ModusToolbox™ Edge Protect Configurator user guide

Edge Protect Configurator version 1.41.0

About this document

A newer revision of this document may be available on the web here.

Scope and purpose

The Edge Protect Configurator is a stand-alone tool included with the ModusToolbox™ software intended to configure the TF-M library.

Intended audience

This document helps application developers understand how to use the Edge Protect Configurator as part of creating a ModusToolbox™ application.

Document conventions

Convention	Explanation
Bold	Emphasizes heading levels, column headings, menus and sub-menus
Italics	Denotes file names and paths.
`Courier New`	Denotes APIs, functions, interrupt handlers, events, data types, error handlers, file/folder names, directories, command line inputs, code snippets
File > New	Indicates that a cascading sub-menu opens when you select a menu item

Abbreviations and definitions

The following define the abbreviations and terms used in this document:

- TF-M – trusted firmware M
- RoT – root of trust
- PSA – platform security architecture
- Application – One or more projects related to each other.
- Configurator – A GUI-based tool used to configure a resource.
- Partition – A software development unit that contains services with the similar functionality.
- App RoT – The security domain in which additional security partitions are implemented.
- PSA RoT – Defines the most trusted security domain within a PSA system.

Reference documents

Refer to the following documents for more information as needed:

- ModusToolbox™ tools package user guide

About this document

- Eclipse IDE for ModusToolbox™ user guide
- VS Code for ModusToolbox™ user guide
- Device Configurator user guide
- TF-M Documentation
- Infineon TF-M Documentation

Table of contents

1 Overview 4

1.1 Supported libraries 4

2 Launch the Edge Protect Configurator 5

2.1 VS Code and Eclipse 5
2.2 From the Device Configurator 5
2.3 make command 5
2.4 Executable (GUI) 6
2.5 Executable (CLI) 6

3 Quick start 7

3.1 Update existing configuration 7
3.2 Create new configuration 7

4 GUI description 8

4.1 Menus 8
4.2 Toolbar 9
4.3 Notice List 9
4.4 Status bar 9
4.5 Logging 9

5 Tabs 10

5.1 General tab 10
5.2 TF-M Partitions and Domains tab 11
5.3 Parameters tab 11
5.4 Dependencies tab 11

6 Parameter configuration 12

6.1 Partitions/Domains 12
6.2 Creating a new TF-M partition 12
6.3 Configuring a custom partition 13
6.4 Generating files for a custom TF-M partition 14
6.5 Importing existing TF-M partitions 14

7 Edge Protect Solution 15

7.1 Protection configuration 15
7.2 Memory configuration 15
7.3 Peripheral configuration 16

8 Code generation 17

8.1 Top-level configuration file 17
8.2 Custom partition files 17

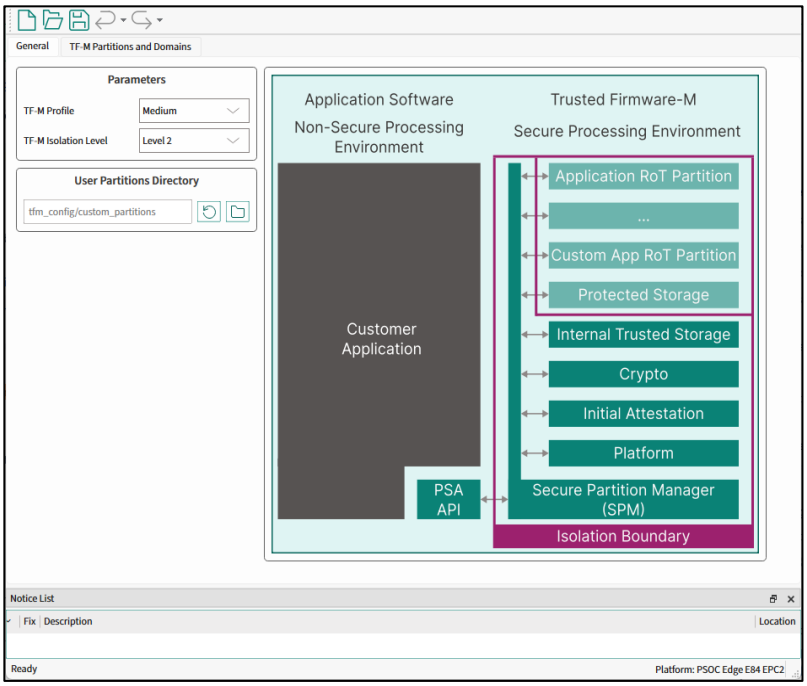
9 Troubleshooting 18

10 Version changes 19

Revision history 20

1 Overview

The Edge Protect Configurator provides a GUI to configure the TF-M library in a way that displays only the options necessary for TF-M operation.



1.1 Supported libraries

Library	Version
`ifx-tf-m-pse84epc2`	2.1
`ifx-tf-m-pse84epc4`	2.1
`ifx-tf-m`	2.3

2 Launch the Edge Protect Configurator

There are several ways to launch the Edge Protect Configurator, and those ways depend on the application, and how you use the various tools.

2.1 VS Code and Eclipse

VS Code and Eclipse have tools to launch the Edge Protect Configurator from within an open application. Refer to the applicable user guide for more details:

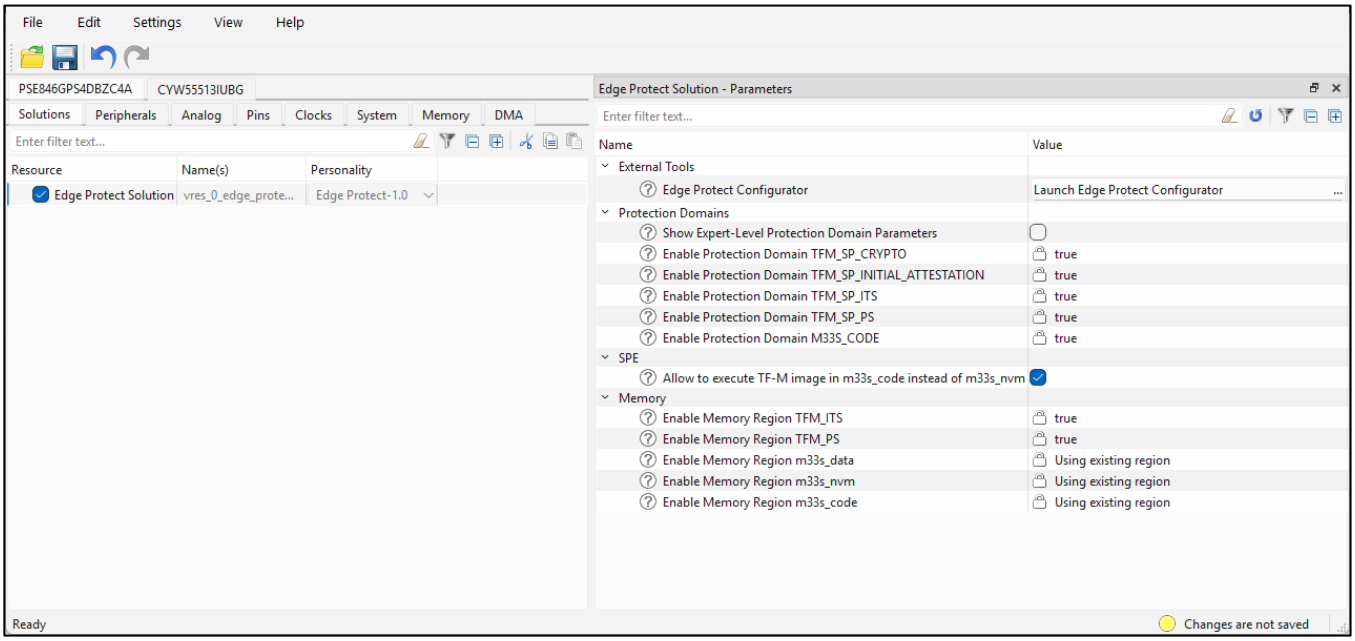
- VS Code for ModusToolbox™ user guide
- Eclipse IDE for ModusToolbox™ user guide

2.2 From the Device Configurator

Launch the Device Configurator. (For details, refer to the Device Configurator user guide.)

On the **Solutions** tab:

1. Enable **Edge Protect Solution**.
2. On the **Parameters** pane, click the **Launch Edge Protect Configurator** button.



2.3 make command

As described in the ModusToolbox™ tools package user guide "ModusToolbox™ build system" chapter, you can run numerous `make` commands in the application directory, such as launching the Edge Protect Configurator. After you have created a ModusToolbox™ application, navigate to the application secure project directory and type the following command in the appropriate bash terminal window:

```
make edge-protect-configurator
```

This command opens the Edge Protect Configurator GUI for the specific application in which you are working.

2.4 Executable (GUI)

You can launch the Edge Protect Configurator GUI by running its executable as appropriate for your operating system (for example, double-click it or select it using the Windows **Start** menu). By default, the Configurator is installed in the Edge Protect Security Suite or relevant Early Access Pack installation directory:

<Suite or Pack Installation Directory>/tools/edge-protect-configurator

When launched this way, the Edge Protect Configurator opens without any configuration file. You can either open a specific configuration file or create a new one.

2.5 Executable (CLI)

The Edge Protect Configurator executable can be run from the command line, and it also has a "cli" version of the executable as well. Running configurator executables from the command line can be useful as part of batch files or shell scripts to re-generate the source code based on the latest configuration settings. The exit code for the executable is zero if the operation is successful, or non-zero if the operation encounters an error. For more information about the command-line options, run the executable using the -h option.

3 Quick start

This section provides a simple workflow for how to use the Edge Protect Configurator for generic use cases.

3.1 Update existing configuration

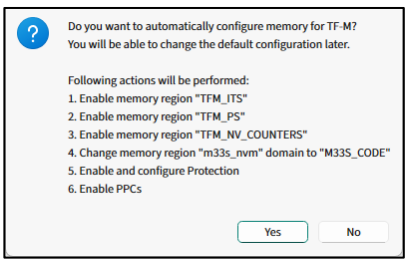
This use case assumes you have a preconfigured application with Edge Protect Configurator configuration that you want to change.

1. Launch the Edge Protect Configurator from Eclipse IDE for ModusToolbox™ Quick Panel or standalone.
2. Configure the parameters as required.
3. Save the Edge Protect Configurator configuration. See Code generation.
4. Open the Device Configurator and navigate to the **Solutions** tab
5. Click the Edge Protect Solution and configure the parameters as required.
6. Save the Device Configurator configuration.
7. The TF-M library automatically uses the configuration generated by the Edge Protect Configurator and the Device Configurator.

3.2 Create new configuration

This use case assumes you have an existing application into which you want to add and configure the TF-M library.

1. Open the Library Manager for your existing application and add libraries to a secure project (usually proj_cm33_s) and a non-secure project (usually proj_cm33_ns).
   - Secure project - ifx-tf-m, ifx-tf-m-port
   - Non-Secure project - ifx-tf-m-ns
2. Launch the Edge Protect Configurator. The Configurator uses a standard configuration with all TF-M partitions enabled.
3. Optionally, apply the standard TF-M configuration of memory and peripheral resources. Select **No** if you want to apply it later, after you have finished with TF-M partition selection.



4. Enable the desired partitions on the **TF-M Partitions and Domains** tab.
5. Optionally create custom partitions.
6. Save the configuration and resolve the remaining tasks (if any) in the Device Configurator.

4 GUI description

The Edge Protect Configurator GUI contains menus and tabs to configure the TF-M library and a Notice List to provide indications.

4.1 Menus

4.1.1 File

- **New** – Click this to create a new file with new configuration.
- **Open…** – Opens a specified **.edgeprotect* configuration file. The current configuration file, if any, will be closed. If there are unsaved changes, a dialog opens asking to save or not.
- **Save** – Saves the existing configuration.
- **Save As…** – Saves the existing file under a different name in the specified location.
- **Close** – Closes the current configuration file**.**
- **Open in System Explorer** – Opens file explorer with the folder that contains the **.edgeprotect* file.
- **Import…** – Imports a specified configuration file.
- **Export…** – Exports the current configuration file into a specified file.
- Recent files – Shows recent files that you can open directly.
- **Exit** – Closes the Configurator.

4.1.2 Edit

- **Undo** – Undoes the last action or sequence of actions.
- **Redo** – Redoes the last undone action or sequence of undone actions.
- **Reset Configuration** – Resets the current configuration.
- **Regenerate All Custom Partitions** – Regenerate files of all custom partitions in the configuration.

4.1.3 View

- **Notice List** – Shows/hides the Notice List.
- **Toolbar** – Shows/hides the toolbar.
- **Reset View** – Resets the view to the default.

4.1.4 Settings

- **ModusToolbox settings…** – Opens the "ModusToolbox settings" window for editing.
- **Analytics**… – Opens the Analytics Permission dialog.

4.1.5 Help

- **View Help** – Opens this document.
- **About Edge Protect Configurator** – Opens the **About** box for version information, with links to open https://www.infineon.com and the current session log files.

4.2 Toolbar

The toolbar contains common commands from the **File** and **Edit** menus. Use the check box under the **View** menu to show or hide the toolbar.

4.3 Notice List

The **Notice List** pane combines notices (errors, warnings, tasks, and notes) from many places in the configuration into a centralized list. If a notice shows a location, you can double-click that entry to display the parameter causing the error or warning.

The Configurator also displays notices from the Device Configurator related to the Edge Protect Solution in the “Device Configurator” location.

For more information, refer to the Device Configurator user guide.

4.4 Status bar

The **Status bar** displays the current platform and the Configurator status.

4.5 Logging

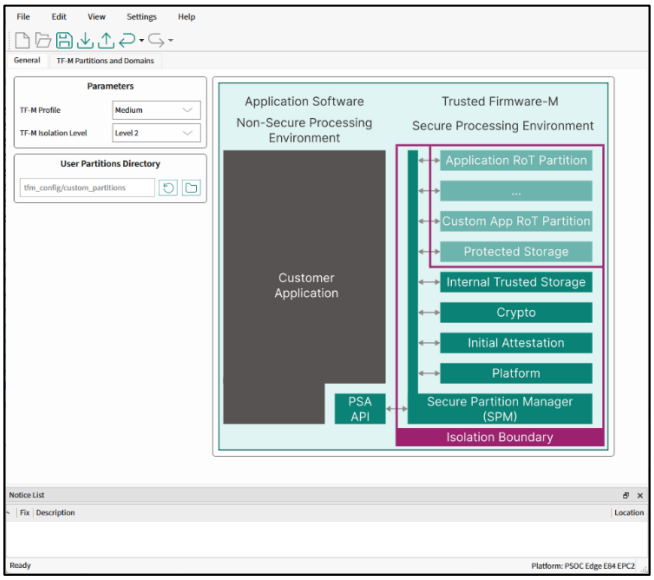
The Configurator automatically generates a log for each session. The file location differs for each operating system and can be found in the **About** dialog. Additionally, the location of the hardware-config-server log file is provided.

5 Tabs

- General
- TF-M Partitions and Domains

5.1 General tab

The **General** tab contains the most basic TF-M parameters and visualization of how TF-M partitions are isolated depending on the chosen TF-M Isolation Level.



Parameters

- **TF-M Profile** – Specifies a list of features for some hardware constraints supported by the TF-M library.
- **TF-M Isolation Level** – Specifies how secure partitions will be isolated.

User Partitions Directory

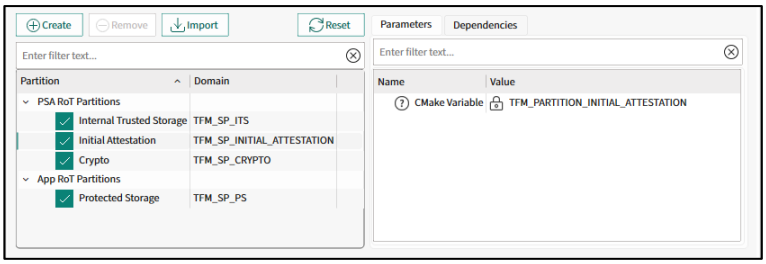
- Path – Displays where custom partitions are stored relative to the configuration file. Non-editable.
- Buttons:
  - **Reset** – Restores the original directory.
  - **Pick** – Picks a new directory.

Isolation Level visualisation

Illustrates the isolation between the application and TF-M partitions.

5.2 TF-M Partitions and Domains tab

The **TF-M Partitions and Domains** tab is used to configure TF-M partitions and their parameters.



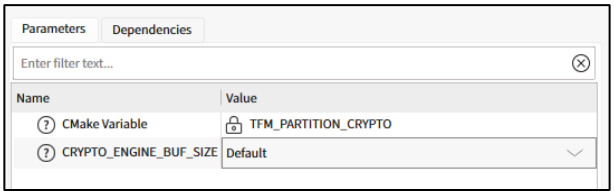
Buttons bar:

- **Create** – Creates a new custom partition.
- **Remove** – Removes the selected partition.
- **Import** – Imports partitions from a manifest-list file.
- **Reset** – Resets the partition selection to default.

The tab contains the **Partitions** tree and the **Parameters** and **Dependencies** subtabs. Check the corresponding box to enable a partition. Observe the partitions parameters in the **Parameters** pane. Hover over the question mark  to display the tooltips.

5.3 Parameters tab

The **Parameters** tab displays the parameters for the selected partition and the message "Select the enabled partition to configure it". The set of parameters and their editability may change depending on the selected partition.

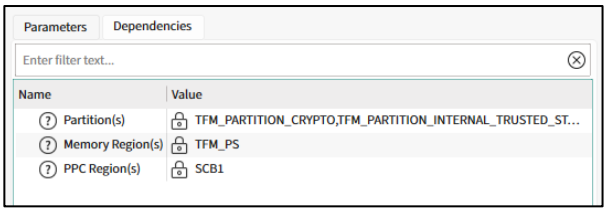


You can configure the memory region on the Device Configurator **Memory** tab.

5.4 Dependencies tab

The **Dependencies** tab displays the selected partition dependencies. These include the other partitions required for the selected partition operation and assigned memory and PPC regions.

The memory and PPC regions can be assigned in the Device Configurator Memory and System tabs.



6 Parameter configuration

6.1 Partitions/Domains

Initially, the **Partitions** tree contains the selection of standard TF-M partitions for the current platform (e.g. PSOC Edge E84 EPC2). Each TF-M partition has its own Protection Domain, responsible for memory, peripherals, and protection configuration.

The partition's Protection Domain is automatically created if the partition is enabled or removed if disabled.

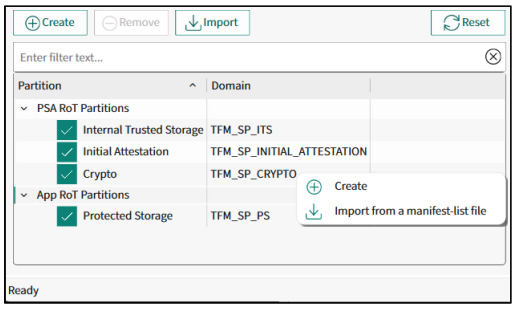
Note: *When you disable a partition, it also removes the Protection Domain in the Device Configurator and unassigns memory and peripheral resources from the removed domain. Enable the partition again to assign them back by: a) applying the proposed fixes from the Edge Protect Configurator and the Device Configurator Notice Lists; b) manually on the Device Configurator **Memory** and **System** tabs.*

Note: *The Edge Protect Configurator does not provide automatic memory and peripheral assignment fixes for custom partitions.*

Refer to the Protection resource documentation, accessible from the Device Configurator, for Protection Domain configuration details.

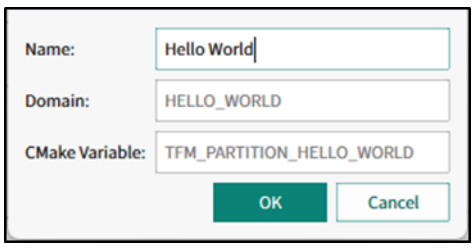
6.2 Creating a new TF-M partition

To create a new custom TF-M partition, click the **Create** button above the partitions tree widget or right-click the **App RoT Partitions** tree group and select **Create** on the opened menu.



In the opened dialog, fill in the partition name. Follow the Configurator guidance on the partition naming, as some character combinations are not allowed.

The Domain name and the CMake variable name will be calculated automatically based on the name. The CMake variable name can be changed later on the **Parameters** pane. The **Protection Domain** name cannot be changed due to the TF-M library constraints.



Click **OK** to add the partition to the tree and the related **Protection Domain** will be created in the Device Configurator.

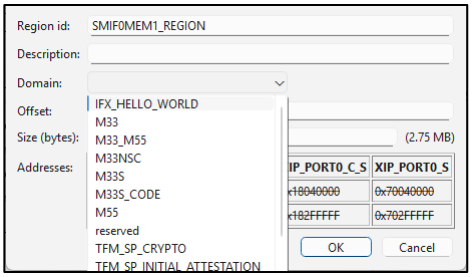
6.3 Configuring a custom partition

By default, the created custom partition accesses neither peripheral nor memory resources. If your partition does not need such access, do not configure it any further.

If you want to access specific memory and peripherals from your partition, add them to the relevant **Protection Domain** first. The name of the domain for your partition is available in the “Domain” column. The Edge Protect Configurator automatically creates the domain in the Device Configurator.

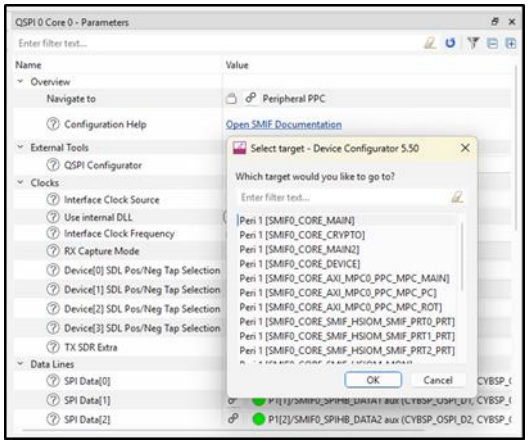
6.3.1 Adding memory regions to a custom partition

To assign memory regions to a custom partition, open the Device Configurator, navigate to the **Memory** tab and click the **+** button in any memory bank. Then select your partition's domain in the **Domain** drop-down.



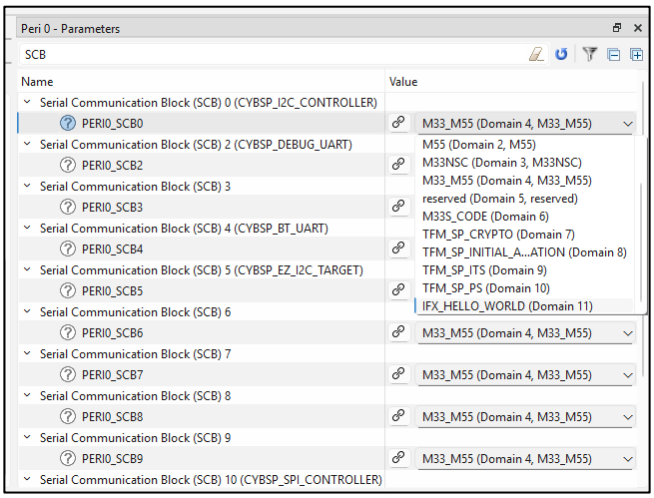
6.3.2 Adding peripherals to a custom partition

To assign a peripheral to a custom partition, you will need to know which PPC regions correspond to your peripheral. To find the PPC regions, which correspond to your peripheral resource, select the resource in the Device Configurator and then, on the Parameters pane, click the **Peripheral PPC** link. The list of PPC regions may vary among the peripherals.



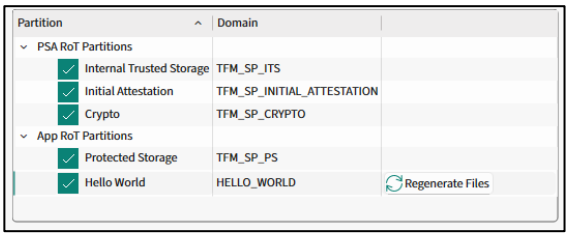
Parameter configuration

Once you find the required PPC regions, open the **System** tab, select the Peri 0 or Peri 1 resource, and assign the required regions to your partition's domain on the drop-down.



6.4 Generating files for a custom TF-M partition

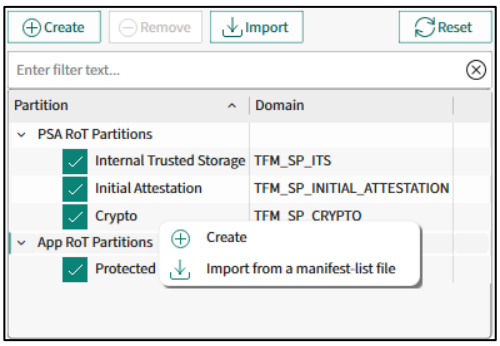
You can generate files for the newly created partition by clicking the **Generate Files** button or by saving the configuration.



You can reset the partition files by clicking **Regenerate Files** in the partition row.

6.5 Importing existing TF-M partitions

You can import the existing TF-M partitions to the Configurator either by clicking **Import** over the partitions tree or selecting the **Import from a manifest-list file** option on the partition tree right-click menu.

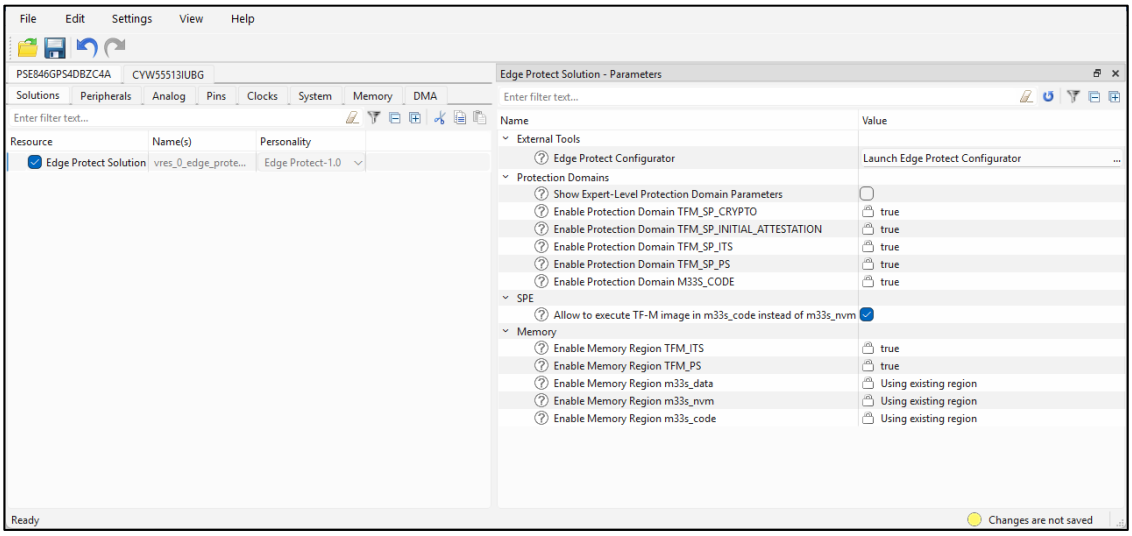


Select a tf-m manifest-list file in the opened dialog and click **Open**. The Configurator imports partitions from the file into the configuration and copies their files to the custom partitions directory.

Note: Only App RoT partitions will be imported because of the TF-M library restrictions.

7 Edge Protect Solution

The Edge Protect Configurator configures memory and peripherals for the TF-M library with the help of the Edge Protect Solution personality.



The **Edge Protect Solution** is a Device Configurator personality that assists with the configuration of memory, peripherals, and their protection. The personality is available on the **Solutions** tab of the Device Configurator.

Note: *The personality is available only when the TF-M library is added to your project.*

Note: *The Edge Protect Configurator works only when the personality is available and enabled in the Device Configurator.*

7.1 Protection configuration

The **Edge Protect Solution** automatically creates Protection Domains for all TF-M partitions. A **Protection Domain** is required for the proper memory and peripheral isolation for a partition. Also, it acts as the connection point between the TF-M partitions and hardware configuration.

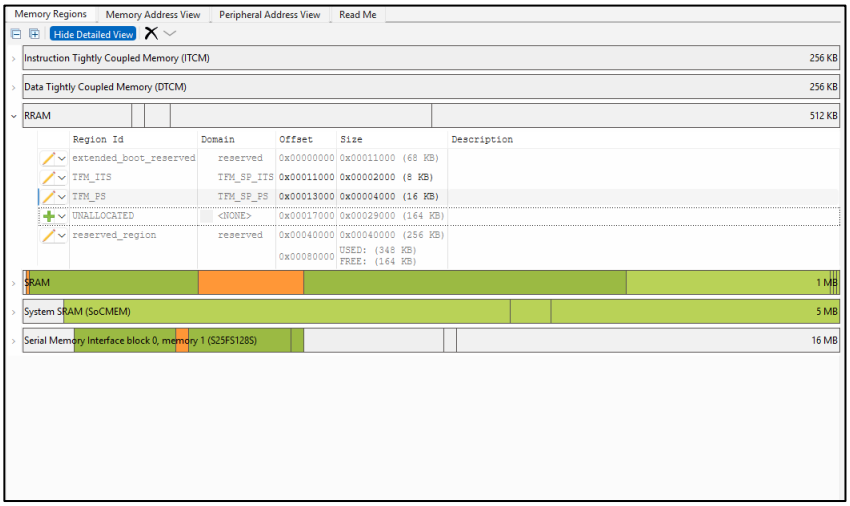
Refer to the "Protection resource" documentation, accessible from the Device Configurator, for Protection Domain configuration details.

7.2 Memory configuration

The **Edge Protect Solution** may propose to configure memory, peripherals, and protection resources in the Device Configurator, depending on the Edge Protect Configurator configuration.

You can apply the **Edge Protect Solution** suggestions from both the Edge Protect Configurator and the Device Configurator. Further memory configuration is available only on the Device Configurator **Memory** tab.

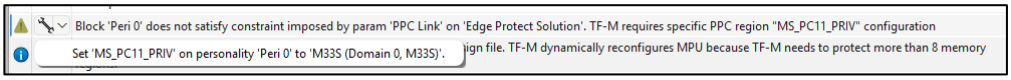
Edge Protect Solution



7.3 Peripheral configuration

The TF-M library requires a specific peripheral configuration for its operation. You can apply such configuration automatically with the help of the Edge Protect Solution.

The Edge Protect Solution offers to update the Peri block configuration depending on your TF-M partition selection in the Edge Protect Configurator. The fixes are available on the Device Configurator Notice List.



To view the PPC configuration, open the Device Configurator, navigate to the **System** tab, and select the Peri resource. You will see the PPC regions configuration on the **Parameters** pane, similar to how it is depicted in Adding peripherals to a custom partition.

8 Code generation

This section describes various files that are generated by the Edge Protect Configurator.

8.1 Top-level configuration file

The Edge Protect Configurator generates a *tfm_config.cmake* file in the <BSP>/config/tfm_config/ folder. The TF-M library automatically includes this file in its build. The file contains parameters from **General** and **TF-M Partitions and Domains** tabs. This file is regenerated automatically on save. Do not edit it manually.

8.2 Custom partition files

The Configurator generates a set of stub files for custom partitions. These files contain the most basic implementation of a custom TF-M partition. The files are not regenerated automatically. You can edit them manually.

Note: *You can select any name for the partition but hereinafter file name references assume it is named "Hello World".*

8.2.1 Partition manifest

The *hello_world.json* file describes the partition and partition properties. See TF-M documentation reference.

8.2.2 Partition CMake

The *CMakeLists.txt* file contains the CMake script to build the partition. See TF-M documentation reference.

8.2.3 Partition API header

The *hello_world_api.h* file declares the function, which does a PSA call to request the secure partition from a non-secure application.

8.2.4 Partition API source

The *hello_world_api.c* file defines the function, which does a PSA call to request the secure partition from a non-secure application.

8.2.5 Partition definitions header

The *hello_world_defs.h* file contains constants, structures, and macros that can be used both secure and non-secure worlds for partition implementation.

8.2.6 Partition manager source

The *hello_world_mngr.c* file defines the function for the partition initialization and PSA call router to the secure partition.

9 Troubleshooting

Problem	Workaround
Import... erases the memory and peripheral configuration of all partitions.	Configure the memory and peripheral resources after the import via the Notice List fixes both in the Edge Protect and Device Configurators.
On Ubuntu versions 22.04 and 24.04, the Edge Protect Configurator may display the "... is not responding" window.	Increase the application response timeout. Enter the following command in the terminal: `gsettings set org.gnome.mutter check-alive-timeout 60000`
Using menu **Edit > Reset Configuration** does not erase protection domains of the custom partitions in the Device Configurator.	First, add a custom partition, then remove it. Alternatively, create a new configuration using **File > New** and replace the current configuration.
On macOS, link "Location on Disk" does not open in a custom partition that was not generated.	Save the configuration or generate the partition files.
In the Device Configurator, the Edge Protect Solution personality proposes moving a memory region to the non-existing memory `SOCMEM_RAM`.	To move the memory region back to the existing memory, click the wrench icon next to the notice "Physical memory `SOCMEM_RAM` does not exist but has memory regions allocated to it" and select the relevant memory from the drop-down list.

10 Version changes

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

Version	Change descriptions
0.10	New tool. PSOC™ Edge 84 Early Access Pack 0.2.4.
1.0	Updated for PSOC™ Edge E84 Early Access Pack 0.3.2: • Added PSOC Edge E84 EPC4 platform support • Added the platform selection dialog • Added platform auto-detection
1.10	Updated for PSOC™ Edge 84 Early Access Pack 0.3.3: • Fixed wrong variable name in the generated code • Added support of Edge Protect Solution personality from the Device Configurator • Added memory configuration and protection support via Edge Protect Solution • Removed Firmware Update Service • Added TF-M Isolation Level visualization to the General tab
1.20	Updated for Edge Protect Security Suite: • Added support of custom TF-M services • Added support of protection domains configuration via Edge Protect Solution • Added support of automatic PPC configuration via Edge Protect Solution
1.30	Updated for PSOC™ Control C3-P8 Early Access Pack, added: • Support of App RoT partitions import • Support of the user-defined custom partitions directory • Dependencies tab
1.40	Updated for PSOC™ Control C3-M6: • Added Analytics collection • Minor UI improvements
1.41	Updated for PSOC™ Control C3-M6: • Minor bug fixes and UI improvements

Table of contents

Revision history

Revision	Date	Description
**	2024-05-15	New document. PSOC™ Edge 84 Early Access Pack 0.2.4.
*A	2024-05-30	Content update.
*B	2025-04-28	Updated to version 1.10.
*C	2025-09-03	Updated to version 1.20.
*D	2025-10-13	Minor update.
*E	2026-04-01	Updated to version 1.30.
*F	2026-08-31	Updated to version 1.40.
*G	2026-09-21	Updated “Troubleshooting” section.
*H	2026-10-30	Updated to version 1.41.

Trademarks
All referenced product or service names and trademarks are the property of their respective owners.

Edition 2026-10-30

Published by

Infineon Technologies AG

81726 Munich, Germany

© 2026 Infineon Technologies AG. All Rights Reserved.

Do you have a question about this document?

Email: erratum@infineon.com

Document reference

002-39923 Rev. *H

Important notice
The information given in this document shall in no event be regarded as a guarantee of conditions or characteristics (“Beschaffenheitsgarantie”)

With respect to any examples, hints or any typical values stated herein and/or any information regarding the application of the product, Infineon Technologies hereby disclaims any and all warranties and liabilities of any kind, including without limitation warranties of non-infringement of intellectual property rights of any third party.

In addition, any information given in this document is subject to customer’s compliance with its obligations stated in this document and any applicable legal requirements, norms and standards concerning customer’s products and any use of the product of Infineon Technologies in customer’s applications.

The data contained in this document is exclusively intended for technically trained staff. It is the responsibility of customer’s technical departments to evaluate the suitability of the product for the intended application and the completeness of the product information given in this document with respect to such application.

Warnings
Due to technical requirements products may contain dangerous substances. For information on the types in question please contact your nearest Infineon Technologies office.

Except as otherwise explicitly approved by Infineon Technologies in a written document signed by authorized representatives of Infineon Technologies, Infineon Technologies’ products may not be used in any applications where a failure of the product or any consequences of the use thereof can reasonably be expected to result in personal injury.