Using Password Security with MachXO4 Devices

Technical Note

FPGA-TN-02408-1.0

December 2025

Disclaimers

Lattice makes no warranty, representation, or guarantee regarding the accuracy of information contained in this document or the suitability of its products for any particular purpose. All information herein is provided AS IS, with all faults, and all associated risk is the responsibility entirely of the Buyer. The information provided herein is for informational purposes only and may contain technical inaccuracies or omissions, and may be otherwise rendered inaccurate for many reasons, and Lattice assumes no obligation to update or otherwise correct or revise this information. Products sold by Lattice have been subject to limited testing and it is the Buyer's responsibility to independently determine the suitability of any products and to test and verify the same. LATTICE PRODUCTS AND SERVICES ARE NOT DESIGNED, MANUFACTURED, OR TESTED FOR USE IN LIFE OR SAFETY CRITICAL SYSTEMS, HAZARDOUS ENVIRONMENTS, OR ANY OTHER ENVIRONMENTS REQUIRING FAIL-SAFE PERFORMANCE, INCLUDING ANY APPLICATION IN WHICH THE FAILURE OF THE PRODUCT OR SERVICE COULD LEAD TO DEATH, PERSONAL INJURY, SEVERE PROPERTY DAMAGE OR ENVIRONMENTAL HARM (COLLECTIVELY, "HIGH-RISK USES"). FURTHER, BUYER MUST TAKE PRUDENT STEPS TO PROTECT AGAINST PRODUCT AND SERVICE FAILURES, INCLUDING PROVIDING APPROPRIATE REDUNDANCIES, FAIL-SAFE FEATURES, AND/OR SHUT-DOWN MECHANISMS. LATTICE EXPRESSLY DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY OF FITNESS OF THE PRODUCTS OR SERVICES FOR HIGH-RISK USES. The information provided in this document is proprietary to Lattice Semiconductor, and Lattice reserves the right to make any changes to the information in this document or to any products at any time without notice.

Inclusive Language

This document was created consistent with Lattice Semiconductor's inclusive language policy. In some cases, the language in underlying tools and other items may not yet have been updated. Please refer to Lattice's inclusive language FAQ 6878 for a cross reference of terms. Note in some cases such as register names and state names it has been necessary to continue to utilize older terminology for compatibility.

Contents

Figures

Tables

Abbreviations in This Document

A list of abbreviations used in this document.

Abbreviation	Definition
AES	Advanced Encryption Standard
IP	Intellectual Property
OTP	One-Time Programmable
NVCM	Non-Volatile Configuration Memory
SRAM	Static Random-Access Memory

1. Introduction

This technical note describes the MachXO4™ Password security feature. The Password security feature uses a Password Protection Key to control access to the device configuration and programming modes, offering both read and write protection. When the Password security feature is enabled, the configuration and programming edit mode operations (such as Write, Verify, and Erase) are allowed only if the Password Protection Key matching the one stored in the device is provided.

For comparison, MachXO4 devices provide a variety of other protection and security protocols to shield valuable customer intellectual property (IP) from being viewed or tampered. In addition to the Password security feature, the one-time programmable (OTP) feature provides permanent *write-protection* against intentional or unintentional corruption of the FPGA configuration image, while still allowing verification operations. The *Secure Device* settings provide a complementary set of *read-protection* features. This feature prevents the read-back of sensitive customer IP or data from the FPGA fabric while still allowing erase and reprogramming operations, such as for in-field updates.

Table 1.1. Password Security Feature Terminology Used in This Document

Terminology	Radiant™/Programmer Software	Also known as	Description
Password Protection Key	Flash Protect Key/Password Key	Device password	64-bit binary Flash Protect Key, stored in the MachXO4 device feature row and in a *.key* file.
Passcode Encrypted File (*.key*)	<design_name>*.key*/Load Key, Save Key	Password file	AES encrypted file stored on a local file system. The Lattice Programmer software utilizes the Flash Protect Key stored within this file when communicating with a protected MachXO4 device.
File Protection Password	Password/Password	Encryption passcode	The 8-16 character passcode used to secure the *.key* file.

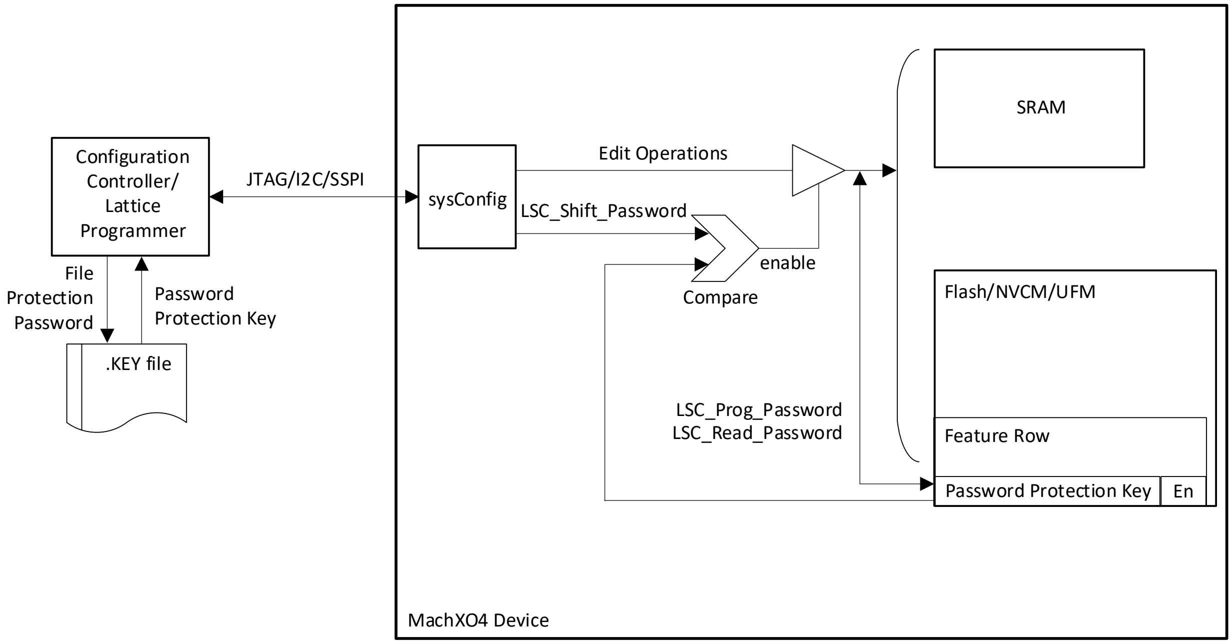


Figure 1.1. Password Security Block Diagram

2. Overview

2.1. Operation

The MachXO4 device Password feature requires that a controller accessing the MachXO4 device through a sysConfig port (JTAG, SSPI, I2C, or WISHBONE) provide a valid Password Protection Key. The Password Protection Key unlocks the device and allows configuration or programming operations to proceed. Without a valid Password Protection Key, you can perform only rudimentary non-configuration operations such as Read Device ID.

The Lattice Radiant™ and Lattice Radiant Programmer software tools support the secure generation and utilization of the Password Protection Key. In addition, for embedded environments, the Deployment Tool of Radiant Programmer supports the generation of algorithm and data files for embedded programming and configuration of Password Protection Key enabled devices.

The Password Protection Key generated using the Lattice Radiant software is stored in a passcode encrypted file (*.key*) on the local file system (Windows or Linux) using Advanced Encryption Standard with a 128-bit encryption key (AES-128). Therefore, the Password Protection Key is reasonably secure against attack. The encryption passcode, also known as the File Protection Password, is required to access the encrypted file for subsequent Password Protection Key enabled programming and configuration operations.

The MachXO4 Password Protection Key field and the feature enable status bit are contained in the Feature Row sector of the device Flash memory array. When the Password feature is enabled, the Password Protection Key field cannot be read, erased, or written without first providing the same Password Protection Key.

2.2. Security Limitations

When performing configuration operations, the Password Protection Key is transmitted unencrypted (in-the-clear) by the configuration controller to the sysConfig port (JTAG, Target SPI, or I2C). For high-security remote operations, such as in-field updates, it may be necessary to restrict physical access to the device. Alternately, methods utilizing the internal WISHBONE sysConfig port to transmit the Password Protection Key may be used to keep the Password Protection Key secure against unauthorized probing.

When using the Deployment tool *Tester* capability to generate *.SVF* debugger files, caution must be applied. The Password Protection Key is contained in the ASCII text *.SVF*. Neither the Password Protection Key nor the *.SVF* file itself are encrypted to prevent unauthorized access. Delete or secure any debugger files as necessary.

Bitstream files (*.bit*) do not contain the Password Protection Key. The Password Protection Key feature is bypassed by the Controller SPI port when booting from external SPI flash devices.

3. Creating and Securing the Password Protection Key

3.1. Overview

The Password Protection Key is specified by you and stored in a *.key* file. The *.key* file is secured using a File Protection Password. The *.key* file may be referenced for subsequent secure configuration and programming operations.

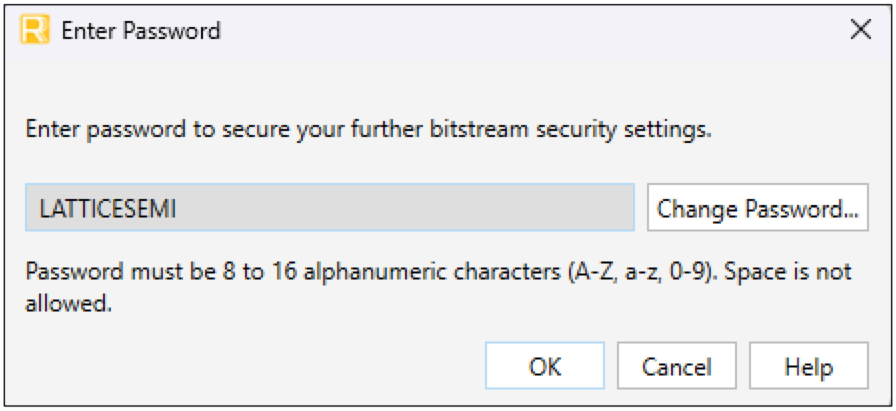
3.2. Software Requirements

The Password Protection Key feature for MachXO4 devices is available in the Lattice Radiant software version 2025.2 or later. To enable this security feature, you must also install the Encryption Control Pack available at www.latticesemi.com.

3.3. Creating and Securing the Password Protection Key Using the Radiant Software

Follow these steps to create and secure the Password Protection Key:

1. In the Tools menu, select Bitstream **Security Settings Tool** to open the passcode file generation tool. The Enter Password dialog opens with a default File Protection Password (file passcode). To enhance password security, change the File Protection Password by clicking **Change Password…**, as shown in the figure below.



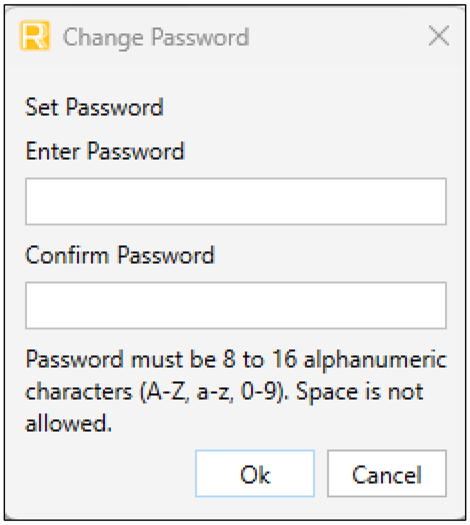
Enter password to secure your further bitstream security settings.

LATTICESEMI

Password must be 8 to 16 alphanumeric characters (A-Z, a-z, 0-9). Space is not allowed.

Figure 3.1. Enter Password Dialog Box

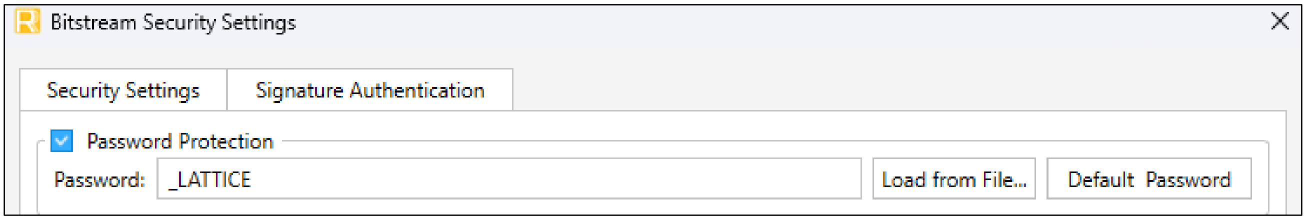
2. The new File Protection Password must have 8 to 16 alpha and numeric characters, and cannot contain spaces or special characters. If you need to record the new File Protection Password for future reference, choose a secure location. In the Change Password dialog box, enter the new **File Protection Password** twice and click **OK**.



Password must be 8 to 16 alphanumeric characters (A-Z, a-z, 0-9). Space is not allowed.

Figure 3.2. Change Password Dialog Box

3. The Bitstream Security Settings dialog box opens for you to specify the Password Protection Key as shown in the figure below.
4. Select the Password Protection check box.
5. Enter the password in the correct format in the Password field. You can also load a previously created password from an existing key file (.*key*). A password is required to open the key file.



☑ Password Protection

Password: _LATTICE

Figure 3.3. Bitstream Security Settings Dialog Box

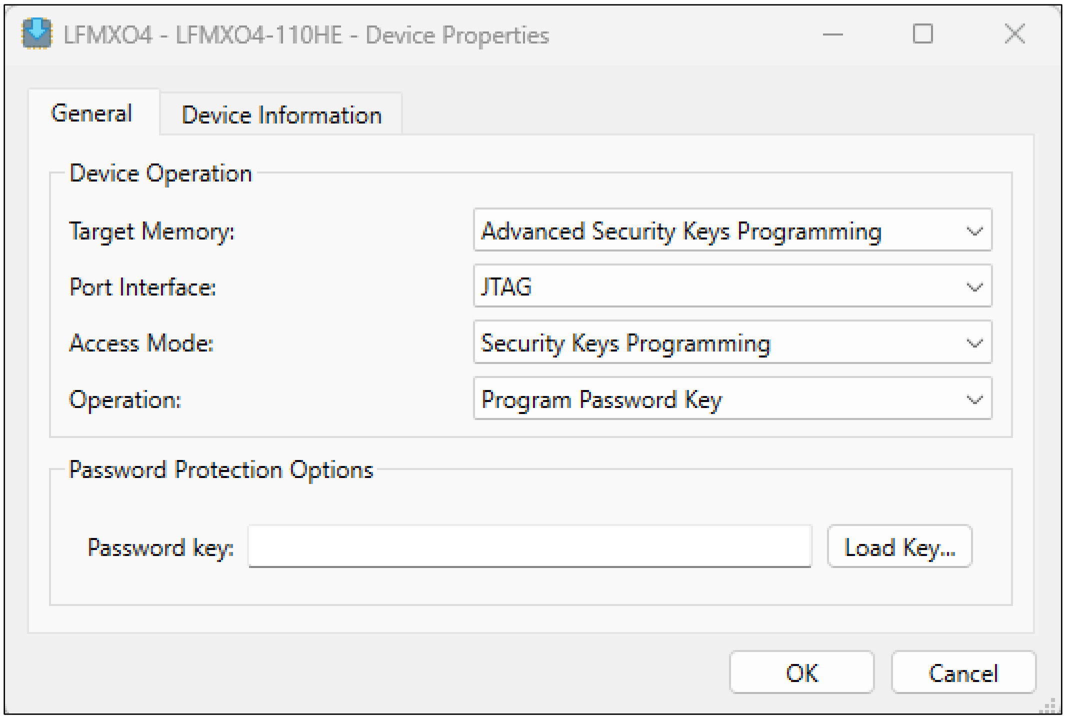
4. Using Password Protection Keys

4.1. Software Requirements

The Password feature for MachXO4 devices is available in the Lattice Radiant and stand-alone Lattice Programmer software version 2025.2 or later.

4.2. Programming the Device Using Programmer

You can use the Programmer software to perform password-related operations, either from within the Lattice Radiant or stand-alone software. The Password Key Options section is available in the Device Properties dialog box as shown in the figure below.



Device Operation

Target Memory: Advanced Security Keys Programming

Port Interface: JTAG

Access Mode: Security Keys Programming

Operation: Program Password Key

Password Protection Options

Password key:

Figure 4.1. Password Key Options

Follow these steps to program the device in the Programmer:

1. Enter the device Password Protection Key into the Password Key field. The 64-bit value is displayed in ASCII (8 character max) or HEX (16 digit max) formats.

   Alternatively, you can load the Password Protection Key from a previously generated *.key* file using the **Load Key** button. When prompted, provide the *.key* file location and the File Protection Password to access and decrypt the file.
2. After completing all sections of the Device Properties dialog box, click **OK** to proceed.

4.3. Programmer Operations

The following password-related operations are supported by the MachXO4 Password feature.

To program the Password Protection Key (Password Key) into an un-protected MachXO4 device, refer to the following table for access mode and password operations.

Table 4.1. Access Mode and Password Operations for MachXO4 Password Feature

Access Mode	Operation
Advanced Security Keys Programming	Program Password Key Program Password Key with Lock Erase Feature Row with Password Key

5. Low-Level Implementation

5.1. Password Feature Commands

The low-level sysConfig commands in the table below are used by the Lattice Radiant software, Programmer software, and Deployment tools to implement Password Protection Key feature operations.

To unlock the device, transmit LSC_SHIFT_PASSWORD along with the Password Protection Key prior to entering a configuration edit mode (ISC_ENABLE or ISC_ENABLE_X). If the transmitted Password Protection Key matches the key previously programmed into the MachXO4 device, the device remains unlocked until the edit mode is exited. Edit modes are cancelled by issuing the ISC_DISABLE or ISC_REFRESH commands, asserting the PROGRAMN pin or power-cycling the device.

5.1.1. Set, Verify, Unlock

Table 5.1. Password Protection Key-Related sysConfig Commands

Command	Op Code	Use	Description
LSC_PROG_PASSWORD	0xF1	0xF1 00 00 00 pp pp pp pp pp pp pp pp	1 byte Opcode + 3 bytes operand + 64-bit Passcode
LSC_READ_PASSWORD	0xF2	0xF2 00 00 00	1 byte Opcode + 3 bytes operand + read 64-bit Passcode
LSC_SHIFT_PASSWORD	0xBC	0xBC 00 00 00 pp pp pp pp pp pp pp pp	1 byte Opcode + 3 bytes operand + 64-bit Passcode

5.1.2. Enable

When the Password Protection Key is successfully programmed and verified, it is made active by setting PWD_EN and PWD_ALL in the Feature Row. Use command opcode 0xF8 LSC_PROG_FEABIT to set PWD_EN and PWD_ALL. Bit 2 represents PWD_EN and bit 3 represents PWD_ALL.

5.2. Password-Required Operations

All sysConfig operations targeting the Feature Row are restricted when PWD_EN is set. Additionally, all sysConfig operations targeting the Configuration NVCM, Flash, or SRAM are restricted when both PWD_EN and PWD_ALL are set.

The following table shows a list of exempt sysConfig commands. These commands can be executed when PWD_EN is set regardless of Password Protection Key match status.

Table 5.2. Exempt sysConfig Commands

Command Name	Op Code
ISC_NOOP Bypass	0xFF
IDCODE_PUB Read Device ID	0xE0
USERCODE Read USERCODE	0xC0
LSC_SHIFT_PASSWORD Check Password Protection Key	0xBC
LSC_READ_STATUS Read Status Register	0x3C
LSC_CHECK_BUSY Check Busy Flag	0xF0
LSC_REFRESH Refresh	0x79
LSC_DEVICE_CTRL Standby	0x7D
ISC_ENABLE Enable Offline Configuration Mode	0xC6
ISC_ENABLE_X Enable Transparent Configuration Mode	0x74
ISC_DISABLE Disable Configuration	0x26

References

- MachXO4 Family Data Sheet (FPGA-DS-02125)
- MachXO4 Programming and Configuration Usage Guide (FPGA-TN-02393)
- MachXO4 Family Devices web page
- Boards, Demos, IP Cores, and Reference Designs
- Lattice Insight for Training Series and Learning Plans

Technical Support Assistance

Submit a technical support case via www.latticesemi.com/techsupport.

For frequently asked questions, refer to the Lattice Answer Database at www.latticesemi.com/Support/AnswerDatabase.

Revision History

Revision 1.0, December 2025

Section	Change Summary
All	Initial release