CEC173x Evaluation Board User's Guide

EV42J24A

Introduction

The EV42J24A CEC173x Evaluation Board is intended as a demonstration, development and testing platform for Real Time Platform Root of Trust applications in Data Center, Telecommunications, Networking, Industrial and Embedded computing markets. This updated board is a replacement for the discontinued EV19K07A development board. The new EV42J24A board has a simplified set of modifiable jumpers, sockets for the SPI Flash memory devices and an upgrade to the SF600 DediProg programming interface. The board can be used with the 84-pin version of either the CEC1736 or the CEC1734 devices. This board features a variety of hardware options (including a power supply, user interface, serial communications and expansion headers) that enable rapid prototyping and development of Real Time Platform Root of Trust applications. This board can support both 3.3V and 1.8V SPI memory chips via the on-board SPI sockets.

This evaluation board is designed to be used with Microchip's Trust Platform Design Suite (TPDS), which has multiple use cases to demonstrate the capabilities of the CEC173x-TFLX and CEC173x-TCSM devices.

- Four sample packs of three units each of CEC173x TrustFLEX™ and TrustCUSTOM™ devices (CEC1736-TFLX-PROTO, CEC1736-TCSM-PROTO, CEC1734-TFLX-PROTO, CEC1734-TCSM-PROTO)
- CEC1736 demo sample for initial board bring up and validation. Not to be used for specific use case or application development – Preprogrammed with the latest Soteria-G3 firmware release
- MEC1723 (emulated as Application Process) – MEC1723 Example firmware is included and upgradeable as part of the TPDS tools
- CEC173x socket – Users have the ability to use a CEC173x-TFLX or CEC173x-TCSM to customize configuration for various security features for their specific designs.

Figure 1. CEC173x Evaluation Board

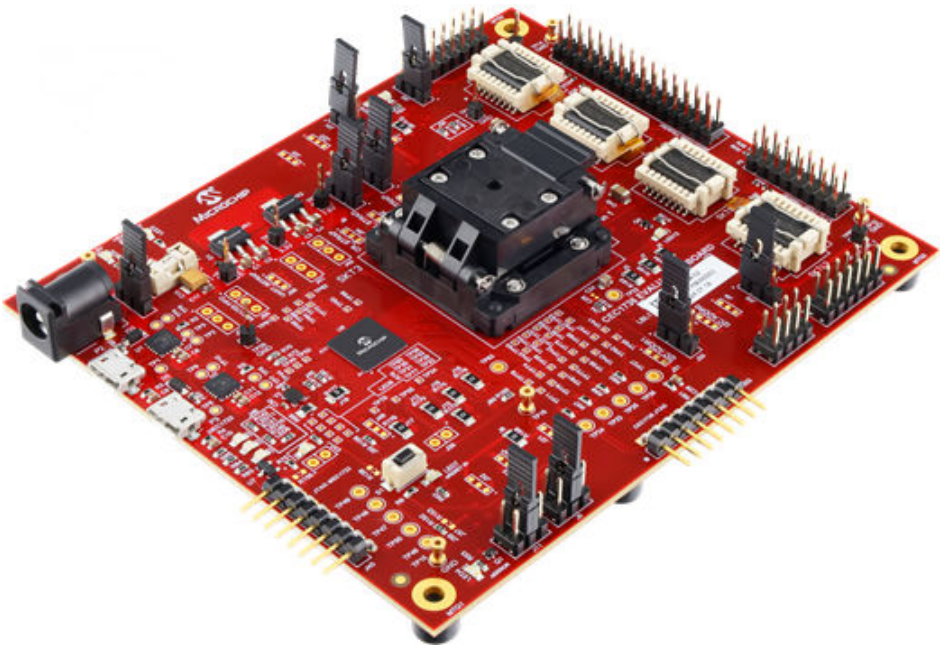
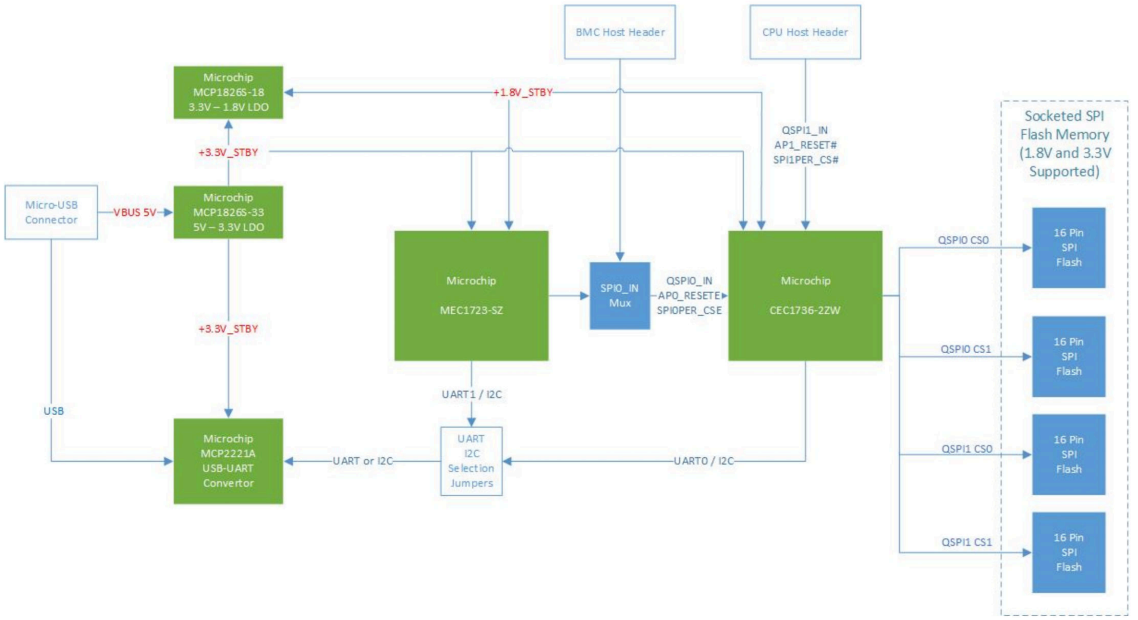


Table of Contents

1. Features

1.1 CEC173x Evaluation Board Block Diagram

Figure 1-1. Block Diagram



1.2 Hardware Features

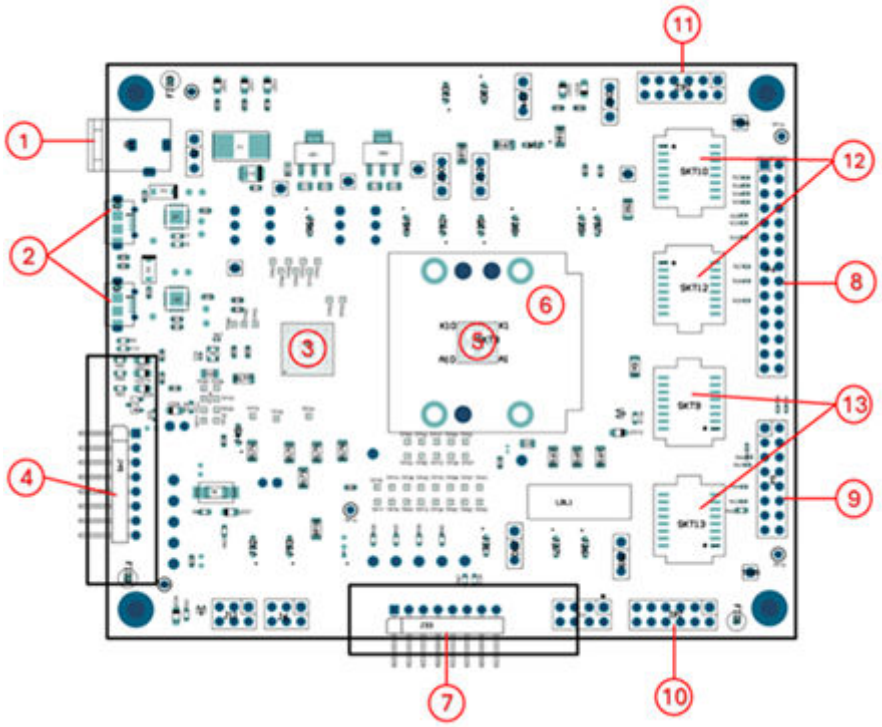
- Socket for CEC173x 84-Pin
- Four 16-Pin 256 Mbit, 3.3V SPI Flashes in Socket for Normal Operation.
- One USB-UART/I^2C Port for CEC173x
- One USB-UART Port for MEC1723
- BMC Host Header
- CPU Host Header
- One 1x8 PICKIT4 Header for CEC173x for Debugging and Programming
- One 1x8 PICKIT4 Header for MEC1723 for Debugging and Programming
- GPIOs/I^2C Headers for Optional Customization Development
- Board Can be Powered By Micro-USB Cable or +5V Power Adapter, Which Are Not Included in the Development Board Kit
- The EV42J24A Comes with a CEC1736 Part, Already Installed in the On-Board Socket for Doing a Board Validation Check. In Addition, the Kit Includes the Following CEC173x Sample Packs for Developing Applications. Each Sample Pack Contains 3 Devices.

Important:
The top marking of the device can distinguish whether a device type is CEC1734 or CEC1736. However, this cannot determine whether or not the type is TFLX or TCSM. Careful handling is required to not mix up the devices. TPDS can be used to identify whether the device is TFLX or TCSM. The TPDS tools will verify what type of device it is prior to programming.

- CEC1736-TFLX-PROTO
- CEC1736-TCSM-PROTO
- CEC1734-TFLX-PROTO
- CEC1734-TCSM-PROTO

1.3 CEC173x Evaluation Board Layout

Figure 1-2. Board Layout Features



1. Power Adapter Plug (P1) – Provides another way to power the board via external +5V power adapter
2. USB micro-B connectors – Provides power to the board and provides an interface for serial input/output or I^2C using the Microchip MCP2221A USB-to-UART/I^2C serial converter to CEC173x (P2) and MEC1723 (P3)
3. Microchip MEC1723N-B0-I/SZ (U6) – Emulated as Application Processor
4. Microchip PICKIT4 1x8 header (J45) for MEC1723
5. Microchip CEC1736-S0-I/2ZW Demo Device (installed in U3 socket)
6. 84-pin 2ZW package socket (U3)
7. Microchip PICKIT4 1x8 header (J33) for CEC173x
8. BMC Host Connection Header (P4)

9. CPU Host Connection Header (P5)
10. DediProg SF600 SPI Flash Programming Header (J61) to program U9 or U13
11. DediProg SF600 SPI Flash Programming Header (J62) to program U10 or U12
12. SPI Flashes in Socket (U10, U12) on CEC173x QSPI1 channel
13. SPI Flashes in Socket (U9, U13) on CEC173x QSPI0 channel

2. Recommended Tools and Accessories

The following tools are recommended for development with the CEC173x Evaluation Board.

Recommended Hardware

1. Microchip MPLAB® X v6.20 or later
2. XC32 Pro Compiler v2.50 or later for TrustCustom customers customizing Soteria software
3. PICkit™ 4/PICkit 5 In-Circuit debugger for direct plug-in
4. Aardvark I2C/SPI Host Adapter
5. DediProg SF600Plus-G2 Programmer (preferred) or DediProg SF100 External SPI Flash programmer.

Recommended Software

The following software is recommended or required to be used with the EV42J24A evaluation board.

1. Microchip Trust Platform Design Suite (TPDS) (See Trust Platform Design Suite (TPDS) for more information)
2. Install MPLAB X IDE
   - For MPLAB version 6.20 and PICKIT5, ensure Toolpack version: 2.5.391, CEC DFP version 2.0.261 are installed
   - Set MPLAB X path in TPDS at File -> Preferences -> MPLAB X Path
3. Install FTDI4222H Drivers.
4. Install Aardvark I2C/SPI Host Adapter Drivers.
5. Install SF Software and USB Driver for DediProg SF600Plus-G2 from Support tab.
6. Tera Term v4.106 or later (or preferred equivalent) for UART debug logs

Technical Reference Material

Many of the documents associated with the CEC173x products and development boards are available only by NDA and are available through myMicrochip. For more information, go to Accessing Microchip's Secure Documents via myMicrochip.

- CEC1736 Website
- CEC1734 Website
- CEC1736-TFLX Website
- CEC173x Summary Data Sheet (The Complete Data Sheet is available through myMicrochip and is under NDA.)
- Additional board (Schematics, Gerber Files and BOM) and other technical collateral are available via myMicrochip and are under NDA.

Contact your Microchip Representative with any further questions.

3. Board Operation and Configuration

3.1 Powering the CEC173x Evaluation Board

The CEC173x Evaluation Board can be powered directly through the USB micro-B port of the USB-Serial converter (P2 and/or P3). The 5V input from the USB voltage rail is regulated to 3.3V by an MCP1826S voltage regulator.

Optionally, the CEC173x Evaluation Board can be powered by an external power supply through the Power Plug (P1). The 5V is regulated to 3.3V, which is the same as using USB micro-B port. This option is selected by J1 1-2; the default is 2-3 power through USB.

A shunt diode (D1) can be used to allow measurement of the total system power consumption when using the USB micro-B port, or a jumper (J1) is provided to allow measurement of the total system power consumption when using an external power supply.

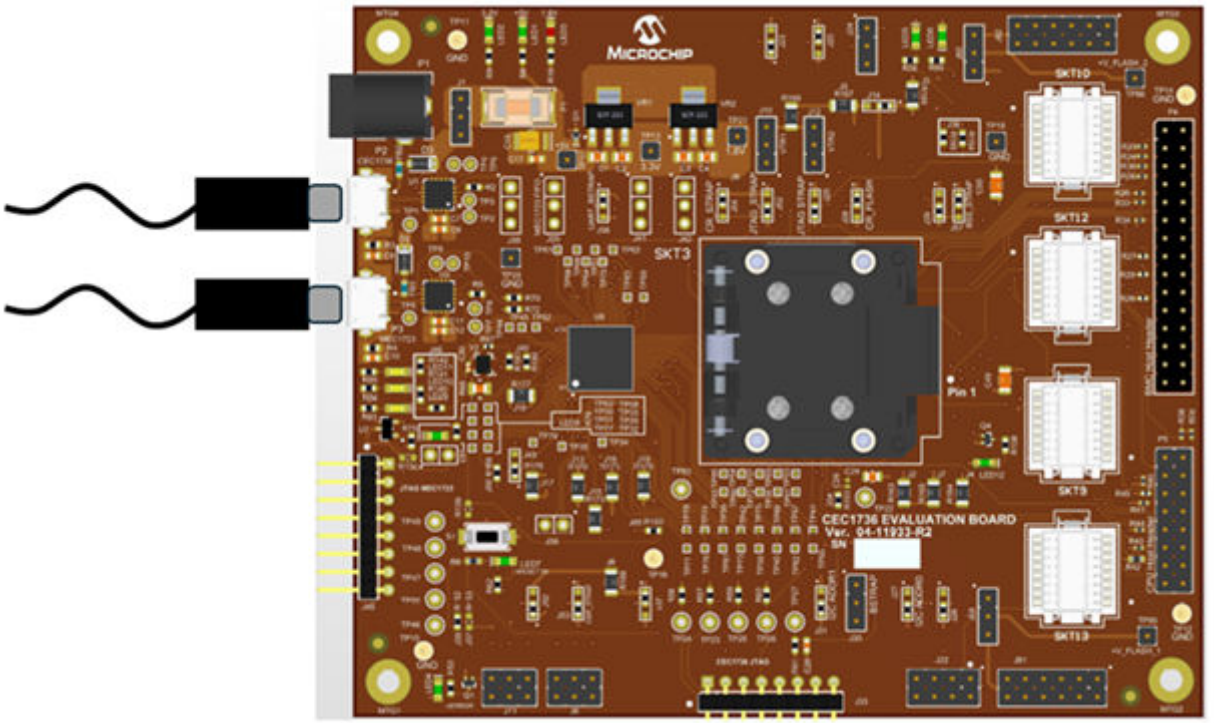
When the board is powered, LED1 (+5V), LED2 (+3.3V) and LED3 (+1.8V) turn on.

LED9, LED10 and LED11 can be blinking depending on the MEC1723 Firmware Application, which indicates that the MEC1723 Firmware is loaded and executing.

LED4, LED5, LED6 and LED12 can be blinking, indicating that the CEC1736 Soteria Firmware is loaded and executing.

Power-up as shown below:

Figure 3-1. Powering The Board

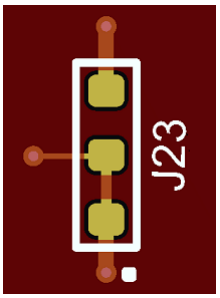


3.2 Jumper Options

The CEC173x Evaluation Board has a variety of configuration jumpers.

The jumpers and headers have a J reference designator. Several of the jumpers were replaced by a special trace-link PCB structure, in which the default value for the jumper is hardwired into the design. A representative picture of this PCB structure for jumper J23 is shown in the figure below labeled “Trace-Link Jumper”. To change the value of these jumpers, the user must cut the default trace and install a resistor across the alternate connection pads. In the example for J23, the user would cut the trace between pin 1 and 2 and install a zero Ohm 0603 surface mount resistor between pads 2 and 3. Some of the jumpers were replaced with a single 0 Ohm resistor. For these jumpers, the options are either installed (IN) or not installed (OUT). The resistors used in these locations are listed in the Jumper Options Description field below. In other cases, a standard shorting block is required to be placed across jumper pins in the default position for default operation of the device.

Figure 3-2. Trace-Link Jumper



The following table of Jumpers was based on the original EV19K07A evaluation board. Regardless of jumper type, an effort was made to maintain the original jumper name to the original kit. A jumper type was added to the table to make it easy to identify what type of jumper was used. The following types were identified:

1. Standard – A standard jumper uses a header and a jumper cap to modify the design.
2. 0 Ohm Short – Instead of a selection jumper, one or more zero Ohm jumpers were used to replace the original jumper. The description field indicates what resistors were used to replace the jumper.
3. Trace-Link – A PCB structure that shorts through a direct metal link to the default position
4. Header – Not a jumper, but a header to interface to the outside world.
5. Removed – A jumper that existed in the original EV19K07A board but was removed from the EV42J24A board.

Table 3-1. Jumper Options and Headers

Jumper	Description	Jumper Type	Description
J1	Board Power Selection	Standard	1-2: Power by external 5V Adapter (P1) 2-3 (Default): Power by micro-USB Port (P2, P3)
J2	VTR power to CEC173x	0 Ohm Short	R163 IN (Default): Connect VTR power OUT: Disconnect VTR power
J3	+3.3V power to MEC1723	0 Ohm Short	R166 IN (Default): Connect +3.3V power OUT: Disconnect +3.3V power
J4	VTR_PLL power to CEC173x	0 Ohm Short	R164 IN (Default): Connect VTR_PLL power OUT: Disconnect VTR_PLL power
J5	+1.8V power to MEC1723	0 Ohm Short	R167 IN (Default): Connect +1.8V power OUT: Disconnect +1.8V power
J6	CEC173x I^2C SCL selection to MCP2221A	Standard	1-2: I^2C10 3-4 (Default): I^2C06 5-6: I^2C00

.....continued

Jumper	Description	Jumper Type	Description
J7	VTR_ANALOG power to CEC173x	0 Ohm Short	R165 IN (Default): Connect VTR_ANALOG power OUT: Disconnect VTR_ANALOG power
J8	+3.3V power to CEC173x	0 Ohm Short	R168 IN (Default): Connect +3.3V power OUT: Disconnect +3.3V power
J9	+1.8V power to CEC173x	0 Ohm Short	R169 IN (Default): Connect +1.8V power OUT: Disconnect +1.8V power
J10	VTR1 power selection for CEC173x	Standard	1-2 (Default): Connect +3.3V power 3-4: Connect +1.8V power
J11	CEC173x I^2C SDA selection to MCP2221A	Standard	1-2: I^2C10 3-4 (Default): I^2C06 5-6: I^2C00
J12	VTR2power selection for CEC173x	Standard	1-2 (Default): Connect +3.3V power 3-4: Connect +1.8V power
J13	VTR_REG power to MEC1723	0 Ohm Short	R170 IN (Default): Connect VTR_REG power OUT: Disconnect VTR_REG power
J14	VTR2 power selection for MEC1723	Trace-Link	1-2 (Default): Connect +3.3V power 3-4: Connect +1.8V power
J15	VTR_PLL power to MEC1723	0 Ohm Short	R173 IN (Default): Connect VTR_PLL power OUT: Disconnect VTR_PLL power
J16	VTR_ANALOG power to MEC1723	0 Ohm Short	R175 IN (Default): Connect VTR_ANALOG power OUT: Disconnect VTR_ANALOG power
J17	VTR1 power to MEC1723	0 Ohm Short	R176 IN (Default): Connect VTR1 power OUT: Disconnect VTR1 power
J18	VBAT power to MEC1723	0 Ohm Short	R177 IN (Default): Connect VBAT power OUT: Disconnect VBAT power
J19	VTR3 power to MEC1723	0 Ohm Short	R178 IN (Default): Connect VTR3 power OUT: Disconnect VTR3 power
J20	CEC173x GPIO012/nEXTRST Pull selection	Trace-Link	1-2 (Default): Pull-high to VTR_REG 2-3: Pull-down
J21	CEC173x GPIO106/AP0_nRESET Pull selection	Trace-Link	1-2 (Default): Pull-high to VTR_REG 2-3: Pull-down
J22	CEC173x GPIOs Header	Header	For debug purposes
J23	CEC173x GPIO1316/AP1_nRESET Pull selection	Trace-Link	1-2 (Default): Pull-high to VTR_REG 2-3: Pull-down
J24	CEC173x nRESET_IN pin	Standard	1-2 (Default): Normal operation 2-3: Hold CEC1736 in reset
J25	CEC173x JTAG _STRAP pin	Trace-Link	1-2: Put in boundary scan mode 2-3 (Default): Normal operation
J26	CEC173x GPIO055 Strap Option	Trace-Link	1-2 (Default)
J27	CEC173x I^2C_ADDR0 Strap	Trace-Link	1-2: Pull-high to VTR_REG 2-3 (Default): Pull-down
J28	CEC173x CR_FLASH Strap	Trace-Link	1-2 (Default): Normal operation 2-3: Boot from crisis recovery flash component
J29	CEC173x GPIO124 Strap Option	Trace-Link	1-2 (Default)
J30	CEC173x BSTRAP Strap	Standard	1-2 (Default): Normal operation 2-3: Boot from I^2C or UART Crisis Port
J31	CEC173x I^2C_ADDR1 Strap	Trace-Link	1-2: Pull-high to VTR_REG 2-3 (Default): Pull-down

.....continued

Jumper	Description	Jumper Type	Description
J32	CEC173x RESET_IN# Delay Circuit Power Source	Trace-Link	1-2 (Default): Connect +3.3V power 2-3: Connect VTR_REG power
J33	CEC173x PICKIT4 1x8 Header	Header	For debug purposes
J34	CEC173x 32KHz Single-End Source	0 Ohm Short	R151 IN (Default): Connect oscillator OUT: Disconnect oscillator
J35	CEC173x RESET_IN# delay circuit	0 Ohm Short	R152 IN (Default): Connect delay circuit OUT: Disconnect delay circuit
J36	CEC173x GPIO157/LED1 & GPIO156/LED0 pins connection	0 Ohm Short	R154 1-2 (Default): Connect GPIO157 to LED5 R155 3-4 (Default): Connect GPIO156 to LED6
J37	CEC173x RESET_IN# pin ground	0 Ohm Short	IN: Hold CEC1736 in Reset R153 OUT (Default): Normal operation
J38	CEC173x UART0 debug header	Standard	For debug purposes
J39	MEC1723 Test Clocks Out header	Standard	For debug purposes
J40	MEC1723 32KHz Single-End Input selection (Optional)	0 Ohm Short	Use R180, R181 and R67 to select the clock source
J41	MEC1723 I^2C02 channel header	Standard	For debug purposes
J42	MEC1723 I^2C07 channel header	Standard	For debug purposes
J43	MEC1723 RESET_IN# delay circuit	Standard	IN: Connect delay circuit OUT (Default): Disconnect delay circuit
J44	MEC1723 RESET_IN# pin ground	0 Ohm Short	IN: Hold MEC1723 in reset R156 OUT (Default): Normal operation
J45	MEC1723 PICKIT4 1x8 Header	Header	For debug purposes
J46	MEC1723 GPIO156/LED0, GPIO157/LED1, and GPIO153/LED2 pins connection	0 Ohm Short	R140 (Default): Connect GPIO156 to LED9 R141 (Default): Connect GPIO157 to LED10 R142 (Default): Connect GPIO153 to LED11
J47	Dediprog SPI Programming Header	Header	Eliminated in this revision
J48	U8 SPI Flash power source selection	Removed	U8 and J48 eliminated in this revision
J49	MEC1723 XTAL2 selection	Trace-Link	1-2 (Default): Connect to 2-pin crystal 2-3: Connect to single-end 32 KHz source
J50	MEC1723 XTAL1 selection	0 Ohm Short	R159 IN (Default): Connect to 2-pin crystal OUT: Use single-end 32 KHz source, floating
J51	U8 SPI Flash isolation jumper	Removed	Eliminated in this revision
J52	MEC1723 JTAG _STRAP pin	Trace-Link	1-2: Put in boundary scan mode 2-3 (Default): Normal operation
J53	MEC1723 CMP_STRAP pin	Trace-Link	1-2 (Default)
J54	MEC1723 CR_STRAP pin	Trace-Link	1-2 (Default): Boot from SHD_SPI flash via CEC1736 2-3: Boot from PVT_SPI flash (U8)
J55	MEC1723 UART0 debug header	Standard	For debug purposes
J56	MEC1723 UART_BSTRAP pin	Trace-Link	1-2 (Default): Normal operation 2-3: Boot from UART Crisis Port
J57	MEC1723 BSS_STRAP pin	Trace-Link	1-2 (Default): Normal operation 2-3: Not boot in this application
J58	CEC173x QSPI0 CS0 Pass/Failure Cases selection for demonstration purpose	Removed	Eliminated in this revision
J59	CEC173x Flash Bus 1 Power select	Standard	1-2 (Default): Connect to board power 2-3: Connect Dediprog power
J60	CEC173x Flash Bus 2 Power select	Standard	1-2 (Default): Connect to board power 2-3: Connect Dediprog power

.....continued			
Jumper	Description	Jumper Type	Description
J61	Dediprog SPI Programming Header	Header	Use for U9 or U13 SPI Flash programming
J62	Dediprog SPI Programming Header	Header	Use for U10 or U12 SPI Flash programming
J63	U9/U11 or U13 SPI Flash Programming Selection	Removed	Eliminated in this revision
J64	U10 or U12 SPI Flash Programming Selection	Removed	Eliminated in this revision
J65	CEC173x AP0_RESET# connect to MEC1723 RESET_IN#	0 Ohm Short	R150 IN (Default): Connect OUT: Disconnect

3.3 Updating the External SPI Flash Firmware

The EV42J24A has four external NOR Flash SPI devices with a Quad SPI interface. The devices are arranged on two SPI channels each with two flash devices per channel.

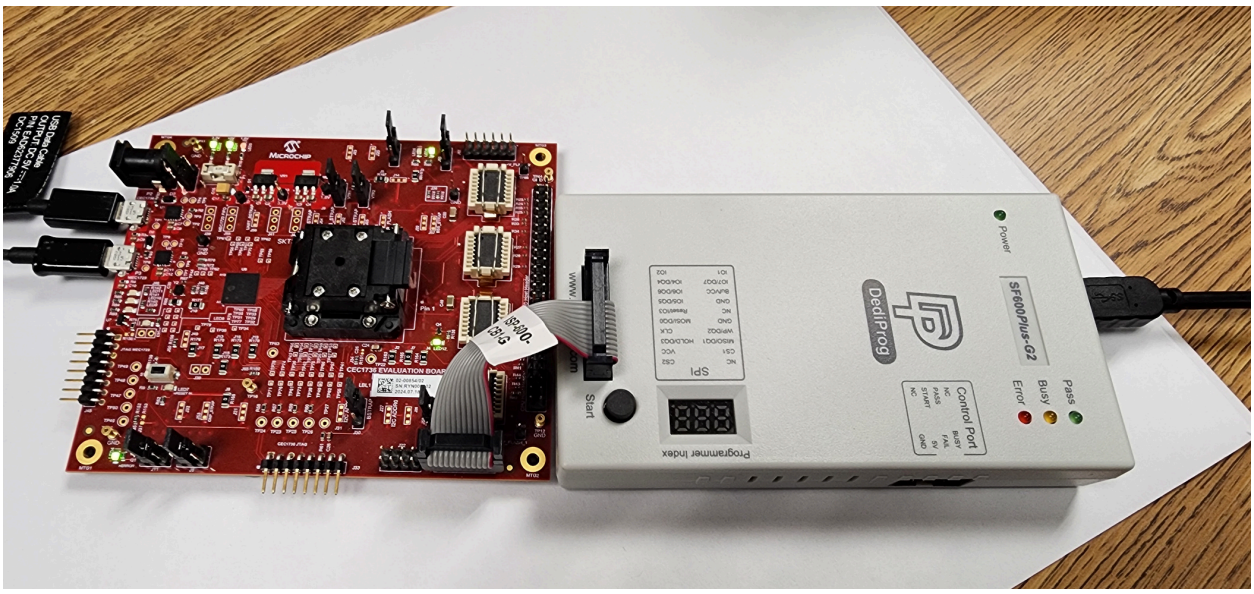
Customer applications may require significantly more memory and can make use of up to all four devices. The following sections describe how the SPI Flash device firmware can be updated.

3.3.1 Programming with the DediProg SF600

The recommended method of programming the SPI NOR Flash Chips on the EV42J24A is via the use of a DediProg SF600 level, in-system programmer. This programmer connects directly via ribbon cable to the 2x6 header on the EV42J24A. There are two programming headers on the board and each header has access to two SPI chips. The Dediprog software is then used to program the memory devices. The assertion of the correct chip select is controlled by the software, so there is no need to manually redirect the chip select line. Each header is connected to two SPI NOR flash chips and are independent of each other.

To program the SPI chips, first power on the development board by connecting USB cables to P2 and P3. Make sure the jumper at J1 is set to draw power from the USB cables and that the board is powered on. Connect the DediProg header to one of the programming headers. The photo below shows how the connection between the board and the programmer is made. Note the orientation of the pin 1 markers on the programming cable and the board connector.

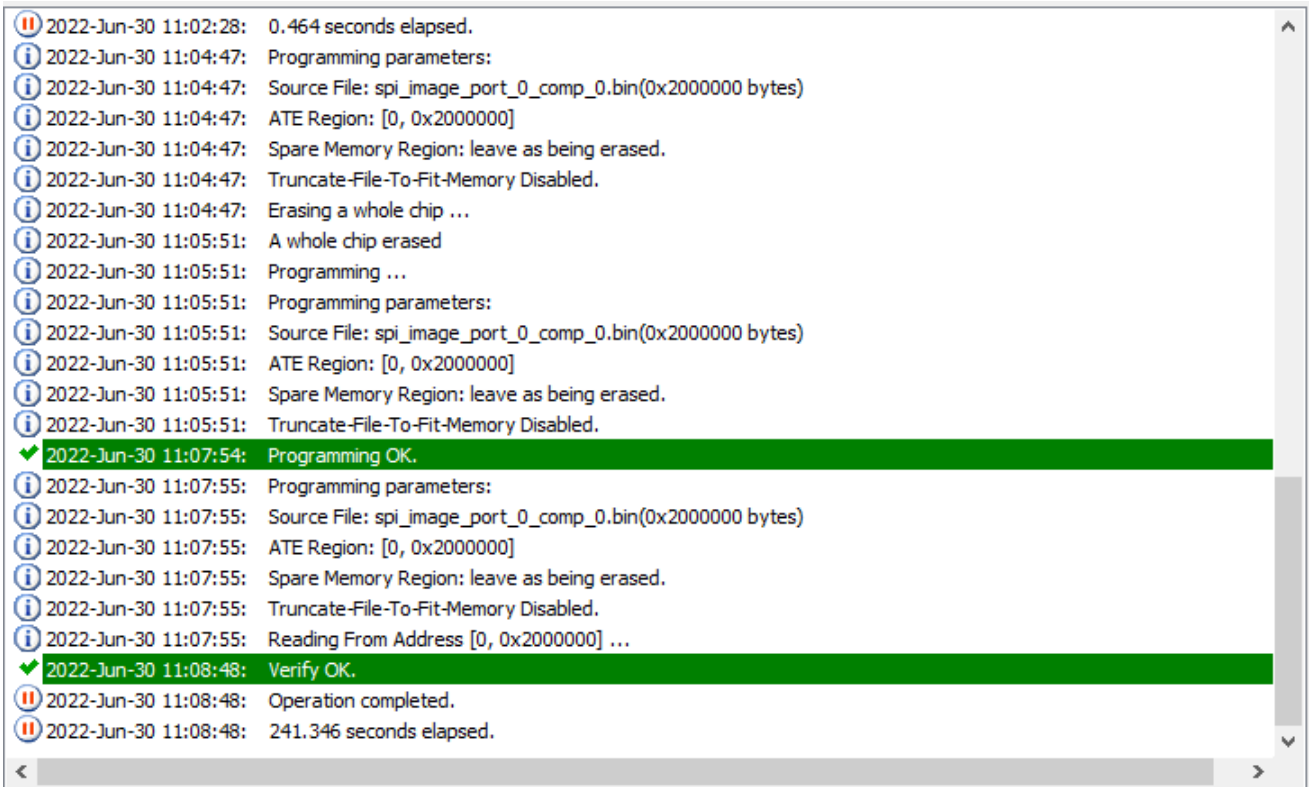
Figure 3-3. SF600 DediProg Connection



The SF600 programming software requires that the user selects the SF600 programmer, which SPI chip the user will be programming (this selects the correct chip select) and the actual manufacturer and device # of the user's memory device. In addition, the user must select the speed they wish

to program at and the mode of operation: single, dual or quad I/O SPI mode. Then, the user can select the actual firmware they intend to load, then click on the batch programming menu item to program the board. If successful, the user will see an output log similar to the following figure. Then, the above process can be repeated for the remaining devices.

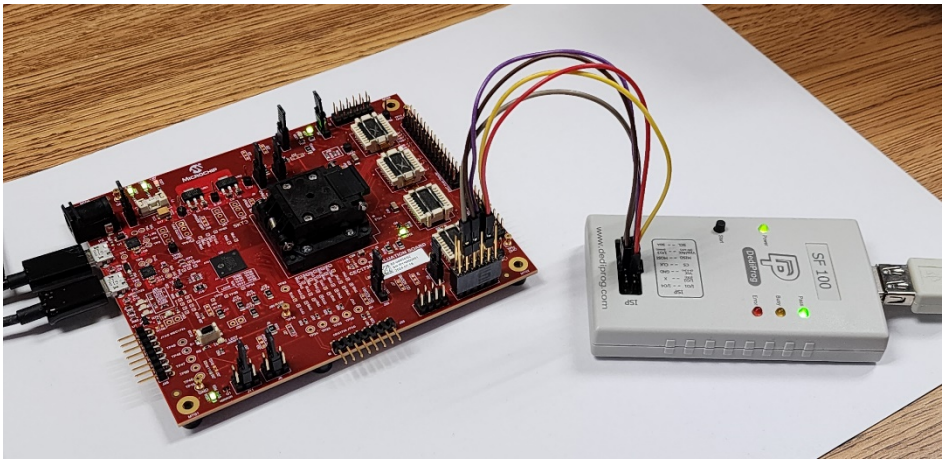
Figure 3-4. SF600 Output Log



3.3.2 Programming with the DediProg SF100

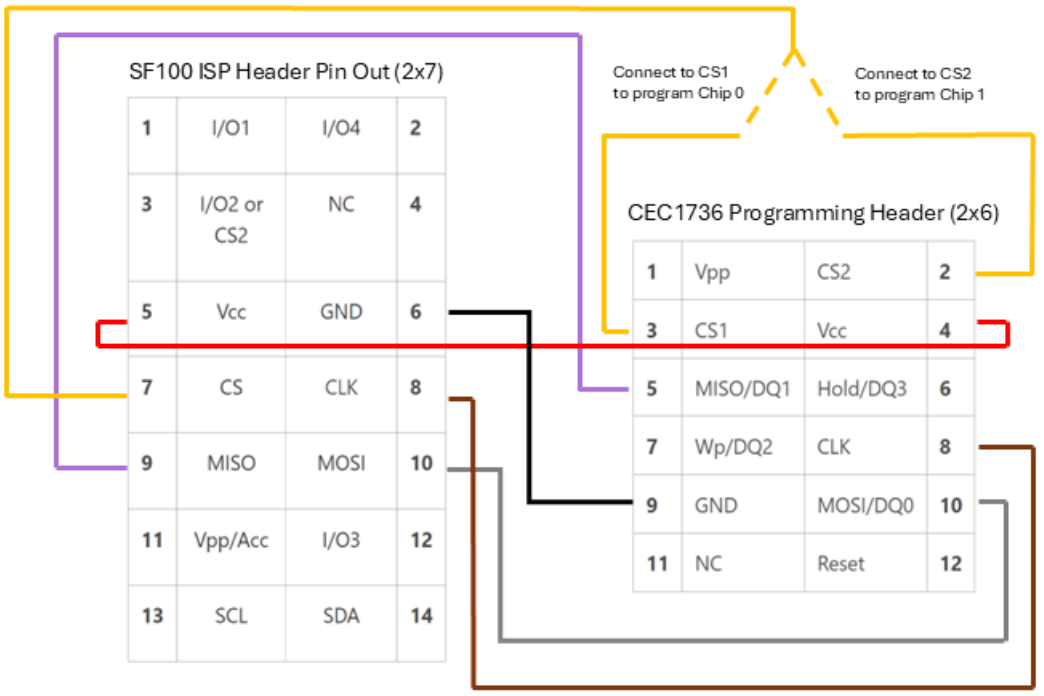
As described in Programming with the DediProg SF600, the recommended method of programming the SPI NOR Flash Chips on the EV42J24A is via the use of a Dediprog SF600 level, in-system programmer. However, many users have only an SF100 level programmer available and the previous board for the CEC173x was only supported by the SF100. The SF100 programmer can be enabled to work with the EV42J24A by use of a flywire connection as shown below. Jumper wires are easily attached between pins on the programmer and the EV42J24A.

Figure 3-5. Programming the EV42J24A using the SF100 programmer and Flywire connections



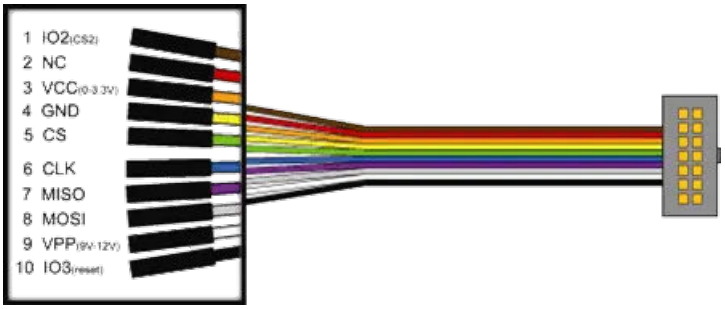
The details of this connection are shown in the figure below. The basic programming procedure remains the same, and the jumpers are recommended to be set to get power from the programmer. Unlike the SF600, the SF100 only supplies a single chip select. So, to program both SPI chips with the SF100, the user must manually move the chip select wire between chip select pins on the header as indicated below. To program all four devices, the SF100 must first be connected to header J61, which connects to SPI Channel 0, and the chip select signal must be sequentially connected between CS1 and CS2. Then, this procedure must be repeated by connecting the SF100 to header J62, which connects to SPI Channel 1 and the respective chip selects.

Figure 3-6. SF100 programmer to CEC1736 Programming Header Flywire connections



Alternatively, DediProg supplies the ISP-SP-CB Flywire cable. Using this cable and a 2x6 header socket, it is easy to make a simple programming cable.

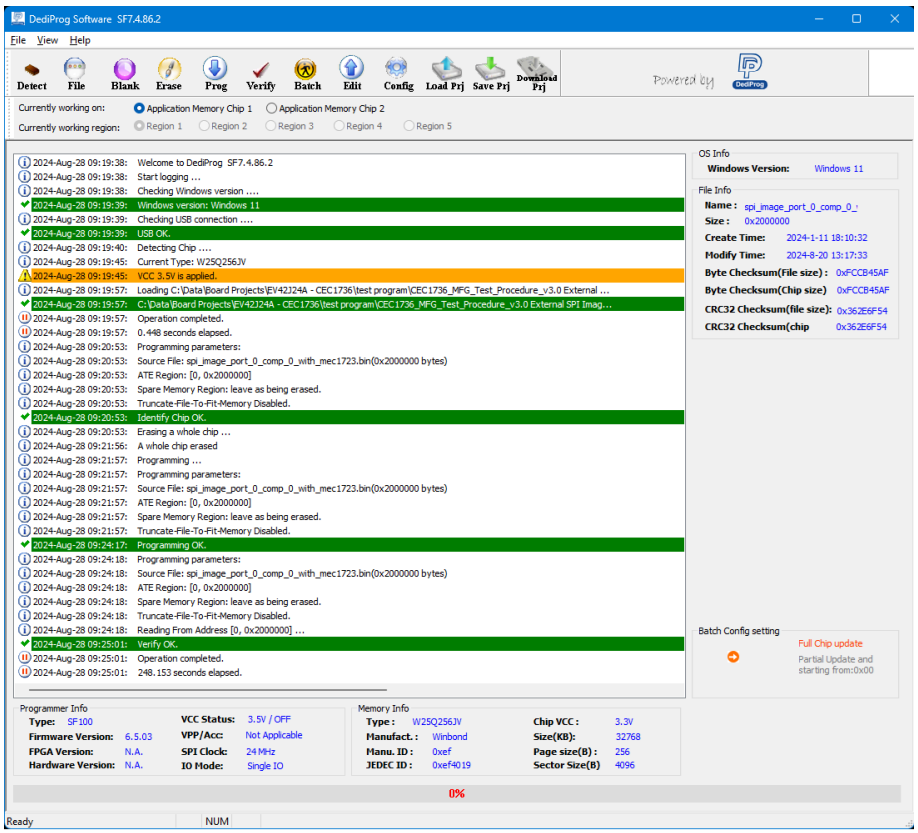
Figure 3-7. Dediprog ISP-SP-CB Flywire cable



The Dediprog ISP-SP-CB 10-pin Split Cable has a 14-pin header (only 10 of them are used for the ISP Split Cable), which can be connected to the SF100 ISP header directly. Each individual split cable has a different color and is labeled with the pin name so that they are easy to identify.

Shown below is a complete programming log using the SF100 programmer and the flywire setup. Note that this setup supports single I/O only but programs at 24 MHz. These settings come from the miscellaneous section under the config button.

Figure 3-8. Programming Log with SF100 Programmer



3.3.3 Swapping the SPI Flash Memory Devices

The EV42J24A development board comes with four 3.3V Quad SPI memory devices installed in the flash memory sockets. Some customer may wish to use specific SPI flash devices from other memory vendors or to install 1.8V devices. If a decision is made to not use the default memory devices, it is the responsibility of the customer to ensure compatibility.

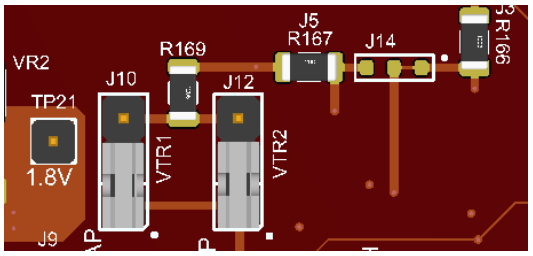
3.3V SPI Flash Devices

To upgrade to a different vendor but still maintain 3.3V operation, power down the board, remove the existing SPI Flash devices and replace them with the new memory devices. Follow the procedures defined in the previous sections for powering up the board and programming the flash devices with the DediProg programmer.

1.8V SPI Flash Devices

To configure the board to run with 1.8V SPI flash devices, some jumper positions must be modified. Prior to making these modifications, power down the board by removing all power to it. There are three jumpers that need to be modified to change the board configuration from the default mode of using 3.3V flash chips to using 1.8V chips. Jumpers J10 and J12 can be changed by moving the jumper cap. J14 is a trace-link jumper and will need to be cut.

Figure 3-9. Jumper Settings for 1.8V SPI



The CEC1736 supports two SPI banks of up to two chips each. Each bank can support either 1.8V or 3.3V SPI chips. J10 and J12 are used to select the voltage for each channel, with VTR1 supporting SPI channel 0 and VTR2 supporting SPI channel 1. The CEC1736 is a flow-through data path; therefore, the supporting application processor interface must also supply the correct voltage signals for the selected SPI. For the EV42J24A, the support application processor is the MEC1723, and its supply voltage is controlled by the trace link jumper J14. The default for this jumper is set to 3.3V. To convert to 1.8V, cut the trace link and install a 0603 zero Ohm resistor in position 2-3 at J14.

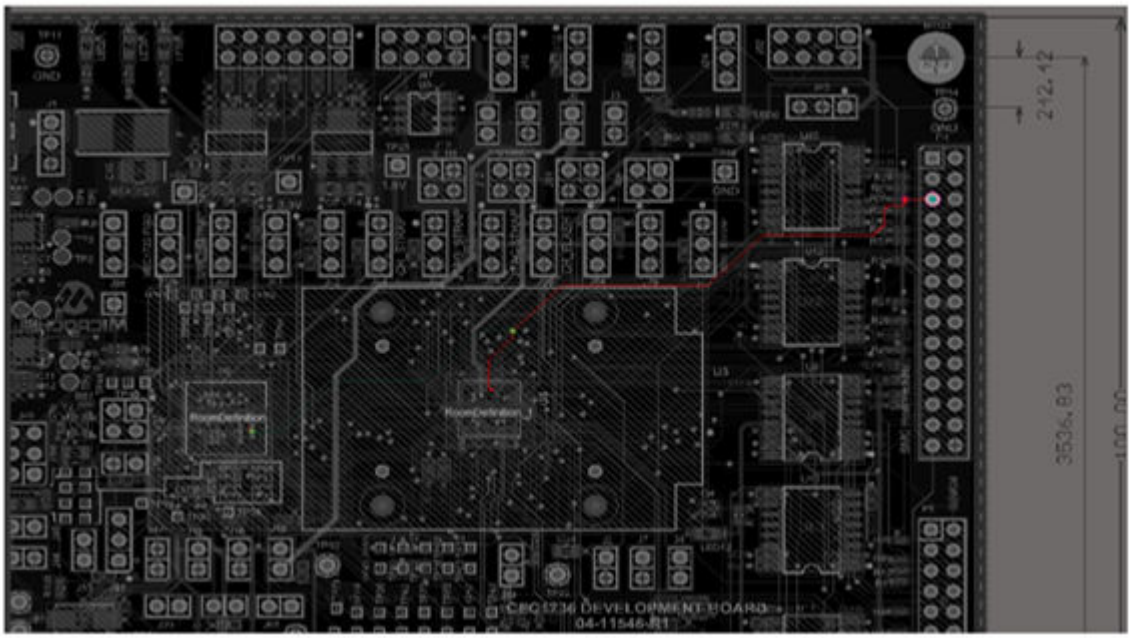
After modifying the desired jumper settings, follow the procedures defined in the previous sections for powering up the board and programming the flash devices with the DediProg programmer.

3.4 SPI0PER Filtering Capacitor

In some development use cases, it is necessary to interface to an external board. In that case, the performance of the interface can be improved by adding a small filtering capacitor to the SPI0PER chip select line. The figure below shows the empirical test results and highlights the SPI0PER trace to the BMC connector.

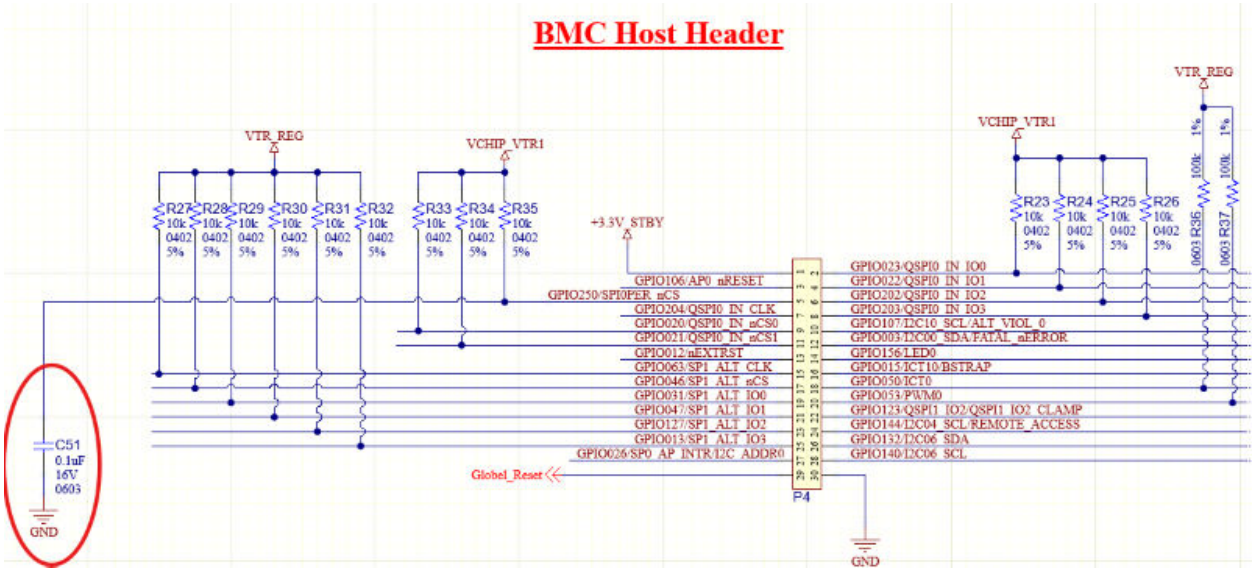
100 nF was added to ground on the CS line (GPIO250/SPI0PER_nCS) using a VIA pad, which is closer to the Glacier ASIC. With this, SPT works reliably up to 30 MHz and the drive strength was tested with max 16 mA.

Figure 3-10. Cap Test Results and Highlighted Trace



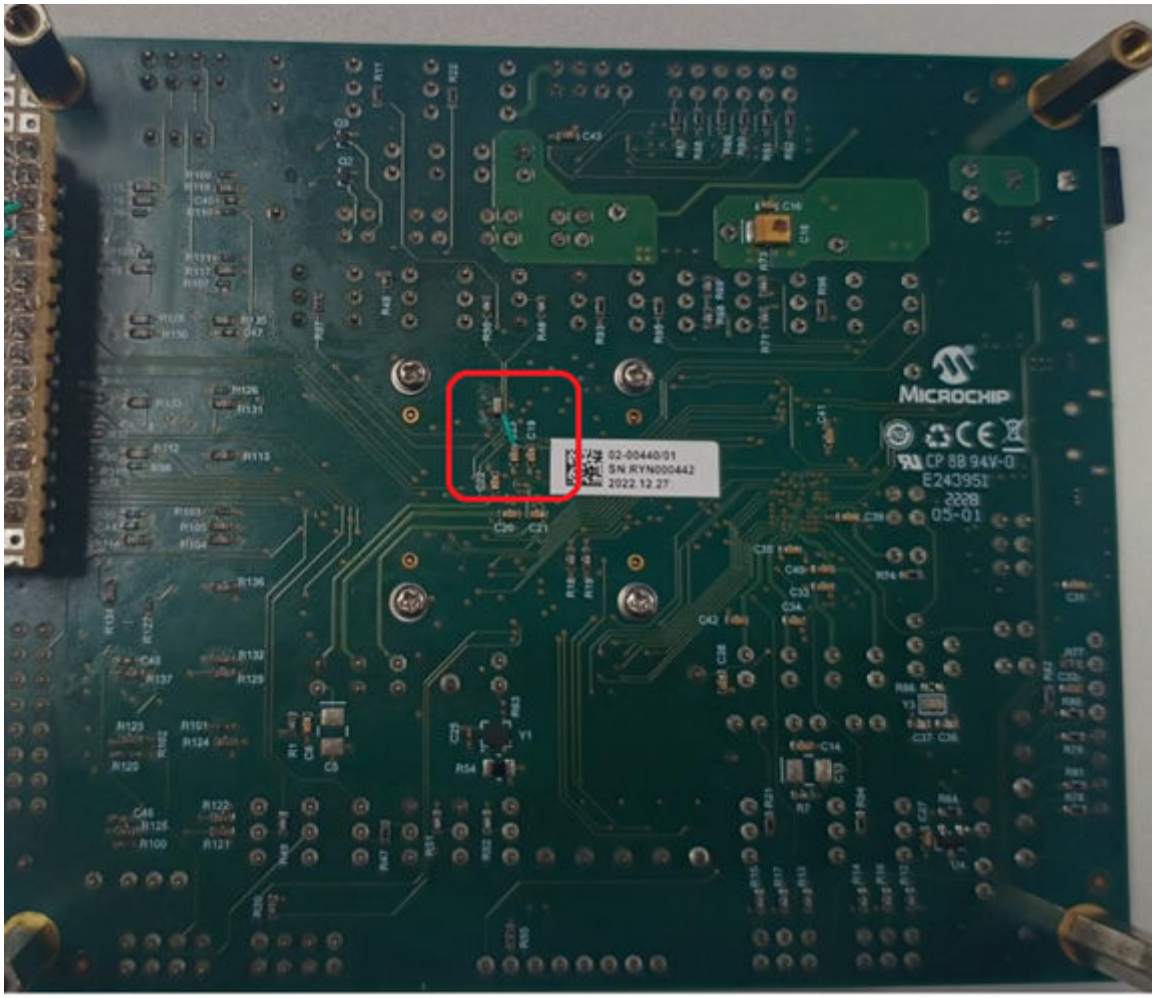
The placement of the cap in the schematics is shown below. Cap C51 was added between the GPIO250/SPI0PER_nCS line and GND.

Figure 3-11. Schematic Indicating the Installation of Cap



The best location for C51 is on the back side of the board, underneath the CEC, as shown below. This picture is of the back of the previous development board. The location on the latest evaluation board is similar.

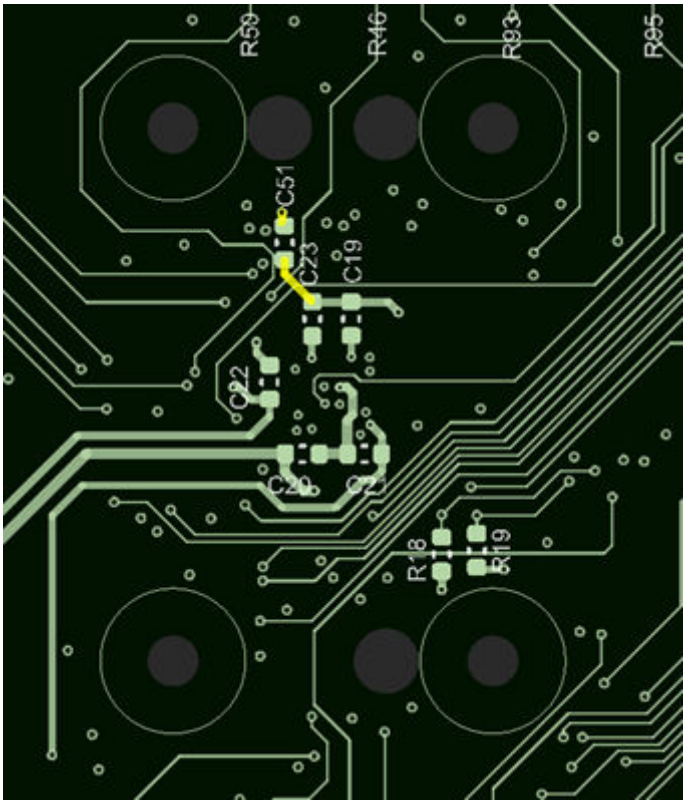
Figure 3-12. Relative Location of the Filtering Cap



The design tools show a detailed view of the required modification in the figure below. This is the database for the latest evaluation board. The yellow trace represents the addition of solder and/or wire needed to complete the modification.

Note: The lead of the resistor is soldered directly to a via pad. The other lead of the resistor is attached to ground via a short piece of wire.

Figure 3-13. Layout View of the Filtering Cap Modification



4. Development Kit Operation

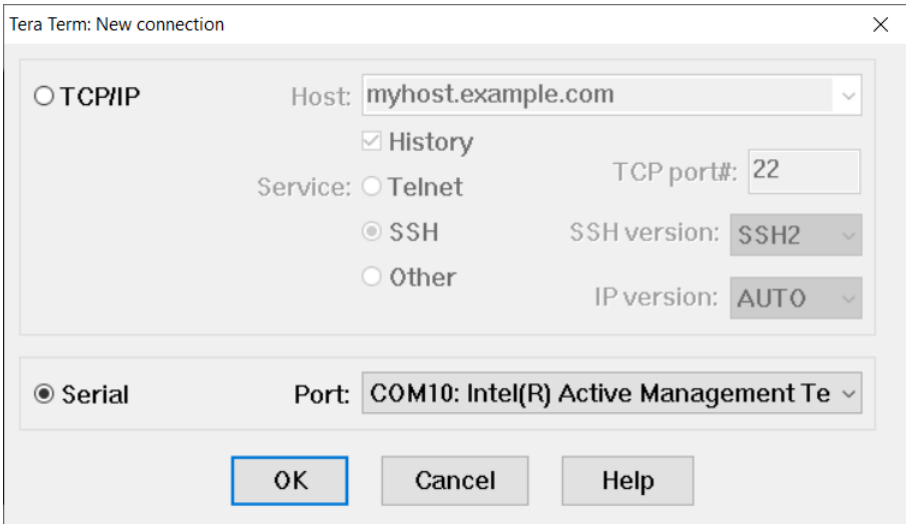
The following sections detail how to operate and use the development board with the various hardware and software tools. The sections cover how to power the development board, optional jumper settings, how to program the Quad SPI flash memories using an external programmer, a quick validation of the board and a high level overview of how to use the tools with Microchip's Trust Platform Design Suite (TPDS) tools.

4.1 Board Validation Check

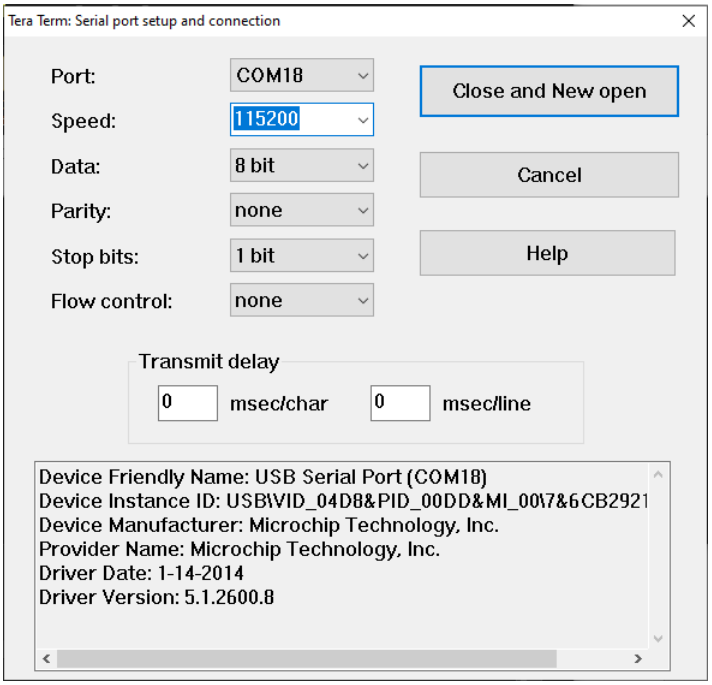
The EV42J24A evaluation kit has a CEC1736 device with pre-defined OTP settings and Soteria-G3 firmware SPI image. With this device, a simple validation check can be performed to verify that the board is properly working.

The following procedure can be used to verify the board is working correctly.

1. Verify the jumpers are all in the default positions as described in the section.
2. Make sure terminal window software is installed on the PC and can run multiple windows. Tera Term was used for this test.
3. Connect micro-USB cables to connectors P2 and P3 and to a PC. These provide power to the board and the ability to monitor the output of the CEC173x and the MEC1723.
4. Open the first "Tera Term" window, then set and select "Serial" new COM port (ex: COM10).

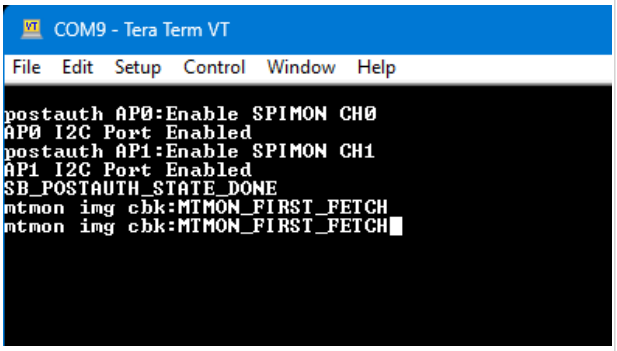
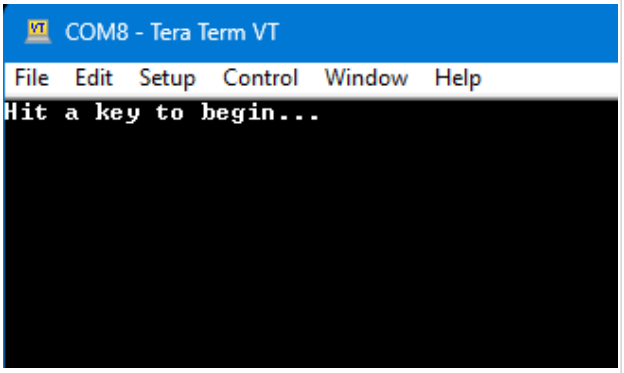


5. Go to "Setup" -> "Serial port", then select "115200-8-n-1-n".



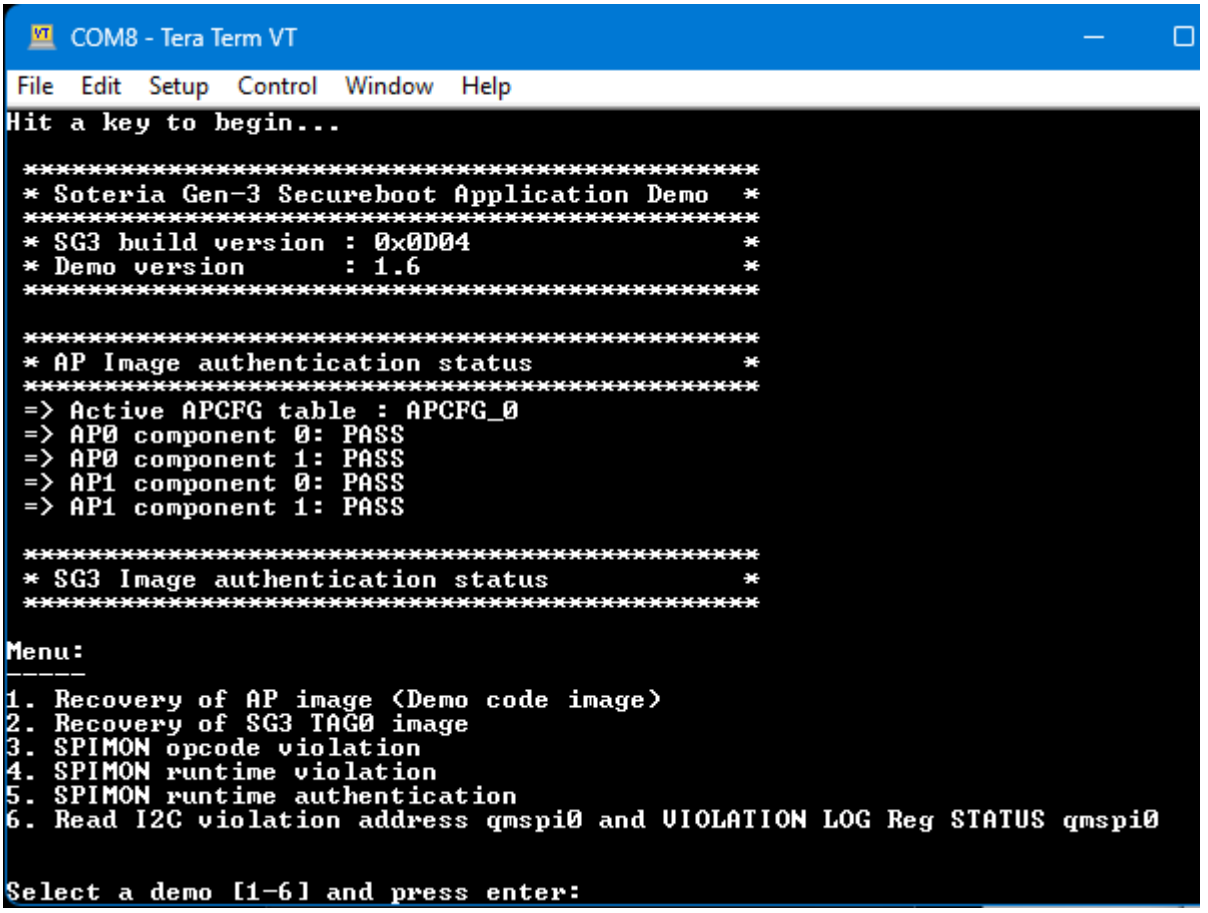
6. Repeat Steps 4 and 5 to set up the other Tera Term window. Both must have their serial port baud rate set to 115200.
7. Press the Reset button S1 on the EV42J24A development board. The board will follow an internally-programmed routine and produce the following Tera Term output logs.

Table 4-1. Board Validation Output Logs

CEC1736 Serial Log Output	MEC1723 Serial Log Output
	

8. Move the cursor to the MEC1723 Output Log and press any key. The following output will appear if everything is operating correctly.

Figure 4-1. Final MEC1723 Output Log



NOTICE The logs shown are an example only. The actual results may vary on the test environment and Soteria-G3 firmware release version being used. The above is expected as of the time of release of this development kit using Tera Term software and the CEC1736 device used for test. Devices programmed with TPDS will overwrite the default test image, and the log will not be the same.

Performing the validation check ensures board operation and that the devices and board will operate with the Trust Platform Design Suite (TPDS) tools.

4.2 Trust Platform Design Suite (TPDS)

The CEC173x-TFLX and CEC173x-TCSM devices are intended to be used with the Microchip Trust Platform Design Suite (TPDS), which is available for download on Windows, Linux and Mac from the Microchip website. The CEC173x-TFLX/TCSM Configurator on TPDS provides a streamlined graphical interface for enabling and configuring the various CEC173x trust versions. The configurator provides the ability to generate packages for both prototyping and production flows and allows the user to program your CEC173x-TFLX-PROTO and CEC173x-TCSM-PROTO parts for testing. The use of the TPDS tools requires Microchip MPLAB® X installation.

CEC173x configurator is a collection of tools and utilities to generate and provision the necessary cryptographic assets to evaluate CEC173x Trust Platform devices for desired use cases. It provides a visual view of different use cases and parameters to generate and provision OTP, keys, certificates chain and the combined SPI images for both the internal and external Flash devices.

The base TPDS tools can be downloaded for free from the Microchip Website. The CEC173x TPDS extensions require a myMicrochip account and an NDA. There will be separate extensions for the TFLX and TCSM versions of the devices. Both the base package and the appropriate extension package are needed in order to be able to operate the TPDS tools and generate a complete solution.

- Base **Trust Platform Design Suite**
- How to **request the CEC1736 TFLX or TCSM TPDS extension**

NOTICE For recommended Hardware and Software tools and additional technical collateral, see Recommended Tools and Accessories.

Using TPDS

The TPDS tools are constantly evolving to enhance the tools' capability and to provide additional use cases associated with each product. After downloading and installing the base TPDS tool, the CEC173x extension package and MPLAB® X IDE tool are now ready to be launched.

Select the CEC173x Trust product that you intend to develop on and place one of the sample devices in the SKT3 CEC1736 socket on the EV42J24A development board. It is recommended that the user starts with the CEC173x-TFLX devices to determine if this product will meet their needs. If more flexibility is needed, the user can move to the CEC173x-TCSM device.

After launching the TPDS tools, the user selects the CEC173x configurator and the correct CEC173x Trust Product. It is recommended that, prior to changing any specific options, the user walks through one or two of the demo projects to get familiar with the TPDS tools and the types of options that are available. Guidance and technical documentation built into the tool will assist in developing this familiarity and will position the user for developing their own application.

Attention: The TPDS tools will overwrite the default image programmed into the SPI Flash memories during manufacturing. The image for TFLX and TCSM devices will also differ from each other.

5. Document Revision History

Revision B (January 2025)

- Added SPI0PER Filtering Capacitor about the capacitor for off-board applications

Revision A (October 2024)

- Initial release of this document

Microchip Information

Trademarks

The “Microchip” name and logo, the “M” logo, and other names, logos, and brands are registered and unregistered trademarks of Microchip Technology Incorporated or its affiliates and/or subsidiaries in the United States and/or other countries (“Microchip Trademarks”). Information regarding Microchip Trademarks can be found at https://www.microchip.com/en-us/about/legal-information/microchip-trademarks.

ISBN: 979-8-3371-0459-1

Legal Notice

This publication and the information herein may be used only with Microchip products, including to design, test, and integrate Microchip products with your application. Use of this information in any other manner violates these terms. Information regarding device applications is provided only for your convenience and may be superseded by updates. It is your responsibility to ensure that your application meets with your specifications. Contact your local Microchip sales office for additional support or, obtain additional support at www.microchip.com/en-us/support/design-help/client-support-services.

THIS INFORMATION IS PROVIDED BY MICROCHIP “AS IS”. MICROCHIP MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WHETHER EXPRESS OR IMPLIED, WRITTEN OR ORAL, STATUTORY OR OTHERWISE, RELATED TO THE INFORMATION INCLUDING BUT NOT LIMITED TO ANY IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY, AND FITNESS FOR A PARTICULAR PURPOSE, OR WARRANTIES RELATED TO ITS CONDITION, QUALITY, OR PERFORMANCE.

IN NO EVENT WILL MICROCHIP BE LIABLE FOR ANY INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL, OR CONSEQUENTIAL LOSS, DAMAGE, COST, OR EXPENSE OF ANY KIND WHATSOEVER RELATED TO THE INFORMATION OR ITS USE, HOWEVER CAUSED, EVEN IF MICROCHIP HAS BEEN ADVISED OF THE POSSIBILITY OR THE DAMAGES ARE FORESEEABLE. TO THE FULLEST EXTENT ALLOWED BY LAW, MICROCHIP’S TOTAL LIABILITY ON ALL CLAIMS IN ANY WAY RELATED TO THE INFORMATION OR ITS USE WILL NOT EXCEED THE AMOUNT OF FEES, IF ANY, THAT YOU HAVE PAID DIRECTLY TO MICROCHIP FOR THE INFORMATION.

Use of Microchip devices in life support and/or safety applications is entirely at the buyer’s risk, and the buyer agrees to defend, indemnify and hold harmless Microchip from any and all damages, claims, suits, or expenses resulting from such use. No licenses are conveyed, implicitly or otherwise, under any Microchip intellectual property rights unless otherwise stated.

Microchip Devices Code Protection Feature

Note the following details of the code protection feature on Microchip products:

- Microchip products meet the specifications contained in their particular Microchip Data Sheet.
- Microchip believes that its family of products is secure when used in the intended manner, within operating specifications, and under normal conditions.
- Microchip values and aggressively protects its intellectual property rights. Attempts to breach the code protection features of Microchip products are strictly prohibited and may violate the Digital Millennium Copyright Act.
- Neither Microchip nor any other semiconductor manufacturer can guarantee the security of its code. Code protection does not mean that we are guaranteeing the product is “unbreakable”. Code protection is constantly evolving. Microchip is committed to continuously improving the code protection features of our products.