

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 device. 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.

NOTICE

This version of the user guide covers both the EV42J24A R2 and R3 revisions of the board. Notes throughout the user guide will indicate where there are functional differences. The modifications for R3 were made to improve the usability of the board and do not change its actual operation.

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, containing one of the CEC173x TrustFLEX™ or 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 cases 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 device to customize configuration for various security features in their specific designs.

Figure 1. CEC173x EV42J24A R2 Evaluation Board

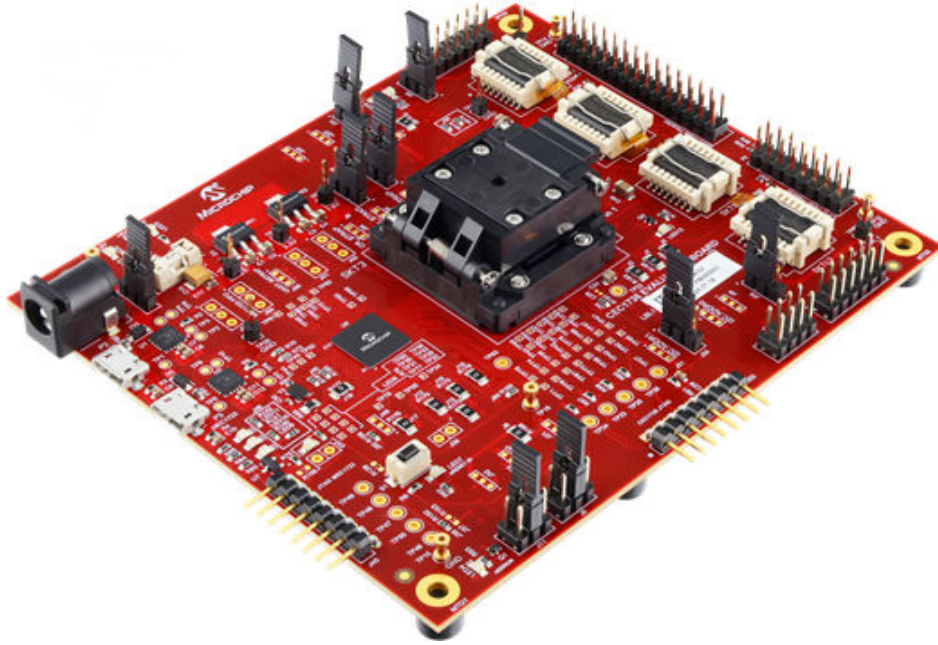


Figure 2. CEC173x EV42J24A R3 Evaluation Board

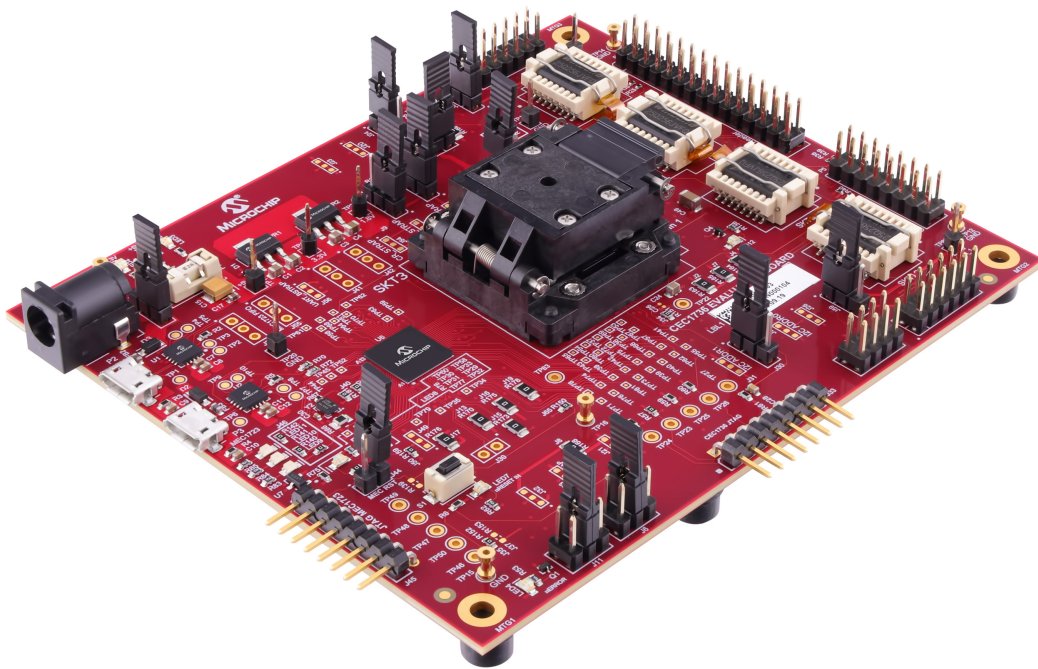


Table of Contents

Introduction.....	1
1. EV42J24A R3 Changes.....	4
2. Features.....	5
2.1. CEC173x Evaluation Board Block Diagram.....	5
2.2. Hardware Features.....	5
2.3. CEC173x Evaluation Board Layout.....	7
3. Recommended Tools and Accessories.....	8
4. Board Operation and Configuration.....	9
4.1. Powering the CEC173x Evaluation Board.....	9
4.2. Jumper Options.....	9
4.3. Updating the External SPI Flash Firmware.....	13
4.3.1. Programming with the DediProg SF600.....	13
4.3.2. Programming with the DediProg SF100.....	15
4.3.3. Swapping the SPI Flash Memory Devices.....	17
4.3.3.1. Revision R2 - 1.8V QSPI Flash Memory Modification.....	18
4.3.3.2. Revision R3 - 1.8V QSPI Flash Memory Modification.....	18
4.4. Filtering Capacitors.....	18
4.4.1. Revision R3 - Filtering Capacitors.....	19
4.4.2. Revision R2 - Filtering Capacitors.....	20
5. Development Kit Operation.....	22
5.1. Board Validation Check.....	22
5.2. Trust Platform Design Suite (TPDS).....	24
6. Document Revision History.....	26
Microchip Information.....	27
Trademarks.....	27
Legal Notice.....	27
Microchip Devices Code Protection Feature.....	27
Product Page Links.....	28

1. EV42J24A R3 Changes

The changes to the R3 version of the board are relatively minor and were made to improve the usability of the board. The functionality of the board has not changed. The contents of the kit have not changed.

Identifying the Kit Version

The easiest way to identify the kit is by looking at the first row of the label on the board. The format of the label is shown in the image below. The ASSY# will be consistent between the revisions and is equal to 02-00854. The REV will be 02 for the R2 revision of the board and 03 for the R3 revision.

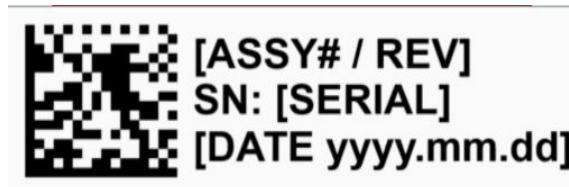


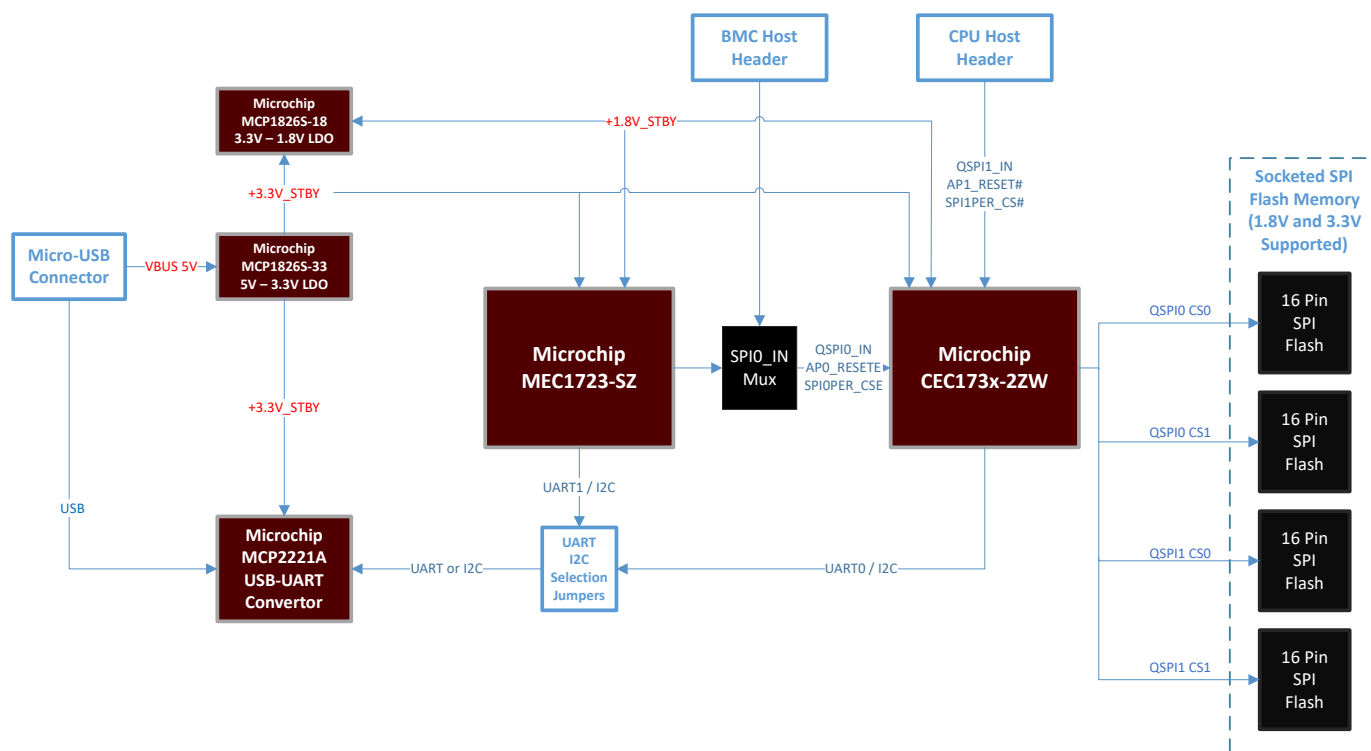
Table 1-1. Summary of R3 Changes

Change	Reason
1) Rotated DediProg Header J61 180 Degrees	Improved connectivity with DediProg Programmer
2) Changed J14 from Trace-Link jumper to regular jumper	Simplifies switching power from 3.3V to 1.8V for VTR2 and the MEC1723
3) Changed J47 to Bypass jumper from shorting resistor	Simplifies putting the CEC173x into and out of Bypass mode
4) Changed J44 shorting resistor to jumper	Simplifies holding the MEC1723 in Reset if desired
5) Added .1 uF capacitor C51 to GPIO250/SPI0PER_nCS line	Improves performance when connecting to an external FTDI device
6) Added .1 uF capacitor C52 to GPIO024/SPI1PER_nCS line	Improves performance when connecting to an external FTDI device

2. Features

2.1. CEC173x Evaluation Board Block Diagram

Figure 2-1. Block Diagram



2.2. Hardware Features

- Socket for CEC173x 84-Pin
- Four 16-Pin, 256 Mbit, 3.3V SPI Flashes in Socket for Normal Operation
- One USB-UART/I²C 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/I²C 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 Board Validation Checks. In Addition, the Kit Includes the Following CEC173x Sample Packs for Developing Applications. Each Sample Pack Contains 3 Devices.



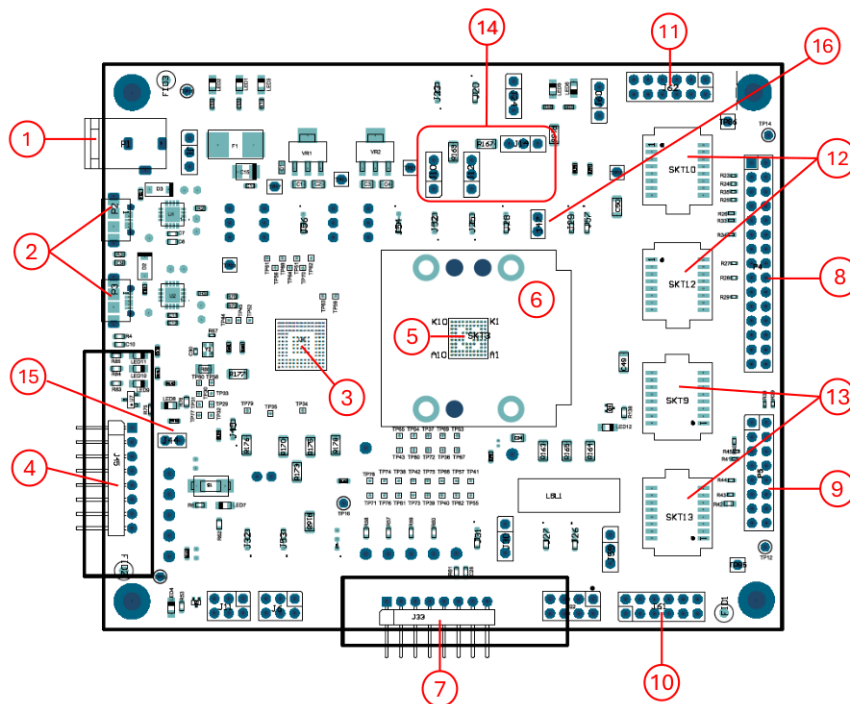
Important:

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

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

2.3. CEC173x Evaluation Board Layout

Figure 2-2. Board Layout Features



- | | |
|---|--|
| <ol style="list-style-type: none"> 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 I²C using the Microchip MCP2221A USB-to-UART/I²C 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) | <ol style="list-style-type: none"> 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 14. Power Jumpers (J10, J12, J14 - R3 Only) 15. MEC1723 Reset Jumper (J44) - R3 Only 16. CEC173x ByPass Jumper (J47) - R3 Only |
|---|--|

3. 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 for use with the EV42J24A evaluation board.

1. Microchip Trust Platform Design Suite (TPDS) (see [5.2. 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 and 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 the 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 under NDA and are available through [myMicrochip](#). For more information, go to [Secure Document Extranet via myMicrochip Portal](#).

- [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 documentation (schematics, Gerber files and BOM) and other technical collateral are available via myMicrochip and are under NDA.

Contact your Microchip representative with further questions.

4. Board Operation and Configuration

4.1. 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.

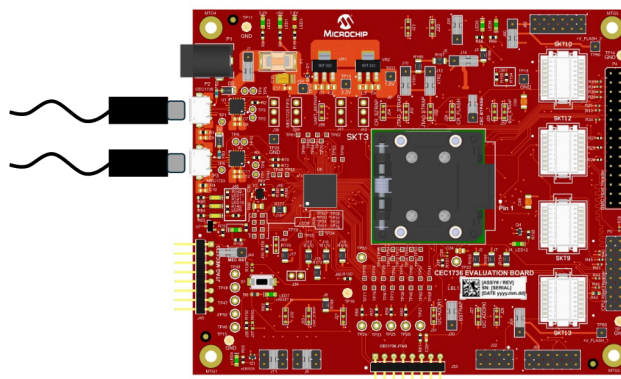
When the board is powered, LED1 (+5V), LED2 (+3.3V) and LED3 (+1.8V) turn on.

LED9, LED10 and LED11 may blink depending on the MEC1723 firmware application, indicating that the MEC1723 firmware is loaded and executing.

LED4, LED5, LED6 and LED12 may blink, indicating that the CEC1736 Soteria firmware is loaded and executing.

Power-up is shown below:

Figure 4-1. Powering The Board

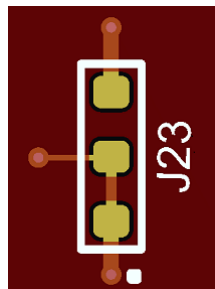


4.2. Jumper Options

The CEC173x evaluation board has a variety of configuration jumpers.

The jumpers and headers have a J reference designator. Several of the jumpers have been 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. For instance, to change the configuration of J23, cut the trace between pins 1 and 2, and install a zero Ohm 0603 surface-mount resistor between pads 2 and 3. In some cases, jumpers have been 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 [Table 4-1](#). In other cases, a standard jumper cap must be placed across jumper pins in the default position for default operation of the device.

Figure 4-2. Trace-Link Jumper



The following table of jumpers is based on the original EV19K07A evaluation board. Where possible, original jumper names have been retained for consistency. A jumper type column was added to make it easy to identify what type of jumper is used. The following types are 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 Configuration Options column indicates which 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 with the outside world.
5. Removed – A jumper that existed on the original EV19K07A board but was removed from the EV42J24A board.

➔ Important: The following table covers both revision 2 and revision 3 of the EV42J24A evaluation board. The jumper type and description columns provide data on both versions of the board when they differ.

Table 4-1. Jumper Options and Headers

Jumper	Function	Board Rev 2/3 Jumper Type	Configuration Options
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 ² C SCL selection to MCP2221A	Standard	1-2: I ² C10 3-4 (Default): I ² C06 5-6: I ² C00
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

Table 4-1. Jumper Options and Headers (continued)

Jumper	Function	Board Rev 2/3 Jumper Type	Configuration Options
J10	VTR1 power selection for CEC173x	Standard	1-2 (Default): Connect +3.3V power 3-4: Connect +1.8V power
J11	CEC173x I ² C SDA selection to MCP2221A	Standard	1-2: I ² C10 3-4 (Default): I ² C06 5-6: I ² C00
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	Rev 2: Trace-Link	Rev 2: 1-2 (Default): Connect +3.3V power 3-4: Connect +1.8V power
		Rev 3: Standard	Rev 3: 1-2 (Default): Connect +3.3V power 2-3: 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 ² C_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 ² C or UART Crisis Port
J31	CEC173x I ² C_ADDR1 Strap	Trace-Link	1-2: Pull-high to VTR_REG 2-3 (Default): Pull-down
J32	CEC173x RESET_IN# Delay Circuit Power Source	Trace-Link	1-2 (Default): Connect +3.3V power 2-3: Connect VTR_REG power

Table 4-1. Jumper Options and Headers (continued)

Jumper	Function	Board Rev 2/3 Jumper Type	Configuration Options
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	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 - R153	IN: Hold CEC1736 in Reset 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 ² C02 channel header	Standard	For debug purposes
J42	MEC1723 I ² C07 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	Rev 2: 0 Ohm Short - R156	Closed: MEC1723 in reset IN: Hold MEC1723 in reset OUT (Default): Normal operation
		Rev 3: Standard	Rev 3: Closed: MEC1723 held in reset Open: MEC1723 not in reset. (Default)
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	CEC173x Bypass Mode	Rev 2: Header	Rev 2: Eliminated in this revision
		Rev 3: 2-pin Header	Rev 3: Closed: ByPass Mode Open: (Default) Normal Operation
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

Table 4-1. Jumper Options and Headers (continued)

Jumper	Function	Board Rev 2/3 Jumper Type	Configuration Options
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
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 APO_RESET# connect to MEC1723 RESET_IN#	0 Ohm Short - R150	IN (Default): Connect OUT: Disconnect

4.3. Updating the External SPI Flash Firmware

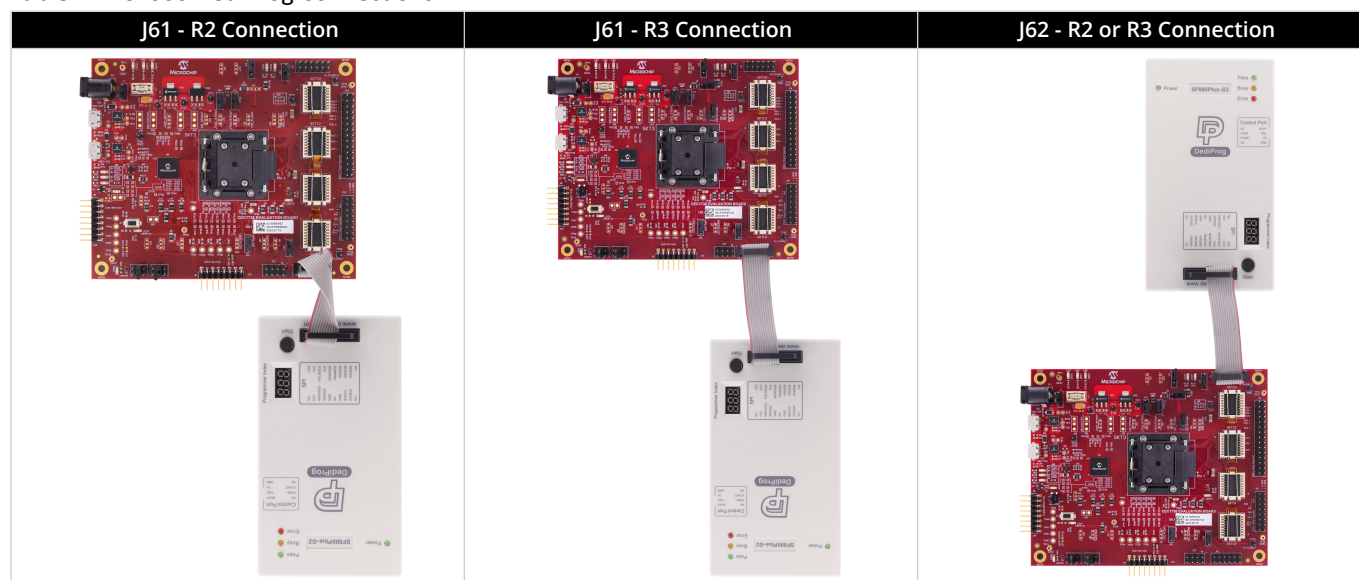
The EV42J24A has four external NOR Flash SPI devices with a Quad SPI interface. The devices are arranged on two SPI channels, with each channel supporting two Flash devices.

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

4.3.1. Programming with the DediProg SF600

The recommended method of programming the SPI NOR Flash chips on the EV42J24A is to use 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 photographs below illustrate the connection between the board and the programmer, which varies depending on the board revision and connector type. Pay close attention to the orientation of the pin 1 markers on both the programming cable and the board connector.

Table 4-2. SF600 DediProg Connections

Attention: Note that the orientation of the J61 DediProg connection differs between the R2 and R3 board revisions.

The SF600 programming software requires the user to select the SF600 programmer, specify which SPI chip to program (this selects the correct chip select), and choose the actual manufacturer and device number of the user's memory device. In addition, the user must select the desired programming speed and the mode of operation: single, dual or quad I/O SPI mode. After making these selections, the user can choose the firmware they intend to load and then click on the batch programming menu item to program the board. If successful, the user will see an output log similar to the figure below. The process can then be repeated for the remaining devices.

Figure 4-3. SF600 Output Log

```

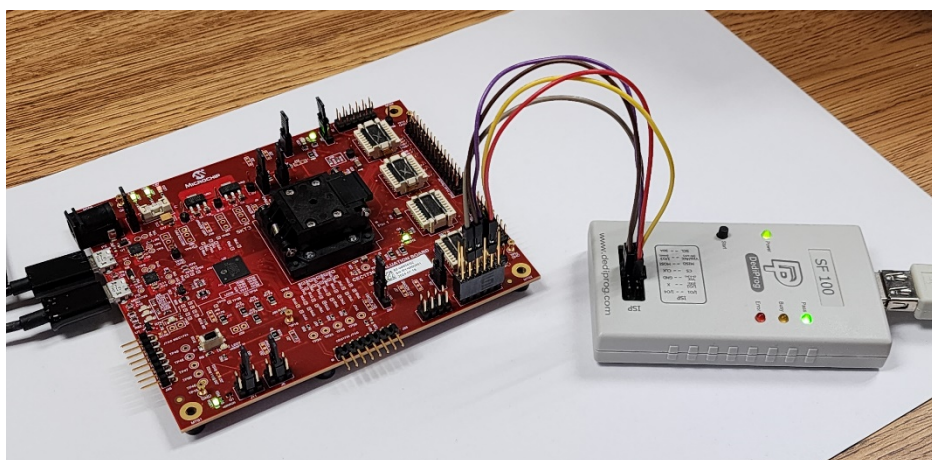
❗ 2022-Jun-30 11:02:28: 0.464 seconds elapsed.
❗ 2022-Jun-30 11:04:47: Programming parameters:
❗ 2022-Jun-30 11:04:47: Source File: spi_image_port_0_comp_0.bin(0x2000000 bytes)
❗ 2022-Jun-30 11:04:47: ATE Region: [0, 0x2000000]
❗ 2022-Jun-30 11:04:47: Spare Memory Region: leave as being erased.
❗ 2022-Jun-30 11:04:47: Truncate-File-To-Fit-Memory Disabled.
❗ 2022-Jun-30 11:04:47: Erasing a whole chip ...
❗ 2022-Jun-30 11:05:51: A whole chip erased
❗ 2022-Jun-30 11:05:51: Programming ...
❗ 2022-Jun-30 11:05:51: Programming parameters:
❗ 2022-Jun-30 11:05:51: Source File: spi_image_port_0_comp_0.bin(0x2000000 bytes)
❗ 2022-Jun-30 11:05:51: ATE Region: [0, 0x2000000]
❗ 2022-Jun-30 11:05:51: Spare Memory Region: leave as being erased.
❗ 2022-Jun-30 11:05:51: Truncate-File-To-Fit-Memory Disabled.
✔ 2022-Jun-30 11:07:54: Programming OK.
❗ 2022-Jun-30 11:07:55: Programming parameters:
❗ 2022-Jun-30 11:07:55: Source File: spi_image_port_0_comp_0.bin(0x2000000 bytes)
❗ 2022-Jun-30 11:07:55: ATE Region: [0, 0x2000000]
❗ 2022-Jun-30 11:07:55: Spare Memory Region: leave as being erased.
❗ 2022-Jun-30 11:07:55: Truncate-File-To-Fit-Memory Disabled.
❗ 2022-Jun-30 11:07:55: Reading From Address [0, 0x2000000] ...
✔ 2022-Jun-30 11:08:48: Verify OK.
❗ 2022-Jun-30 11:08:48: Operation completed.
❗ 2022-Jun-30 11:08:48: 241.346 seconds elapsed.

```

4.3.2. Programming with the DediProg SF100

As described in 4.3.1. [Programming with the DediProg SF600](#), the recommended method for 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 using a flywire connection, as shown below. Jumper wires can be easily attached between pins on the programmer and the EV42J24A.

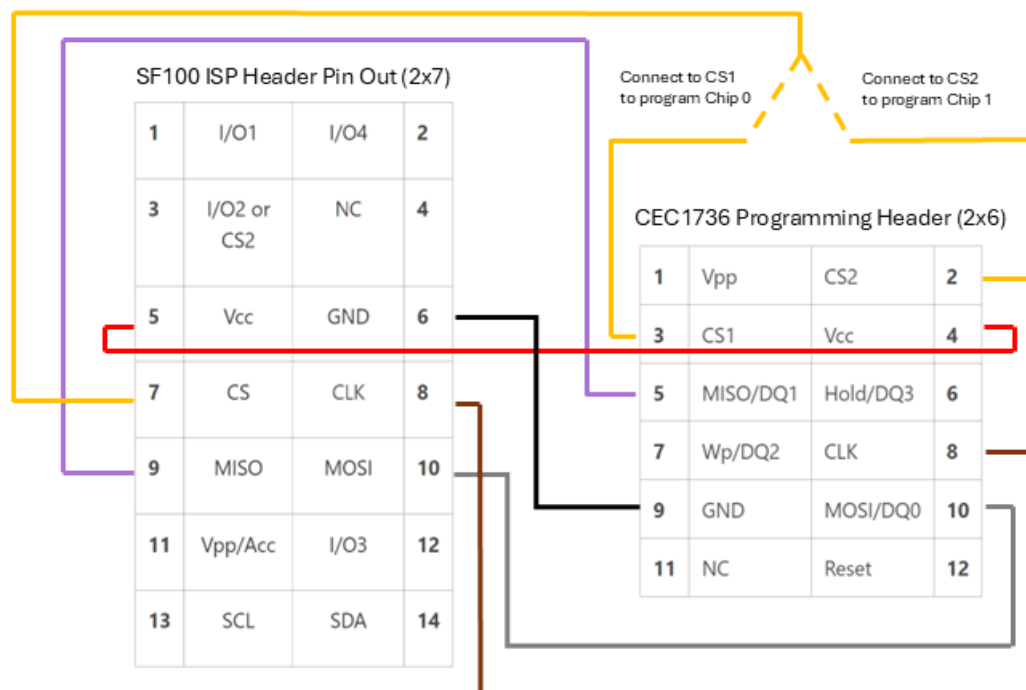
Figure 4-4. Programming the EV42J24A using the SF100 programmer and Flywire connections



The details of this connection are shown in the figure below. The basic programming procedure remains the same, and it is recommended to set the jumpers to obtain power from the programmer. Unlike the SF600, the SF100 supplies only a single chip select. Therefore, to program

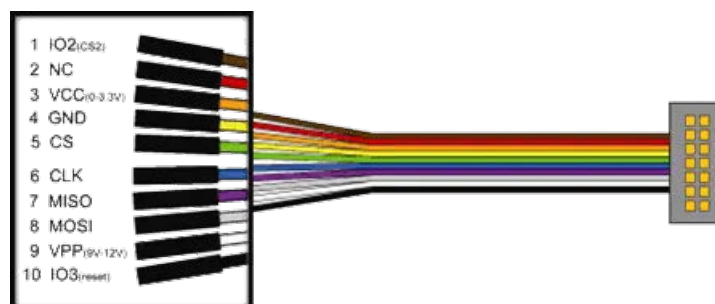
both SPI chips with the SF100, the user must manually move the chip select wire between chip select pins on the header, as indicated below. To program all four devices, the SF100 must first be connected to header J61, which connects to SPI Channel 0, and the chip select signal must be sequentially connected 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 4-5. 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.

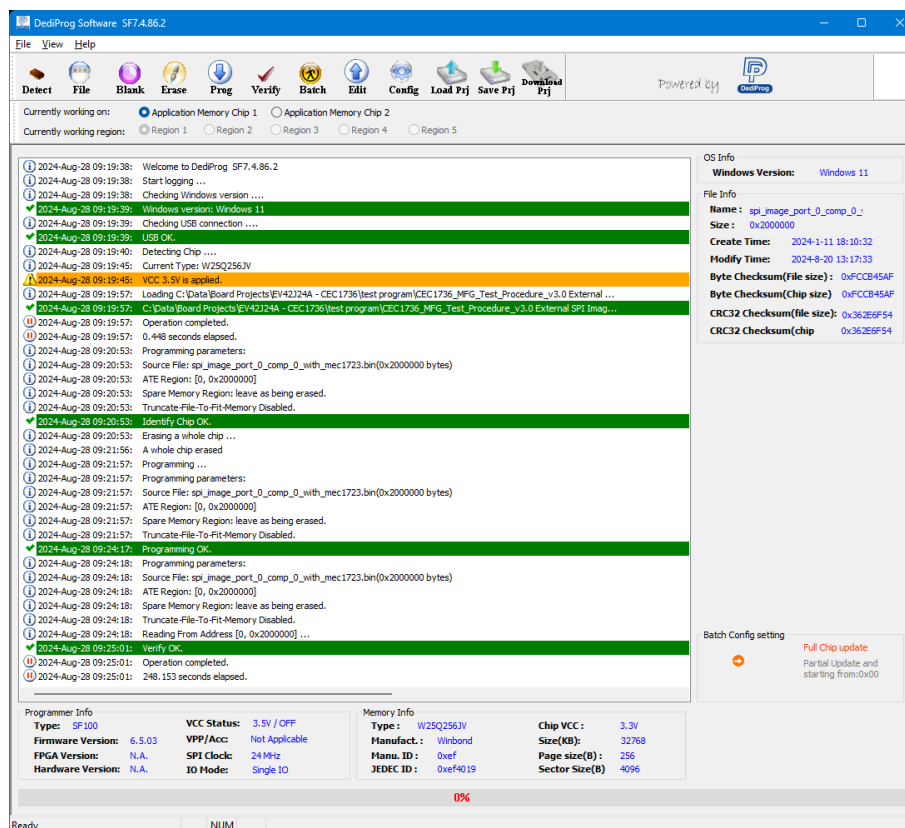
Figure 4-6. DediProg ISP-SP-CB Flywire cable



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

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 4-7. Programming Log with SF100 Programmer



4.3.3. 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 customers may wish to use specific SPI Flash devices from other memory vendors or to install 1.8V devices. If a decision is made not to 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 while maintaining 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

The CEC173x supports two SPI banks of up to two chips each. Each bank can support either 1.8V or 3.3V SPI chips. The voltage on each bank can be controlled separately. J10 is used to connect VTR1, which powers SPI Channel 0. J12 is used to connect VTR2, which powers 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, which is connected to VTR2. Its supply voltage is controlled by jumper J14. J12 and J14 must always be set to the same supply voltage level.

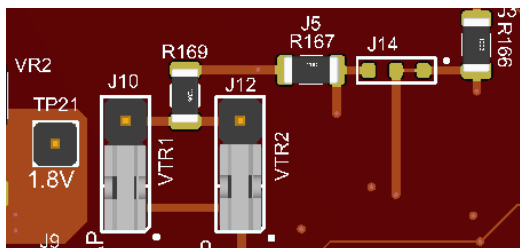
To configure the board to run with 1.8V QSPI Flash devices, some jumper positions must be modified. Prior to making these modifications, power down the board by removing all power to it. Then, follow the jumper modifications specified in the R2 or R3 revision subsections below.

After modifying the desired jumper settings, follow the procedures defined in [4.1. Powering the CEC173x Evaluation Board](#) and [4.3. Updating the External SPI Flash Firmware](#) for powering up the board and programming the Flash devices with the DediProg programmer.

4.3.3.1. Revision R2 - 1.8V QSPI Flash Memory Modification

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, while J14 is a trace-link jumper and will need to be cut.

Figure 4-8. R2 Revision - Jumpers for Settings 1.8V SPI Operation



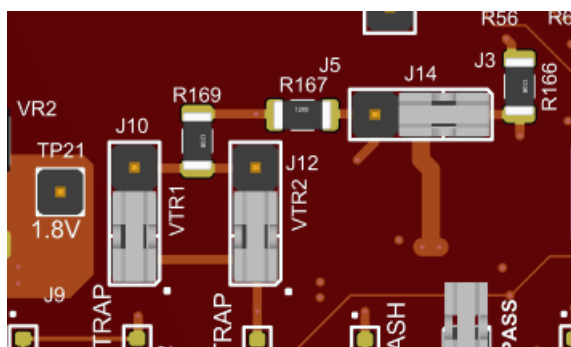
Note: Pin 1 is indicated by the dot near the connector

The diagram above shows the 3.3V default settings. To power VTR1 with 1.8V, move jumper J10 from the (1-2) position to the (2-3) position. Note that this power setting must match the BMC Host power setting. To Power VTR2 with 1.8V, move the jumper cap on J12 from the (1-2) position to the (2-3) position and modify the J14 trace-link jumper. To modify J14, cut the trace between positions (1-2) and place a 0603 zero-ohm resistor at position (2-3). Both of these must be set to the same voltage level.

4.3.3.2. Revision R3 - 1.8V QSPI Flash Memory Modification

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, J12 and J14 can be changed by moving the jumper cap. No trace-link jumper needs to be cut for the R3 board revision.

Figure 4-9. R3 Revision - Jumpers for Settings 1.8V SPI Operation



Note: Pin 1 is indicated by the dot near the connector

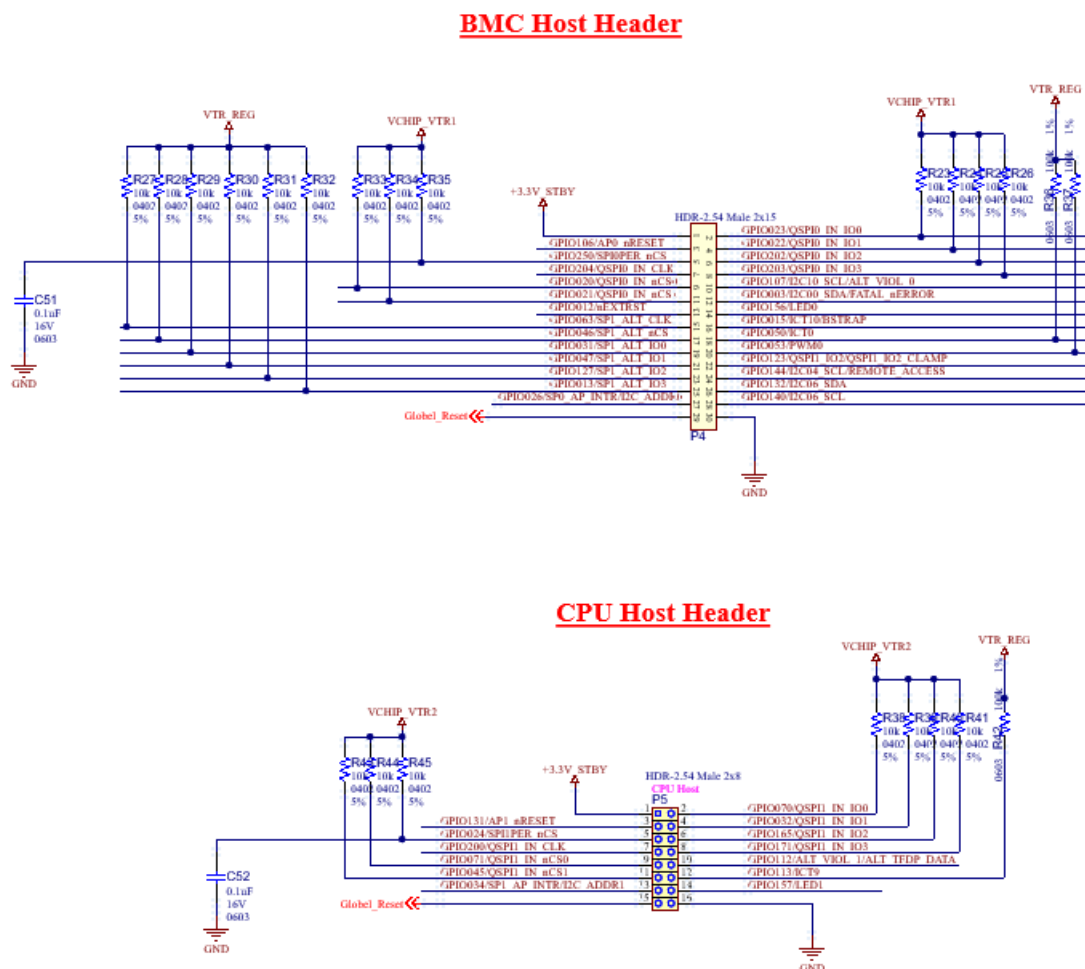
The diagram above shows the 3.3V default settings. To power VTR1 with 1.8V, move jumper J10 from the (1-2) position to the (2-3) position. Note that this power setting must match the BMC Host power setting. To Power VTR2 with 1.8V, move jumper J12 and Jumper J14 to the (2-3) position. Both J12 and J14 must be set to the same supply voltage level.

4.4. Filtering Capacitors

For some development use cases, it is necessary to interface to an external board such as the [UMFT4222EV-D](#) - FT4222H evaluation module, USB Hi-Speed to SPI/I2C Master/Slave. It has been found that the performance of the interface can be improved by adding a small filtering capacitor to the SPI0PER_nCS chip select line. For the R3 revision of the board, this capacitor has been integrated into the design. For the R2 revision, these need to be added. The schematic location of

the capacitors is identical between the R2 and R3 revisions of the board and can be seen in figure [Figure 4-10](#)

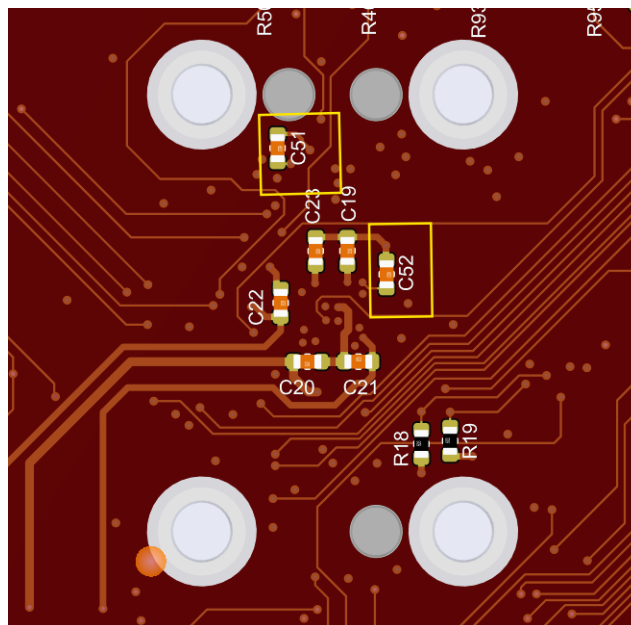
Figure 4-10. Schematic Filter Cap Locations



4.4.1. Revision R3 - Filtering Capacitors

Revision R3 of the EV42J24A evaluation board implements the required 100 nF filtering capacitors directly on the SPI0PER_nCS (C51) and SPIPER1_nCS (C52). No modifications to the revision 3 boards are required in order to get the boards to work reliably with an external board such as the [UMFT4222EV-D](#) - FT4222H evaluation module.

The schematic images are shown in [Figure 4-10](#). The layout image is shown in the figure below. The capacitors are located on the back side of the board, underneath the socket.

Figure 4-11. Layout Filter Cap Locations

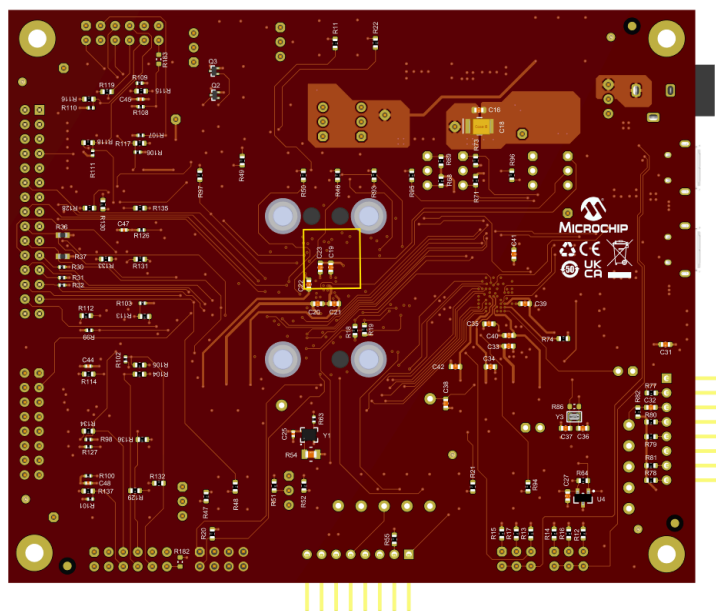
4.4.2. Revision R2 - Filtering Capacitors

For some development use cases, it is necessary to interface with an external board such as the [UMFT4222EV-D](#) - FT4222H evaluation module, USB Hi-Speed to SPI/I2C Master/Slave. It has been found that the performance of the interface can be improved by adding a small filtering capacitor to the SPI0PER_nCS chip select line. The schematic location of the capacitors is identical between the R2 and R3 revisions of the board and can be seen in figure [Figure 4-10](#)

A value of 100 nF was used in each location. Cap C51 was added between the GPIO250/SPI0PER_nCS line and GND. Cap C52 was added between the GPIO024/SPI1PER_nCS line and GND. With these additions, SPT works reliably up to 30 MHz, and the drive strength was tested with max 16 mA.

The best location for C51 and C52 is on the back side of the board, underneath the CEC, as shown below. This image is a 3D rendering of the R2 revision development board.

Figure 4-12. Relative Location of the C51 and C52 Filtering Cap



The following images show a detailed view of the required modifications in the figure below. These are based on the database for the R2 version of the evaluation board. The blue box and wire represent the location of the capacitor and the addition of solder and/or wire needed to complete the modifications.

Note: The signal pad of the capacitor is soldered directly to a via pad. The other capacitor pad is connected to ground via a short piece of wire.

Figure 4-13. SPI0PER_nCS (C51) Capacitor Placement

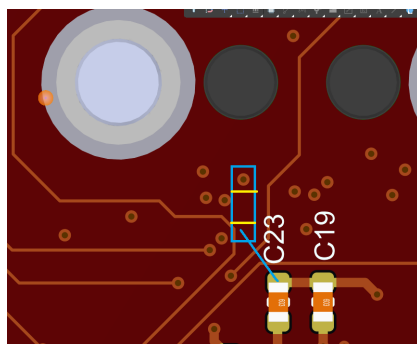
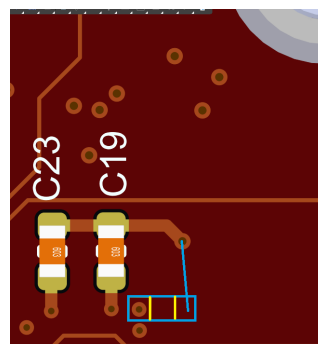


Figure 4-14. SPI1PER_nCS (C52) Capacitor Placement



5. Development Kit Operation

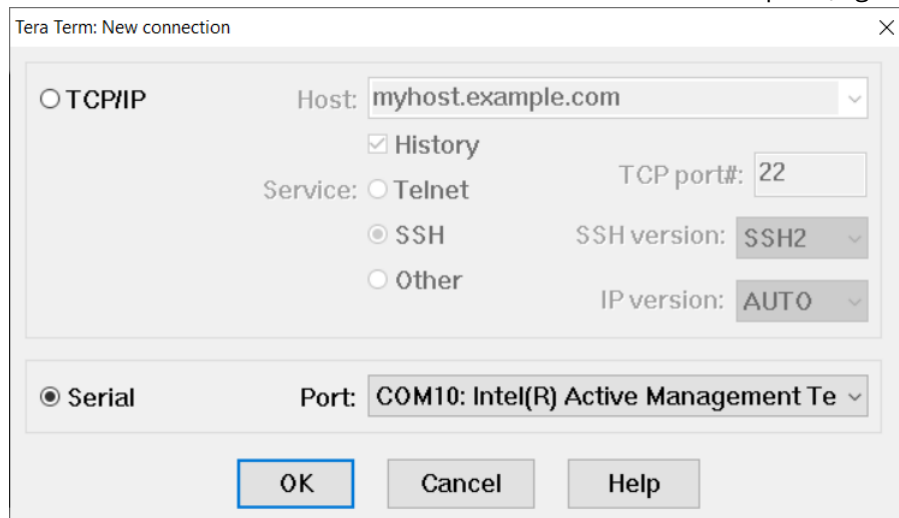
The following sections detail how to operate and use the development board with various hardware and software tools. The sections cover how to power the development board, optional jumper settings, how to program the Quad SPI Flash memories using an external programmer, a quick validation of the board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

5.1. Board Validation Check

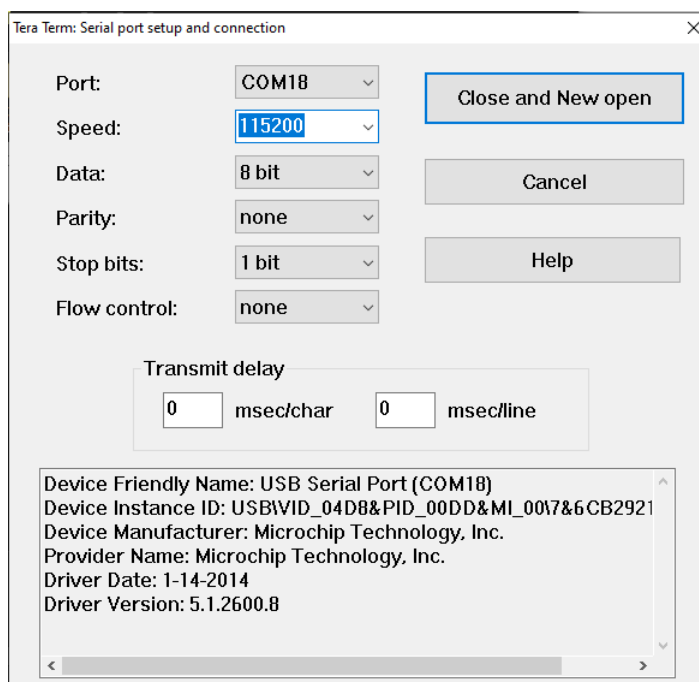
The EV42J24A evaluation kit has a CEC1736 device with predefined OTP settings and a Soteria-G3 firmware SPI image. With this device, a simple validation check can be performed to verify that the board is working properly.

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

1. Verify that all jumpers are in their default positions as described in the relevant 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 allow monitoring of the output from the CEC173x and the MEC1723.
4. Open the first "Tera Term" window, then set and select "Serial" new COM port (e.g., 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 5-1. 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 5-1. Final MEC1723 Output Log

```

COM8 - Tera Term VT
File Edit Setup Control Window Help
Hit a key to begin...

*****
* Soteria Gen-3 Secureboot Application Demo *
*****
* SG3 build version : 0x0D04 *
* Demo version : 1.6 *
*****

*****
* AP Image authentication status *
*****
=> Active APCFG table : APCFG_0
=> AP0 component 0: PASS
=> AP0 component 1: PASS
=> AP1 component 0: PASS
=> AP1 component 1: PASS

*****
* SG3 Image authentication status *
*****

Menu:
1. Recovery of AP image (Demo code image)
2. Recovery of SG3 TAG0 image
3. SPIMON opcode violation
4. SPIMON runtime violation
5. SPIMON runtime authentication
6. Read I2C violation address qmspi0 and VIOLATION LOG Reg STATUS qmspi0

Select a demo [1-6] and press enter:

```

NOTICE

The logs shown are examples only. The actual results may vary depending on the test environment and the 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 testing. 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 confirms that the devices and board will operate with the Trust Platform Design Suite (TPDS) tools.

5.2. 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 the 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 enables them to program their CEC173x-TFLX-PROTO and CEC173x-TCSM-PROTO parts for testing. Use of the TPDS tools requires Microchip MPLAB® X installation.

The CEC173x Configurator is a collection of tools and utilities used to generate and provision the necessary cryptographic assets to evaluate CEC173x Trust Platform devices for desired use cases. It provides a visual overview of different use cases and parameters to generate and provision OTP, keys, certificates chains 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 are 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 operate the TPDS tools and generate a complete solution.

- Base [Trust Platform Design Suite](#)
- How to request the CEC1736 TFLX or TCSM TPDS extensions:
 - Follow the directions in the [Secure Document Extranet via myMicrochip Portal](#)
 - Navigate to the [CEC173x-TFLX](#) or [CEC173x-TCSTM](#) and download the appropriate extension package

NOTICE

For recommended hardware and software tools and additional technical collateral, see [3. Recommended Tools and Accessories](#).

Using TPDS

The TPDS tools are constantly evolving to enhance their capabilities and to provide additional use cases associated with each product. After downloading and installing the base TPDS tool, the CEC173x extension package and the 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, select 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 become 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 images for TFLX and TCSM devices will also differ from each other.

6. Document Revision History

Revision C (November 2025)

- Updated to include information on R3 revision of the board
- [Introduction](#):
 - Added note indicating that this user guide covers both R2 and R3 revisions of the EV42J24A board
 - Added R3 board image
- [1. EV42J24A R3 Changes](#): Added this section to summarize the R3 revision changes
- [2.1. CEC173x Evaluation Board Block Diagram](#): Updated block diagram for improved readability
- [2.3. CEC173x Evaluation Board Layout](#): Modified with R3 image and added additional jumper locations
- [4.2. Jumper Options](#): Updated jumper options to indicate differences between R2 and R3 board revisions
- [4.3.1. Programming with the DediProg SF600](#): Updated DediProg connection images
- [4.3.3. Swapping the SPI Flash Memory Devices](#): Created individual sections for updating the R2 and R3 board revisions
- [4.4. Filtering Capacitors](#)
 - Created individual sections for R2 and R3 board revision operation
 - Modified section describing how to add the filtering capacitor to the SPI0PER_nCS
 - Added information on adding SPI1PER_nCS line for the R2 revision
- [5.2. Trust Platform Design Suite \(TPDS\)](#): Updated/expanded information on how to get access to TPDS extensions

Revision B (January 2025)

- Added [4.4. Filtering Capacitors](#) section 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: 979-8-3371-1949-6

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.

Product Page Links

[CEC1734](#), [CEC1734-TFLX](#), [CEC1736](#), [CEC1736-TFLX](#)