SimpleLink™ MSP432P4xx Security and Update Tool

The SimpleLink™ MSP432P4xx Security and Update Tool is a graphical user interface (GUI) and command line interface (CLI) tool that helps the user to configure the security features of the SimpleLink MSP432P4xx microcontrollers. The configuration is saved to a firmware image file that is downloaded to the device.

NOTE: The MSP432P4xx Security and Update Tool v1.0.0.0 supports only silicon revision C of the MSP432P401x MCUs. Because the XMS432P401x material has a different Flash Mailbox structure, the output of this tool cannot be used.

The software described in this user's guide is free and can be downloaded from MSP432P4xx Security and Update Tool.

Contents

List of Figures

List of Tables

Trademarks

SimpleLink, MSP432 are trademarks of Texas Instruments.
All other trademarks are the property of their respective owners.

1 Introduction

The MSP432P4xx Security and Update Tool is a graphical user interface (GUI) and command line interface (CLI) tool that helps the user to configure the security features of the MSP432P4xx microcontrollers. The configuration is saved to a firmware image file that is downloaded to the device (see Figure 1).

After the configuration is stored in the device and the device is rebooted, the boot code executes the commands and parameters.

The deployment of the configuration file to the device is not in the scope of this tool. Options to transport the configuration firmware image to the device include using a debugger through JTAG or serial wire debug (SWD), or through the bootloader (BSL).

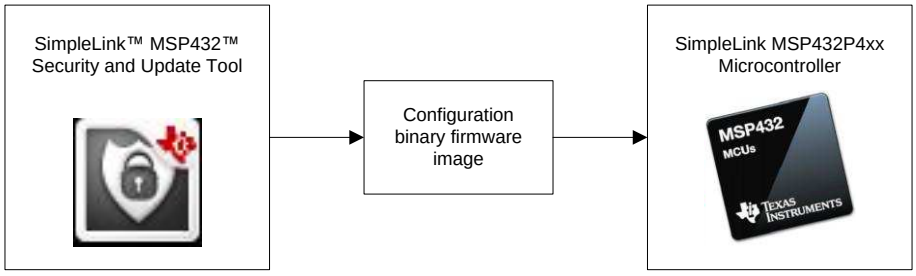

Figure 1. High-Level Security Tool Flow

This user's guide explains the details of using the MSP432P4xx Security and Update Tool GUI and some of necessary information of the security features. For the detailed explanation about the device security, see the *Device Security* section in the *System Controller (SYSCTL)* chapter of the *MSP432P4xx SimpleLink™ Microcontrollers Technical Reference Manual*. *MSP432 Security Overview* gives a general overview of the security features in MSP432P4xx MCUs and lists all the documents that are related to those security features. *Configuring Security and Bootloader (BSL) on MSP432P4xx Microcontrollers* gives the examples of using the Flash Mailbox configuration in IDEs during application development.

2 MSP432™ Security Features

The *Device Security* section in the *System Controller (SYSCTL)* chapter of the *MSP432P4xx SimpleLink™ Microcontrollers Technical Reference Manual* explains the security features that are provided in MSP432P4xx family of microcontrollers. These security features include:

- Factory reset
- Bootloader (BSL) configuration
- IP protected secure zone and update
- JTAG/SWD lock configuration and update
- Factory reset configuration

The security features are configured using a memory section called the Flash Mailbox. The Flash Mailbox is located in the information memory of the device, and starts from address 0x0020:0000 with a length of 0x290 (see the device-specific data sheet for details on the available memories). The device security is configured by populating the Flash Mailbox commands and their parameters.

After the configuration is set inside the Flash Mailbox, a reboot reset or power-on reset (POR) is applied to execute the configuration. The result of the execution, whether it is successful or not, is written in the acknowledge (ACK) field in the Flash Mailbox area by the boot code.

2.1 Flash Mailbox Structure

Table 1 lists the structure of the Flash Mailbox.

Table 1. MSP432P4xx Flash Mailbox Structure

Group	Offset	Description
Command and General Parameters	0x0	Command for the boot-override operation
JTAG/SWD Lock Configuration	0x10	Enable or disable lock, AES-CBC password for encrypted update
IP Protection – Zone 0	0x60	Address and AES-CBC password for IP Protection - Zone 0
IP Protection – Zone 1	0xC0	Address and AES-CBC password for IP Protection - Zone 1
IP Protection – Zone 2	0x120	Address and AES-CBC password for IP Protection - Zone 2
IP Protection – Zone 3	0x180	Address and AES-CBC password for IP Protection - Zone 3
BSL Configuration	0x1E0	BSL address, interface selection, and hardware invoke
JTAG/SWD Encryption Update	0x1F8	Address and length for encrypted update firmware
IPP Update - Zone 0	0x20C	Address and length for encrypted update firmware for IPP-0
IPP Update - Zone 1	0x21C	Address and length for encrypted update firmware for IPP-1
IPP Update - Zone 2	0x22C	Address and length for encrypted update firmware for IPP-2
IPP Update - Zone 3	0x23C	Address and length for encrypted update firmware for IPP-3

For details of the byte fields in the Flash Mailbox structure, see the *Device Security* section in the *System Controller (SYSCTL)* chapter of the *MSP432P4xx SimpleLink™ Microcontrollers Technical Reference Manual*.

Table 2 compares the naming conventions used in the MSP432P4xx Security and Update Tool and in the TRM.

Table 2. Naming Convention for the Security Features

MSP432P4xx Security and Update Tool	*MSP432P4xx SimpleLink™ Microcontrollers Technical Reference Manual* **(Group)**
JTAG/SWD Lock Configuration	JTAG_SWD_LOCK_PARAMS
IP Protected Secure Zone 0 Configuration	SEC_ZONE0_PARAMS
IP Protected Secure Zone 1 Configuration	SEC_ZONE1_PARAMS
IP Protected Secure Zone 2 Configuration	SEC_ZONE2_PARAMS
IP Protected Secure Zone 3 Configuration	SEC_ZONE3_PARAMS
Bootloader (BSL) Configuration	BSL_PARAMS
JTAG/SWD Lock Update	JTAG_SWD_LOCK_ENC_UPDATE
IP Protected Secure Zone 0 Update	SEC_ZONE0_UPDATE
IP Protected Secure Zone 1 Update	SEC_ZONE1_UPDATE
IP Protected Secure Zone 2 Update	SEC_ZONE2_UPDATE
IP Protected Secure Zone 3 Update	SEC_ZONE3_UPDATE
Factory Reset Parameters Configuration	FACTORY_RESET_PARAMS
Factory Reset Perform	FACTORY_RESET

Table 3 lists the configuration for the command field.

Table 3. Command Field

Command	Value
FACTORY_RESET	0x0001:0000
BSL_CONFIG	0x0002:0000
JTAG_SWD_LOCK_SECEN	0x0008:0000
SEC_ZONE0_EN	0x0010:0000
SEC_ZONE1_EN	0x0020:0000
SEC_ZONE2_EN	0x0040:0000
SEC_ZONE3_EN	0x0080:0000
SEC_ZONE0_UPDATE	0x0100:0000
SEC_ZONE1_UPDATE	0x0200:0000
SEC_ZONE2_UPDATE	0x0400:0000
SEC_ZONE3_UPDATE	0x0800:0000
JTAG_SWD_LOCK_ENC_UPDATE	0x1000:0000
FACTORY_RESET_PARAMS	0x2000:0000
No command are configured	0x0000:0000 or 0xFFFF:FFFF

In general, configuring a security feature means selecting whether the feature is enabled or disabled (see Figure 2). When a certain feature is enabled, the parameters for the feature are also set up. When a feature is disabled, the parameters are set to the default "Disable" state. When the feature is not configured at all, the parameters are set to the default state.

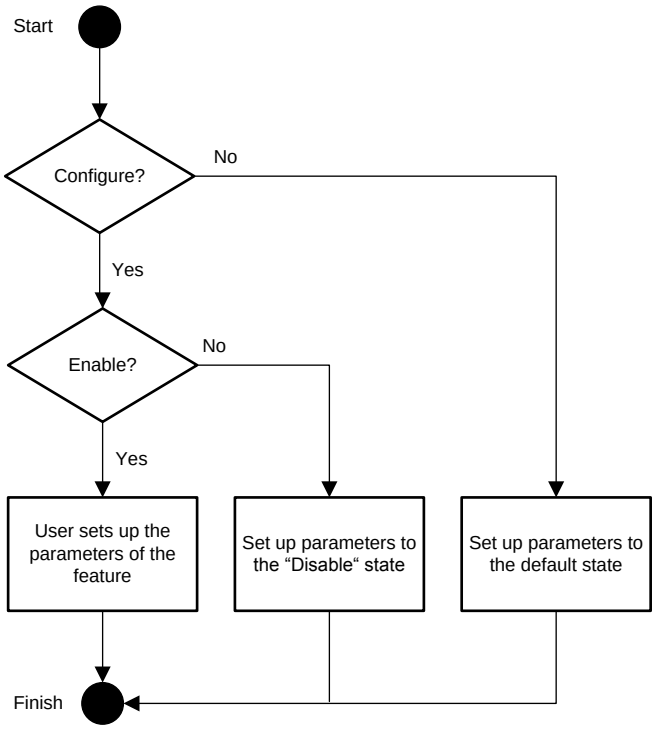

Figure 2. Configure the Security Features

2.2 Factory Reset

The configuration of Factory Reset involves these points (also see Figure 3):

The initial Factory Reset state in an empty device is:

- Factory Reset is enabled.
- Password enable for Factory Reset is disabled.

The configuration of Factory Reset involves:

- Configure the Factory Reset Parameters to enable or disable it.
- If Factory Reset is enabled, select the option to use password or not when executing the Factory Reset. When a password is enabled, specify four 32-bit passwords. When the password is not enabled, the password is set to the default of 0xFFFF:FFFF.
- If Factory Reset is disabled, it is permanently disabled and cannot be enabled or configured.

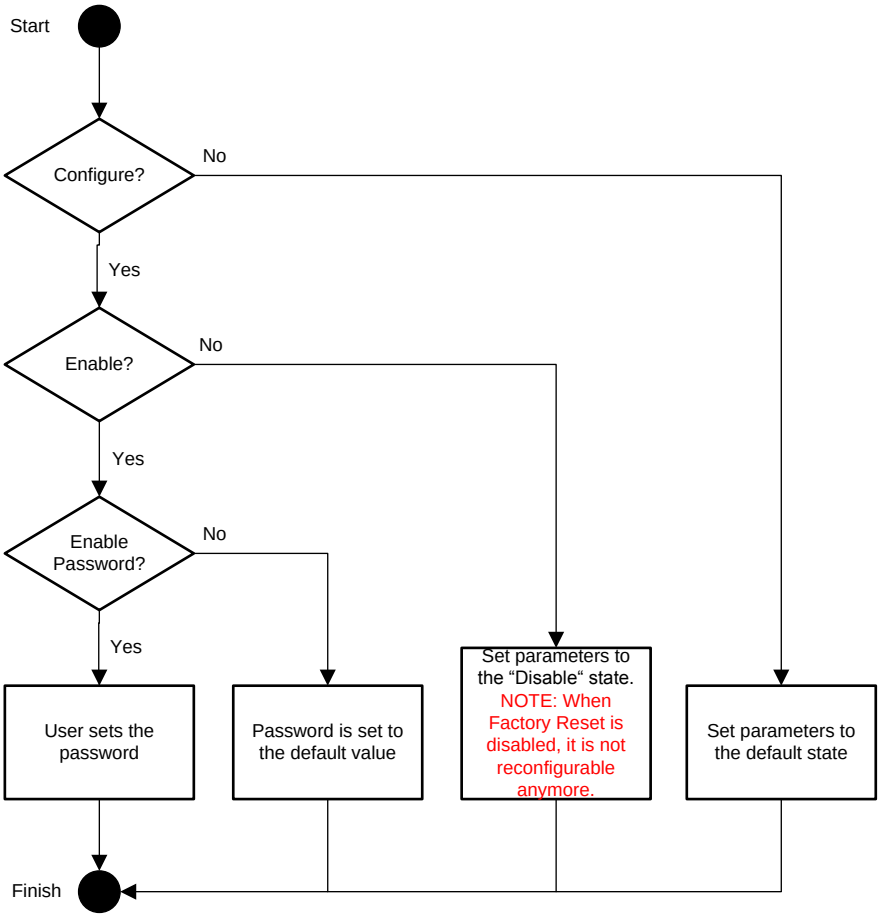

Figure 3. Flow Diagram for Factory Reset Configuration

Table 4 and Table 5 are examples of setting up Factory Reset parameters with and without a password, respectively.

Table 4. Example to Configure Factory Reset With Password

Address	Parameters	Value
0x0020:0000	MB_START	0x0115:ACF6
0x0020:0004	COMMAND	0x2000:0000
0x0020:0250	FACTORY_RESET_ENABLE	0xFFFF:FFFF
0x0020:0254	FACTORY_RESET_PWDEN	0x0000:0000
0x0020:0258	FACTORY_RESET_PWD[0]	0x1234:5678
0x0020:025C	FACTORY_RESET_PWD[1]	0x1234:5678
0x0020:0260	FACTORY_RESET_PWD[2]	0x1234:5678
0x0020:0264	FACTORY_RESET_PWD[3]	0x1234:5678
0x0020:028C	MB_END	0x0011:E11D

Table 5. Example to Configure Factory Reset Without Password

Address	Parameters	Value
0x0020:0000	MB_START	0x0115:ACF6
0x0020:0004	COMMAND	0x2000:0000
0x0020:0250	FACTORY_RESET_ENABLE	0xFFFF:FFFF
0x0020:0254	FACTORY_RESET_PWDEN	0xFFFF:FFFF
0x0020:0258	FACTORY_RESET_PWD[0]	0xFFFF:FFFF
0x0020:025C	FACTORY_RESET_PWD[1]	0xFFFF:FFFF
0x0020:0260	FACTORY_RESET_PWD[2]	0xFFFF:FFFF
0x0020:0264	FACTORY_RESET_PWD[3]	0xFFFF:FFFF
0x0020:028C	MB_END	0x0011:E11D

After the Factory Reset parameters are configured and executed by the boot code, a Factory Reset can be performed at any time. If the password-enable is applied, the password must be provided with the Factory Reset command, and the boot code verifies the supplied password against the password in the configuration (see Figure 4).

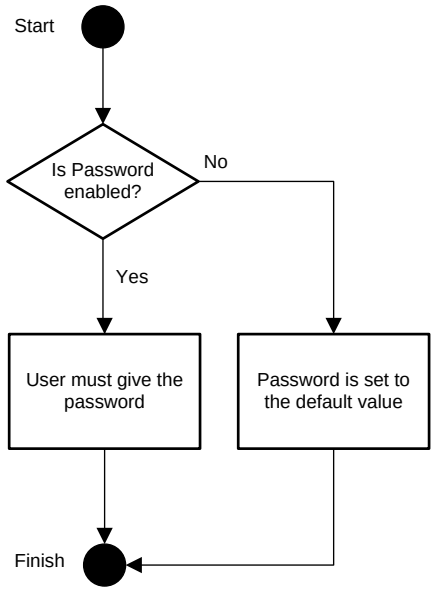

Figure 4. Flow Diagram to Perform Factory Reset

Table 6 and Table 7 are examples of performing a Factory Reset with and without a password, respectively.

Table 6. Perform Factory Reset With Password

Address	Parameters	Value
0x0020:0000	MB_START	0x0115:ACF6
0x0020:0004	COMMAND	0x0001:0000
0x0020:0270	FACTORY_RESET_PWD[0]	0x1234:5678
0x0020:0274	FACTORY_RESET_PWD[1]	0x1234:5678
0x0020:0278	FACTORY_RESET_PWD[2]	0x1234:5678
0x0020:027C	FACTORY_RESET_PWD[3]	0x1234:5678
0x0020:028C	MB_END	0x0011:E11D

Table 7. Perform Factory Reset Without Password

Address	Parameters	Value
0x0020:0000	MB_START	0x0115:ACF6
0x0020:0004	COMMAND	0x0001:0000
0x0020:0270	FACTORY_RESET_PWD[0]	0xFFFF:FFFF
0x0020:0274	FACTORY_RESET_PWD[1]	0xFFFF:FFFF
0x0020:0278	FACTORY_RESET_PWD[2]	0xFFFF:FFFF
0x0020:027C	FACTORY_RESET_PWD[3]	0xFFFF:FFFF
0x0020:028C	MB_END	0x0011:E11D

If the Factory Reset is successfully performed, the device is in this condition:

- Factory Reset is reconfigured into default state: it is enabled with password is disabled.
- All IP Protected Secure Zones are removed.
- Parameters in the Flash Mailbox are erased (applicable for silicon Rev C only).
- JTAG/SWD lock is disabled and its parameters are erased.
- BSL configuration is not erased if it has been set up before.

2.3 Bootloader (BSL) Configuration

The BSL is a programming method other than JTAG or SWD. The BSL is an application that is located in information memory flash to communicate with the host (which could be a PC or other programmer) to write and read the MCU memory. The BSL communicates through serial communication; in most cases, therefore, a USB-to-serial-communication converter is required as most host programmers use USB communication.

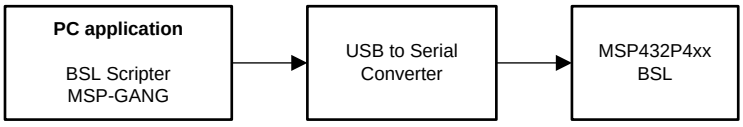

Figure 5. High-Level BSL Ecosystem

For the host to communicate with the BSL application, invocation must be successfully executed at device start-up. Invocation is the process in which that the host starts the communication with the BSL, and the BSL sends back a response to indicate that the BSL application is running.

For an empty or erased device, when the device starts, the boot code waits for the BSL firmware to be invoked. The BSL has a time-out when waiting for the invocation of approximately 10 seconds. If no invocation occurs, the device enters LPM4.5 mode.

For a programmed device, every time the device starts, it executes the main application. To run the BSL instead and perform a firmware update on a programmed device, BSL code can be called through software or hardware invocation. For details, see the *MSP432™ SimpleLink™ Microcontrollers Bootloader (BSL) User's Guide*. The security features of the MSP432 MCU provide the configuration for the BSL hardware invocation.

The BSL hardware invocation configuration involves:

- Communication protocol to use (automatic, UART, I^2C, or SPI)
- Which input pin is used to invoke the BSL (any one of P1.0 to P1.7, P2.0 to P2.7, or P3.0 to P3.7)
- What polarity (high or low) is used to invoke the BSL on the input pin

The BSL hardware invoke pin setup in the Flash Mailbox is located in 0x0020:01E8 with parameters listed in Table 8.

Table 8. BSL Hardware Invoke Pin Parameters

Bit	Function
31	Hardware invoke enable Disable: 1b Enable: 0b
30:26	Reserved Default: 0x1F
25:16	I^2C slave address Default: 0x48
15:13	Interface selection Automatic: 111b UART: 110b SPI: 101b I^2C: 100b Reserved: 000b to 011b
12	Polarity of invoke pin High: 1b Low: 0b
11:7	Reserved Default: 0x1F
6:4	Pin invoke number BIT0: 000b BIT1: 001b BIT2: 010b BIT3: 011b BIT4: 100b BIT5: 101b BIT6: 110b BIT7: 111b
3:0	Port invoke number PORT1: 0000b PORT2: 0001b PORT3: 0010b Reserved: 0011b to 1111b

To use hardware invocation, apply the specified polarity (high or low) on the specified pin when the device starts. For example, assume that P1.1 is chosen as the hardware invoke pin with high polarity. When the device starts or powers up, the boot code reads the polarity in P1.1. If the pin has high polarity, then the BSL code is executed. If the pin has low polarity, the main application code is executed.

Any pin of Port 1, Port 2, or Port 3 can be configured as the hardware invoke pin. Table 9 lists the dedicated pins for BSL communication for the UART, SPI, and I^2C protocols.

Table 9. Dedicated Pins for BSL Communication in MSP432P401x

No	Communication Protocol	Pin Functionality	Location
1	UART	BSLRXD	P1.2
		BSLTXD	P1.3
2	SPI	BSLSTE	P1.4
		BSLCLK	P1.5
		BSLSIMO	P1.6
		BSLSOMI	P1.7
3	I^2C	BSLSDA	P3.6
		BSLCLK	P3.7

The following is one example configuration to set up the BSL hardware invocation parameters:

- BSL hardware address: 0x0020:2000
- Communication protocol: UART
- Polarity invoke: High
- Port, Pin invoke: PORT1, PIN3

Table 10 lists the values that are written for this example configuration.

Table 10. Example to Configure BSL

Address	Parameter	Value
0x0020:0000	MB_START	0x0115:ACF6
0x0020:0004	COMMAND	0x0002:0000
0x0020:01E0	BSL_ENABLE	0x0000:0000
0x0020:01E4	BSL_START_ADDRESS	0x0020:2000
0x0020:01E8	BSL_HARDWARE_INVOKE_PARAMETERS	0x7C48:DFB0
0x0020:028C	MB_END	0x0011:E11D

BSL configuration is not erased by a factory reset, and it is reconfigurable to use another pin and polarity.

2.4 IP Protected Secure Zone

IP Protection Zone is a security feature that is available in MSP432P4xx MCUs to protect dedicated memory sections from debug intrusion and malicious code.

During a typical software development cycle, the application developer develops and debugs the complete application software. After the development cycle, the device debug path (JTAG or SWD) is blocked using a user-configurable setting of JTAG/SWD Lock parameters to prevent the unauthorized debug of the device.

Locking the JTAG/SWD debug access does not fully protect the software IP. Other pieces of code in the device may be able to read the software IP and hence the software IP is not secure. IP Protected Secure Zone marks certain memory areas that contain critical software IP as execute only. The MSP432P4xx devices support up to four different IP Protected Secure Zones. In an empty device, there is no secured memory section in the device, and all of the memory is accessible to be read and written.

The configuration of an IP Protection Zone is done by these steps:

1. Define the start address of memory section to secure. The address must be aligned with:
   - 4KB for MSP432P401x devices
   - 16KB for MSP432P4x1V, MSP432P4x1Y, and MSP432P4x11 devices

2. Define the length of the memory section to secure. The length must be a multiple of:
   - 4KB for MSP432P401x devices
   - 16KB for MSP432P4x1V, MSP432P4x1Y, and MSP432P4x11 devices
3. Provide the unencrypted password for authentication. This is the password that is required to update the firmware after the section is secured.
4. If the encryption mode is chosen, provide the AES-CBC initialization vector and the AES-CBC security keys. These passwords are used by the AES-CBC decryption process in the device.

Figure 6 shows the flow to configure the IP Protected Secure Zone.

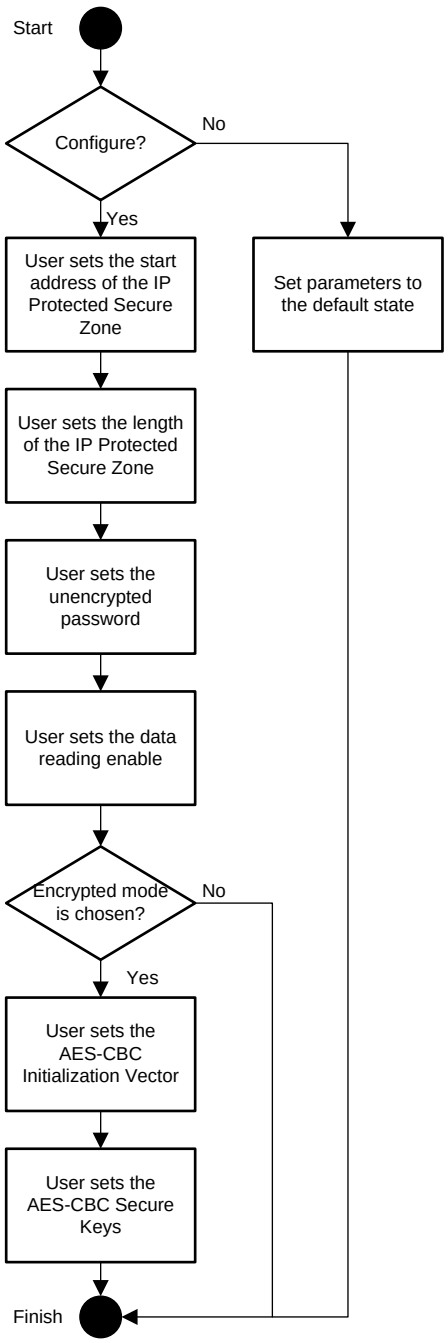

Figure 6. Flow Chart to Configure the Parameters in the IP Protected Secure Zone

As previously stated, the BSL uses memory addresses 0x0000:0000 to 0x0000:0100 as a password reference. Therefore, this range must not be secured if the BSL is used. If this address range is secured, the BSL cannot compare the password and cannot operate.

The secure memory section must be located in flash bank 0 to prevent DMA access into it. For detailed setup information about the IP Protected Secure Zone, see the *MSP432P4xx SimpleLink™ Microcontrollers Technical Reference Manual*.

Table 11 and Table 12 are examples of configuring the IP Protected Secure Zone with and without encrypted mode, respectively. Both examples set IP Protected Secure Zone 0 to start from address 0x0000:1000 with length of 0x0000:1000.

Table 11. Example to Configure IP Protection Secure Zone 0 With Unencrypted Mode

Address	Parameters	Value
0x0020:0000	MB_START	0x0115:ACF6
0x0020:0004	COMMAND	0x0002:0000
0x0020:0060	SEC_ZONE0_EN	0x0000:0000
0x0020:0064	SEC_ZONE0_START_ADDR	0x0000:1000
0x0020:0068	SEC_ZONE0_LENGTH	0x0000:1000
0x0020:006C to 0x0020:0078	SEC_ZONE0_AESINIT_VECT[0-3]	0xFFFF:FFFF
0x0020:007C to 0x0020:0098	SEC_ZONE0_SECKEYS[0-7]	0xFFFF:FFFF
0x0020:009C	SEC_ZONE0_UNENC_PWD[0]	0x1234:5678
0x0020:00A0	SEC_ZONE0_UNENC_PWD[1]	0x1234:5678
0x0020:00A4	SEC_ZONE0_UNENC_PWD[2]	0x1234:5678
0x0020:00A8	SEC_ZONE0_UNENC_PWD[3]	0x1234:5678
0x0020:00AC	SEC_ZONE0_ENCUPDATE_EN	0xFFFF:FFFF
0x0020:00B0	SEC_ZONE0_DATA_EN	0x0000:0000
0x0020:028C	MB_END	0x0011:E11D

Table 12. Example to Configure IP Protected Secure Zone 0 With Encrypted Mode

Address	Parameters	Value
0x0020:0000	MB_START	0x0115:ACF6
0x0020:0004	COMMAND	0x0002:0000
0x0020:0060	SEC_ZONE0_EN	0x0000:0000
0x0020:0064	SEC_ZONE0_START_ADDR	0x0000:1000
0x0020:0068	SEC_ZONE0_LENGTH	0x0000:1000
0x0020:006C	SEC_ZONE0_AESINIT_VECT[0]	0x0000:1111
0x0020:0070	SEC_ZONE0_AESINIT_VECT[1]	0x2222:3333
0x0020:0074	SEC_ZONE0_AESINIT_VECT[2]	0x4444:5555
0x0020:0078	SEC_ZONE0_AESINIT_VECT[3]	0x6666:7777
0x0020:007C	SEC_ZONE0_SECKEYS[0]	0x0011:2233
0x0020:0080	SEC_ZONE0_SECKEYS[1]	0x4455:6677
0x0020:0084	SEC_ZONE0_SECKEYS[2]	0x8899:AABB
0x0020:0088	SEC_ZONE0_SECKEYS[3]	0xCCDD:EEFF
0x0020:008C	SEC_ZONE0_SECKEYS[4]	0x0011:2233
0x0020:0090	SEC_ZONE0_SECKEYS[5]	0x4455:6677
0x0020:0094	SEC_ZONE0_SECKEYS[6]	0x8899:AABB
0x0020:0098	SEC_ZONE0_SECKEYS[7]	0xCCDD:EEFF
0x0020:009C	SEC_ZONE0_UNENC_PWD[0]	0x1234:5678
0x0020:00A0	SEC_ZONE0_UNENC_PWD[1]	0x1234:5678
0x0020:00A4	SEC_ZONE0_UNENC_PWD[2]	0x1234:5678
0x0020:00A8	SEC_ZONE0_UNENC_PWD[3]	0x1234:5678

Table 12. Example to Configure IP Protected Secure Zone 0 With Encrypted Mode (continued)

Address	Parameters	Value
0x0020:00AC	SEC_ZONE0_ENCUPDATE_EN	0xFFFF:FFFF
0x0020:00B0	SEC_ZONE0_DATA_EN	0x0000:0000
0x0020:028C	MB_END	0x0011:E11D

Figure 7 shows the process that protects the secure zone. The user provides the initial firmware image along with the firmware image of the Flash Mailbox configuration, and downloads them to the flash memory. Based on the previous example, the IP Protected Secure Zone is located in the 0x0000:1000 with length of 0x0000:1000. When the reboot reset or POR is applied, the boot code reads the parameters in the Flash Mailbox, and protects the IP Protected Secure Zone (shown by the black marked area). The commands and parameters in the Flash Mailbox itself are erased.

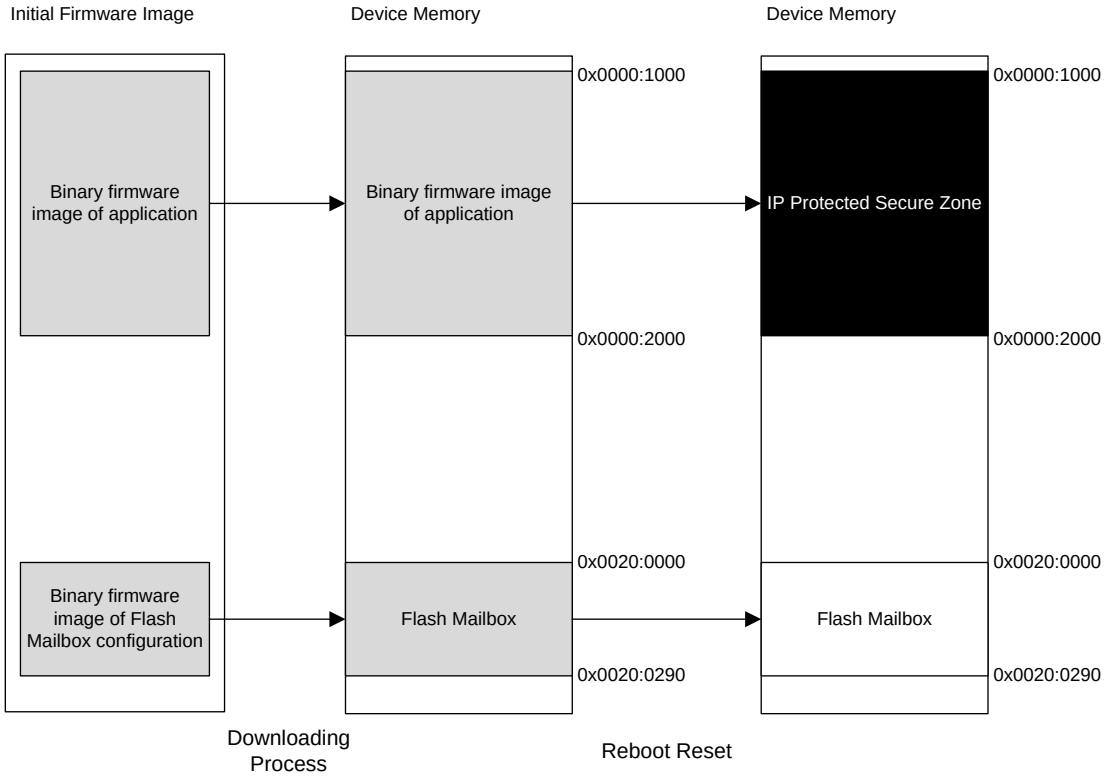

Figure 7. Set up an IP Protected Secure Zone

After the IP Protected Secure Zone is set by the boot code, the firmware update process must also be performed by setting the Flash Mailbox. As mentioned in the previous examples, there are two kinds of mode in the firmware image mode of the IP Protected Secure Zone. First is the unencrypted mode, and second is the encrypted mode. The first step preparation of the new firmware is the same. The updated firmware image must be appended with the unencrypted password that been set in the IP Protected Secure Zone configuration with 0x0000:1000 alignment.

Figure 8 shows an example of an updated firmware image that is located in nonsecured zone 0x0002:0000 with 0x0000:1000 byte length. The unencrypted password is appended starting at 0x0002:0000.

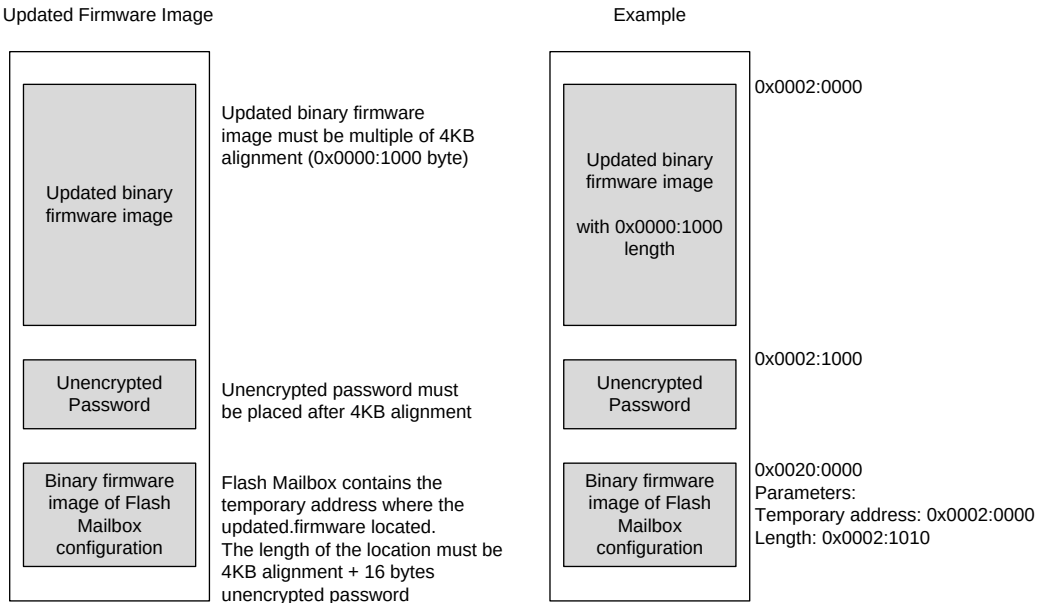

Figure 8. Updated Firmware Image

For encrypted mode, the updated-firmware image with the unencrypted password has to be encrypted using the AES-CBC initialization vectors and the secure keys that were configured before (see Figure 9).

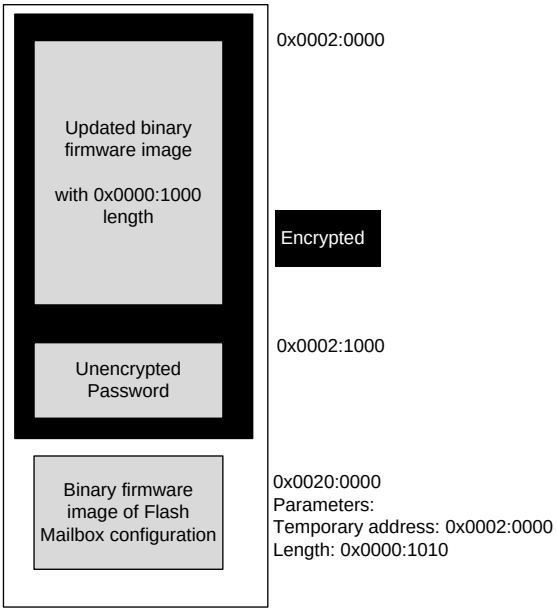

Figure 9. Encrypted Updated Firmware Image

Figure 10 shows how the update is done for an IP Protected Secure Zone. On the left side, the user already provided the updated firmware image (either for unencrypted or encrypted mode) concatenated with the configuration for Flash Mailbox configuration. The user chooses flash bank 1 as a temporary address for the updated firmware image in the device, in this case 0x0002:0000. Flash bank 1 starts from an address that is half of total flash main memory of the device.

When the device is reset or a POR is applied, the boot code writes the IP Protected Secure Zone with the new firmware that is located in 0x0002:0000 if the unencrypted password is correct. If the password wrong, the update is not executed. If the encrypted mode is chosen, the decryption takes place before placing the new firmware image to the IP Protected Secure Zone.

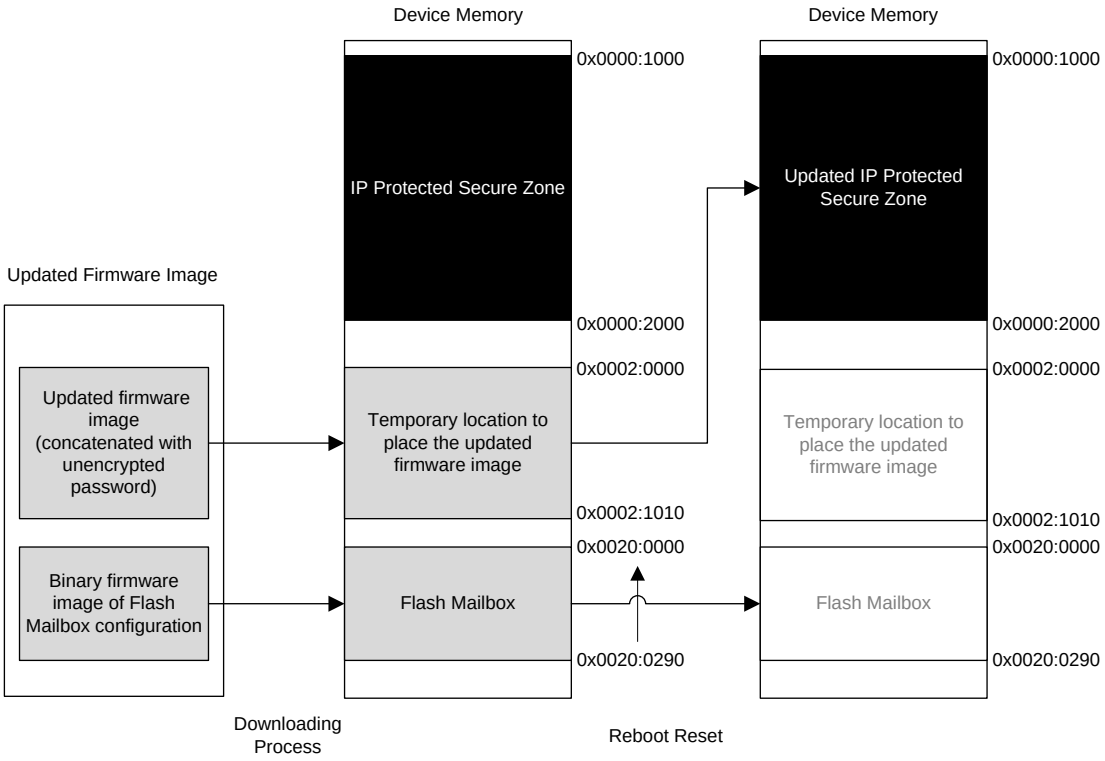

Figure 10. Updating IP Protected Secure Zone

2.5 JTAG/SWD Lock

After the development phase, debugging access is usually not required and is locked. The locking of the access for the debugger (both JTAG and SWD) is intended to prevent unintended debug access. The JTAG/SWD lock prevents debug access to all parts of memory.

In an unprogrammed or empty device, JTAG and SWD access is available. After JTAG and SWD locking is successfully performed, debug access is not available for the device. The JTAG/SWD Lock configuration always follows the encrypted mode. Therefore, the user must provide the unencrypted keys, AES-CBC initialization vectors, and the AES-CBC secure keys.

Figure 11 shows one example to configure the JTAG/SWD Lock.

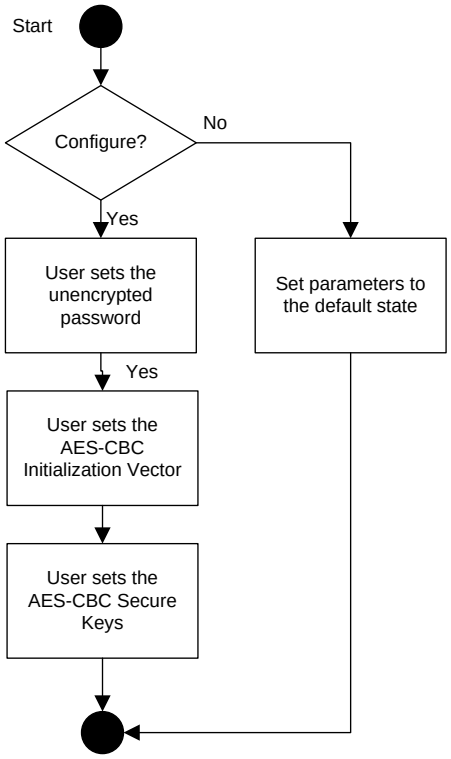

Figure 11. Configure the JTAG/SWD Lock Parameters

Table 13 is an example of configuring JTAG/SWD parameters.

Table 13. Example of Configuration for JTAG/SWD Parameters

Address	Parameters	Value
0x0020:0000	MB_START	0x0115:ACF6
0x0020:0004	COMMAND	0x0008:0000
0x0020:0010	JTAG_SWD_LOCK_SECEN	0x0000:0000
0x0020:0014	JTAG_SWD_LOCK_AESINIT_VECT[0]	0x0000:1111
0x0020:0018	JTAG_SWD_LOCK_AESINIT_VECT[1]	0x2222:3333
0x0020:001C	JTAG_SWD_LOCK_AESINIT_VECT[2]	0x4444:5555
0x0020:0020	JTAG_SWD_LOCK_AESINIT_VECT[3]	0x6666:7777
0x0020:0024	JTAG_SWD_LOCK_SECKEYS[0]	0x0011:2233
0x0020:0028	JTAG_SWD_LOCK_SECKEYS[1]	0x4455:6677
0x0020:002C	JTAG_SWD_LOCK_SECKEYS[2]	0x8899:AABB
0x0020:0030	JTAG_SWD_LOCK_SECKEYS[3]	0xCCDD:EEFF
0x0020:0034	JTAG_SWD_LOCK_SECKEYS[4]	0x0011:2233
0x0020:0038	JTAG_SWD_LOCK_SECKEYS[5]	0x4455:6677
0x0020:003C	JTAG_SWD_LOCK_SECKEYS[6]	0x8899:AABB
0x0020:0040	JTAG_SWD_LOCK_SECKEYS[7]	0xCCDD:EEFF
0x0020:0044	JTAG_SWD_LOCK_UNENC_PWD[0]	0x1234:5678
0x0020:0048	JTAG_SWD_LOCK_UNENC_PWD[1]	0x1234:5678
0x0020:004C	JTAG_SWD_LOCK_UNENC_PWD[2]	0x1234:5678
0x0020:0050	JTAG_SWD_LOCK_UNENC_PWD[3]	0x1234:5678
0x0020:028C	MB_END	0x0011:E11D

The scheme for JTAG/SWD Lock configuration is similar to IP Protected Secure Zone configuration. After the configuration in the Flash Mailbox is downloaded to the device and executed by the boot code, the JTAG/SWD is not accessible (see Figure 12).

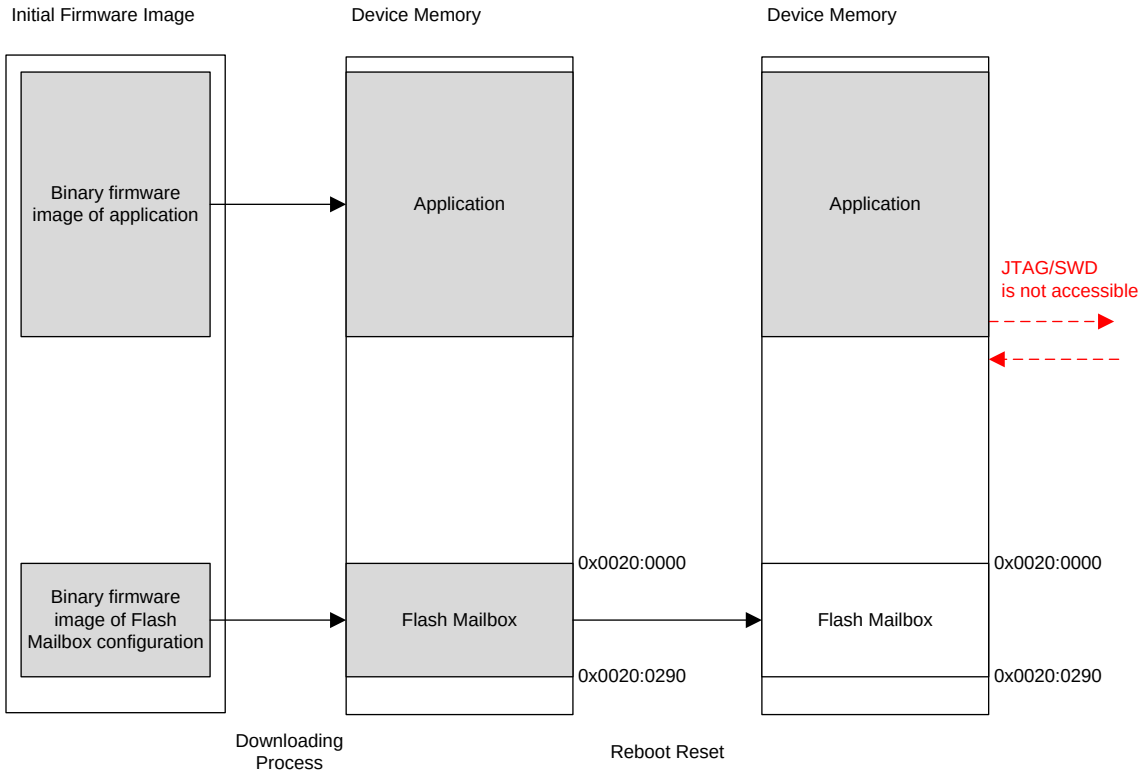

Figure 12. JTAG/SWD Lock Configuration Scheme

Two options are available for a firmware update when the JTAG/SWD Lock is enabled:

- Using the BSL

  When no IP Protected Secure Zone is configured and the JTAG/SWD is locked, the firmware update can be done by using BSL. The BSL can erase and write the memory. For details of using BSL commands, see the *MSP432™ SimpleLink™ Microcontrollers Bootloader (BSL) User's Guide*.

- Using the JTAG/SWD lock update with Flash Mailbox setting (see Figure 13)

  A firmware update through Flash Mailbox for JTAG/SWD locked condition is similar to the IP Protected Secure Zone update. The main difference between firmware update in IP Protected Secure Zone and the JTAG/SWD lock update is that in JTAG/SWD lock, the user must set a parameter that indicates the location to update. In IP Protected Secure Zone, the start address of the IP Protected Secure Zone is stored by the boot code. But in the JTAG/SWD lock configuration, there is no specific address where the memory is secured, because all parts of memory are secured from JTAG/SWD access.

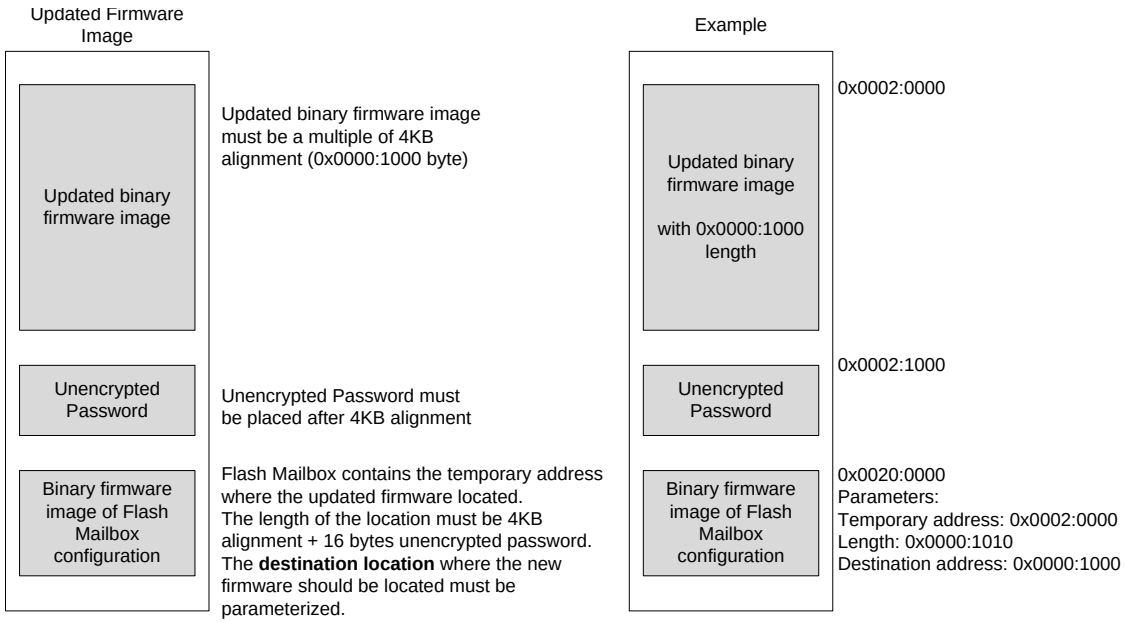

Figure 13. Updated Firmware Image for Updating in JTAG/SWD Lock Condition

The updated firmware image must be encrypted for this mode. In Figure 14, the firmware update is to be done at address 0x0000:1000. The updated firmware is temporarily located at flash bank 1, in this case 0x0002:0000. Note that flash bank 1 starts from an address that is half of the total flash main memory of the device.

When the device is reset or POR applied, the boot code updates the firmware at address 0x0000:1000 with the new firmware at the temporary location.

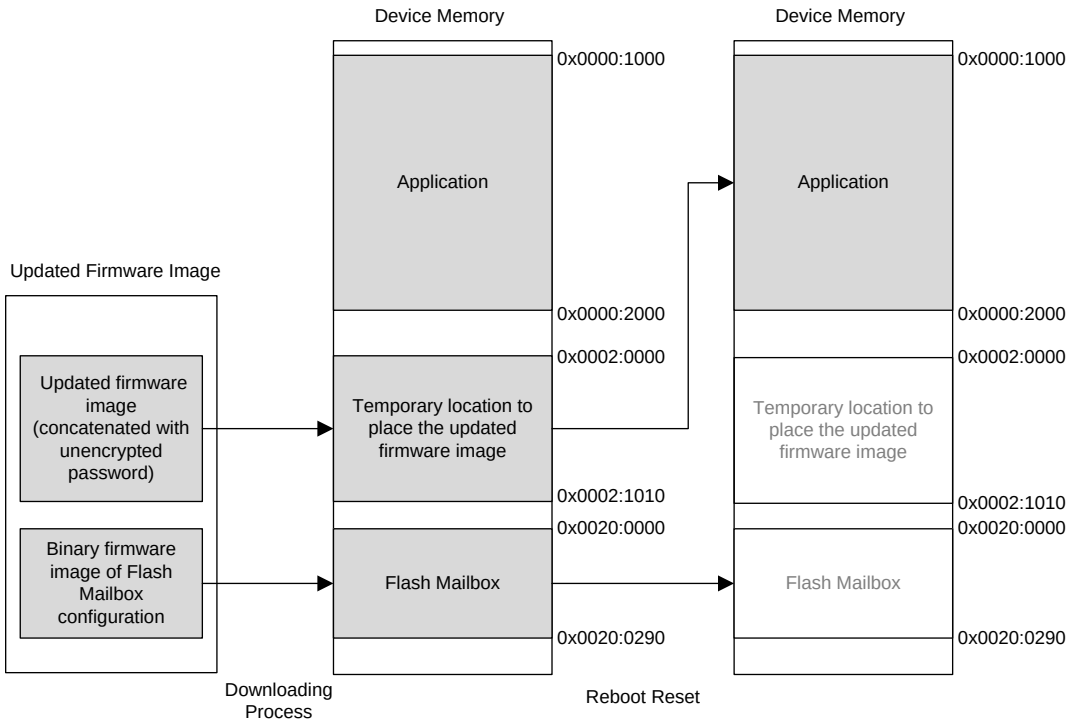

Figure 14. JTAG/SWD Lock Firmware Update

3 MSP432P4xx Security and Update Tool

The MSP432P4xx Security and Update Tool is a GUI and CLI application that offers ease-to-use interfaces to configure the security features in the MSP432P4xx devices. The use of this tool is divided into two major cases: the initial programming case and the firmware update case.

Figure 15. MSP432P4xx Security and Update Tool Icon

3.1 Initial Programming Case

In the initial programming case, build the firmware image from any supported IDE. At the same time, configure the intended security features through the GUI of MSP432P4xx Security and Update Tool. The configuration could be generated into these file formats:

- TI TXT File
- Intel Hex File
- C file
- XML file as saved configuration file to be loaded later

Using the CLI mode of the MSP432P4xx Security and Update Tool, concatenate the firmware image and the downloadable format configuration file. The complete firmware image that contains the application firmware image and the flash mailbox configuration firmware image can be downloaded into the MSP432P4xx device using the BSL Scripter (see Figure 16). The BSL Scripter supports input files in the TI TXT file format only.

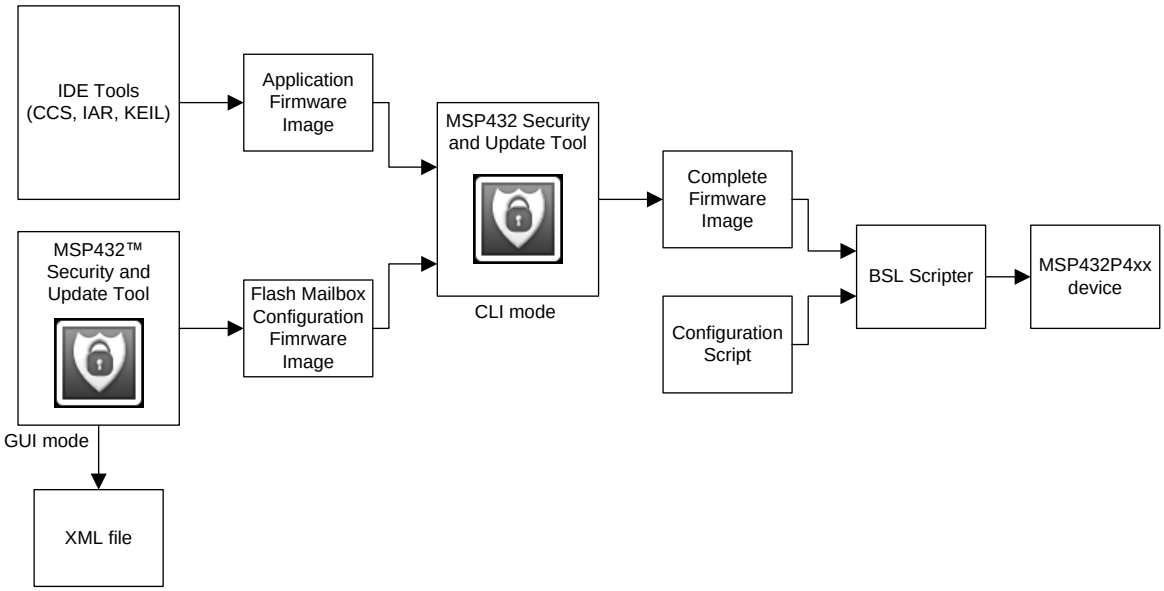

Figure 16. Initial Programming Case

3.2 Firmware Update Case

To apply a firmware update, build the new firmware image through any supported IDE. The parameters of the firmware update that will be deployed in the flash mailbox are configured using the GUI mode of the MSP432P4xx Security and Update Tool. Nevertheless, there are other parameters that are required, such as the unencrypted password and the encryption keys. You can configure these parameters manually through the GUI mode.

Figure 17 shows the high-level description of how the GUI of MSP432P4xx Security and Update Tool generates the updated firmware image that is concatenated with the configuration firmware image. The steps are explained in detail in Section 3.3.

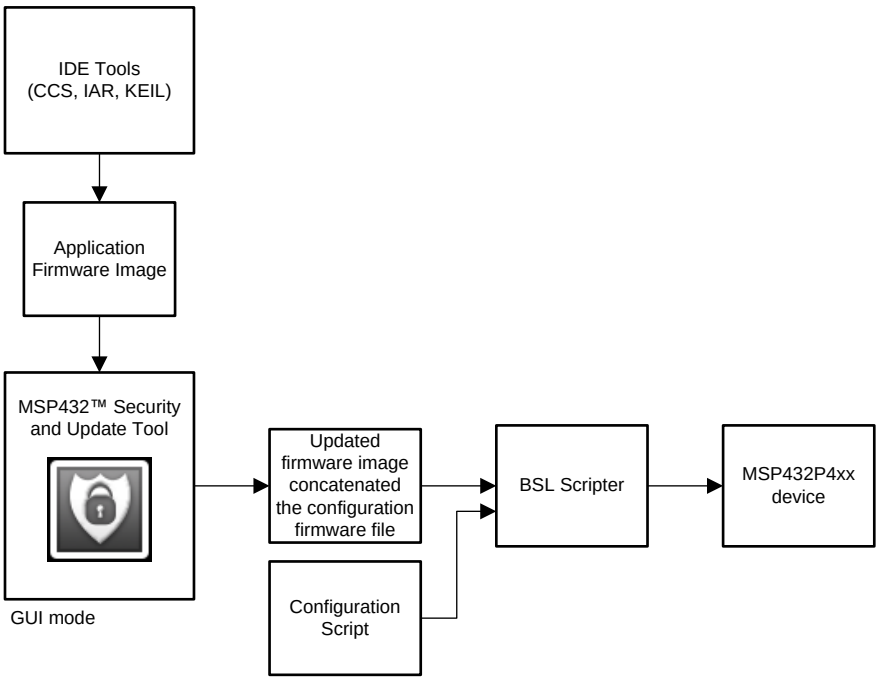

Figure 17. Firmware Update Case

Other than that, user can use the existing xml file that was previously generated to generate the updated firmware image that is also concatenated with the configuration firmware file (see Figure 18). The steps are explained in detail in Section 3.3.

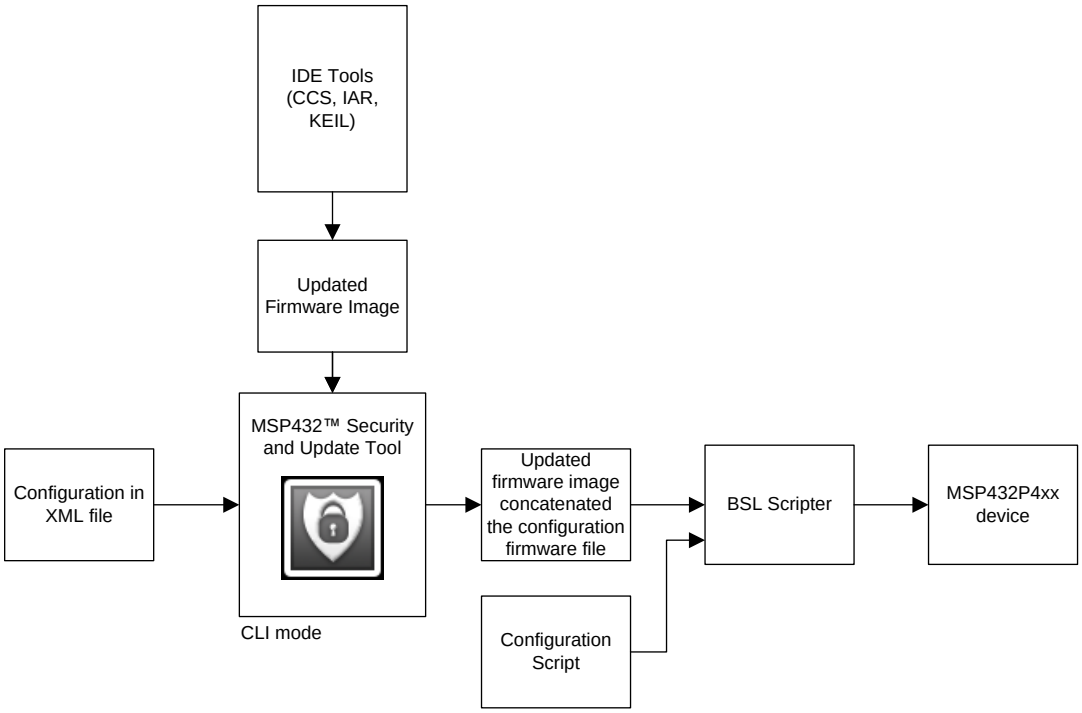

Figure 18. Firmware Update Case With XML

3.3 GUI Use

The graphical user interface (GUI) for the MSP432P4xx Security and Update Tool is divided into five tabs.

- Factory Reset (see Section 3.3.2)
  - Configure Factory Reset Parameters
  - Perform Factory Reset
- Bootloader (see Section 3.3.3)
- IP Protected Secure Zone (see Section 3.3.4)
  - Configure IP Protected Zone Parameters (Zone 0 , Zone 1, Zone 2, and Zone 3)
  - Update Firmware in IP Protected Zone (Zone 0, Zone 1, Zone 2, and Zone 3)
- JTAG/SWD Lock (see Section 3.3.5)
  - Configure JTAG/SWD Lock Parameters
  - Update Firmware
- Summary (see Section 3.3.6)

3.3.1 Device Selection

Starting with software version 1.01.00.00, a device selection list is available at the top of the GUI view (see Figure 19). The device selection affects parameters related to the placement of the IP Protected Secure Zone and the firmware update. The following options are available:

- MSP432P401M (128kB Main Flash Memory)
- MSP432P401R (256kB Main Flash Memory)
- MSP432P4x1V (512kB Main Flash Memory)
- MSP432P4x1Y (1024kB Main Flash Memory)
- MSP432P4x11 (2048kB Main Flash Memory)

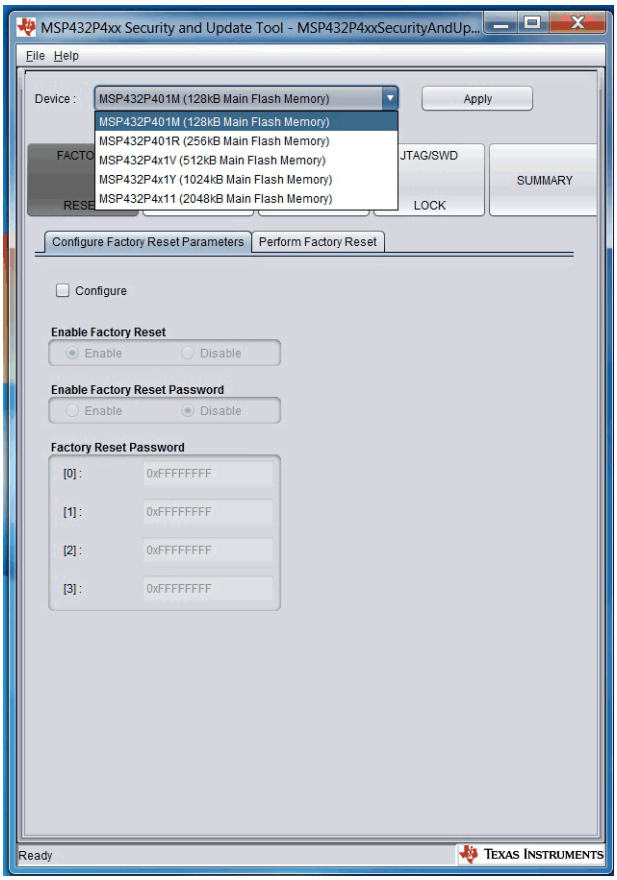

Figure 19. Device Selection

The following rules are related to the device selection:

- The IP Protected Zone is placed on flash bank 0 (the first half of main memory)
- Updated firmware is placed on flash bank 1 (the second half of main memory)
- For MSP432P401M and MSP432P401R, the IP Protected Secure Zone is aligned with 4KB (0x1000 bytes).
- For MSP432P4x1V, MSP432P4x1Y, and MSP432P4x11, the IP Protected Secure Zone is aligned with 16KB (0x4000 bytes).

If a configuration has been made in the GUI, and new device is selected, a warning message is shown (see Figure 20). Click Yes to continue with the new device and reset all configurations. Click No to cancel the new device selection and continue with the existing configuration.

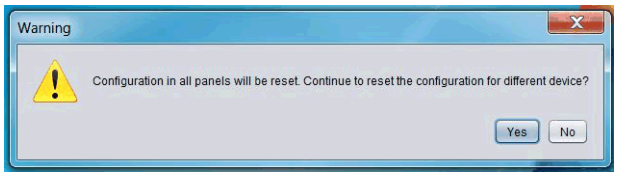

Figure 20. Device Selection Warning

3.3.2 Factory Reset Tab

3.3.2.1 Configure Factory Reset Parameters

Figure 21 shows the Configure Factory Reset Parameters tab.

Figure 21. Configure Factory Reset Parameters Tab

When the Configure check box in this panel is checked, the panel for Perform Factory Reset is disabled. This option sets the command to configure the Factory Reset parameters (CMD sets with 0x2000:000). The configuration consists of:

- Enable or Disable Factory Reset

  This sets the value of FACTORY_RESET_ENABLE. After the Factory Reset is disabled and configured successfully in the device, the Factory Reset cannot be enabled again.
- Enable or Disable Factory Reset Password

  This sets the value of FACTORY_RESET_PWDEND.
- Factory Reset Password (enabled only if Enable Factory Reset is selected)

  Password is stored as FACTORY_RESET_PWD[0-3].

3.3.2.2 Perform Factory Reset

Figure 22 shows the Perform Factory Reset tab.

Figure 22. Perform Factory Reset Tab

Selecting the Configure check box sets the CMD field with 0x0001:0000. The Factory Reset Password panel is enabled and the password can be entered and later stored as PASSWORD[0-3].

If on the previous configuration, the Factory Reset Password is disabled, then simply leave all fields with the default value 0xFFFFFFFF.

Other panels are disabled, because the other configuration does not take effect when the Factory Reset is performed.

3.3.3 Bootloader Tab

3.3.3.1 Bootloader (BSL) Configuration

Figure 23 shows the Bootloader tab.

Figure 23. Bootloader Configuration

Select the Configure check box to set the command to configure the bootloader (the CMD field is set with 0x0002:0000). The BSL Firmware address is set to the default address 0x0020:2000 and the Enable Hardware Invoke check box can be chosen.

The hardware invoke parameters consist of:

- I^2C Address has a default of value 0x0000:0048, and it is configurable.
- Interface is the communication protocol that is available for the bootloader communication. Interfaces that available are Automatic protocol recognition, UART, SPI and I^2C.
- Polarity can be either low or high polarity.
- Port and Pin specify the I/O pin that can invoke the bootloader.

3.3.4 IP Protected Secure Zone Tab

3.3.4.1 IP Protected Secure Zone Configuration

Figure 24 shows the Configure IP Protected Zone Parameters tab. Individual tab for each zone (Zone 0 to Zone 3) are included.

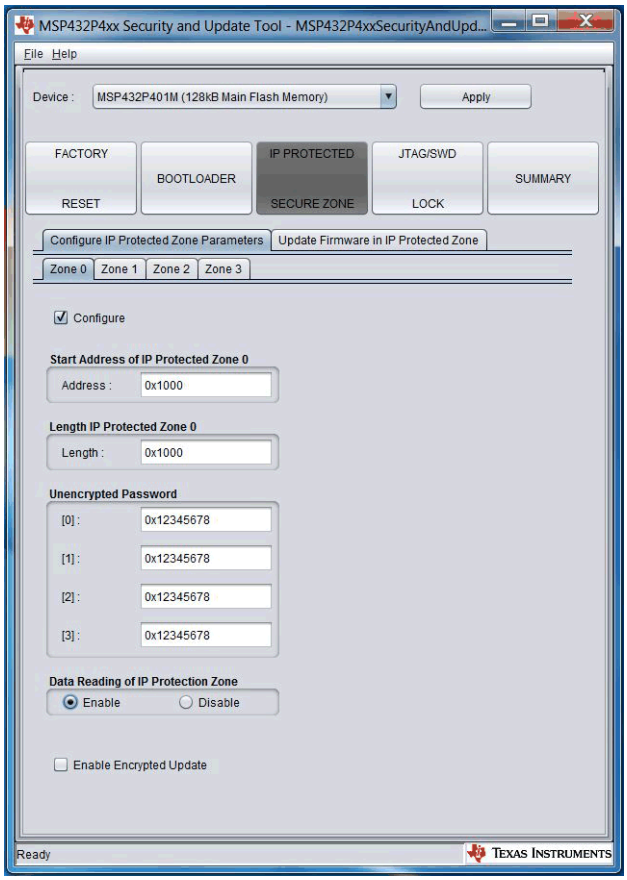

Figure 24. Configure IP Protected Zone Parameters Tab

When the Configure checkbox in Configure IP Protected Secure Zone Parameters – Zone x panel is selected, the Update Firmware in IP Protected Zone x panel is disabled. Options on this tab are:

- Start address of the IP Protected Zone

  The value that is inserted here must be aligned with:

  – 4KB for MSP432P401x devices

  – 16KB for MSP432P4x1V, MSP432P4x1Y, and MSP432P4x11 devices

  The GUI displays a warning message if the input is not aligned correctly (see Figure 25). If the warning message is displayed, the GUI does not change the value—the user must enter a valid value.

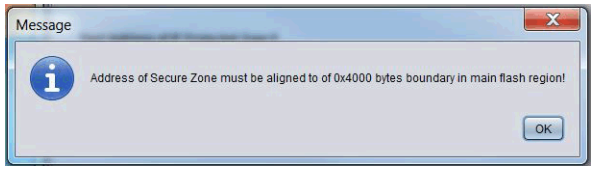

Figure 25. Warning Message for Invalid Input in Start Address Input

- Length of the IP Protected Zone

  The value that is entered must be a multiple of:

  – 4KB for MSP432P401x devices

  – 16KB for MSP432P4x1V, MSP432P4x1Y, and MSP432P4x11 devices

  The GUI displays a warning message if the input is not valid (see Figure 26). If the warning message is displayed, the GUI does not change the value—the user must enter a valid value.

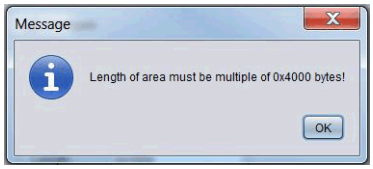

Figure 26. Warning Message for Invalid Input in Length Input

- Unencrypted password
- Data Reading of IP Protection Zone
- Enable encrypted update

  Choose any value between 0x0000:0000 and 0xFFFF:FFFF for the unencrypted password, initialization vector, and the security keys. The input must be entered with "0x" in the beginning.

  If three characters are entered without "0x" in the beginning, the GUI displays a warning message (see Figure 27).

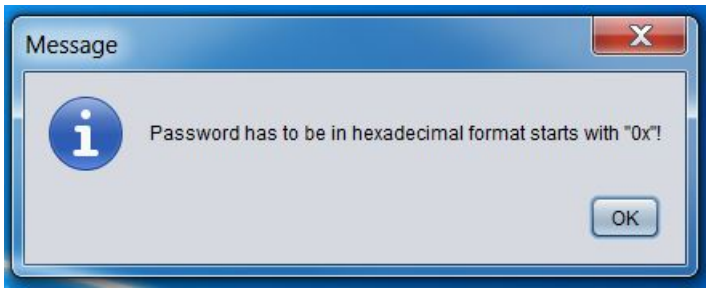

Figure 27. Warning Message for Wrong Input Format in Password Field

If the value that is entered for the password is not valid, the GUI displays a warning message (see Figure 28).

Figure 28. Warning Message for Wrong Input Value in Password Field

When the Enable Encrypted Update checkbox is selected, the panel shows (see Figure 29):

- Initialization (Init) Vector for AES-CBC Decryption
- Security Keys for AES-CBC Decryption

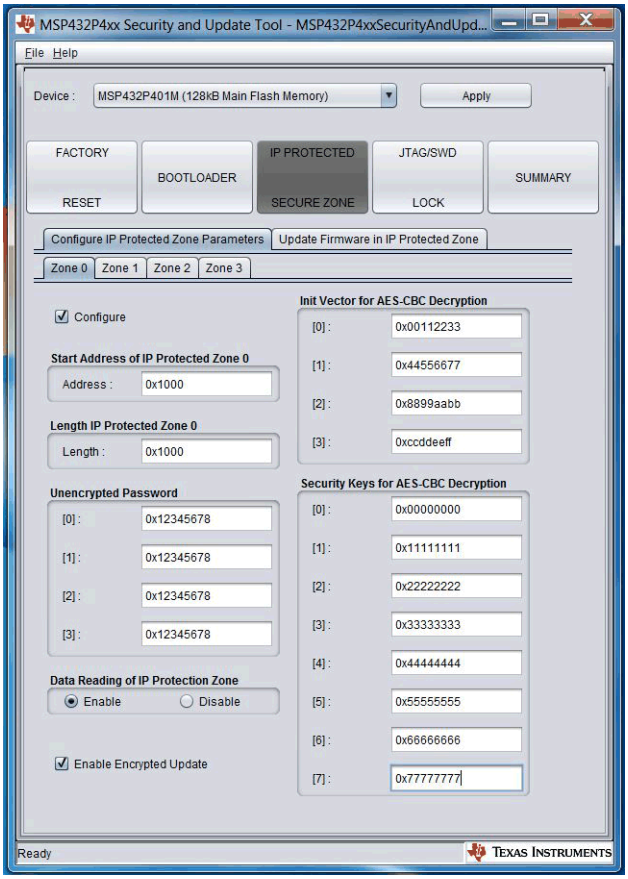

Figure 29. Configure IP Protected Zone Parameters Tab With Encrypted Update Selected

3.3.4.2 IP Protected Secure Zone Update

Figure 30 shows the Update Firmware in IP Protected Zone tab. Individual tabs for each zone (Zone 0 to Zone 3) are included.

Figure 30. Update Firmware in IP Protected Zone Tab When Encrypted Update Not Selected

There are two types of update:

1. Unencrypted update
   - When the Configure checkbox is selected, the update is set for unencrypted update. Choose the new firmware image with click the Open File in New Firmware image panel.
   - The Start address of the new firmware location and the length of firmware are automatically filled. A pop up window reminds the user that the new firmware image must be concatenated with the unencrypted password. This helps user to prepare a correct new firmware image. The correct length must be a multiple of one of the following plus 0x10 for the password:
     - 4KB for MSP432P401x devices
     - 16KB for MSP432P4x1V, MSP432P4x1Y, and MSP432P4x11 devices
   - The password is also required to generate a correct XML file. In Update Password, type the password or click Open File to select an XML to load.

     When entering the password from an XML file, the dialog in Figure 31 is shown. Here, the previous configuration file is entered. This figure shows the loading of config_1.xml. This file is the configuration that is saved when the IP Protected Secure Zone configuration is done. In config_1.xml, assume that the IP Protected Secure Zone 0 is set and has the parameters for an unencrypted password. By loading the config_1.xml, user does not have to type the unencrypted password; instead, the tool reads the password from the file.

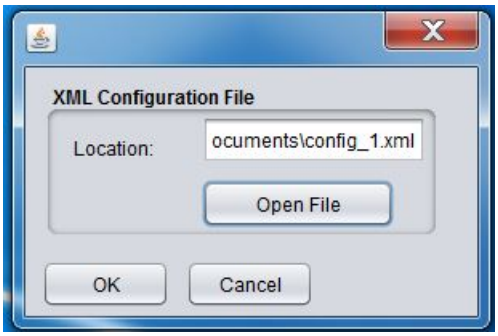

Figure 31. Enter Password With XML File

The password can also be manually entered. When this option is chosen, a new dialog view is shown. With the unencrypted mode, only the unencrypted password panel is available (see Figure 32).

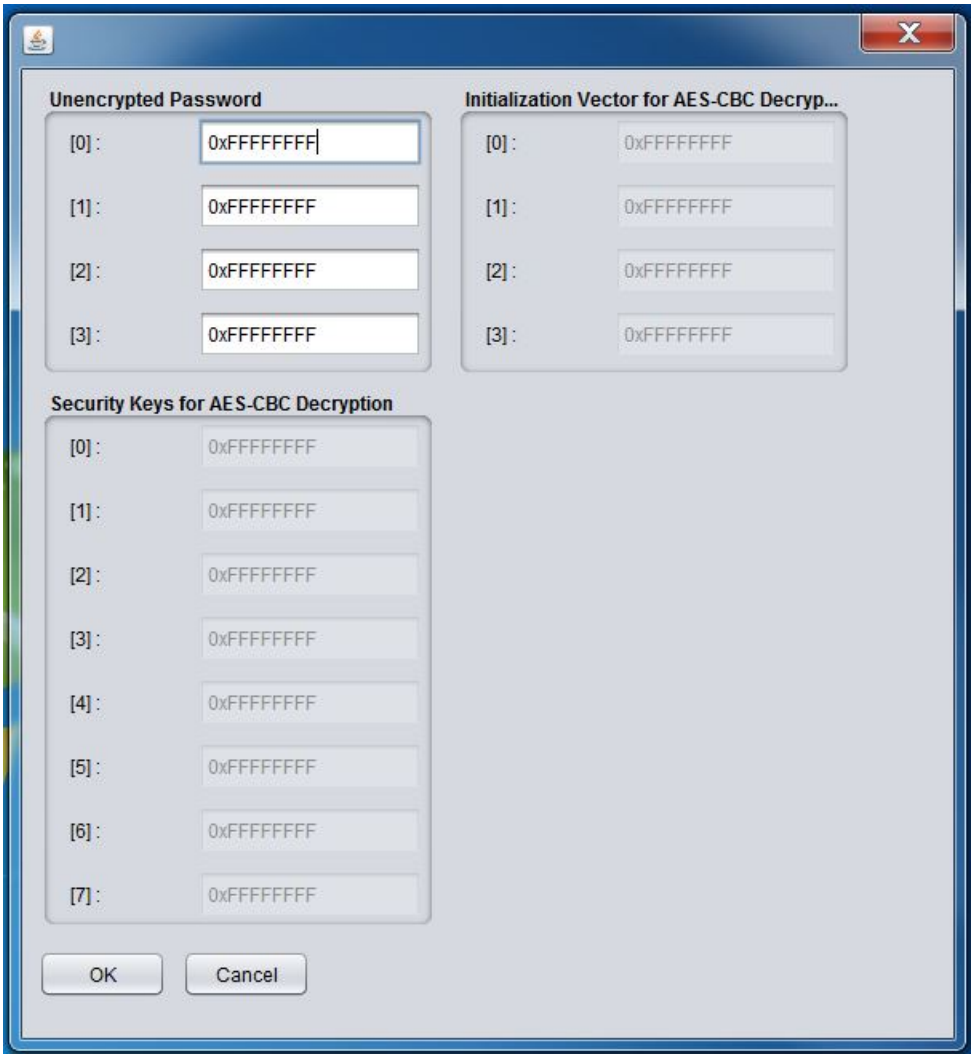

Figure 32. Manually Enter Unencrypted Password

2. Encrypted update
   - When Configure and Encrypted Mode are selected, Output Encrypted Firmware Image is enabled. The new firmware image is encrypted, and the encrypted output must be stored in a specific location. For MSP432P4xx Security and Update Tool 1.00.00.01, the Encryption Tool supports only the TI TXT file format input image; therefore, the New Firmware Image and the Output Encrypted Firmware Image must be in TI TXT file format.
   - The setup for unencrypted password, initialization vectors AES-CBC, and the secure key AES-CBC is the same as for the Unencrypted Mode. This configuration can be done by loading from an XML file.

Figure 33. Update Firmware in IP Protected Zone Tab With Encrypted Update Selected

3.3.5 JTAG/SWD Lock Tab

3.3.5.1 JTAG/SWD Configuration

Figure 34 shows the Configure JTAG/SWD Lock Parameters tab.

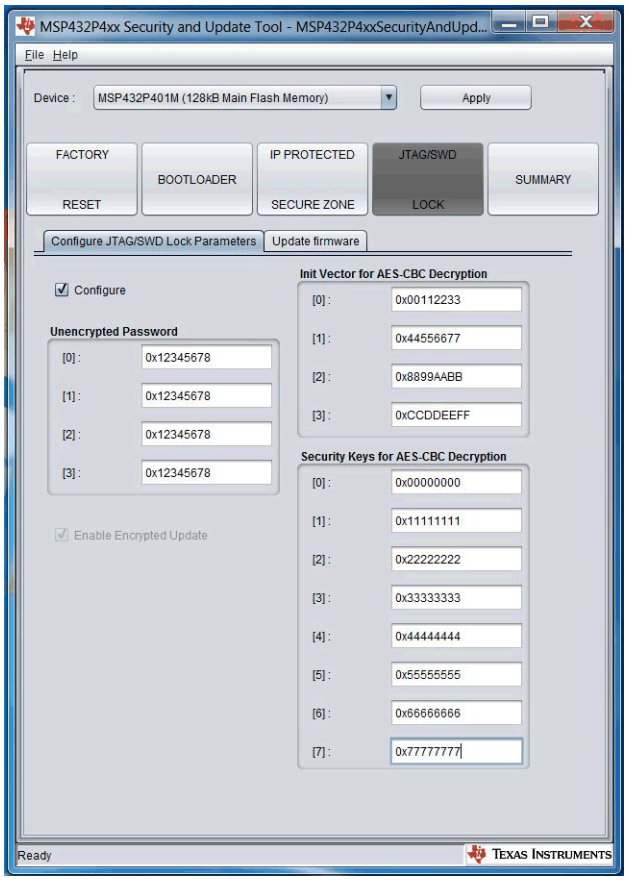

Figure 34. Configure JTAG/SWD Lock Parameters Tab

When the JTAG/SWD lock is configured, the encrypted mode is automatically chosen. Therefore, JTAG/SWD Lock always has encrypted update mode. The parameters that are required for this feature are:

- Unencrypted Password
- Initialization (Init) Vector for AES-CBC Decryption
- Security Keys for AES-CBC Decryption

3.3.5.2 JTAG/SWD Lock Update

Figure 35 shows the Update Firmware tab of the JTAG/SWD Lock Update panel.

Figure 35. Update Firmware Tab

Important points to be noted for configuring the parameters in JTAG/SWD lock update:

- The JTAG/SWD lock update is applicable for encrypted mode only. Therefore, the new firmware image must be encrypted, and the output encrypted firmware image must be defined.
- Start Address of Firmware Location and Length of Firmware are automatically generated when the new firmware image location is chosen. The GUI displays a window to remind the user that the correct length must be a multiple of one of the following plus the 0x10-byte concatenated password:
  - 4KB for MSP432P401x devices
  - 16KB for MSP432P4x1V, MSP432P4x1Y, and MSP432P4x11 devices
- Update Password must be loaded either by loading an XML file that has JTAG/SWD Lock configuration or by manually typing.
- Destination Address is a mandatory field that specifies the location to be updated.

3.3.6 Summary Tab

After the configuration setup is done, go to the Summary panel to get the final configuration file. Figure 36 shows the Summary tab.

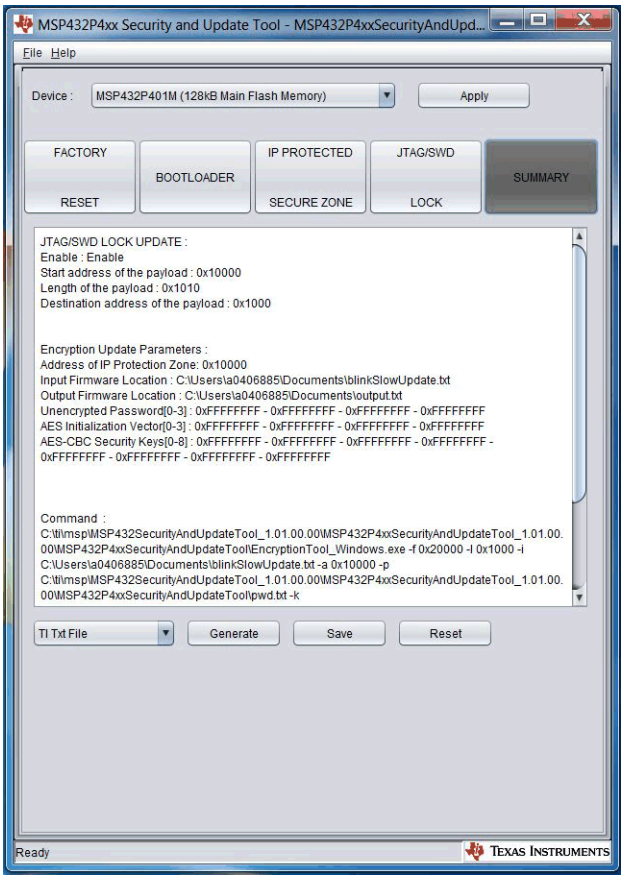

Figure 36. Summary Tab

The available output file formats are TI TXT file, Intel Hex file, and the C-array format in C-file. After the output format is selected, click Generate and select the location to save the configuration.

Click the Save button and select the location to save the XML configuration file.

To reset all configuration in all panels, click the Reset button.

3.4 Command Line Interface (CLI) Use

There are two cases that are managed by the CLI mode.

3.4.1 Initial Programming Case

The initial programming sends the configuration and the firmware image to the device. In the command prompt (for Windows) or terminal (for Ubuntu and MacOS), run the following command:

```
java -jar MSP432SecurityAndUpdateTool.jar <config_file> <firmware_file> <output_file>
```

The supported file formats are:

- TI TXT file (.txt)
- Intel Hex file (.hex)

The arguments of three file have the same format; otherwise, the CLI returns an error message.

Example of the command use:

```
java -jar MSP432SecurityAndUpdateTool.jar config.txt app.txt output.txt
java -jar MSP432SecurityAndUpdateTool.jar config.hex app.hex output.hex
```

3.4.2 Firmware Update Case

```
java -jar MSP432SecurityAndUpdateTool <config_file_in_xml_format> <output_file>
```

For the MSP432P4xx Security and Update Tool 1.00.00.01 release, the Encryption Tool supports only the TI TXT file format. Therefore, the file parameter of the new firmware image must have the TI TXT file format, and the output file is also this format.

Example of the command use:

```
java -jar MSP432SecurityAndUpdateTool.jar config.xml output.txt
```

4 References

1. *Configuring Security and Bootloader (BSL) on MSP432P4xx Microcontrollers*
2. *Software IP Protection on MSP432P4xx Microcontrollers*
3. *MSP432P4xx SimpleLink™ Microcontrollers Technical Reference Manual*
4. *MSP432 Security Overview*
5. *MSP432™ SimpleLink™ Microcontrollers Bootloader (BSL) User's Guide*

Revision History

NOTE: Page numbers for previous revisions may differ from page numbers in the current version.

Changes from July 18, 2017 to August 2, 2019	Page
• Corrected the base for values as needed (changed "h" to "b") in Table 8, *BSL Hardware Invoke Pin Parameters*	9
• Added rows for the MB_START and MB_END parameters in Table 10, *Example to Configure BSL*	10
• Changed the value for the BSL_START_ADDRESS parameter in Table 10, *Example to Configure BSL* and in the preceding list	10

IMPORTANT NOTICE AND DISCLAIMER

TI PROVIDES TECHNICAL AND RELIABILITY DATA (INCLUDING DATASHEETS), DESIGN RESOURCES (INCLUDING REFERENCE DESIGNS), APPLICATION OR OTHER DESIGN ADVICE, WEB TOOLS, SAFETY INFORMATION, AND OTHER RESOURCES “AS IS” AND WITH ALL FAULTS, AND DISCLAIMS ALL WARRANTIES, EXPRESS AND IMPLIED, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT OF THIRD PARTY INTELLECTUAL PROPERTY RIGHTS.

These resources are intended for skilled developers designing with TI products. You are solely responsible for (1) selecting the appropriate TI products for your application, (2) designing, validating and testing your application, and (3) ensuring your application meets applicable standards, and any other safety, security, or other requirements. These resources are subject to change without notice. TI grants you permission to use these resources only for development of an application that uses the TI products described in the resource. Other reproduction and display of these resources is prohibited. No license is granted to any other TI intellectual property right or to any third party intellectual property right. TI disclaims responsibility for, and you will fully indemnify TI and its representatives against, any claims, damages, costs, losses, and liabilities arising out of your use of these resources.

TI’s products are provided subject to TI’s Terms of Sale (www.ti.com/legal/termsofsale.html) or other applicable terms available either on ti.com or provided in conjunction with such TI products. TI’s provision of these resources does not expand or otherwise alter TI’s applicable warranties or warranty disclaimers for TI products.

Mailing Address: Texas Instruments, Post Office Box 655303, Dallas, Texas 75265