UG10241

MCUXpresso 安全配置快速入门指南

Rev. 2.0 — 10 October 2025 **User guide**

Document information

Information	Content
Keywords	MCUXpresso 安全配置工具
Abstract	MCUXpresso Secure Provisioning Tool (SEC，MCUXpresso 安全配置工具）是一个旨在简化 NXP MCU 平台上可启动的可执行文件的生成和配置过程的 GUI 工具。它建立在由 NXP 提供的、经验证的且成熟稳定的安全特性布署工 具集之上，并利用了 BootROM 提供的丰富的编程接口。

1 概述

本快速入门指南提供了分步概述，帮助您高效地安装、配置和开始使用 MCUXpresso 安全配置工具。无论您是安全启动和加密工作流程的新手，还是希望将安全配置集成到您的生产流程中，本指南都将帮助您快速入门。

MCUXpresso 安全配置工具（SEC 工具）是 NXP 开发的一款功能强大的实用程序，用于简化嵌入式设备的安全配置。该工具旨在支持各种 NXP 微控制器，使开发人员能够配置安全功能、生成加密密钥并以最少的设置安全地编程设备。

2 硬件要求

- 建议从 NXP 的参考设计板（FRDM/EVK）开始。
- Secure Provisioning Tool Release Notes 列出了启动安全配置工具的详细要求。

3 软件要求

MCUXpresso 安全配置工具可以在 Windows、Linux 或 Mac 操作系统上执行。Secure Provisioning Tool Release Notes 列出了详细要求。

4 安装并配置 SEC 工具

安全配置工具安装程序适用于 Windows、Linux 或 Mac 操作系统，可从 NXP 安全配置网站下载。对于 Windows 和 Mac 操作系统，安装程序以向导的形式引导您逐步完成安装过程。Debian 软件包可用于 Linux。 有关安装的详细信息，请参阅 Secure Provisioning Tool User Guide。

5 使用工具

5.1 前提条件

作为该工具的输入，使用在处理器上运行的应用程序二进制文件（S19、HEX、ELF/AXF 或 BIN 文件格式）。根据启动设备，为 RAM 或 Flash 构建应用程序。建议从任何 MCUXpresso SDK 示例开始，该示例已预先配置了正确的地址。 在使用安全配置工具之前，请在调试器中运行应用程序并检查它是否按预期工作。

对于 FRDM 和 EVK 板，提供了二进制形式的示例应用程序，通常会使板载 LED 闪烁。即使您还没有任何特定的应用程序，它也可以用于评估工具功能。

要将应用程序加载到开发板中，请将开发板切换到 In-System-Programming (ISP) 模式。有关如何执行此操作的详细信息，请查阅开发板文档或处理器参考手册。

5.2 新工作区

当您第一次启动安全配置工具时，它会要求您创建一个新的工作区，该文件夹包含项目所需的所有文件。您也可以稍后使用命令创建新的工作区：**main menu > File > New Workspace**。

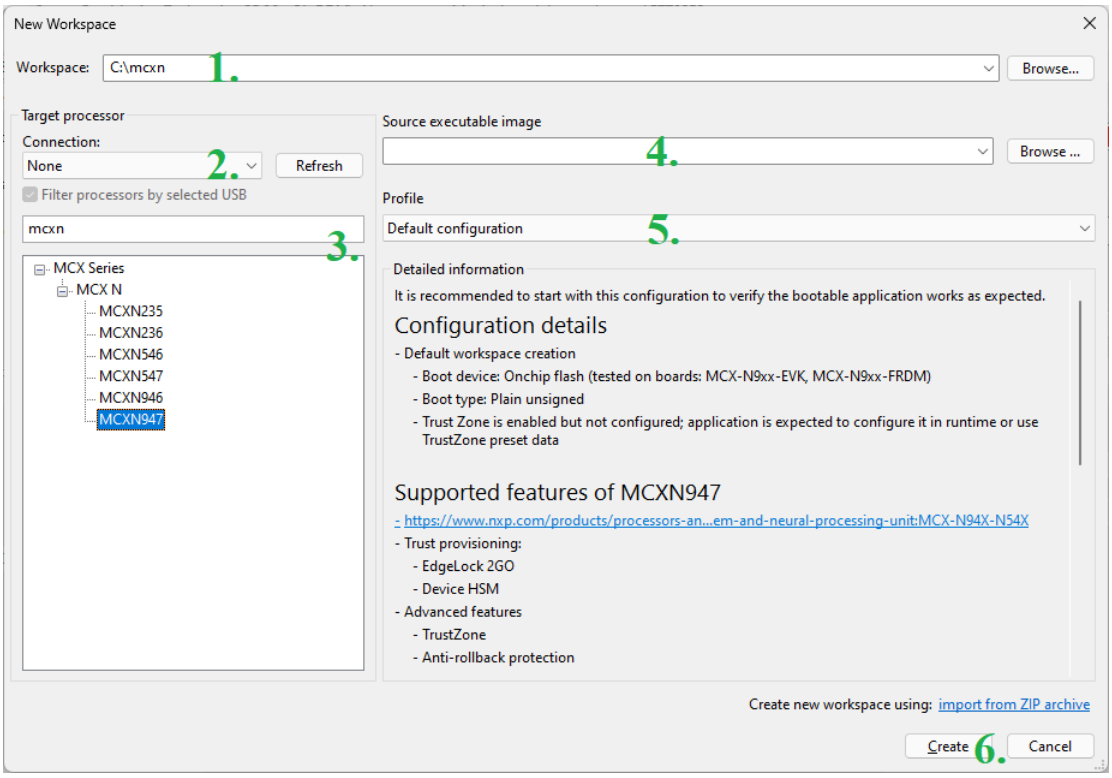

Figure 1. 新工作区

要创建工作区，请填写以下参数：

1. 选择磁盘上的工作区路径。建议为每个项目创建一个新文件夹。
2. 将设备连接到您的计算机并选择使用的连接，例如 UART COM 端口或 USB。使用 USB 连接，该工具可以自动选择处理器系列。
3. 可以直接从树中选择处理器或使用搜索栏。也可以使用开发板名称来查找处理器。
4. 选择应用程序的路径作为源可执行镜像（image）。
   注意： 对于 NXP 开发板，该工具包含可从下拉列表中选择的预编译 SDK 示例。
5. 要验证应用程序的构建和写入过程，请使用应用程序代码未签名且纯文本（未加密）的默认配置文件。稍后，当您已经在工具中测试了应用程序时，您可以选择一个安全配置文件，并且该工具会生成密钥并预生成安全启动的配置。
6. 单击 **Create** 按钮来创建工作区。

5.3 工具图形用户界面

创建工作区后，将显示工具主窗口。主窗口包含：

1. 主菜单
2. 工具栏
3. “Build image”、“Write image”和“PKI management”选项卡
4. 日志视图
5. 状态行

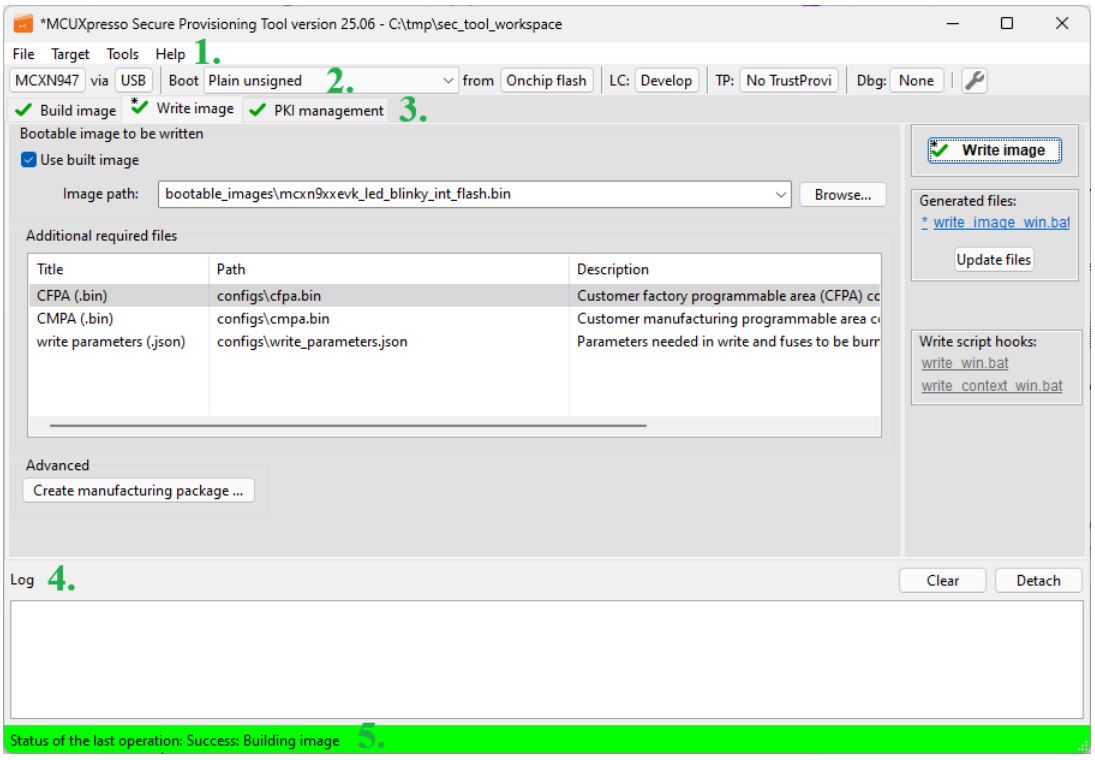

Figure 2. 工具图形用户界面

第一步，仔细检查工具栏上的配置是否符合您的要求。您将在那里找到：

1. 选定的处理器（已在向导中选择）
2. 连接的处理器（已在向导中选择）
3. 启动模式（已在向导中选择）
4. 启动内存
5. 生命周期（建议从默认值开始）
6. 信任配置（建议从默认值开始）
7. 调试探针（对于大多数处理器来说，您不需要这个；它可能用于设置代替 fuse 的影子寄存器）
8. 快速修复按钮

Figure 3. 工具栏

5.4 检查连接

可以使用 **main menu > Target > Connection** 命令或单击工具栏中的“connection”按钮，然后在连接配置对话框中选择 **Test connection**。这会在 ISP 模式下对处理器进行 ping 操作并检查是否可以建立连接。如果连接成功建立，对话框将显示所连接处理器的检测状态。

如果连接不起作用，请检查开发板是否配置为 ISP/SDP 模式并重置开发板。

5.5 生成 bootable image

如果您使用向导创建工作区，则构建页面上不应该出现任何错误。错误以红色显示，问题描述显示在工具提示中，因此如果有任何错误，请修复它们。注意： 忽略写入页面上的错误，直到您构建镜像（image）时才会出现错误。

单击 **Build image**以生成一个 bootable image。进度显示在日志中。如果有任何问题，请阅读日志并修复。生成的文件作为该过程的一部分显示在按钮下方。最重要的列为第一个。它被称为 “build_image” 脚本，是在构建过程中执行的脚本。可以点击它并检查内容。

5.6 测试 bootable image

一旦构建了 bootable image，您就可以继续留在 **Write image** 页面并将其写入引导内存。仔细检查确认没有报告错误，然后单击 **Write image** 按钮开始该过程。写入过程与构建过程类似。它将进行预检查，如果没有发现问题，它将生成写入脚本。如果写入脚本在处理器中做了任何不可逆的更改，GUI 将显示一个带有更改列表的确认对话框。之后，执行写入脚本，并在日志视图中列出详细信息。

应用程序编写完成后，验证其是否正确启动（从 ISP 切换到 RUN 模式并重置）。

5.7 接下来是什么

一旦可启动应用程序开始运行，就可以添加其他安全配置，例如：

- 使用签名或加密的镜像（image）进行安全启动
- 双镜像（image）启动
- 防卷退配置
- One-Time-Programamble（OTP）配置

建议每次更改后检查应用程序。如果应用程序无法启动，请恢复并找出导致问题的更改。 该工具提供各种检查以防止无效配置。错误（红色）是阻塞问题，以防止将任何无效配置应用于处理器。警告（黄色）是不寻常/不推荐的设置，但它们是非阻塞的。

一旦应用程序的安全配置最终确定并稳定，您就可以继续制造。该工具可以生成制造包 - 一个包含制造所需的所有文件的 ZIP 文件。在制造工厂中，导入包并应用（制造工具允许将其并行应用于多个开发板）。

5.8 特定处理器的工作流程

有一些特定于处理器的功能需要配置。这就是 Secure Provisioning Tool User Guide 中描述处理器特定工作流程的原因，“特定于处理器的工作流程”部分包含如何配置不同安全配置的分步过程。

6 参考资料

6.1 Release Notes

https://docs.mcuxpresso.nxp.com/secure/latest/release_notes.html

Secure Provisioning Tool Release Notes（文档 MCUXSPTRN）

6.2 User Guide

https://docs.mcuxpresso.nxp.com/secure/latest/01_introduction.html

Secure Provisioning Tool User Guide（文档 MCUXSPTUG）

6.3 NXP 安全配置网络

https://nxp.com/mcuxpresso/secure

6.4 社区、论坛、知识库

https://community.nxp.com/t5/MCUXpresso-Secure-Provisioning/tkb-p/mcux-secure-tool

7 修订记录

文档ID	发布日期	说明
UG10241 v.2.0	2025 年 10 月 10 日	SEC 工具版本 25.09 的小更新。
UG10241 v.1.0	2025 年 6 月 30 日	初始版本。

Legal information

Definitions

Draft — A draft status on a document indicates that the content is still under internal review and subject to formal approval, which may result in modifications or additions. NXP Semiconductors does not give any representations or warranties as to the accuracy or completeness of information included in a draft version of a document and shall have no liability for the consequences of use of such information.

Disclaimers

Limited warranty and liability — Information in this document is believed to be accurate and reliable. However, NXP Semiconductors does not give any representations or warranties, expressed or implied, as to the accuracy or completeness of such information and shall have no liability for the consequences of use of such information. NXP Semiconductors takes no responsibility for the content in this document if provided by an information source outside of NXP Semiconductors.

In no event shall NXP Semiconductors be liable for any indirect, incidental, punitive, special or consequential damages (including - without limitation - lost profits, lost savings, business interruption, costs related to the removal or replacement of any products or rework charges) whether or not such damages are based on tort (including negligence), warranty, breach of contract or any other legal theory.

Notwithstanding any damages that customer might incur for any reason whatsoever, NXP Semiconductors' aggregate and cumulative liability towards customer for the products described herein shall be limited in accordance with the Terms and conditions of commercial sale of NXP Semiconductors.

Right to make changes — NXP Semiconductors reserves the right to make changes to information published in this document, including without limitation specifications and product descriptions, at any time and without notice. This document supersedes and replaces all information supplied prior to the publication hereof.

Suitability for use — NXP Semiconductors products are not designed, authorized or warranted to be suitable for use in life support, life-critical or safety-critical systems or equipment, nor in applications where failure or malfunction of an NXP Semiconductors product can reasonably be expected to result in personal injury, death or severe property or environmental damage. NXP Semiconductors and its suppliers accept no liability for inclusion and/or use of NXP Semiconductors products in such equipment or applications and therefore such inclusion and/or use is at the customer's own risk.

Applications — Applications that are described herein for any of these products are for illustrative purposes only. NXP Semiconductors makes no representation or warranty that such applications will be suitable for the specified use without further testing or modification.

Customers are responsible for the design and operation of their applications and products using NXP Semiconductors products, and NXP Semiconductors accepts no liability for any assistance with applications or customer product design. It is customer's sole responsibility to determine whether the NXP Semiconductors product is suitable and fit for the customer's applications and products planned, as well as for the planned application and use of customer's third party customer(s). Customers should provide appropriate design and operating safeguards to minimize the risks associated with their applications and products.

NXP Semiconductors does not accept any liability related to any default, damage, costs or problem which is based on any weakness or default in the customer's applications or products, or the application or use by customer's third party customer(s). Customer is responsible for doing all necessary testing for the customer's applications and products using NXP Semiconductors products in order to avoid a default of the applications and the products or of the application or use by customer's third party customer(s). NXP does not accept any liability in this respect.

Terms and conditions of commercial sale — NXP Semiconductors products are sold subject to the general terms and conditions of commercial sale, as published at https://www.nxp.com/profile/terms, unless otherwise agreed in a valid written individual agreement. In case an individual agreement is concluded only the terms and conditions of the respective agreement shall apply. NXP Semiconductors hereby expressly objects to applying the customer's general terms and conditions with regard to the purchase of NXP Semiconductors products by customer.

Export control — This document as well as the item(s) described herein may be subject to export control regulations. Export might require a prior authorization from competent authorities.

Suitability for use in non-automotive qualified products — Unless this document expressly states that this specific NXP Semiconductors product is automotive qualified, the product is not suitable for automotive use. It is neither qualified nor tested in accordance with automotive testing or application requirements. NXP Semiconductors accepts no liability for inclusion and/or use of non-automotive qualified products in automotive equipment or applications.

In the event that customer uses the product for design-in and use in automotive applications to automotive specifications and standards, customer (a) shall use the product without NXP Semiconductors' warranty of the product for such automotive applications, use and specifications, and (b) whenever customer uses the product for automotive applications beyond NXP Semiconductors' specifications such use shall be solely at customer's own risk, and (c) customer fully indemnifies NXP Semiconductors for any liability, damages or failed product claims resulting from customer design and use of the product for automotive applications beyond NXP Semiconductors' standard warranty and NXP Semiconductors' product specifications.

HTML publications — An HTML version, if available, of this document is provided as a courtesy. Definitive information is contained in the applicable document in PDF format. If there is a discrepancy between the HTML document and the PDF document, the PDF document has priority.

Translations — A non-English (translated) version of a document, including the legal information in that document, is for reference only. The English version shall prevail in case of any discrepancy between the translated and English versions.

Security — Customer understands that all NXP products may be subject to unidentified vulnerabilities or may support established security standards or specifications with known limitations. Customer is responsible for the design and operation of its applications and products throughout their lifecycles to reduce the effect of these vulnerabilities on customer's applications and products. Customer's responsibility also extends to other open and/or proprietary technologies supported by NXP products for use in customer's applications. NXP accepts no liability for any vulnerability. Customer should regularly check security updates from NXP and follow up appropriately.

Customer shall select products with security features that best meet rules, regulations, and standards of the intended application and make the ultimate design decisions regarding its products and is solely responsible for compliance with all legal, regulatory, and security related requirements concerning its products, regardless of any information or support that may be provided by NXP.

NXP has a Product Security Incident Response Team (PSIRT) (reachable at PSIRT@nxp.com) that manages the investigation, reporting, and solution release to security vulnerabilities of NXP products.

NXP B.V. — NXP B.V. is not an operating company and it does not distribute or sell products.

Trademarks

Notice: All referenced brands, product names, service names, and trademarks are the property of their respective owners.

NXP — wordmark and logo are trademarks of NXP B.V.

Contents