value will pop up.

Step 4. Enter new value in the update value window

After pressing "OK", the new value update is displayed in the configuration menu.

Step 5. Confirm update configuration

After pressing "Update", the new value will be written to Device.

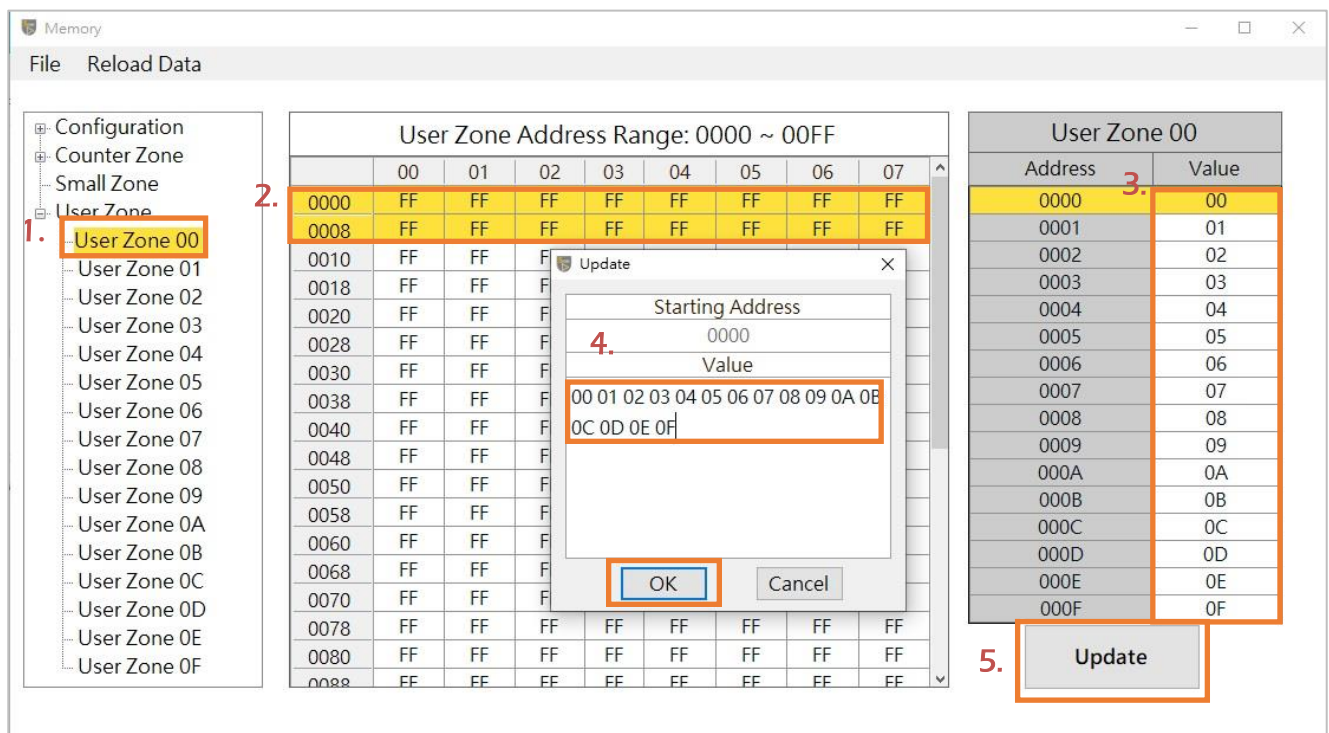


Figure 42 SQ710x Memory: User Zone update

4.3.3 Menu Bar

There are File and Reload Data menus on the memory menu, as shown in the figure below:

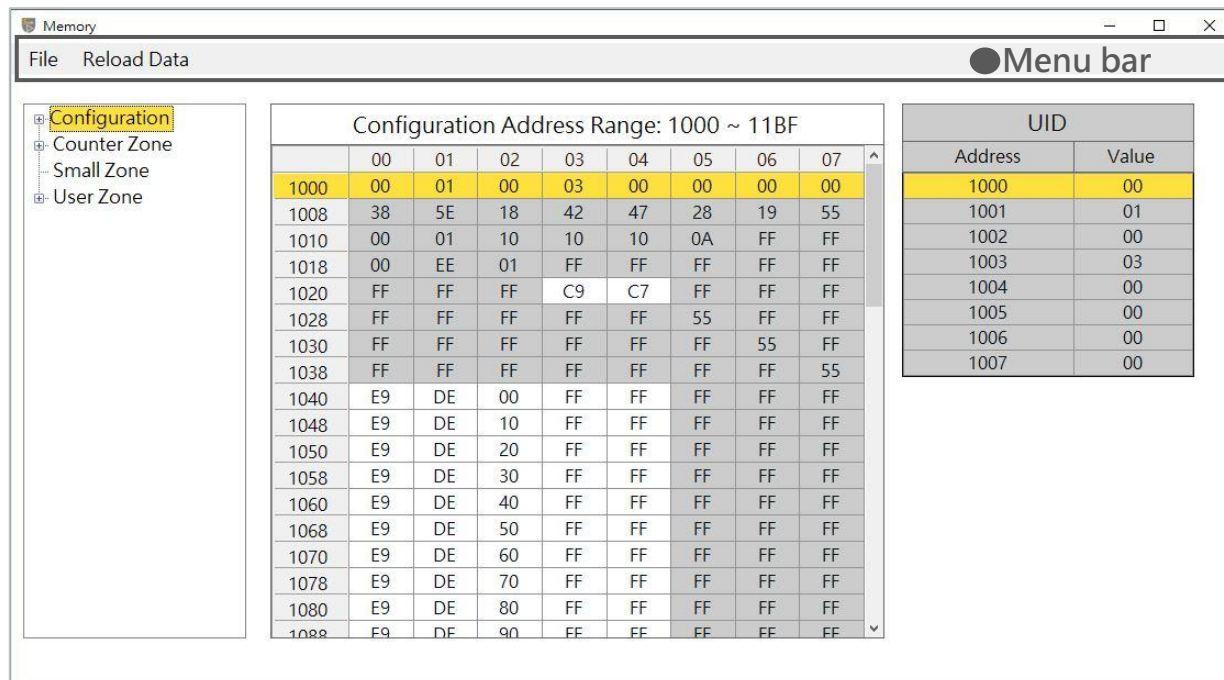


Figure 43 SQ710x Memory: Menu bar

4.3.3.1 File sub-Menu

Click File to export or import the data of the device memory block.

a. Export file

Can export device memory configuration data.

Step 1. At menu select File\ Export Data

The export file format is .Json format.

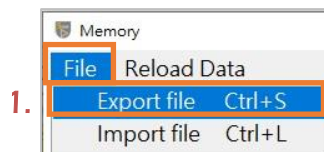


Figure 44 SQ710x Memory: File sub menu/Export file

Step 2. After selecting the save path, press Save

You can choose the save path, use the default file name or name it yourself.

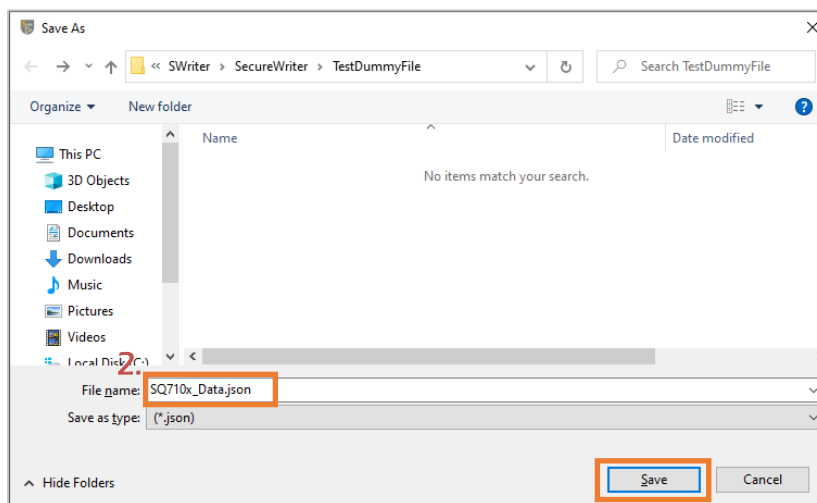


Figure 45 SQ710x Memory: Export file dialog

Note: The default export file name is SQ710x_Data.json, and user can name it.

Step 3. After exporting the data, the Export Finish message box will pop up, press OK.

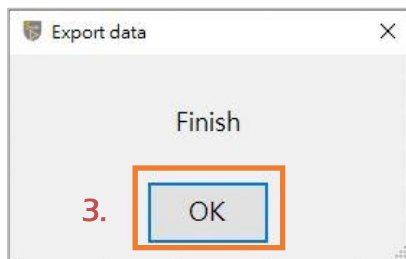


Figure 46 SQ710x Memory: Export finish message

b. Import Data

Can import previously exported configuration data.

Step 1. At menu select File\Import Data

The import file format is .Json format.

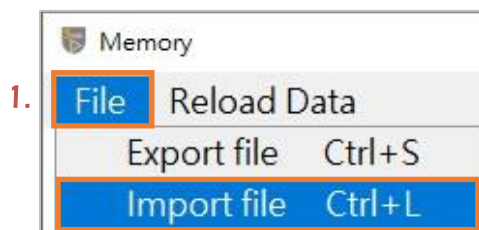


Figure 47 SQ710x Memory: File sub menu/Import file

Step 2. After selecting the .json/.jsfw file to be loaded, click "Open"

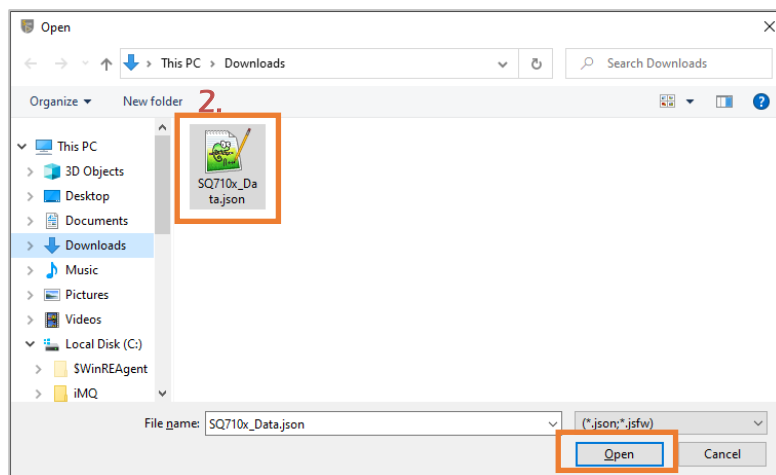


Figure 48 SQ710x Memory: Import file dialog

Step 3. Popup display memory zone list for user to select the zone to import

The user can choose to import a single zone or all zones. In the following example, after selecting "All", press OK to import the data of all zones.

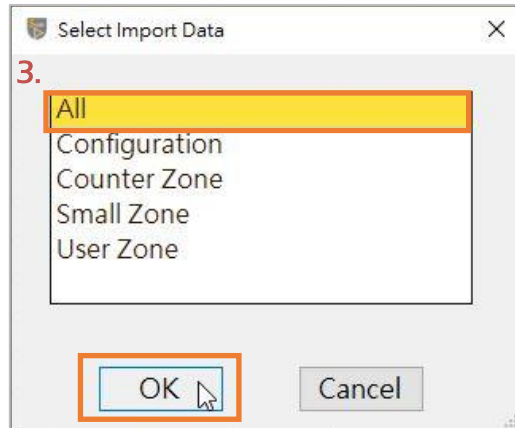


Figure 49 SQ710x Memory: Select import data dialog

Step 4. After importing the data, the Import Finish message box will pop up, press OK.

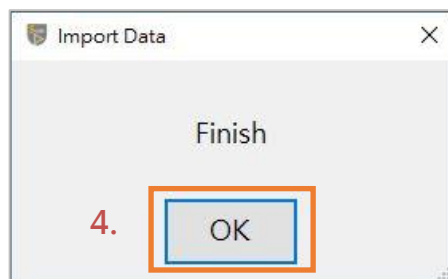


Figure 50 SQ710x Memory: Import data finish message

Note: After the import is finished and press OK, it will automatically execute reload data.

c. Reload Data

Reload device all memory configuration data and display on screen.

Step 1. At Menu click Reload Data.

Reload device all memory configuration data.



Figure 51 SQ710x Memory: Reload Data sub menu item

Step 2. Wait for the reload to complete

Note 1: **Do not remove the Secure Starter Kit from the computer while the data is read.**

Note 2: After modifying any configuration on the memory window, you must press "Reload Data", and the data on the window will display the updated value.

Note 3: The shortcut key for the "Reload Data" button is "Ctrl+r"

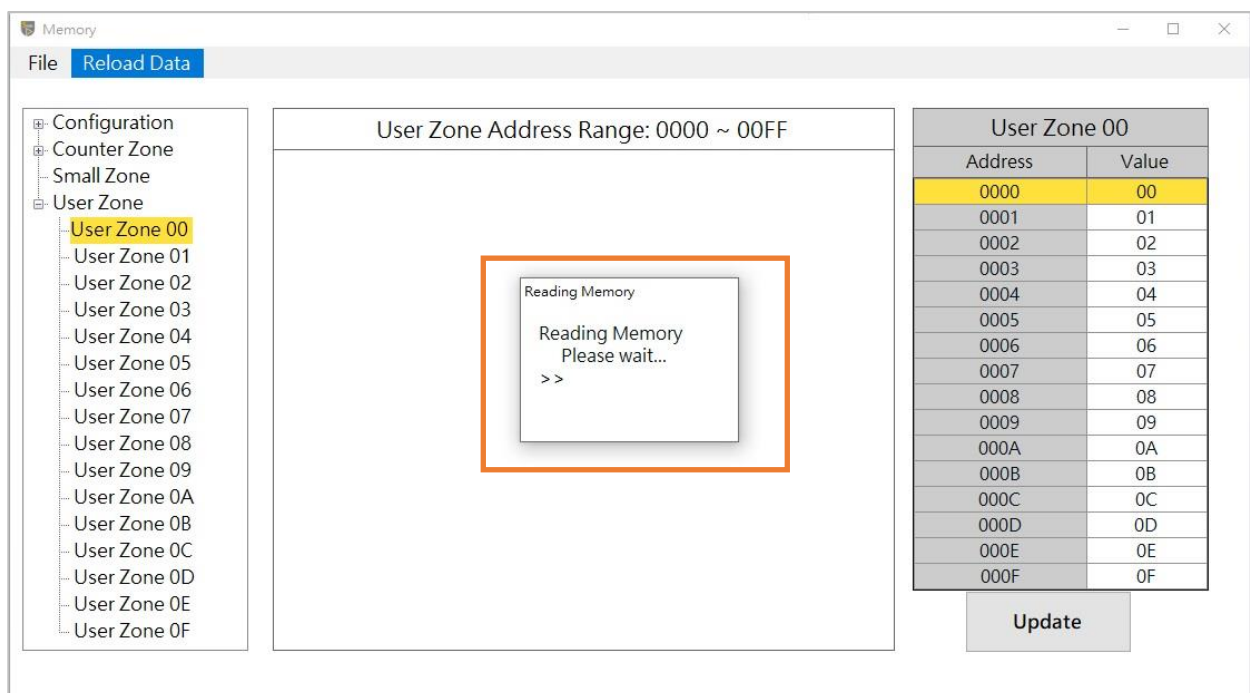


Figure 52 SQ710x Memory: Reloading memory dialog

4.4 Program Device

After clicking Tool\Program Device, the program device window will pop up. This function can only program Socket devices.

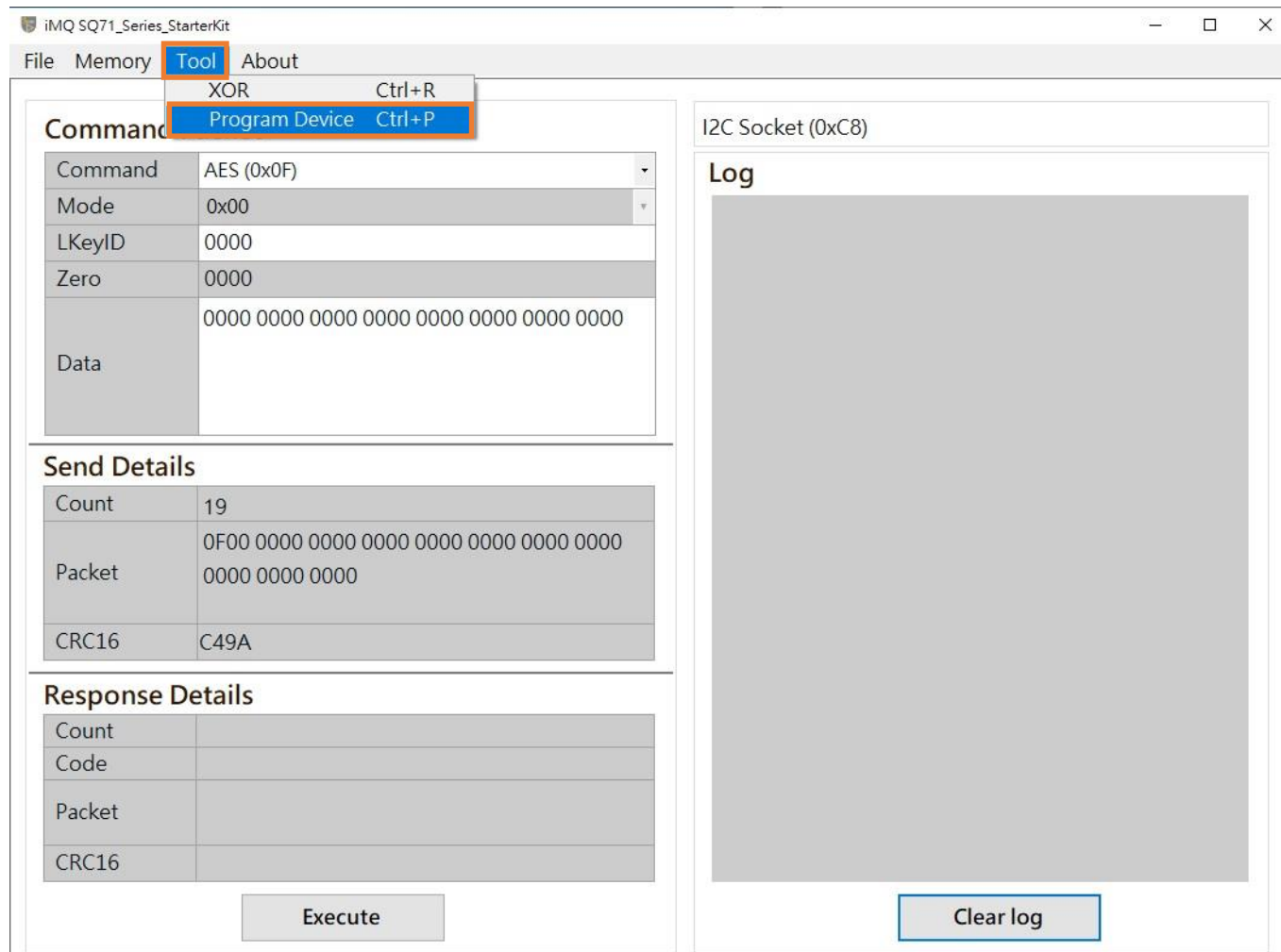


Figure 53 SQ710x Starter Kit Tool sub menu/Program Device

The program device window can be divided into memory configuration, function options, menu bar, and log window are described in the following sections.

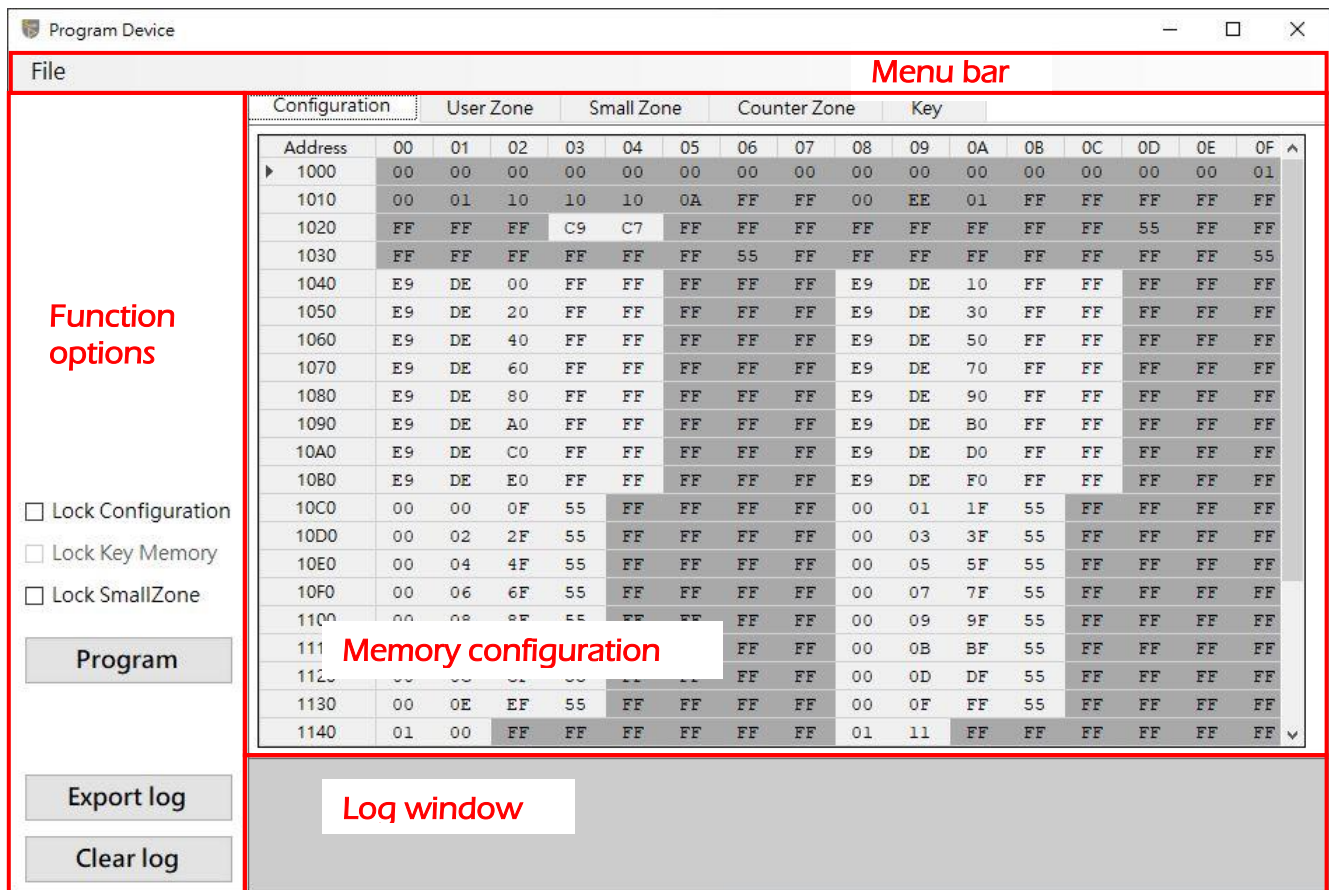


Figure 54 SQ710x Program Device window

4.4.1 Memory Configuration

The Tab Page displays each memory zone that can be viewed. After the user clicks, it will switch to the corresponding memory zone page. The value of the memory zone is displayed in the middle field (expressed in hexadecimal).

4.4.1.1 Configuration

This page can set the configuration of chip, key, user zone and counter zone. User can directly click on the field to edit, but if the field background is gray, it means read-only information.

The configuration address range is 0x1000 ~ 0x11BF.

Program Device

File

☐ Lock Configuration
☐ Lock Key Memory
☐ Lock SmallZone

Program

Export log

Clear log

Configuration	User Zone	Small Zone	Counter Zone	Key												
Address	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
1000	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	01
1010	00	01	10	10	10	0A	FF	FF	00	EE	01	FF	FF	FF	FF	FF
1020	FF	FF	FF	C9	C7	FF	FF	FF	FF	FF	FF	FF	FF	55	FF	FF
1030	FF	FF	FF	FF	FF	FF	55	FF	FF	FF	FF	FF	FF	FF	FF	55
1040	E9	DE	00	FF	FF	FF	FF	FF	E9	DE	10	FF	FF	FF	FF	FF
1050	E9	DE	20	FF	FF	FF	FF	FF	E9	DE	30	FF	FF	FF	FF	FF
1060	E9	DE	40	FF	FF	FF	FF	FF	E9	DE	50	FF	FF	FF	FF	FF
1070	E9	DE	60	FF	FF	FF	FF	FF	E9	DE	70	FF	FF	FF	FF	FF
1080	E9	DE	80	FF	FF	FF	FF	FF	E9	DE	90	FF	FF	FF	FF	FF
1090	E9	DE	A0	FF	FF	FF	FF	FF	E9	DE	B0	FF	FF	FF	FF	FF
10A0	E9	DE	C0	FF	FF	FF	FF	FF	E9	DE	D0	FF	FF	FF	FF	FF
10B0	E9	DE	E0	FF	FF	FF	FF	FF	E9	DE	F0	FF	FF	FF	FF	FF
10C0	00	00	0F	55	FF	FF	FF	FF	00	01	1F	55	FF	FF	FF	FF
10D0	00	02	2F	55	FF	FF	FF	FF	00	03	3F	55	FF	FF	FF	FF
10E0	00	04	4F	55	FF	FF	FF	FF	00	05	5F	55	FF	FF	FF	FF
10F0	00	06	6F	55	FF	FF	FF	FF	00	07	7F	55	FF	FF	FF	FF
1100	00	08	8F	55	FF	FF	FF	FF	00	09	9F	55	FF	FF	FF	FF
1110	00	0A	AF	55	FF	FF	FF	FF	00	0B	BF	55	FF	FF	FF	FF
1120	00	0C	CF	55	FF	FF	FF	FF	00	0D	DF	55	FF	FF	FF	FF
1130	00	0E	EF	55	FF	FF	FF	FF	00	0F	FF	55	FF	FF	FF	FF
1140	01	00	FF	FF	FF	FF	FF	FF	01	11	FF	FF	FF	FF	FF	FF

Figure 55 SQ710x Program Device: Configuration Zone

4.4.1.2 User Zone

This page can edit the content of the User Zone. Users can directly click on the field to edit.

The User Zone address range is 0x0000 ~ 0x00FF.

Program Device

File

Configuration	User Zone	Small Zone	Counter Zone	Key												
Address	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
0000	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
0010	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
0020	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
0030	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
0040	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
0050	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
0060	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
0070	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
0080	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
0090	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
00A0	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
00B0	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
00C0	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
00D0	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
00E0	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
00F0	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF

☐ Lock Configuration
☐ Lock Key Memory
☐ Lock SmallZone

Program

User Zone

Export log

Clear log

Figure 56 SQ710x Program Device: User Zone

This page can edit the content of the Small Zone, users can directly click on the field to edit.

The Small Zone address range is 0x1300 ~ 0x15FF.

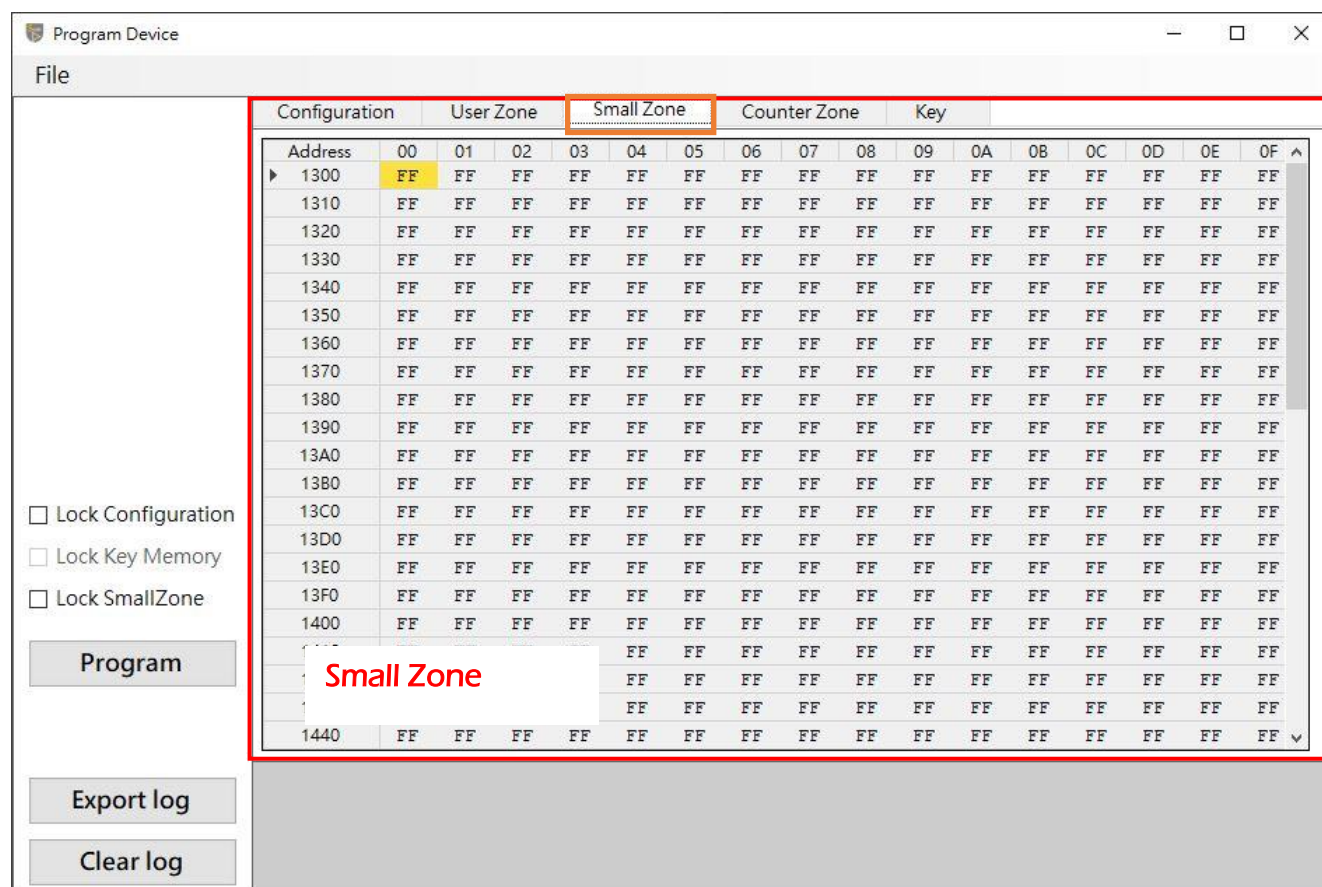


Figure 57 SQ710x Program Device: Small Zone

4.4.1.4 Counter Zone

This page can edit the content of the Counter Zone. Users can directly click on the field to edit.

The Counter Zone address range is 0x1200 ~ 0x127F.

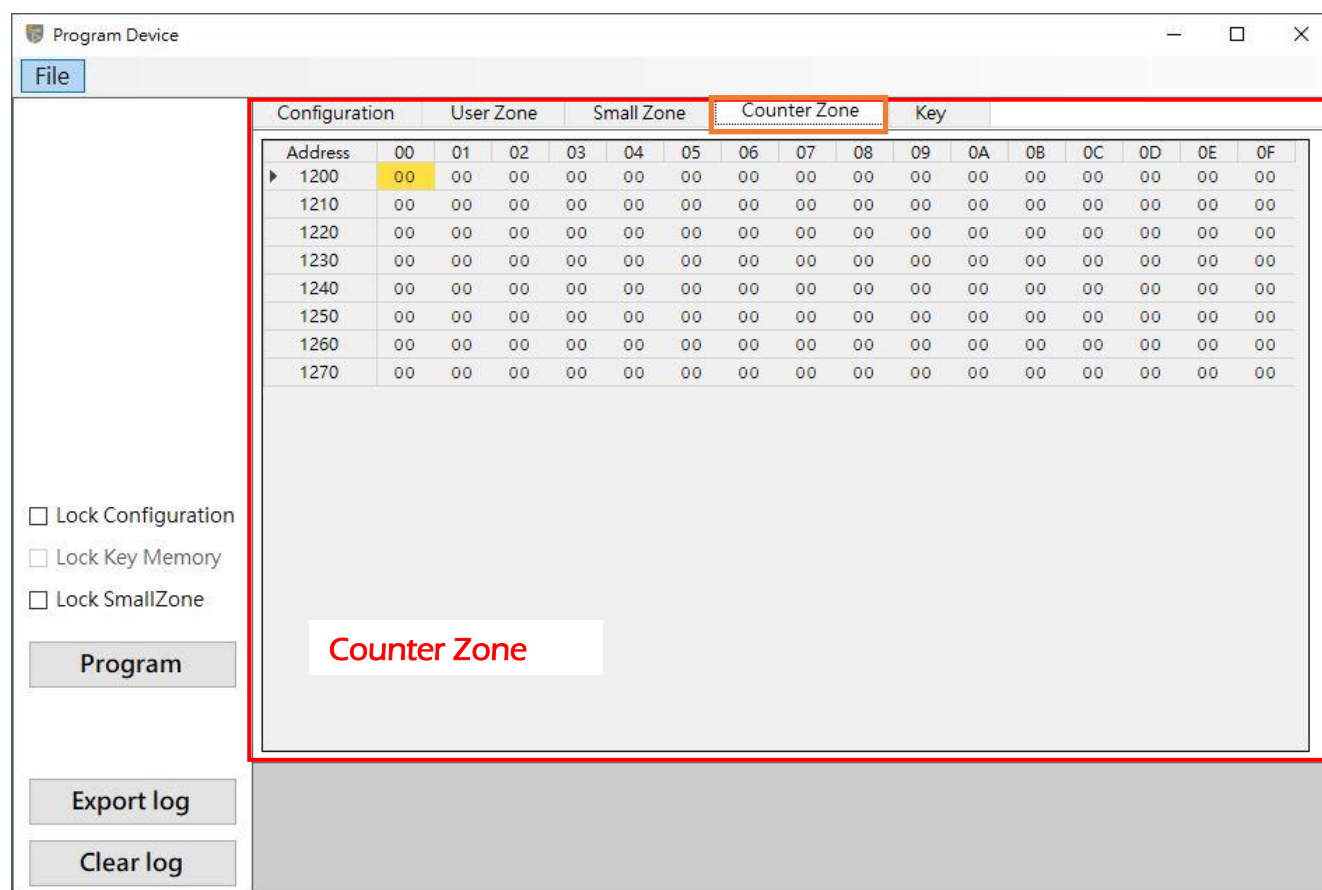


Figure 58 SQ710x Program Device: Counter Zone

4.4.1.5 Key

This page can edit the content of the Key. Users can directly click on the field to edit.

The Key address range is 0xF200 ~ 0xF2FF.

The function of each field is described as follows:

1. **Selected:** When checked, it means that the key is enabled and the key can be edited. The key will be written when program.
2. **AES256:** When checked, it means to enable AES256, and the Key Value can input a value of 256 Bits. (If the AES256 enabled, the memory location of the next key will be used when writing to the IC, so when this field is checked, the content of the next key will be closed and the user cannot edit it.)
3. **Key Generator:** You can use this function to randomly generate Key Value or reset it.
 - a. Select the target Key.
 - b. Generate the Key Value of the target Key as a random number. (It can only be clicked when the target Key is enabled)
 - c. Reset the Key Value of the target Key to all 0xFF. (It can only be clicked when the target Key is enabled)

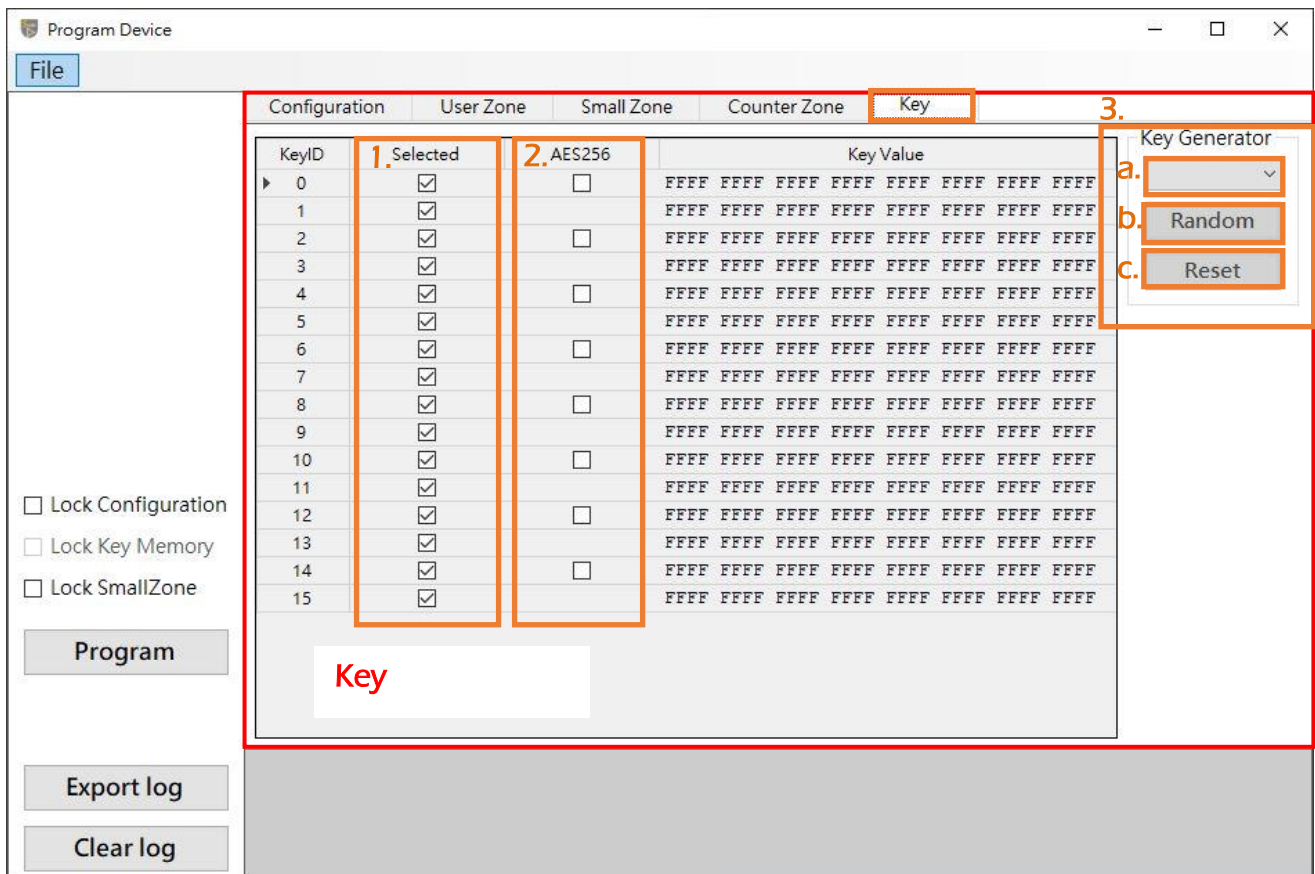


Figure 59 SQ710x Program Device: Key Zone

4.4.2 Function Options

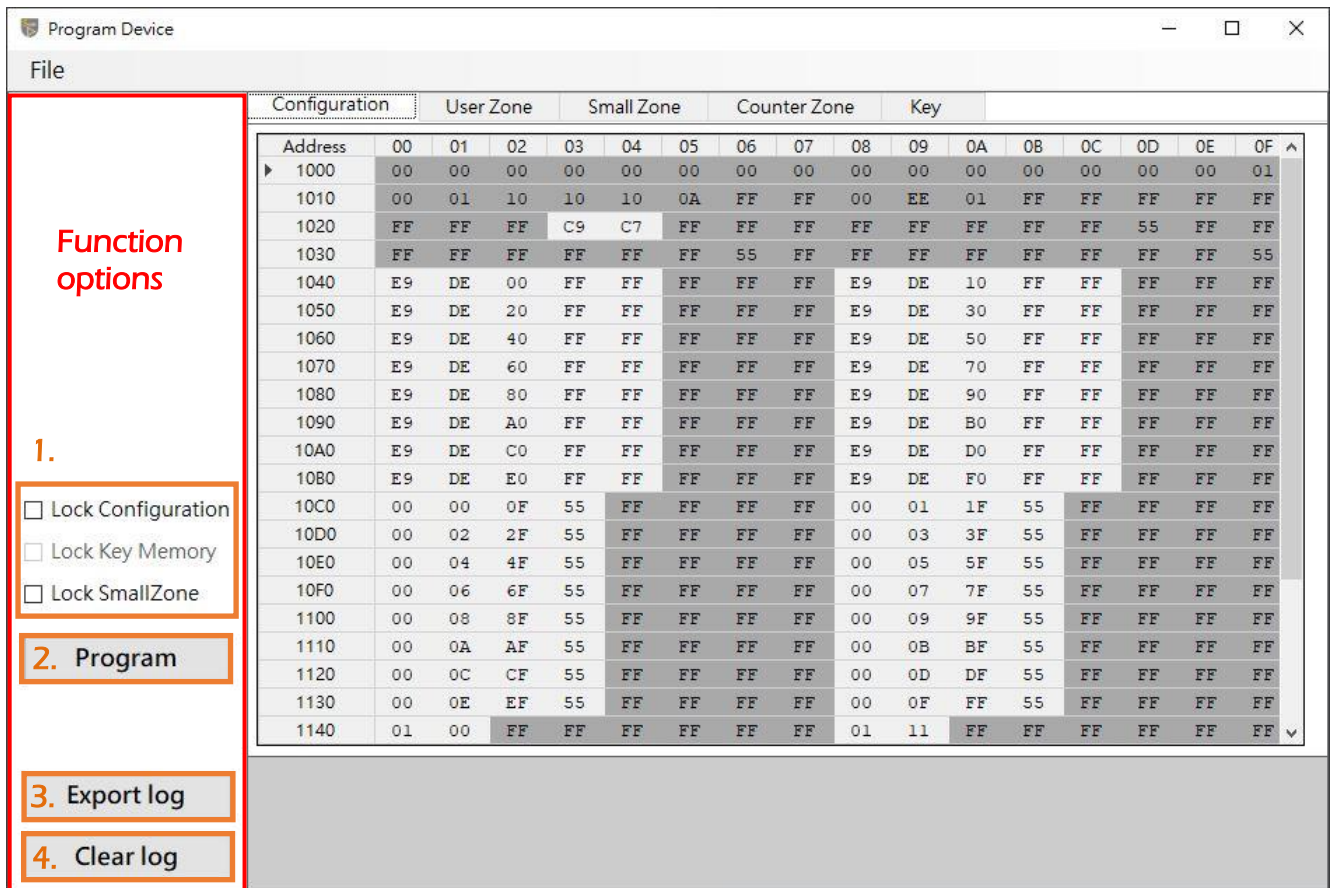


Figure 60 SQ710x Program Device: Function Options

Function options are divided into 4 parts :

1. **Lock options:** User can select the memory zone to be locked. After the program is completed, it will be locked according to the checked items.
 - a. **Lock Configuration:** Configuration zone can no longer be written after locking, you can only use Block Read command to read.
 - b. **Lock Key Memory:** Key Memory Key memory can no longer be written after locking. (Lock Configuration must be locked before Lock Key Memory.)
 - c. **Lock Small Zone:** Small zone can no longer be written after locking, you can only use Block Read command to read.

2. **Program:** After the user clicks, a confirmation window will pop up, and the program process will start after clicking "Yes".

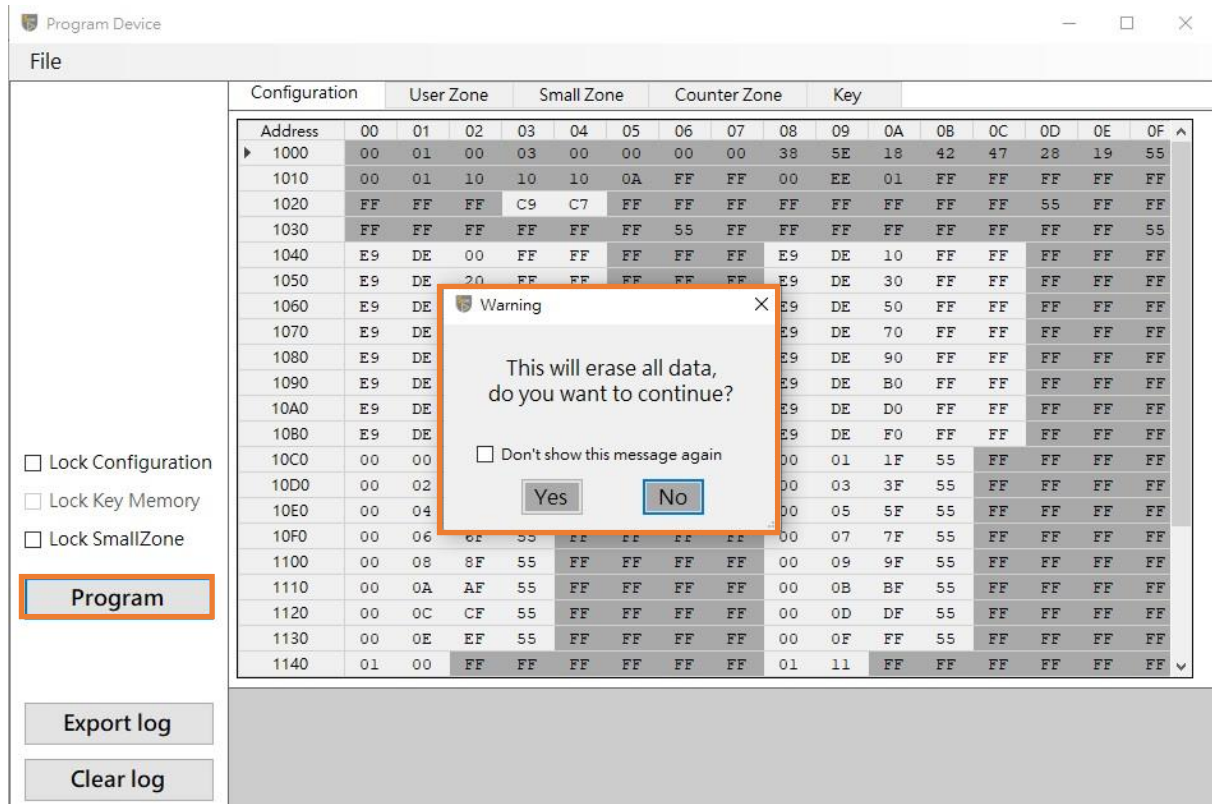


Figure 61 SQ710x Program Device: Program confirm message box

The program process is as follows:

- Check if the Socket device exists, when the device does not exist, an error window will be displayed and the programming will stop.

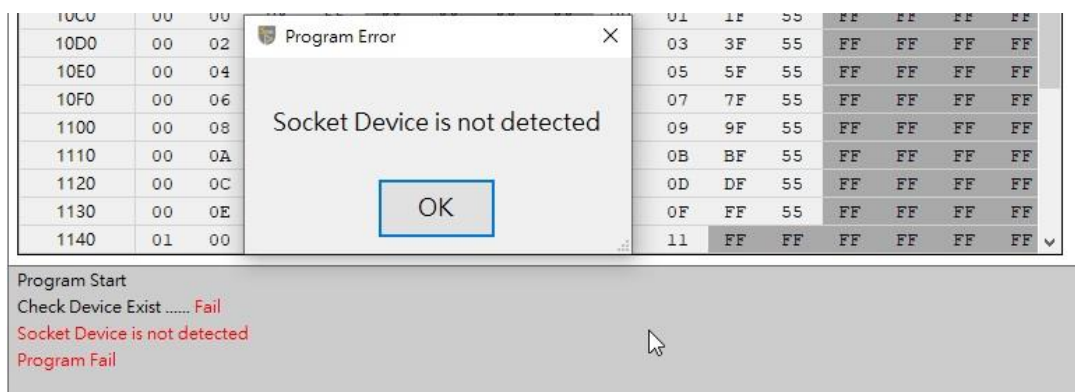


Figure 62 SQ710x Program Device: Socket device not detected message box

- b. Check that the communication mode of the device matches the configuration settings, if there is a mismatch, an error window will be displayed and the programming will stop.

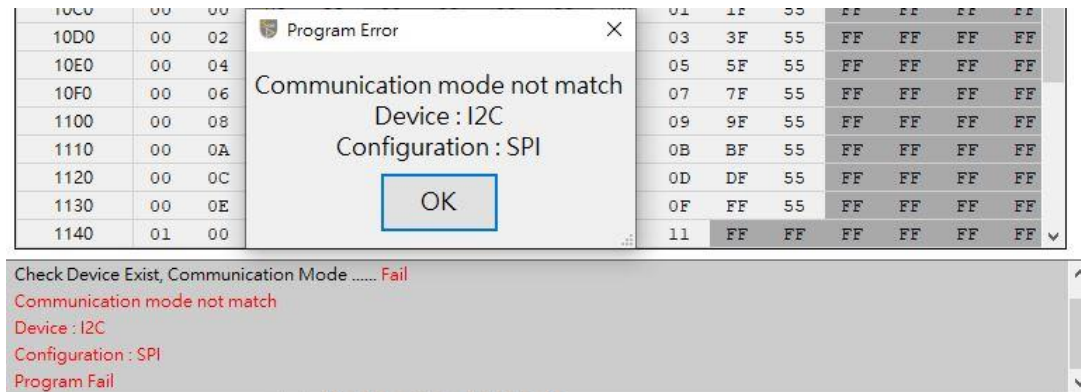


Figure 63 SQ710x Program Device: Communication mode not match message box

- c. Check if the device is locked. When the Configuration is locked, an error window will be displayed and the programming will stop. When only the Small zone is locked, ask the user whether to continue programming other parts except the Small zone.

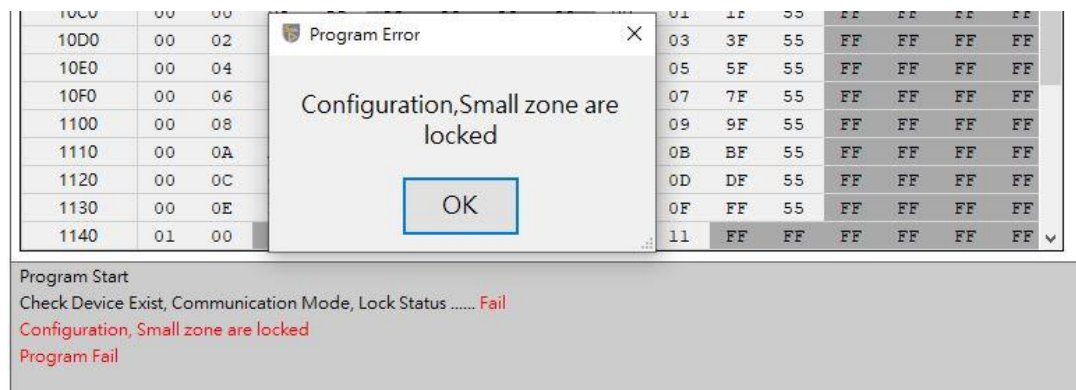


Figure 64 SQ710x Program Device: Zone Locked message box

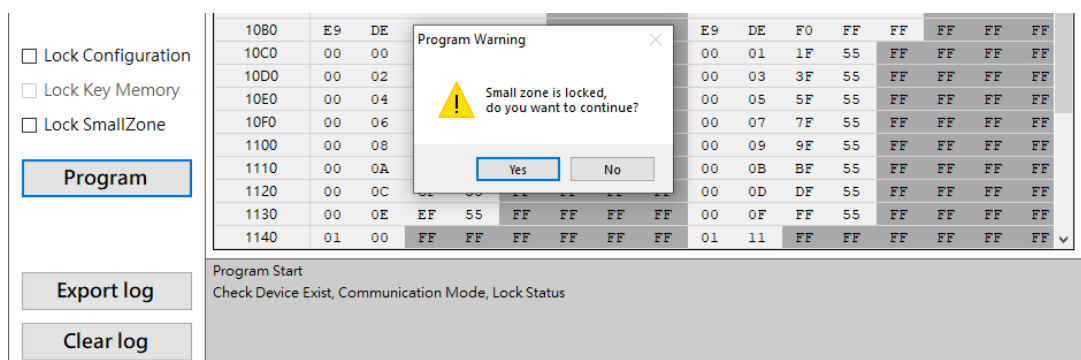


Figure 65 SQ710x Program Device: Small zone locked, continue dialog.

- d. Check whether the enable status of Key AES256 matches the setting in Configuration, if there is a mismatch, an error window will be displayed and the programming will stop.

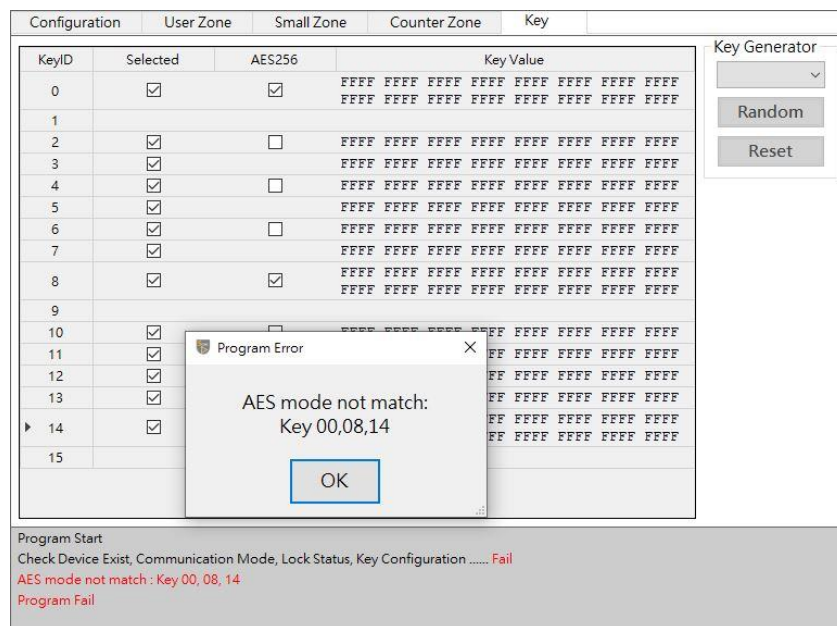


Figure 66 SQ710x Program Device: AES mode not match message box

- e. Write Key AES256 settings to Key configuration memory.
 f. Write Key Value.
 g. Write Counter Zone, Small Zone and User Zone.
 h. Finally, write Configuration.
 i. Check whether the user has checked the Lock options, and lock according to the lock options.
 j. Program is complete.

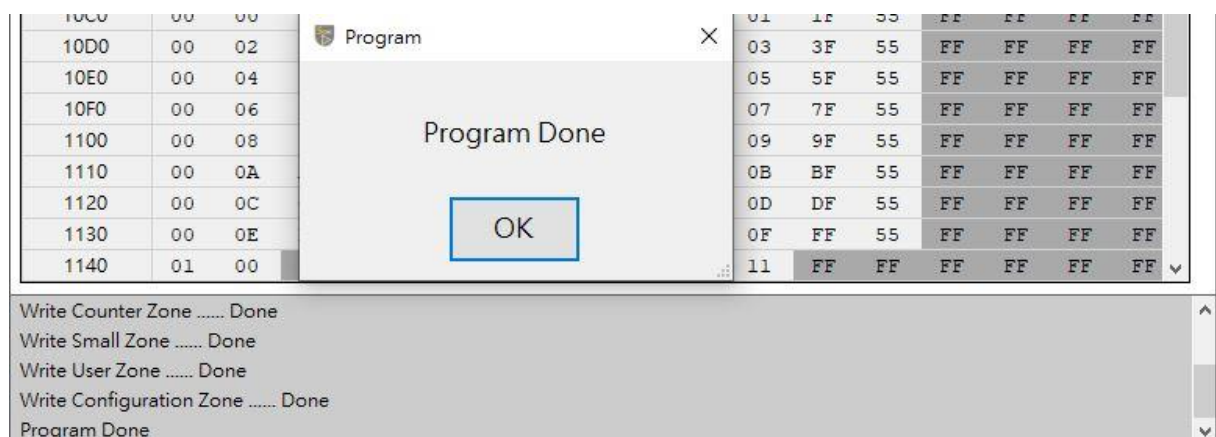


Figure 67 SQ710x Program Device: Program Done message box

3. **Export log:** Users can click this button to export the content of the Log Window into a .log file.

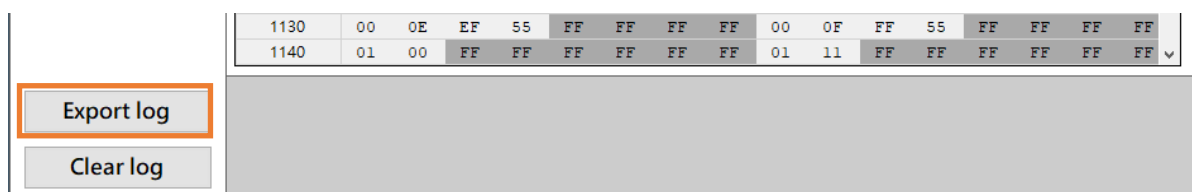


Figure 68 SQ710x Program Device:Export log

Select the save path and file name, the default file name is "Log_YYMMDD.log" (YYMMDD is the current date)

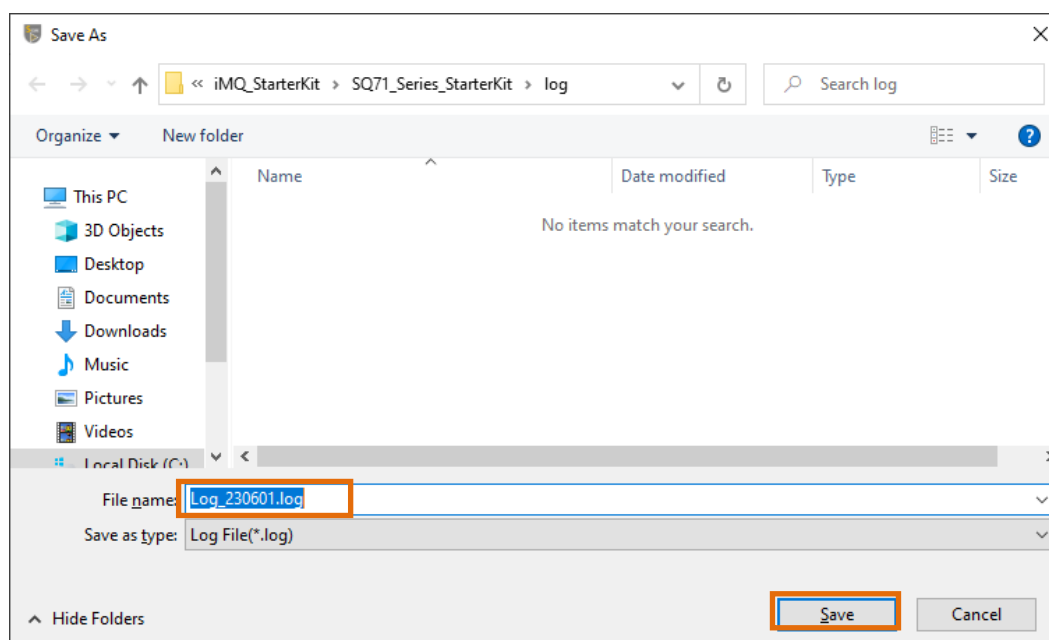


Figure 69 SQ710x Program Device: Export log dialog

4. **Clear log:** Users can click this button to clear the content of the Log Window.

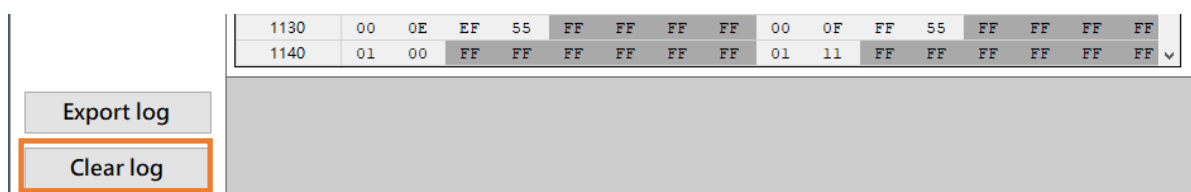


Figure 70 SQ710x Program Device: Clear Log

4.4.3 Menu Bar

There is a File menu on the menu bar, as shown in the figure below:

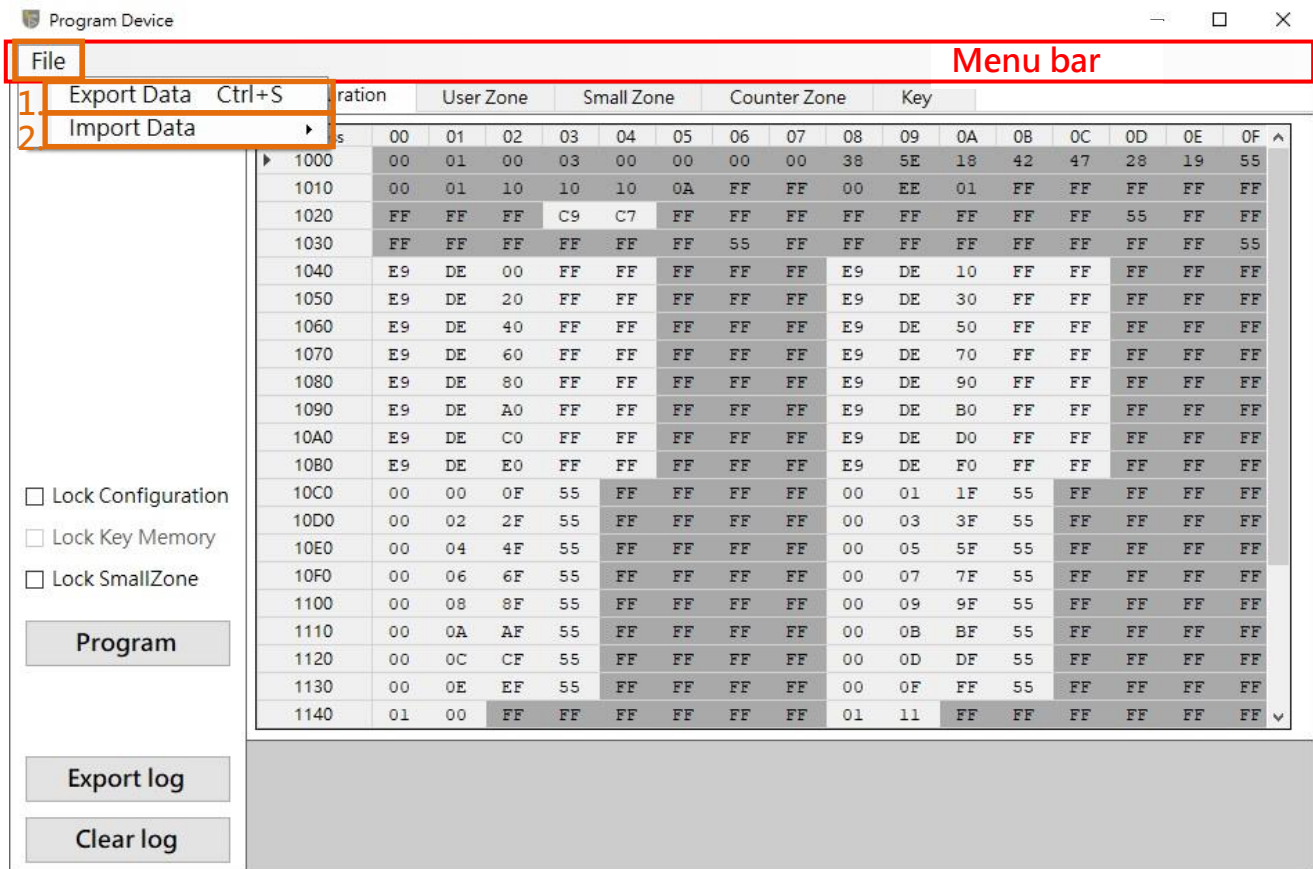


Figure 71 SQ710x Program Device: Menu bar

1. Export Data

After clicking Export Data, all the data in the memory configuration (Configuration, User Zone, Small Zone, Counter Zone and Key Value) can be exported into a file in .Json format (The file extension is .jsfw).



Figure 72 SQ710x Program Device: File menu/Export Data

Select the save path and file name, the default file name is "SQ710x_YYMMDD.jsfw" (YYMMDD is the current date)

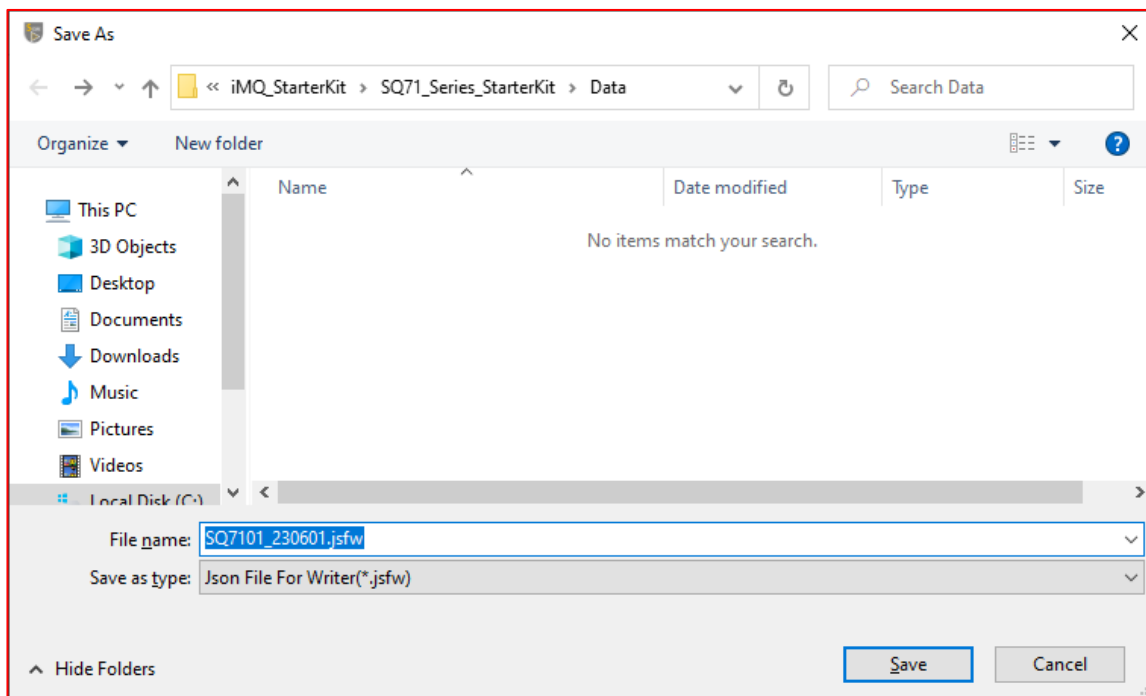


Figure 73 SQ710x Program Device: Export Data dialog

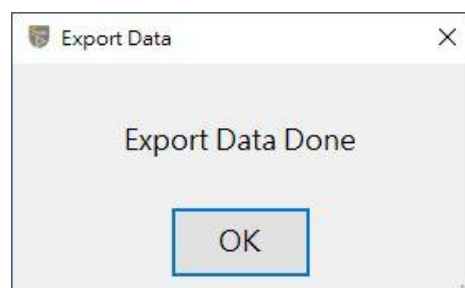


Figure 74 SQ710x Program Device: Export data done message box

2. Import Data

After clicking Import Data, select the source of the memory configuration data to be imported.

- a. **Socket Device:** Import memory configuration data from the currently connected Socket Device.

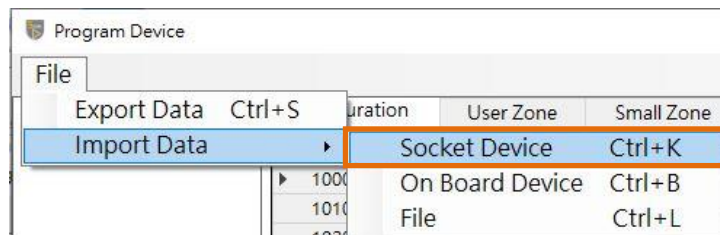


Figure 75 SQ710x Program Device: File menu/Import Data/Socket Device

- b. **On Board Device:** Import memory configuration data from the On Board Device. (This feature is currently not supported, it is reserved to be enabled in the future.)

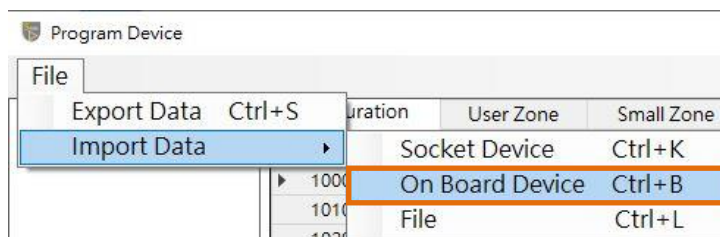


Figure 76 SQ710x Program Device: File menu/Import Data/On Board Device

- c. **File:** From the previously exported .Json format file (The file extension is .json/.jsfw) Import data.

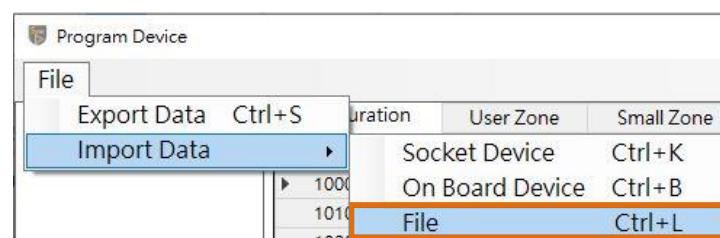


Figure 77 SQ710x Program Device: File menu/Import Data/File

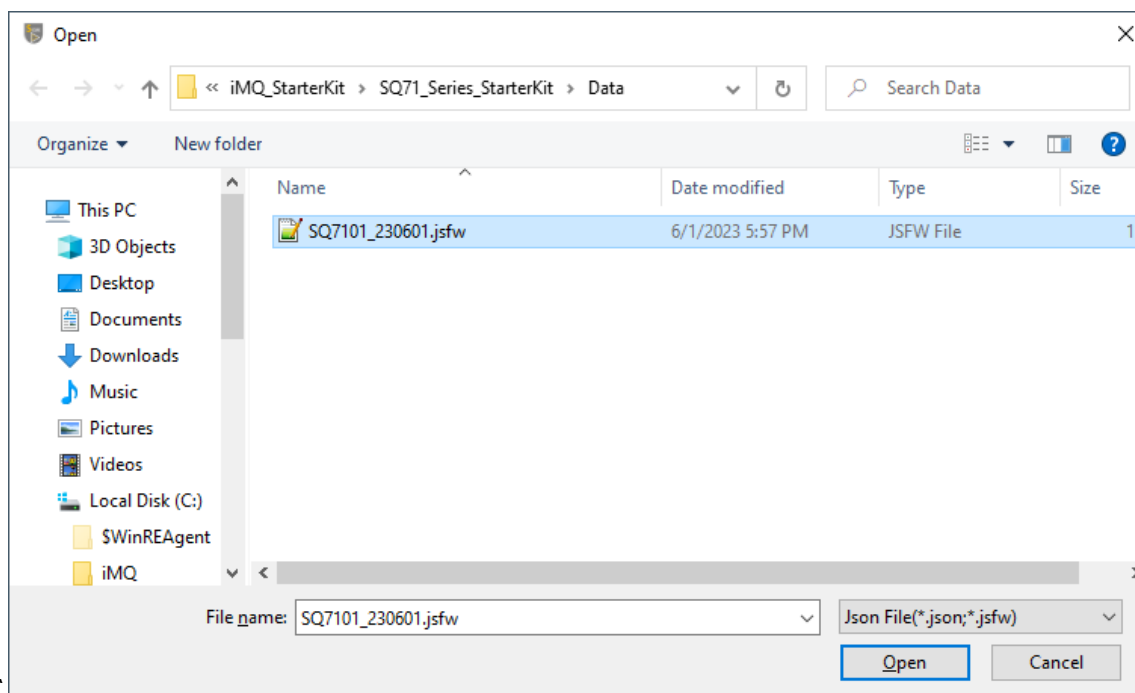


Figure 78 SQ710x Program Device: Import file dialog

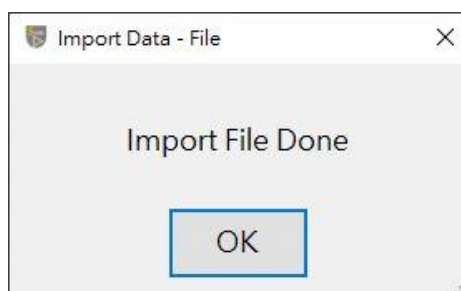


Figure 79 SQ710x Program Device: Import file done message

If the import data fails to be read, an error message will be displayed, and the address where the error occurred and related information will be recorded in the Log Window, and the fields that failed to be read will be displayed in red fonts for users to identify and modify.

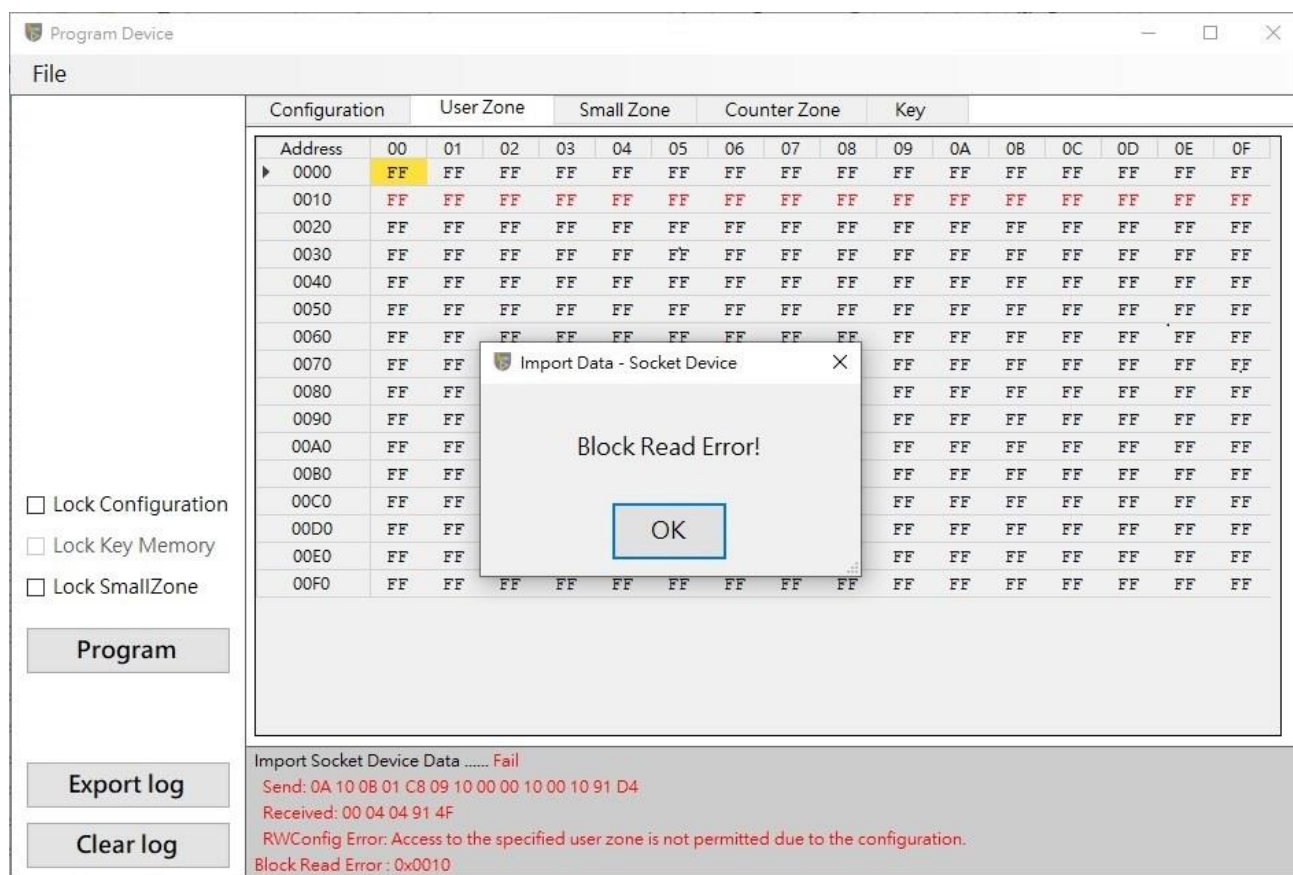


Figure 80 SQ710x Program Device: Import Data: Block Read Error message box

4.4.4 Log Window

Log Window will automatically record the operation status, programming status and error information. User can use the mouse to select, copy, select all, or clear the contents of the Log Window or use the Export log button to export the Log file, or use the Clear log button to clear the contents of the Log Window

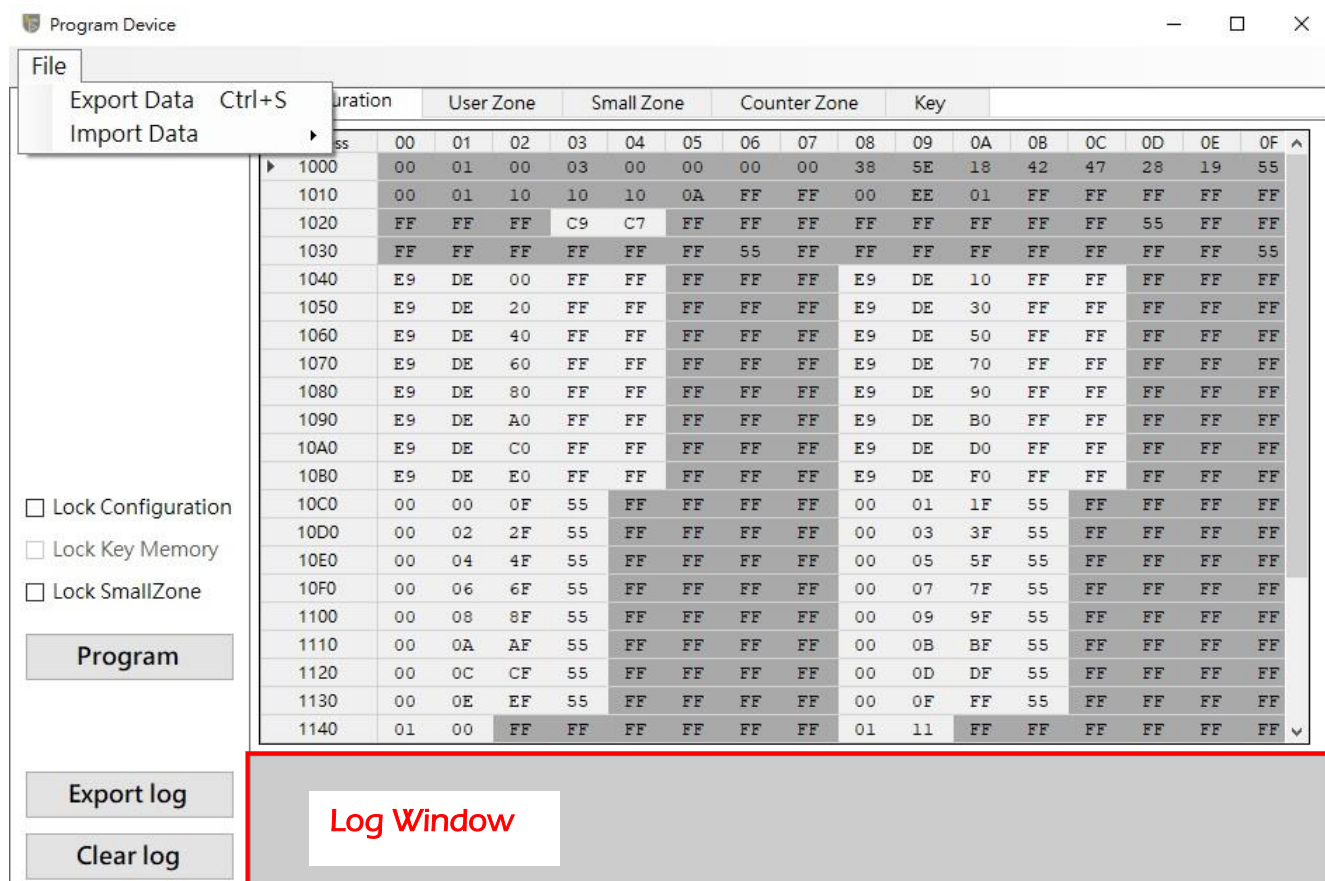


Figure 81 SQ710x Program Device: Log Window

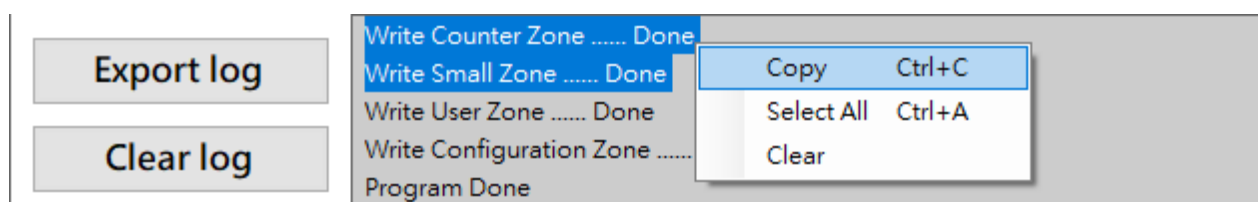


Figure 82 SQ710x Program Device: Copy contents of Log Window

5 Starter Kit Software Function Description (SQ713x)

5.1 Software Introduction

SQ713x (x= 1:I2C, 3:SPI, 5:SWI) is a hardware-based key storage with a secure hardware accelerator that can implement AES/ECC encryption functions, SHA hash algorithm, ECDH key exchange, ECDSA digital signature, and TRNG.

The SQ713x Starter Kit program is a Windows program for learning how to configure, access memory, test commands, security test, and lock areas for the EVB board.

5.2 Starter Kit Main Screen

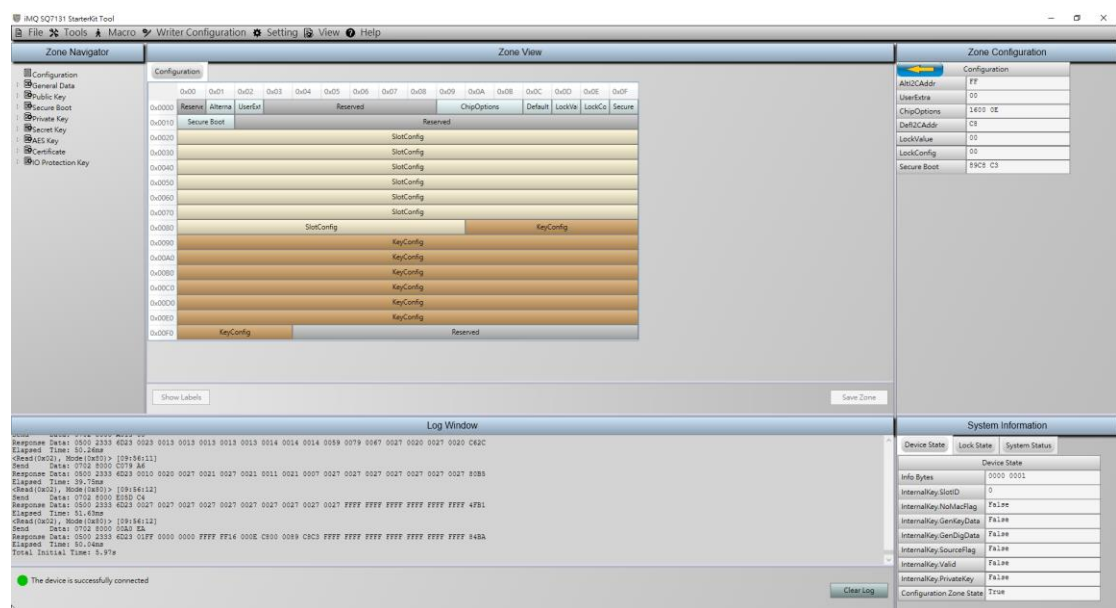


Figure 83 SQ713x Main screen

5.2.1 Main Menu

Main menu includes seven main items, File; Tools; Macro; Writer Configuration; Setting; View; Help.



Figure 84 SQ713x Main menu

5.2.1.1 File

File item includes 5 sub items, Export/Import Zone; Export/Import Log; Exit.

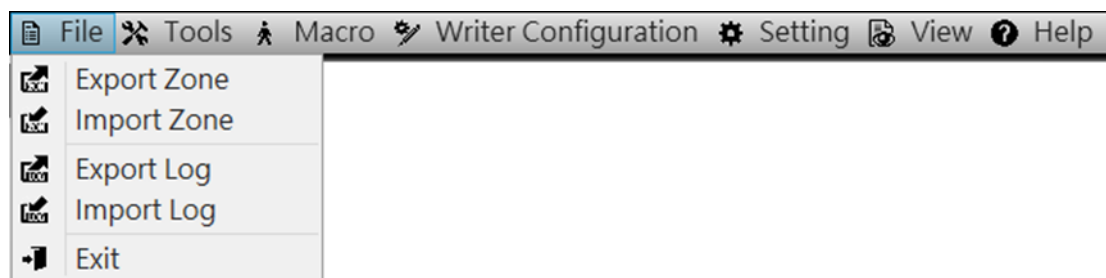


Figure 85 SQ713x File sub menu

Export/Import Zone: Export/Import the byte data of the current area to/from a Json file in the zone view window.

Export/Import Log: Export/Import the text data of the current area to/from a Json file in the log window.

Exit: Exit the program immediately.

5.2.1.2 Tools

Tools item includes two sub items, Crypto Calculator; Command Builder.

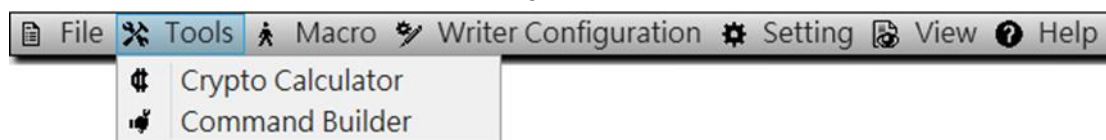


Figure 86 SQ713x Tools sub menu

Crypto calculator: This function can perform trial calculations on cryptographic functions.

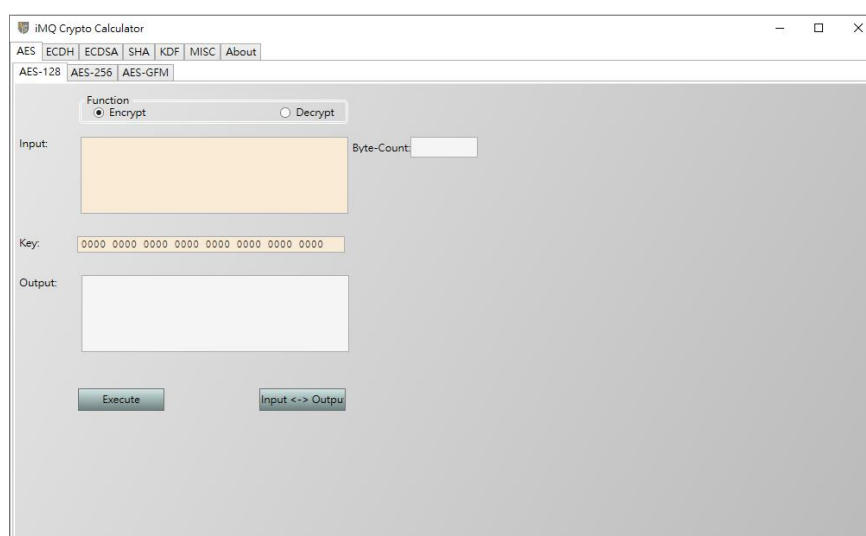


Figure 87 SQ713x Cryptor Calculator

Command builder: This function can communicate and test commands with SQ713x through USB HID protocol. (Refer to SQ713x Datasheet for command usage)



Figure 88 SQ713x Command Builder

Click Execute button to execute the command

Click Clear Details button to clear the content of Send Details/Response Details.

Click Export Macro button to export the command to be a Json file as a macro.

Click Import Macro button to import an existed macro file to compose the command.

5.2.1.3 Macro

Macro item includes two sub items, Generate Macro by Log; Run Macro.

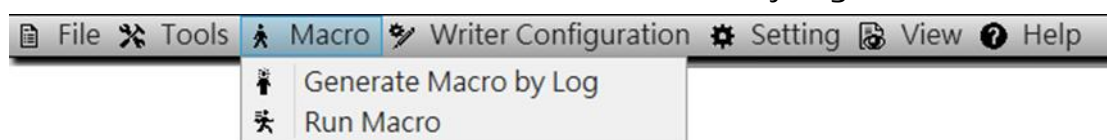


Figure 89 SQ713x Macro sub menu

Generate Macro by Log: This function generate a Json file as a macro from the

contents of the log window.

Run Macro: This function loads a macro file and executes its instructions in sequence.

5.2.1.4 Writer Configuration

Writer Configuration item includes a sub item, Writer Configuration Utility.

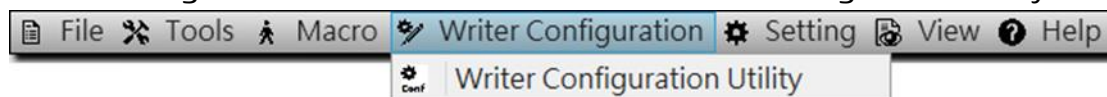


Figure 90 SQ713x Writer Configuration sub menu

Writer Configuration Utility: This function is a utility for one time chip configuration. (How to configure, please refer to SQ713x Datasheet)

Configuration Zone tab list the modifiable parameters in configuration zone.

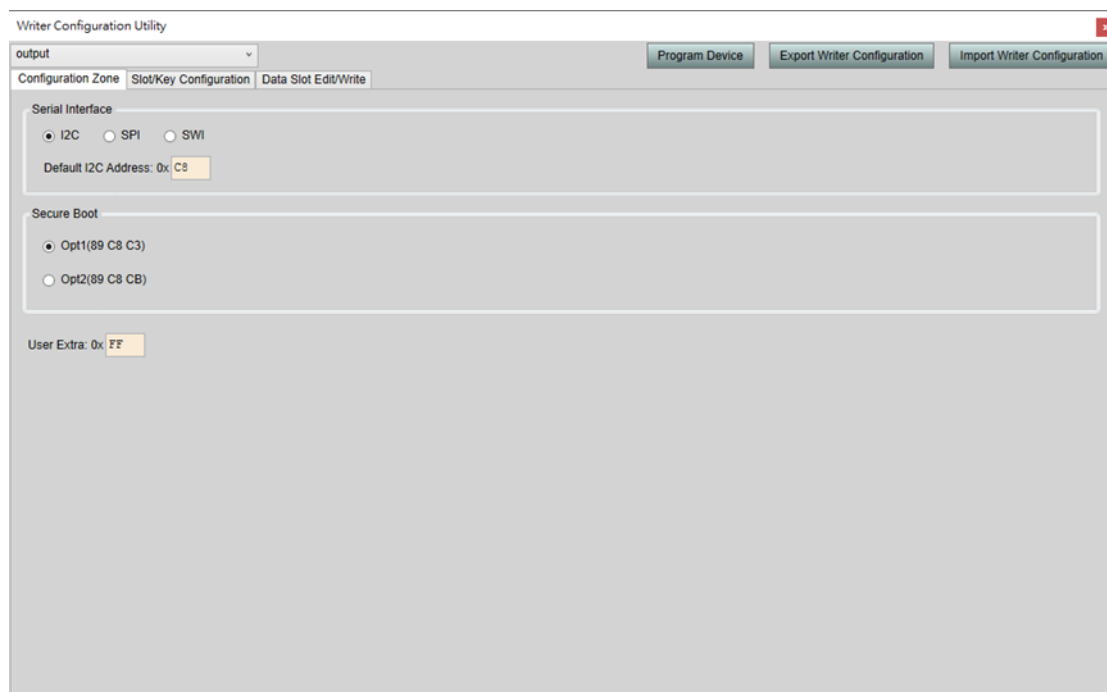


Figure 91 SQ713x Writer Configuration Utility/Configuration Zone

Click “Program Device” button to start programming the connected device.

Click “Export Writer Configuration” button to export the configuration data to a Json file.

Click “Import Writer Configuration” button to import the configuration data from a Json file.

Slot/Key Configuration tab list the slot options, most of them can be changed.

Except option2 of slot1 is persistent latched, all other option2 are locked and the lockable of option1 are opposite.

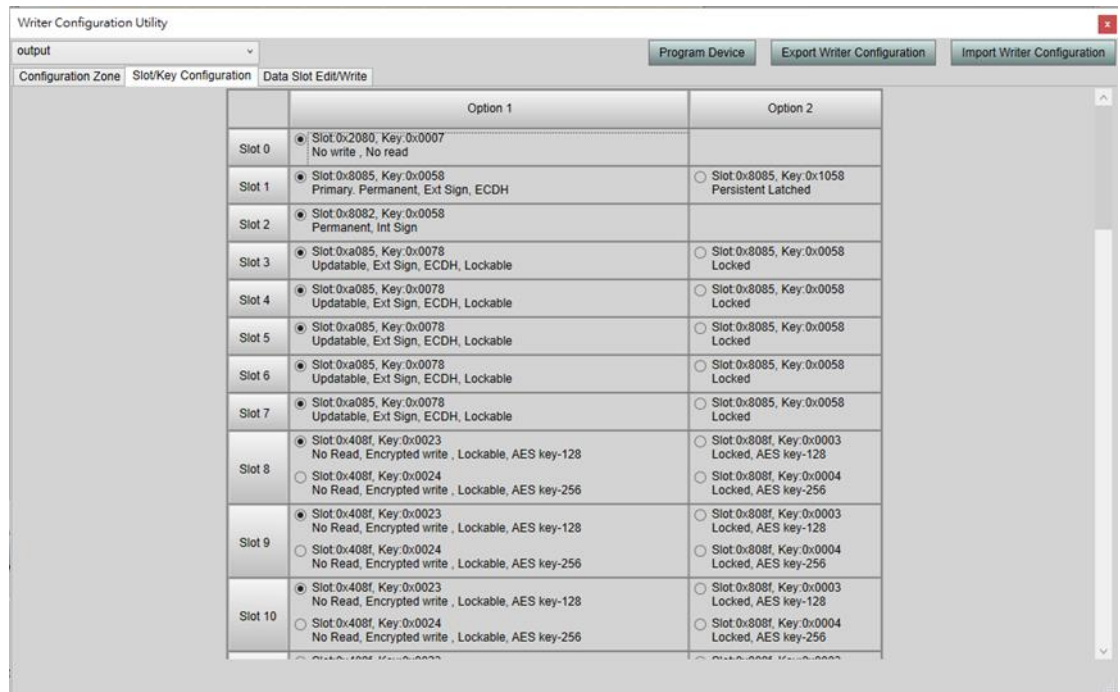


Figure 92 SQ713x Writer Configuration Utility/SlotKey Configuration

Data Slot Edit/Write tab provides a user interface to edit slot data and check the slots to write. In left navigator window, click on the item to read the associated data and update the slot contents on the right data grid window. The user can edit the data in the data grid. When the user ticks the checkbox of the item, it means that the slot data will be written to the device when the device is programmed.

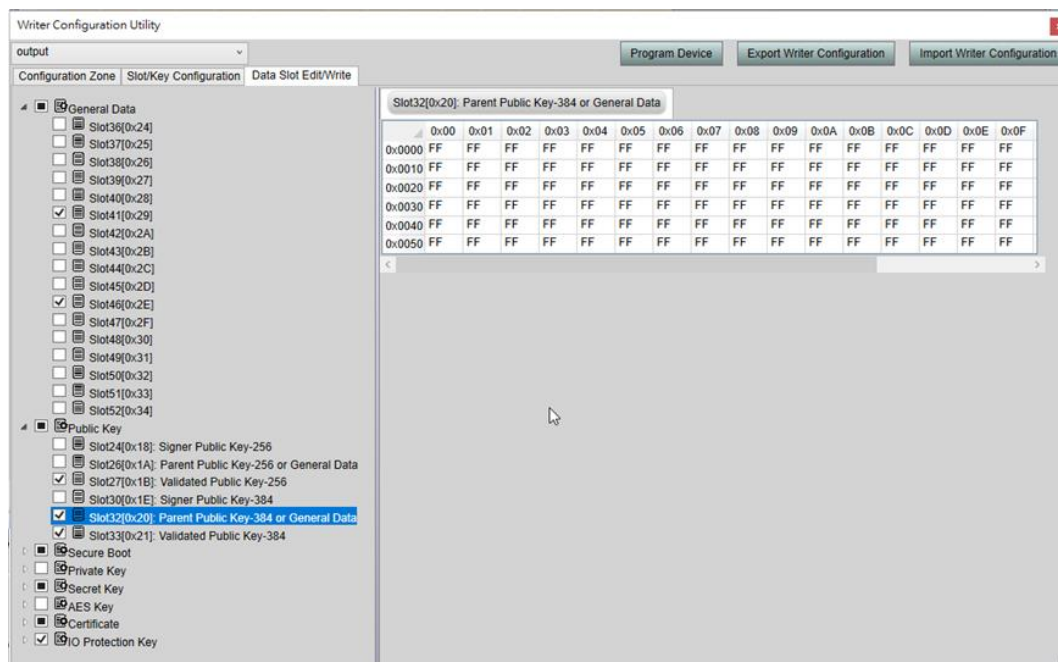


Figure 93 SQ713x Writer Configuration Utility/Data Slot Edit/Write

Due to the limitation of one time configuration, if the user tries to program the device on the same chip for the second time, the message "The configuration zone is locked and device programming cannot be performed!" will appear and stop the programming process immediately.

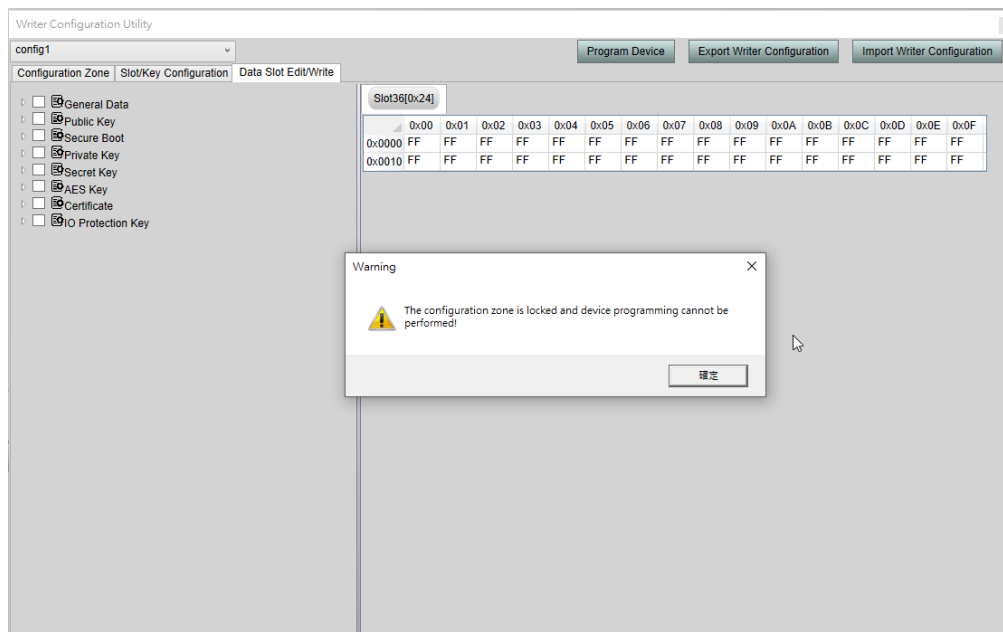


Figure 94 SQ713x Programming device twice inhibition message

5.2.1.5 Setting

Setting item includes a sub item, I/O Setting.



Figure 95 SQ713x Setting sub menu

I/O Setting: This function can adjust the I/O frequency at runtime. Depending on the interface between the host and the chip, one of the following three I/O setting dialog boxes will pop up.

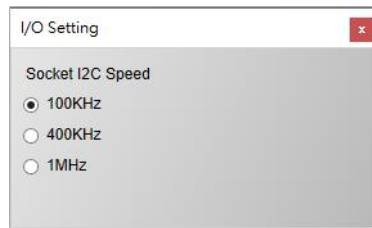


Figure 96 SQ713x I2C I/O Setting

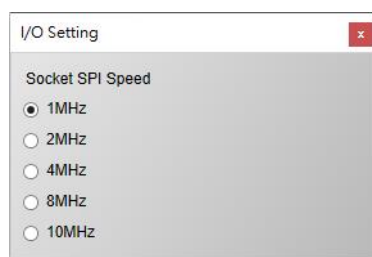


Figure 97 SQ713x SPI I/O Setting

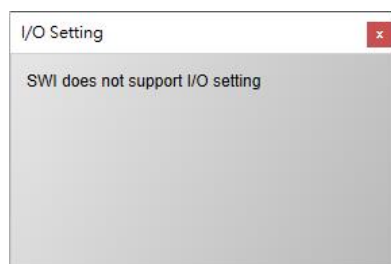


Figure 98 SQ713x SWI does not support I/O Setting

5.2.1.6 View

View item includes a sub item, Restore Default Layout.



Figure 99 SQ713x View sub menu

Restore Default Layout: Executing this function will reset the height and width of all screens to their default values.

5.2.1.7 Help

Help item includes a sub item, About.



Figure 100 SQ713x Help sub menu

About item displays a dialog to show the product and company information.



Figure 101 SQ713x About dialog

5.2.2 Main Windows

This program includes five main windows: zone navigator, zone view, zone configuration, system information and log window.

5.2.2.1 Zone Navigator Window

Zone navigator window collects zone slots in tree view for user to search and select a zone slot easily.

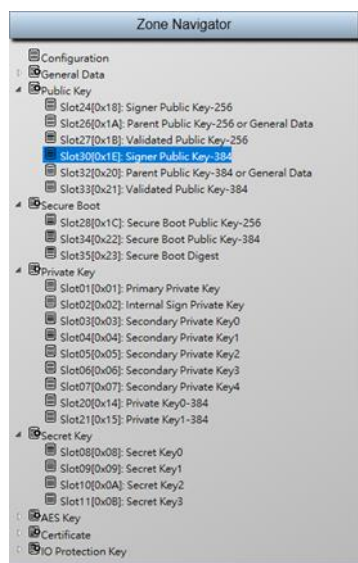


Figure 102 SQ713x Zone navigator window

5.2.2.2 Zone View Window

Zone view window displays the selected slot zone data, some of them are editable and savable, some of them are not editable and non-savable (please refer to the datasheet definition). It can also export/import data to/from secondary storage. Configuration zone has two types of views, one is label view and the other is data grid view, it can export only.

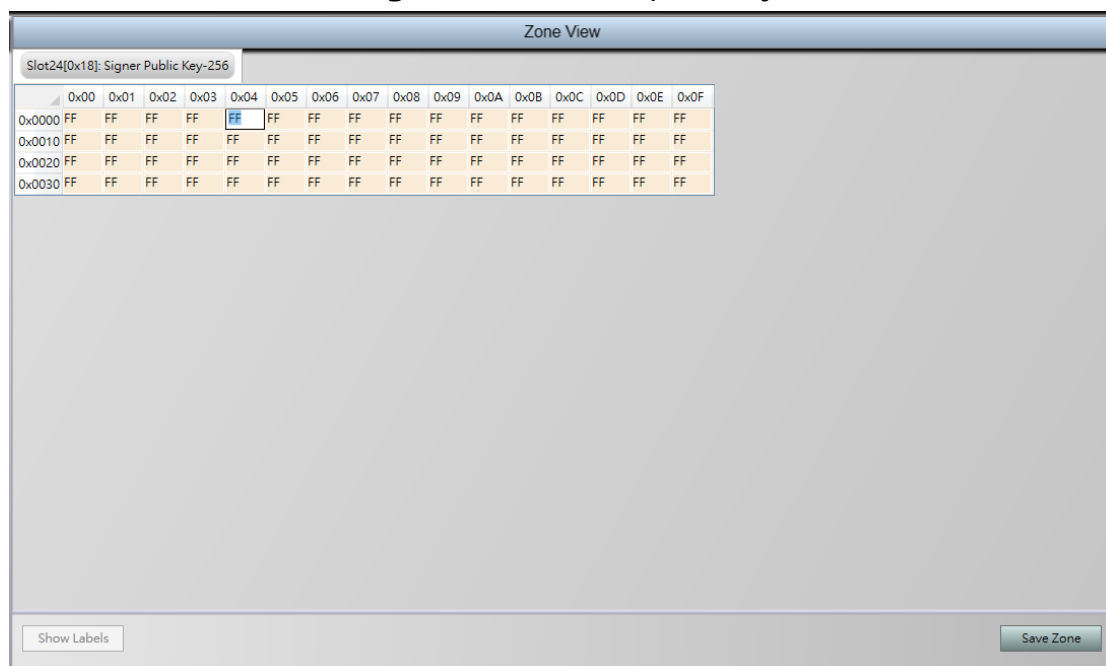


Figure 103 SQ713x Editable and savable data grid view

Click the “Save Zone” button to save the data grid's data to the relevant slot.

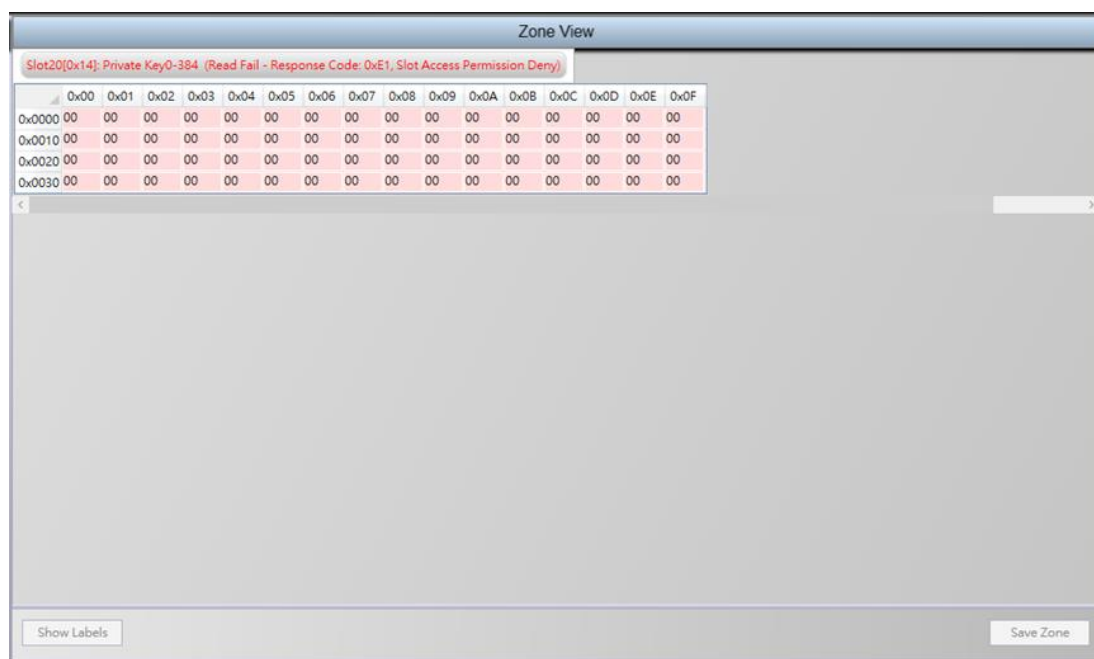


Figure 104 SQ713x Non-editable and non-savable data grid view

5.2.2.3 Configuration Label View

User can click on any label to switch to the data grid view and the cursor will focus on the corresponding cell of the label.

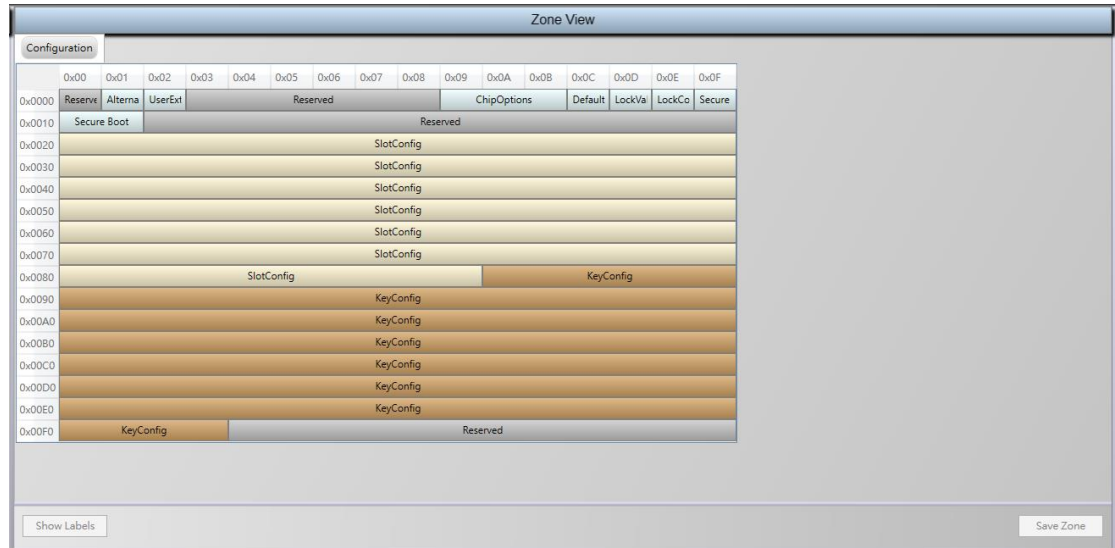


Figure 105 SQ713x Configuration label view

5.2.2.4 Configuration Data Grid View

When the cursor is focused on any cell in the data grid, the label next to the “Show Label” button displays the data grid byte offset, the label name, and the byte index within the label. Click “Show Labels” button can switch back to Configuration Label View.

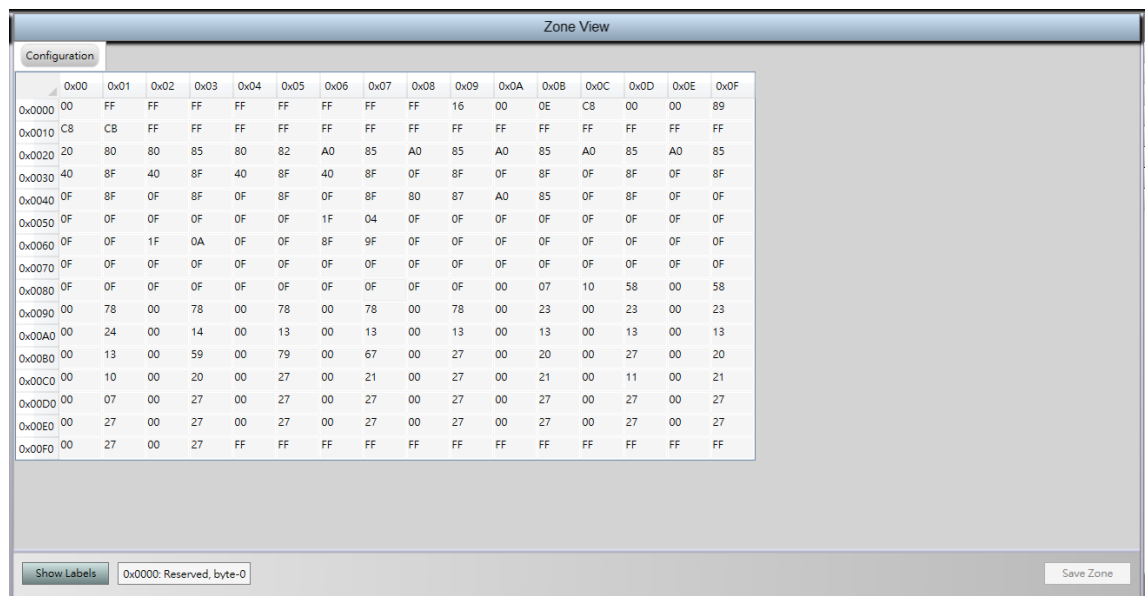


Figure 106 SQ713x Configuration data grid view

5.2.2.5 Zone Configuration Window

Zone configuration window displays the selected zone slot configuration.

Zone configuration of Configuration Zone:

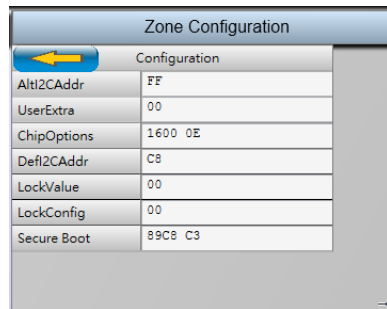


Figure 107 SQ713x Zone configuration window (Configuration zone)

Zone configuration of Data/Key Slot Zone:

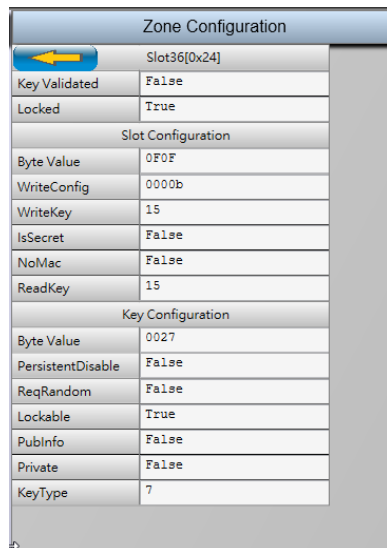



Figure 108 SQ713x Zone configuration window (Slot zone)

The button  can be dragged and clicked to switch the configuration area between data grid mode and description mode, data grid mode contains relevant configuration information of the current data zone, the description mode contains relevant description of the current data zone.

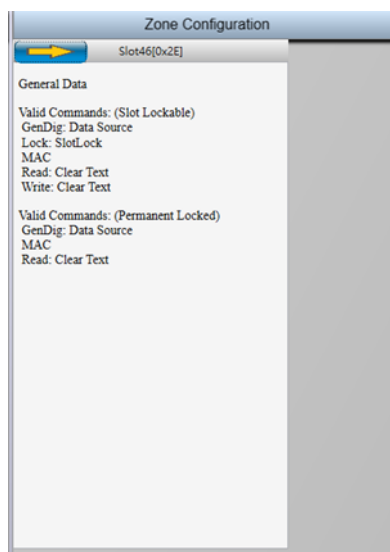


Figure 109 SQ713x Zone description of Data/Key Slot Zone

5.2.2.6 System Information Window

The Device Status tab of the System Information window displays the current status of the device.

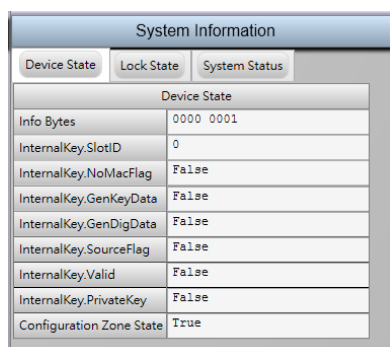


Figure 110 SQ713x System information window/Device state

Lock state tab of the System Information window displays configuration zone lock state and data zone lock state

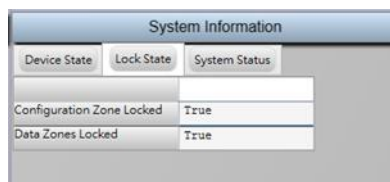
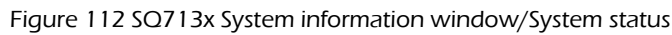
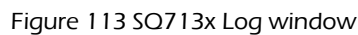


Figure 111 SQ713x System information window/Lock state

System status tab of the System Information window displays system and device information.



Log window displays communication log data.



Device connection status: Green light on indicates successful device connection; red light on indicates device connection failure.

6 Starter Kit Software Function Description (HQS600x)

6.1 Software Introduction

HQS600x is a hardware-based key storage with a secure hardware accelerator that can implement SHA hash algorithm, and TRNG.

The HQS600x Starter Kit program is a Windows program for learning how to test commands for the EVB board.

6.2 Starter Kit Main Screen

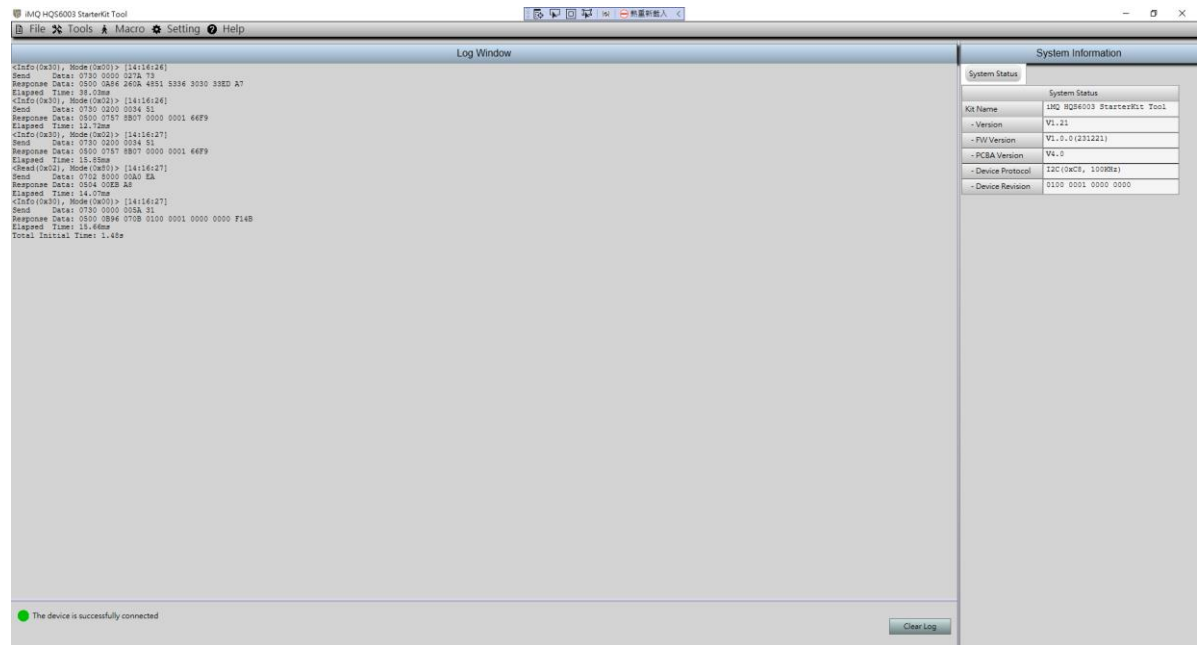


Figure 1 14 HQS600x Main screen

6.2.1 Main Menu

Main menu includes five main items, File; Tools; Macro; Setting; Help.



Figure 1 15 HQS600x Main menu

6.2.1.1 File

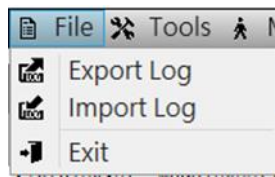


Figure 116 HOS600x File sub-menu

File item includes three sub-items, Export/Import Log; Exit.

Export/Import Log: Export/Import the text data of the current area to/from a Json file in the log window.

Exit: Exit the program immediately.

6.2.1.2 Tools

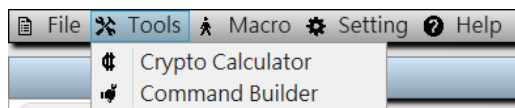


Figure 117 HOS600x Tools sub-menu

Tools item includes two sub-items, Crypto Calculator; Command Builder.

Crypto calculator: This function can perform trial calculations on cryptographic functions.

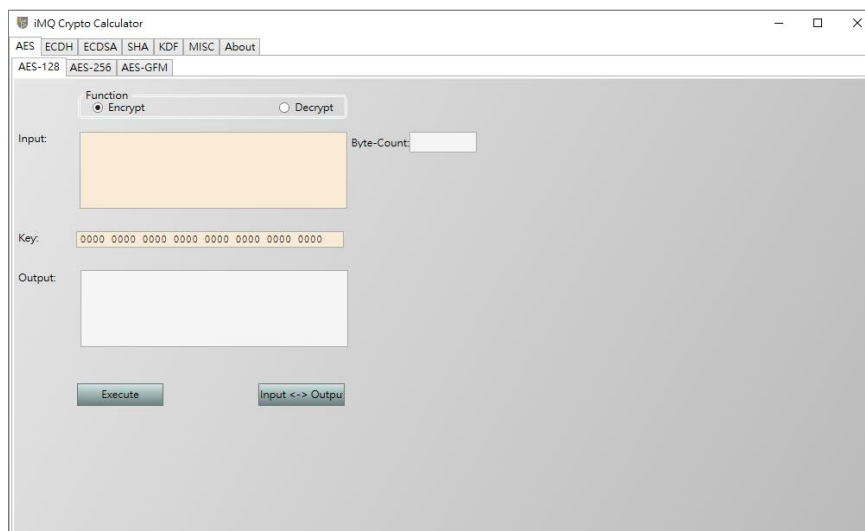


Figure 118 HOS600x Crypto calculator

Command builder: This function can communicate and test commands with HOS600x through USB HID protocol. (Refer to HOS600x Datasheet for command usage)

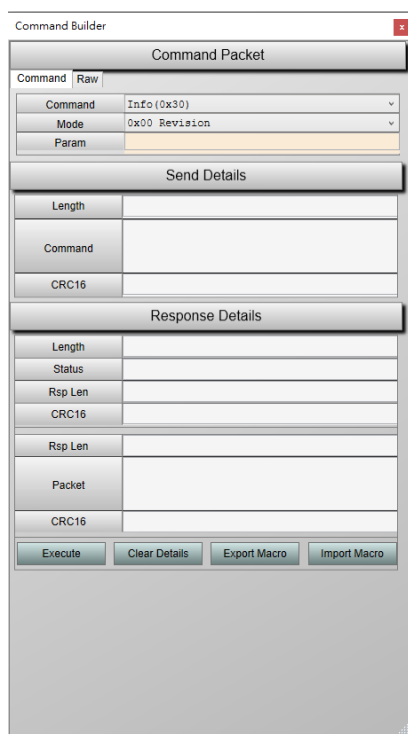


Figure 119 HOS600x Command builder

6.2.1.3 Macro

Macro item includes two sub-items, Generate Macro by Log; Run Macro.

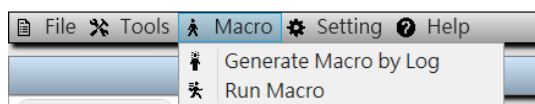


Figure 120 HOS600x Macro sub-menu

Generate Macro by Log: This function generate a Json file as a macro from the contents of the log window.

Run Macro: This function loads a macro file and executes its instructions in sequence.

6.2.1.4 Setting

Setting item includes a sub-item, I/O Setting.



Figure 121 HOS600x Setting sub-menu

I/O Setting: This function can adjust the I/O frequency at runtime.

Depending on the interface between the host and the chip, one of the following three I/O setting dialog boxes will pop up.

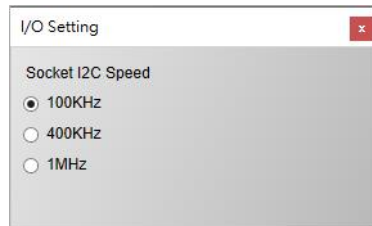


Figure 122 HOS600x I2C I/O Setting

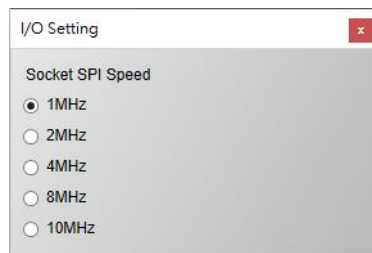


Figure 123 HOS600x SPI I/O Setting

6.2.1.5 Help

Help item includes a sub-item, About.



Figure 124 HOS600x Help sub-menu

About item displays a dialog to show the product and company information.



Figure 125 HOS600x About dialog

6.2.2 Main Windows

6.2.2.1 Log Window

System status tab of the System Information window displays system and device information.

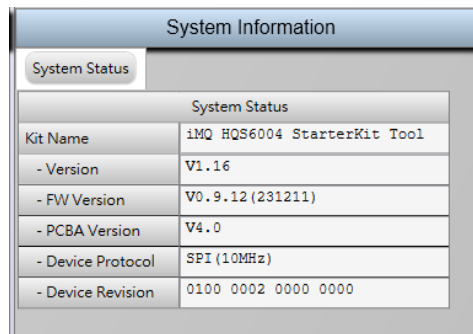


Figure 126 HOS600x System information/System status

6.2.2.2 Log Window

Log window displays communication log data.

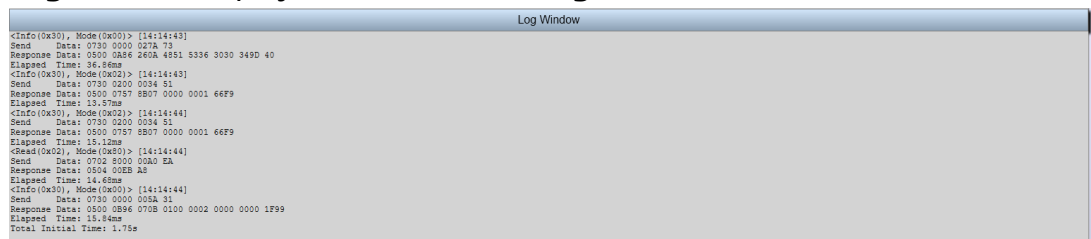


Figure 127 HOS600x Log window

Click "Clear Log" button to clear the content of Log Window.

Device connection status: Green light on indicates successful device connection; red light on indicates device connection failure.

Appendix A: Hardware Settings Precautions for Prototyping SQ7515

To develop general functions and Security Processor for SQ7515, the following hardware is required:

- Starter Kit (Left)
- SQ7515 EVB (Middle)
- MQ-Link (Right)

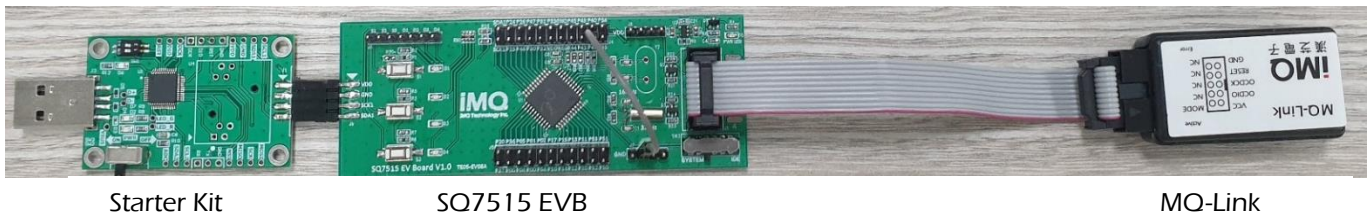


Figure 128 SQ7515 hardware settings

A.1 Security Processor application development for SQ7515

1. Confirm that P42 (reset) and GND on the SQ7515 EVB is shorted (EVB V1.1 uses Jumper to complete).
2. Confirm that the slide switch on the SQ7515 EVB switch to the system setting.
3. Use MQ-link to connect SQ7515 EVB for power supply, and connect the other side of MQ-link to PC as power source (Before this step, the EVB is power off).
4. The Starter kit is connected to the SQ7515 EVB, and the other end of the Starter kit is connected to the PC.
5. Open the GUI software on the PC and start setting the Security processor key or Config.

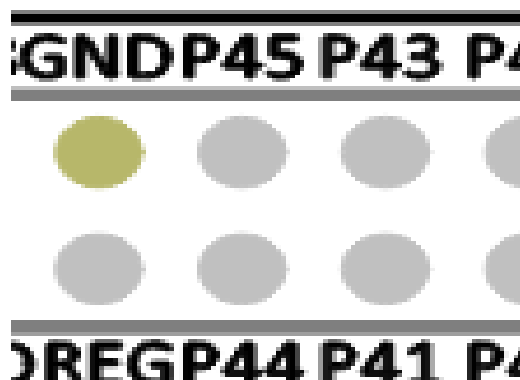


Figure 129 EVBV 1.1 Add a Reset grounding jumper

No. : TDUM02- TE002-EN	Name: Secure Starter Kit User Manual	Version : V2.0
------------------------	--------------------------------------	----------------

A.2 Host Processor application development for SQ7515 (using IDE)

1. Confirm that P42 (reset) and GND on the SQ7515 EVB is open (EVB V1.1 uses Jumper to complete).
2. Confirm that the slide switch on the SQ7515 EVB switch to the IDE setting.
3. Connect the MQ-link to the SQ7515 EVB, and connect the other side of the MQ-link to the PC.
4. Open the IDE software and develop the application.

Note1: If you want to execute the StarterKit GUI to develop the Security Processor after executing the IDE first, the system must be powered on again. (according to the setting in A.1)

Note2: For IDE software function description, please refer to "MQ-LINK User Manual".

No. : TDUM02- TE002-EN	Name: Secure Starter Kit User Manual	Version : V2.0
------------------------	--------------------------------------	----------------

Change history

Version	Approved Date	Description
V2.0	2024/02/20	1. Re-organize bullet in Ch4/Ch5/Ch6 2. Type error correction 3. Update figure 10, 11, 87, 106, 114, 118
V1.9	2024/02/02	4. Update figure 10, 11 5. Add 2.2 Starter Kit firmware update
V1.8	2024/01/04	1. Update SQ713x for screen shot change 2. Update HQS600x for screen shot change 3. Add Programming device twice inhibition message figure 92
V1.7	2023/11/01	1. Reorganize the structure of the manual and move common parts to earlier chapters (CH1, CH2, CH3) 2. Renumber figures 3. Change some pictures
V1.6	2023/10/17	1. Added SQ713x user manual in CH2; HQS600x user manual in CH3 2. Rearrange chapter numbers for SQ710x in CH1
V1.5	2022/11/23	1. "SQ71 Series Secure Starter Kit User Manual" rename to "Secure Starter Kit User Manual" 2. "CH3 Starter Kit software installation" updated 3. "CH4.2.1 Build Command" updated 4. "CH4.2.2 Menu bar" updated
V1.0	2021/01/15	First release