Please note that Cypress is an Infineon Technologies Company.
The document following this cover page is marked as “Cypress” document as this is the company that originally developed the product. Please note that Infineon will continue to offer the product to new and existing customers as part of the Infineon product portfolio.

Continuity of document content
The fact that Infineon offers the following product as part of the Infineon product portfolio does not lead to any changes to this document. Future revisions will occur when appropriate, and any changes will be set out on the document history page.

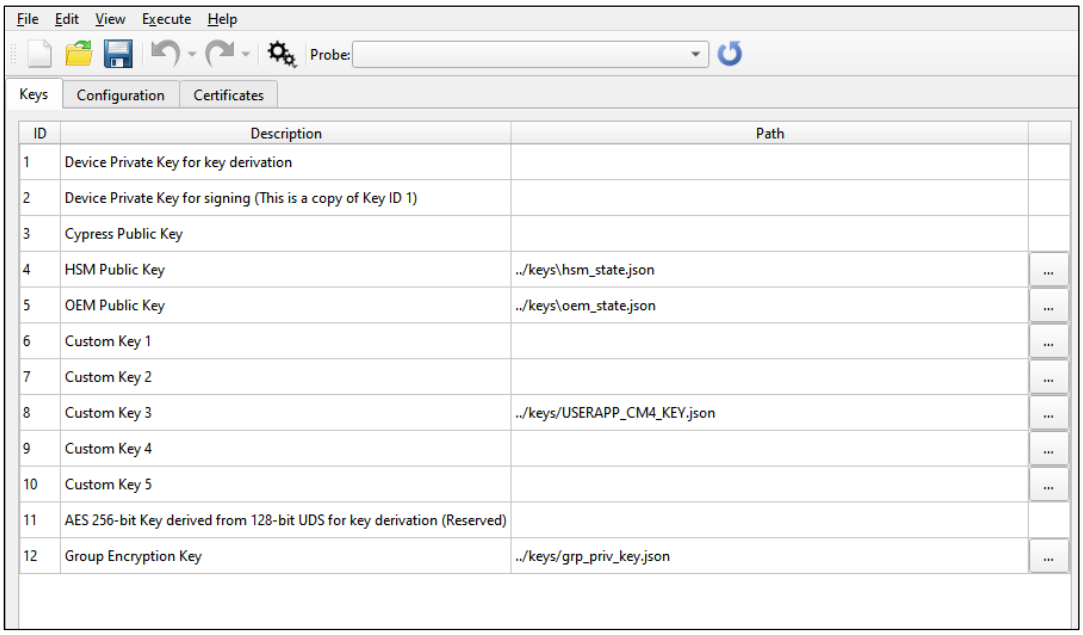
Continuity of ordering part numbers
Infineon continues to support existing part numbers. Please continue to use the ordering part numbers listed in the datasheet for ordering.

ModusToolbox® Secure Policy Configurator Guide

Version 1.0

Overview

The Secure Policy Configurator is part of a collection of tools included with the ModusToolbox software. You can use the Secure Policy Configurator to open, create or change policy configuration files for the Secure MCU devices. For details, refer to the PSoC® 64 Secure MCU Secure Boot SDK User Guide.



Definitions

The following are the terms used in this guide that you may not be familiar with:

- **CySecureTools** – A set of Python scripts and policy templates to perform provisioning for the PSoC 64 devices.
- **Provisioning** – The act of configuring a device with an authorized set of keys, certificates, credentials, and firmware images. Executed in two steps: 1. Provisioning identity – the unique device secret (UDS) and the device public/private key pair. **Note** This occurs only once in a secure manufacturing environment. 2. Provisioning keys and policies.
- **Reprovisioning** – The act of reconfiguring a device with a new certificate.
- **DAPLink** – Arm Mbed DAPLink is an open-source software project that enables programming and debugging application software running on Arm Cortex CPUs.
- **JSON** file –Stores simple data structures and objects in the JavaScript Object Notation (**JSON**) format, which is a standard data interchange format.
- **Public key certificate** – The X.509 type certificate is a standard public key certificate used in many Internet protocols, including TLS/SSL. A certificate is a message, digitally signed by a “Certificate Authority (CA)”, linking a public key to the identity of the certificate holder (can be a URL, name/address, ID/serial number).
- **Monotonic counter ID –** The counter to prevent a rollback during the upgrade process. Indicates the monotonic counter value associated with the image, which is booted. During secure boot, this counter

value is compared with this image version code. During the upgrade process, this counter is incremented to the value from the image header of the upgrade image.

- **RMA (**Return Merchandise Authorization) **mode** – The device transitions to this mode when the user wants Cypress to perform failure analysis on the device. Before provisioning, the provisioning JWT file updates the RMA section of the Debug policy, which means that any areas of the user's flash that may contain proprietary code or sensitive data are erased automatically. For detail on the format of the JWT file, see PSoC 64 Secure MCU Secure Boot SDK User Guide.

Installation

The Secure Policy Configurator requires CySecureTools to be installed; it is available for download here:

https://github.com/cypresssemiconductorco/cysecuretools

Note For Windows, CySecureTools is automatically installed as a part of the Python package with ModusToolbox 2.2 and later.

For detailed CySecureTools installation instructions, refer to the PSoC® 64 Secure MCU Secure Boot SDK User Guide.

Quick Start

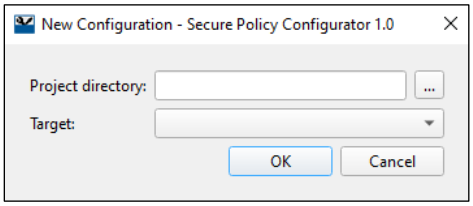
This section provides a simple workflow for how to use the Secure Policy Configurator. See Launch the Secure Policy Configurator to open the tool.

Create a policy file

To create a new policy file:

1. Select – **File > New**.

   The New Configuration dialog displays.



2. Click the **Browse** [. . .] button next to **Project directory** and navigate to and select the *secure* subdirectory, if available.

   Note The *secure* subdirectory is created automatically for specific devices. If there is not a *secure* subdirectory, we recommend creating one. However, you can save the policy file in any subdirectory.

3. In the Target pull-down menu, select the appropriate device family or kit, and click OK.
4. Select File > Save in the main GUI to generate the user keys.

Open an existing policy file

To open an existing policy file:

1. Select **File > Open**.
2. Navigate to the location of the policy file, select it, and click **Open**.

Provision a device

These are the minimum steps if you want to use the default policy settings:

1. Create or open an existing policy file.
2. Connect the device to your computer with a USB cable.
3. The kit must be in DAPLink mode. Press the ‘Mode’ button on the kit until the Status LED blinks fast. For more details, refer to the KitProg3 User Guide.
4. Click **Refresh Probe List** on the toolbar.
5. Select the device from the **Probe** list in the toolbar.
6. Select **Execute > Run Entrance Exam**.
7. Select **Execute > Provision Device**.

   If the device is already provisioned, select **Execute > Reprovision Device** instead.

   Note The device must be initially configured to be reprovisioned (check the Reprovisioning Options in the Advanced tab) in order to be reprovisioned later.

Launch the Secure Policy Configurator

As a Stand-Alone Tool

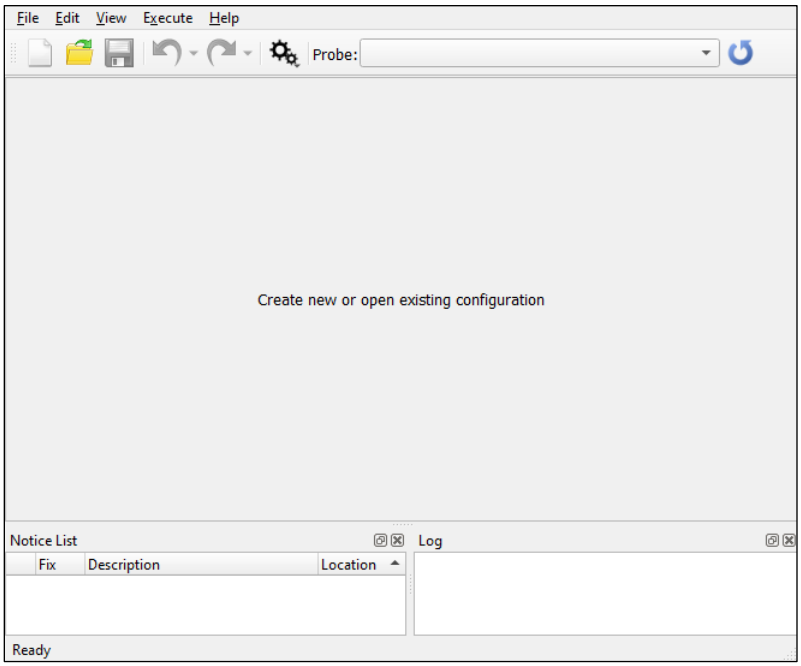
You can launch the Secure Policy Configurator as a stand-alone tool without the Eclipse IDE. By default, it is installed here:

<install_dir>/ModusToolbox/tools_<version>/secure-policy-configurator<version>

On Windows, you can launch the tool from the **Start** menu.

For other operating systems, the installation directory will vary, based on how the software was installed.

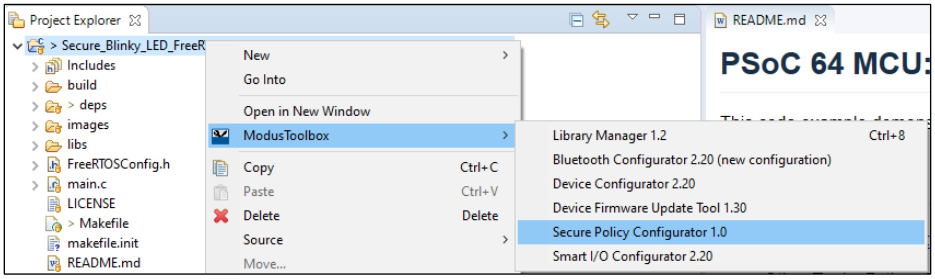
When run independently, the Secure Policy Configurator opens without a policy configuration file.



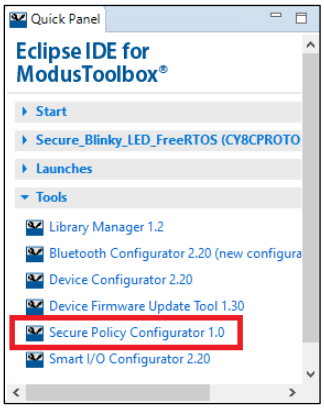
You can either open a specific policy configuration file or create a new one. See Menus for more information.

From the Eclipse IDE

To launch the Secure Policy Configurator from the Eclipse IDE, right-click on the project and select **ModusToolbox > Secure Policy Configurator.**



You can also open the Secure Policy Configurator by clicking the link in the Eclipse IDE for ModusToolbox Quick Panel:



From the Command Line

For information about the command-line options, run the secure-policy-configurator executable using the `-h` option.

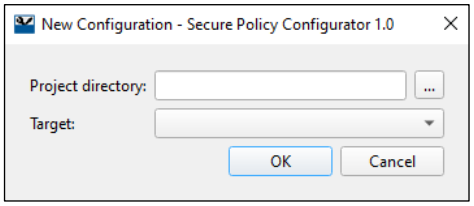
GUI Description

The Secure Policy Configurator GUI contains menus, tabs, and dialogs to configure secure policy configuration files.

Menus

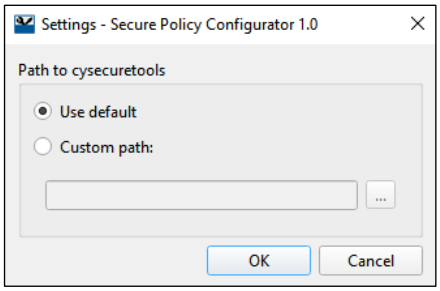
File

- **New** – Creates a new secure-policy directory in the New Configuration dialog.



  - Project directory – The path to the folder where a project will be created.

  - Target– A drop-down menu to choose a device or a device family to create a project.
- **Open** – Opens an existing secure policy configuration file (.json).
- **Save** – Saves changes to the secure policy configuration file. This command generates a user key if it does not exist already.
- **Settings** –Click this menu to display the Settings dialog window, where you can choose either the default path to the CySecureTools software or customize the path.



- **Recent Files** – Shows recent files that you can open directly.
- **Exit** – Closes the configurator.

Edit

- **Undo** – Undoes the previous change.
- **Redo** – Redoes the last undone change.

View

- **Advanced** – Opens a dialog to edit additional secure policy configuration settings.
- **Notice List, Log**, **Toolbar** – Hide or show these options respectively.
- **Reset View** – Restores the GUI to the default view.

Execute

- **Get Device Info** – Provides a list of available device information in the Log window. This information includes but is not limited to the following:
  - Target
  - Flashboot revision
  - Silicon ID, Family, and revision
  - Probe ID
- **Run Entrance Exam** – Must confirm that the device is genuine and blank.
- **Run Entrance Exam and Erase User Flash** – Confirms that the device is genuine and blank and erases the user's flash. The user is responsible for erasing any secret information.
- **Provision Device** – Configures the device with an authorized set of keys, certificates, credentials, and firmware images.
- **Reprovision Device** – Provides the device with a new certificate.
- **Read Public Keys** – Reads the selected key into the Log window. This drop-down menu displays the public keys, which can be read from the device.

Help

- **View Help** – Opens this User Guide.
- **About Secure Policy Configurator** – Shows version information.

Toolbar

The toolbar contains several commands also available from the menus.

- **New** – Creates a new secure-policy directory.
- **Open** – Opens an existing policy file (.json).
- **Save** – Saves changes to the policy file. Generates a user key if it does not exist already.
- **Undo** – Undoes the previous change.
- **Redo** – Redoes the last undone change.
- **Execute** – Equivalent to the Execute menu.
- **Probe** – This is a drop-down menu of all the available probes currently connected to the PC. The user may select any of the listed probes for the actions in the Execute menu. A note displays to remind the user to switch the kit or programmer to DAPLink mode.
- **Refresh Probe List** – Searches for a kit or programmer currently attached to the PC and repopulates the Probe list.

Tabs

The Secure Policy Configurator contains several tabs in which to update various settings.

- Keys Tab
- Configuration Tabs

  The Secure Policy Configurator operates in Single-image and Multi (two)-image modes, so different tabs display depending on the selected policy file mode.
- Certificates Tab

Notice List

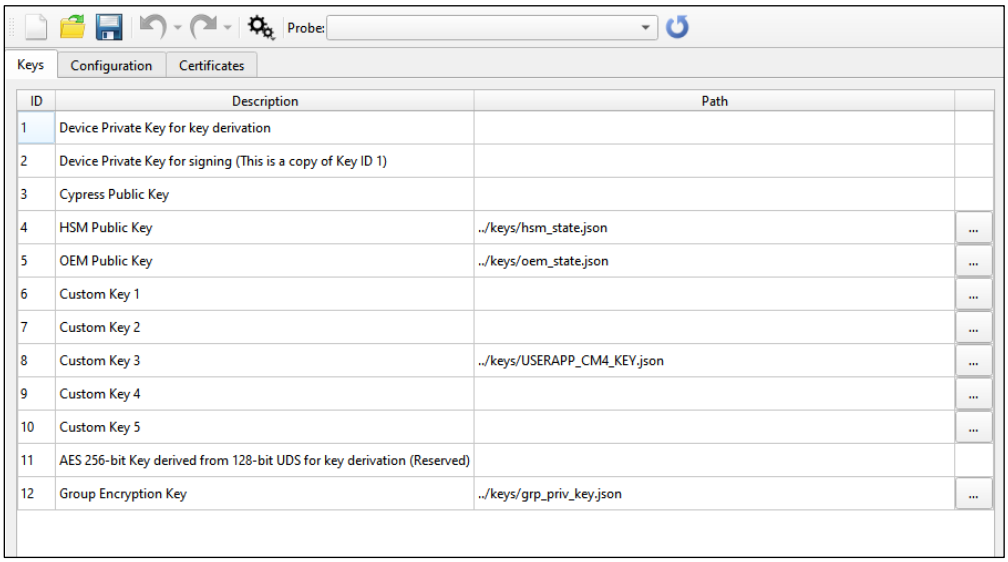
The **Notice List** combines notices (errors, warnings, tasks, and any other information) from many places in your design into a centralized list. If a notice shows a location, you can double-click the entry to navigate to the error or warning. For details, refer to the description in the Device Configurator Guide.

Log

The log pane shows any errors or status. A log file collects the output of any executed script to the log pane. The placement of this log file is consistent with other tools in the build system.

Keys Tab

This tab provides a method to associate a Key ID with the appropriate key file.



ID

- **1 , 2, 3, 11** – These keys cannot be modified by the configurator. They are reserved for other purposes.
- **4, 5, 6, 7, 8, 9, 10, 12** – The user keys whose entries can be modified. These keys can be loaded with keys provided by the OEM. Key ID **8** is the default user application key.

Description

This field provides the Keys' assignments.

Path

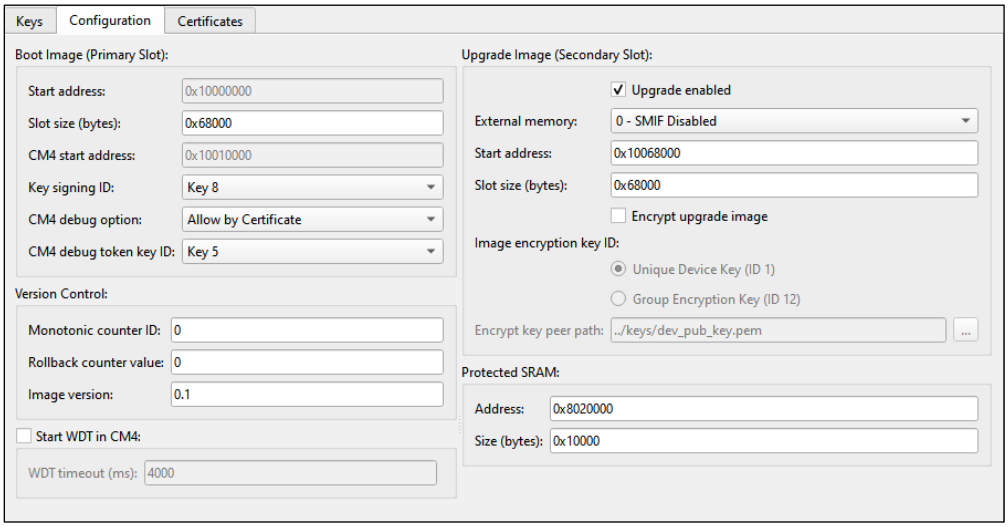
The **Browse** [**. . .**] button on the right – to select which key is associated with the Key ID and configure the path to each key file.

Configuration Tabs

Depending on the selected device and policy file, you will see varying tabs for configuration.

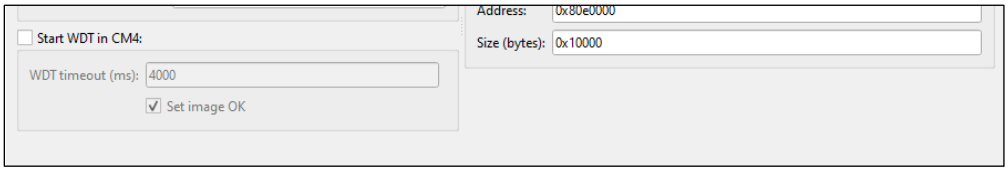
Single-Image

If you open or create a single-image policy file the tab display as follows:



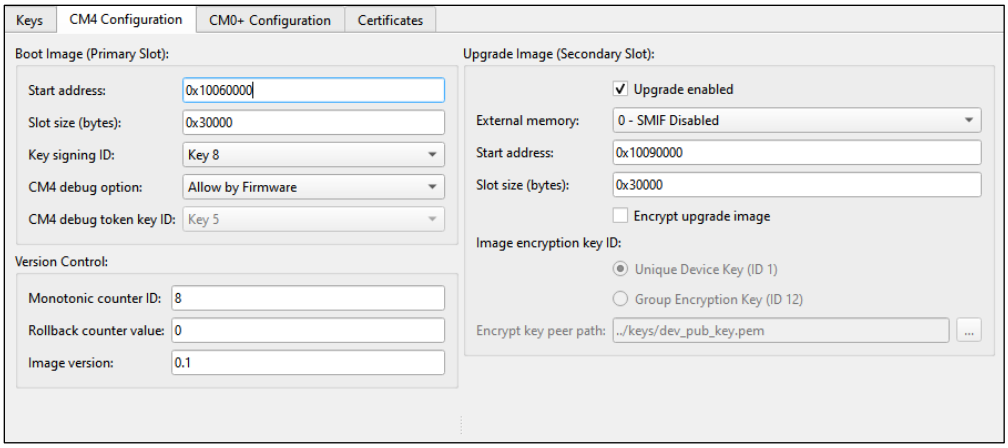
Single-Image Swap Mode

If you open or create a single-image policy file with the `swap` suffix, then the tool adds a parameter called "Set image OK."



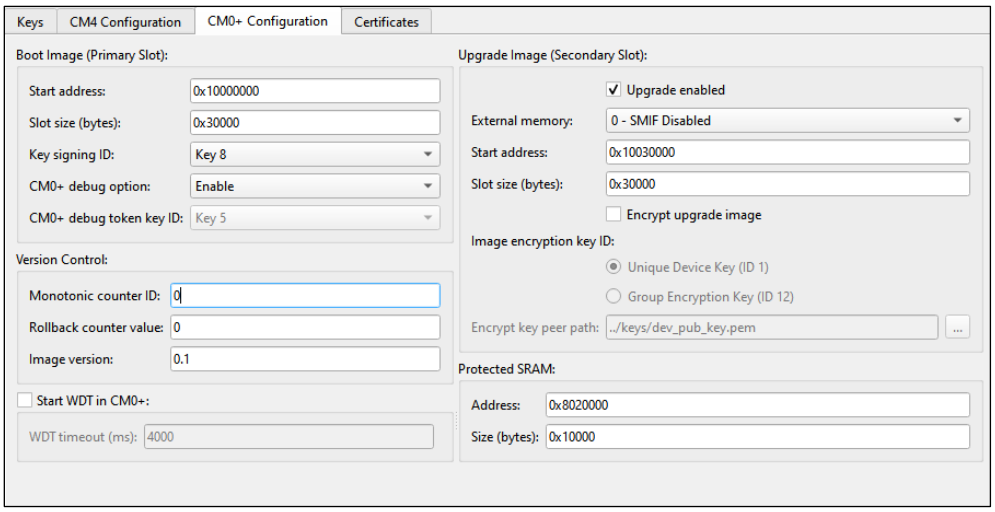
Multi-Image CM4 Configuration

For a multi-image policy file, there are two tabs: CM4 and CM0+. The following shows CM4 configuration settings:



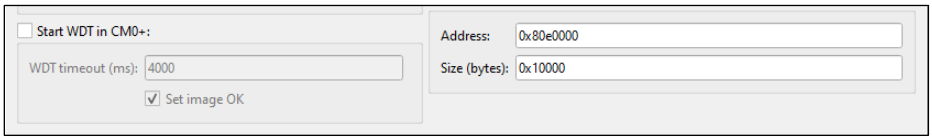
Multi-Image CM0+ Configuration

For a multi-image policy file, there are two tabs: CM4 and CM0+. The following shows the CM0+ configuration settings:



Multi-Image Swap mode

If you open or create a multi-image policy file with the `swap` suffix, then the tool adds a parameter called "Set image OK" to the CM0+ Configuration tab.



Configuration Parameters

The following describe the configuration parameters available in the Configuration tabs.

Note Some of the parameters display only in the specified tab.

Boot image (Primary Slot)

The memory location to execute code.

Start address

The location of the boot image.

Slot size (bytes)

The size of the boot image.

CM4 start address (Configuration tab)

This is the location in which the CM4 portion of the image starts. In Single-image mode, the CM0+ binary is combined with the user's CM4 code binary.

Key signing ID

The key ID to check the boot image signature. The user must select one of the Custom keys (6-10) in the Keys tab prior to provisioning.

CM4 debug option (Configuration and CM4 Tabs)

Determines how to debug the CM4. The options:

- **Enable** – Always enabled.
- **Disable** – Always disabled.
- **Allow by Firmware** – The debug access port may be enabled by the firmware.
- **Allow by Certificate** – The debug access port may be enabled by the certificate.

CM4 debug token key ID (Configuration and CM4 Tabs)

The key to authenticate the debugger.

CM0+ debug option (CM0+ Configuration Tab)

Determines how to debug the CM0+. The options:

- **Enable** – Always enabled.
- **Disable** – Always disabled.
- **Allow by Firmware** – The debug access port may be enabled by the firmware.
- **Allow by Certificate** – The debug access port may be enabled by the certificate.

CM0+ debug token key ID

The key to authenticate the debugger.

Version control

This box includes three options for firmware upgrade version control and rollback.

Monotonic counter ID

Prevents a rollback during the upgrade process

Rollback counter value

The initial counter value.

Image version

The version of the image for the MCUBoot header.

Start WDT

This check box is available on the single-image Configuration tab or the multi-image CM0+ Configuration tab. The watchdog timer is used to protect the device from freezing after updating with an incorrect CM4 or CM0+ image. If this check box is enabled, the timer is used to reset the device and revert to the previous image. This setting applies to the entire application, and it is separate from the Start WDT setting on the Advanced dialog.

Note This occurs only if Swap mode was enabled on the CY8C64x8 or CY8C64xA device.

WDT timeout (ms)

The parameter to set the time (in milliseconds) after which the device resets automatically (if the watchdog timer has not been reset previously by the firmware).

Set image OK (Swap mode only)

After a swap upgrade is completed, the new image updates the flash contents to mark itself "**OK**", so the bootloader can choose to run it during the next boot. On a startup, the bootloader inspects the flash contents to decide if swapping of the application images was completed.

Depending on the use case, the swap can also be made permanent directly (by setting the “image OK” flag during the image signing). In this case, the bootloader will never attempt to revert the images on the next reset.

Note In a multi-image case, the bootloader considers “image OK” flags of each image separately, so both user applications must set the “image ok” flag in their own areas because they consider the image OK flags of images separately.

Upgrade image (Secondary Slot)

The memory location to stage code for the CM0+ upgrade.

Upgrade enabled

If checked, firmware upgrades are allowed.

External memory

Specifies the SMIF ID (if any) to upgrade the image. The options:

- 0 – SMIF Disabled
- Slave Select – 1
- Slave Select – 2
- Slave Select – 3
- Slave Select – 4

Start address

The location (Secondary/Slot 1) where the upgrade firmware is stored or staged prior to the bootloader transferring it to the Primary Slot.

Slot size (bytes)

The size of the upgraded image.

Encrypt upgrade image

This check box determines if the upgrade image must be encrypted

Image encryption key ID

Specifies the key to use the upgrade image encryption.

- Unique Device Key (ID 1)
- Group Encryption Key (ID 12)

Encrypt peer key path

The path to the public key file for image encryption. The key is of the Elliptic Curve Digital Signature Algorithm (ECDSA) type; the file is of the Privacy Enhanced Mail (PEM) format.

Protected SRAM (Configuration and CM0+Tabs)

Indicates the memory region for the secure CM0+ CPU. The user must not change this from the default unless the CM0+ code has been changed for a special case.

Address

The start address of the Protected SRAM location.

Size (bytes)

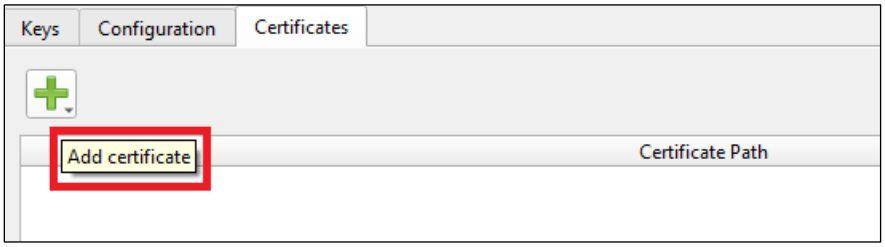
The size of the Protected SRAM region.

Certificates Tab

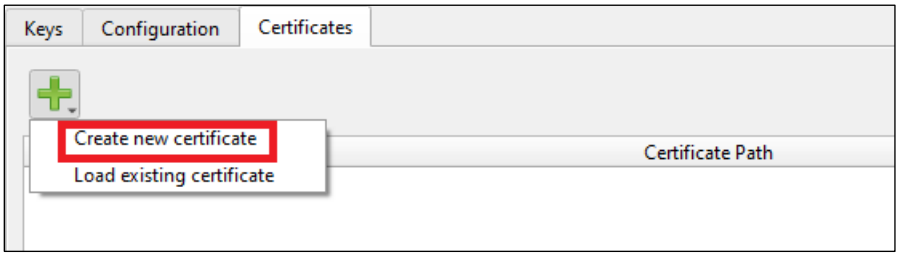
This tab is used to create and add certificates.

Add certificate

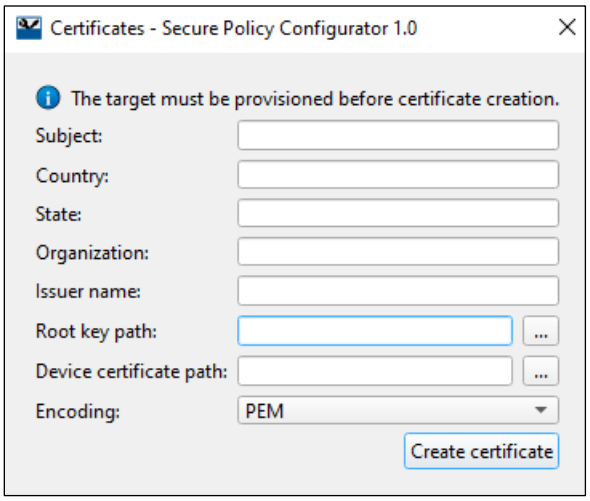
Clicking the **Add Certificate** button provides the user with the options to obtain a certificate.



Create new certificate



Choosing the “Create new certificate” option displays the Certificates window.



Providing a new public key certificate ensures the secure communication over the Internet. Certificate creation will be skipped if a certificate file already exists.

Note Certificate creation cannot be executed if the target device is not provisioned.

The user completes the following fields:

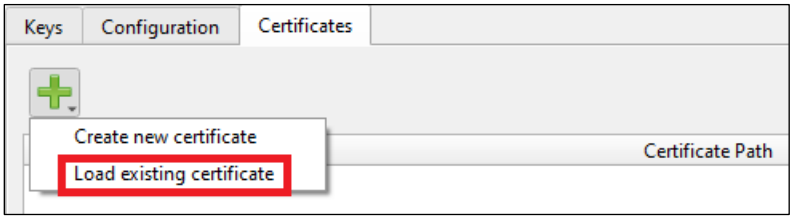
- **Subject** – The title for the certificate.
- **Country** – The name of the country where the certificate is issued.
- **State** – The name of the state where the certificate is issued.
- **Organization** – The name of the organization where the certificate is issued.
- **Issuer name** – The name of the person by whom the certificate is issued.
- **Root key path** – The path to the private key file.
- **Device certificate path** –The location to store the created certificate.
- **Encoding** – Displays the format of the certificate to be created – PEM or DER. The default is PEM.

Note The Subject, Country, State, Organization, and Issuer name parameters must include only alphanumeric symbols.

After completing the fields, click the **Create certificate** button to add a new entry to the certificates table.

Load existing certificate

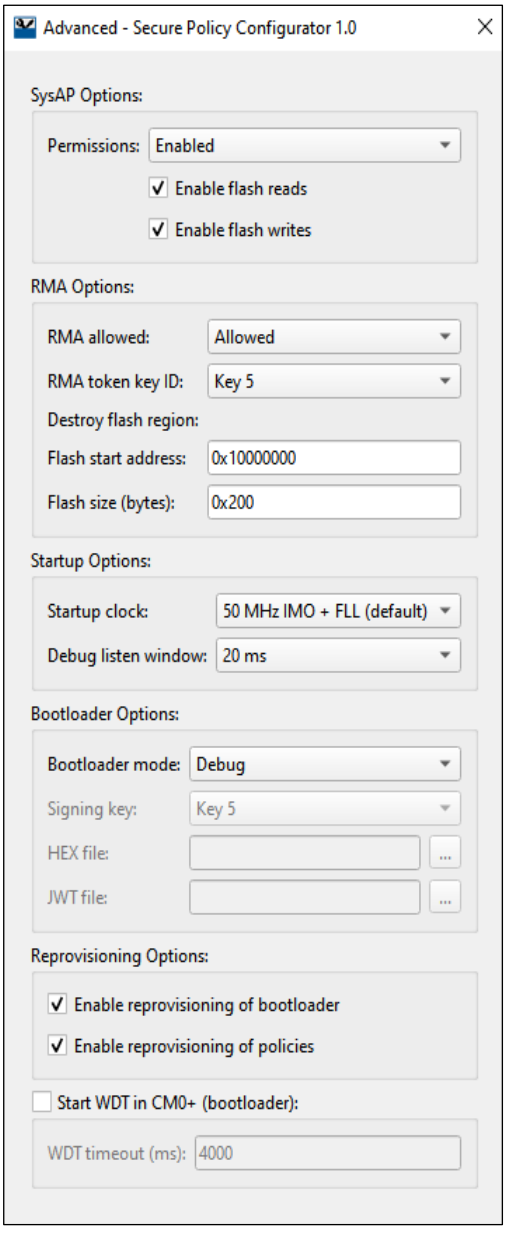
Choosing the “Load existing certificate” option displays a file dialog box to allow the user to select an-existing certificate file.



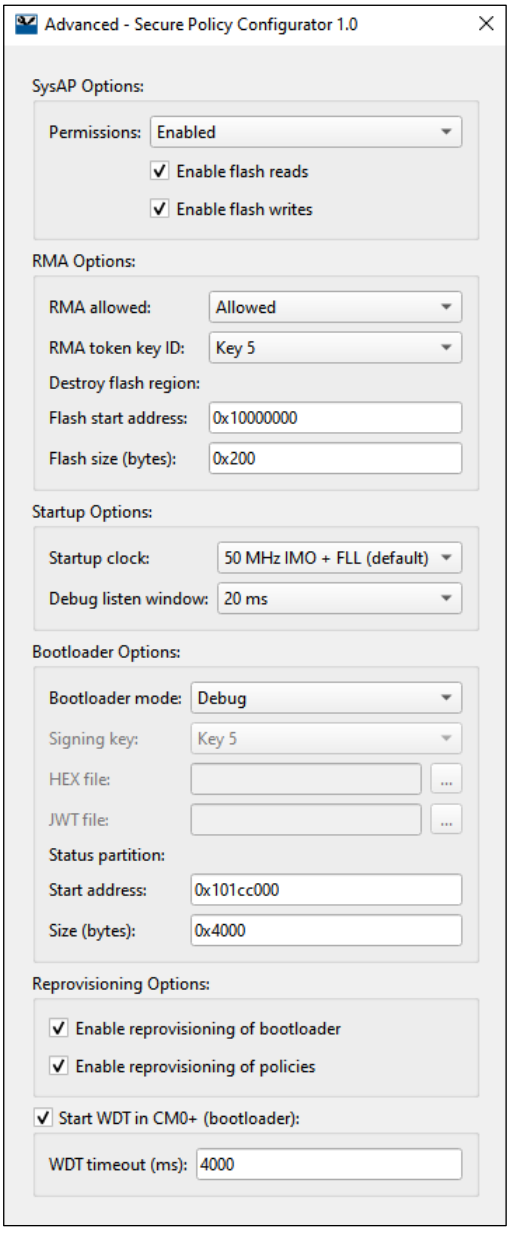
Advanced Dialog

The Advanced dialog contains the parameters used for editing policy files. Two versions of the Advanced dialog display depending on the selected policy file: for Overwrite and Swap upgrade modes. For Swap mode, select a policy file with the `swap` suffix.

Overwrite Mode



Swap Mode



The following describe the configuration parameters available in the Advanced dialog.

Note Some of them display only under operation in Swap mode (specified).

SysAP Options

These options configure the system access port.

Permissions

- **Enabled** –Always enabled. The default option – debugging of the CM4 application is always allowed.
- **Disabled** – Always disabled. Debugging of the CM4 application is never allowed.
- **Allowed** – Controlled by the firmware.

Note Leaving the SysAP in production will create a security risk.

Enable flash Reads

If checked, the SysAP can read the flash memory.

Enable flash writes

If checked, the SysAP can write the flash memory.

RMA Options

These options control if RMA is allowed, which key to use, and what memory to be erased.

RMA allowed

Enables or disables the RMA process.

- **Enabled** – Always enabled.
- **Disabled** – Always disabled.
- **Allowed** – Controlled by the firmware.

RMA token key ID

Key IDs of the RMA certificate keys.

Destroy flash region

If there are secrets in the user's flash, the Destroy Flash region option allows erasing the user's secrets in flash to prevent their disclosure.

Note This option does not destroy the device; it merely erases flash.

Flash start address

Configures the range of flash to be erased during the RMA process.

Flash size (bytes)

Configures the range of flash to be erased during the RMA process.

Startup Options

Startup clock

Configures the initial clock speed.

Debug listen window

Configures the amount of time the device waits for an SWD command during the startup.

Bootloader Options

Bootloader mode

Configures the debugging output.

- **Debug** – The bootloader produces debugging messages.
- **Release** – The bootloader does not produce debugging messages.
- **Custom** – This enables the user to build their own bootloader and provision it. This feature is not currently supported.

Signing key

The private key to sign the booloader certificate.

HEX file

The bootloader application/program file.

JWT file

The booloader certificate file.

Status partition (Swap mode)

Extra flash area to store the Swap status for the upgrade and revert images.

Start address

The start address of the Swap status area.

Size (bytes)

The size of the Swap status area.

Reprovisioning Options

- **Enable reprovisioning of bootloader** – Check this box to enable the bootloader reprovisioning. This allows the OEM to update the bootloader at a later date (not only during development).
- **Enable reprovisioning of policies** – Check this box to enable the policy reprovisioning. This allows the OEM to reprovision policies at a later date.

Start WDT in CM0+ (bootloader)

This watchdog timer is used to protect the device from freezing after updating with an incorrect CM0+ image. If this check box is enabled for the bootloader, the timer is used to reset the device and revert to the previous image. This setting applies only to the bootloader, and it is separate from the Start WDT setting on the Configuration tab.

WDT timeout (ms)

The parameter to define the time after which the device resets automatically (if the watchdog timer has not been reset previously by the firmware).

References

Refer to the following documents for more information, as needed:

- Eclipse IDE for ModusToolbox User Guide
- API Reference Guides
- Device Datasheets
- Device Technical Reference Manuals
- PSoC® 64 Secure MCU Secure Boot SDK User Guide
- KitProg3 User Guide

Version Changes

This section lists and describes the changes for each version of this tool.

Version	Change Descriptions	Notes
1.0	New tool.	