Using Password Security with MachXO4 Devices

Technical Note

FPGA-TN-02408-1.1

September 2026

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.

© 2026 Lattice Semiconductor Corp. All Lattice trademarks, registered trademarks, patents, and disclaimers are as listed at www.latticesemi.com/legal.
All other brand or product names are trademarks or registered trademarks of their respective holders. The specifications and information herein are subject to change without notice.

Contents

Contents 3
Abbreviations in This Document 4
1. Introduction 5
2. Overview 7
2.1. Operation 7
2.2. Security Design Considerations 7
3. Creating and Securing the Password Protection Key 8
3.1. Overview 8
3.2. Software Requirements 8
3.3. Creating and Securing the Password Protection Key Using the Radiant Software 8
4. Using Password Protection Keys 10
4.1. Software Requirements 10
4.2. Programming the Device Using Programmer 10
4.3. Programmer Operations 11
5. Low-Level Implementation 11
5.1. Password Feature Commands 11
5.1.1. Set, Verify, Unlock 11
5.1.2. Enable 12
5.2. Password-Required Operations 12
References 13
Technical Support Assistance 14
Revision History 15

Figures

Figure 1.1. Password Security Block Diagram 6
Figure 3.1. Enter Password Dialog Box 8
Figure 3.2. Change Password Dialog Box 9
Figure 3.3. Bitstream Security Settings Dialog Box 9
Figure 4.1. Password Key Options 10

Tables

Table 1.1. Password Security Feature Terminology Used in This Document 5
Table 4.1. Access Mode and Password Operations for the Password Feature 11
Table 5.1. Password Protection Key-Related sysConfig Commands- MachXO4 11
Table 5.2. Password Protection Key-Related sysConfig Commands – MachXO4 RoT 11
Table 5.3. Exempt sysConfig Commands 12

© 2026 Lattice Semiconductor Corp. All Lattice trademarks, registered trademarks, patents, and disclaimers are as listed at www.latticesemi.com/legal.
All other brand or product names are trademarks or registered trademarks of their respective holders. The specifications and information herein are subject to change without notice.

Abbreviations in This Document

A list of abbreviations used in this document.

Abbreviation	Definition
AES	Advanced Encryption Standard
ASCII	American Standard Code for Information Interchange
ECIES	Elliptic Curve Integrated Encryption Scheme
HEX	Hexadecimal
I2C	Inter-Integrated Circuit
IP	Intellectual Property
JTAG	Joint Test Action Group
NVCM	Non-Volatile Configuration Memory
OTP	One-Time Programmable
RoT	Root of Trust
SPI	Serial Peripheral Interface
SSPI	Secondary Serial Peripheral Interface
SRAM	Static Random-Access Memory
SVF	Serial Vector Format

© 2026 Lattice Semiconductor Corp. All Lattice trademarks, registered trademarks, patents, and disclaimers are as listed at www.latticesemi.com/legal.
All other brand or product names are trademarks or registered trademarks of their respective holders. The specifications and information herein are subject to change without notice.

1. Introduction

This technical note describes the Lattice MachXO4™ and Lattice MachXO4 Root of Trust (RoT) Password Security feature. The Password Security feature uses a Password Protection Key to control access to device configuration and programming modes, providing both read and write protection. When enabled, configuration and programming edit-mode operations, such as Write, Verify, and Erase, are permitted only when the correct Password Protection Key matching the value stored in the device is provided.

MachXO4 and MachXO4 RoT devices provide different levels of protection to safeguard sensitive customer data and intellectual property (IP) from unauthorized access and potential tampering. In addition to the Password Security feature, the Secure Device settings provide read-protection by preventing the read-back of sensitive customer IP or data from the FPGA fabric, while still allowing erase and reprogramming operations for applications such as in-field updates. The permanent write-protection policy implemented through the one-time programmable (OTP) feature helps prevent intentional or unintentional modification of the FPGA configuration image while still allowing verification operations.

For MachXO4 RoT devices, the Password Security feature should be considered an additional layer of protection rather than a standalone security mechanism. It is recommended to use the password feature in combination with stronger cryptographic authentication mechanisms, such as challenge-response protocols based on ECIES, to control access to protected interfaces and operations. In such a layered security approach, cryptographic authentication can be used to unlock access to device ports or services, while the password feature provides an additional safeguard against accidental or unauthorized configuration changes, erase operations, or device reprogramming.

Table 1.1. Password Security Feature Terminology Used in This Document

Terminology	Lattice Radiant™ or Programmer Software	Also Known As	Description
Password Protection Key	Flash Protect Key/Password Key	Device password	64-bit (MachXO4) or 128-bit (MachXO4 RoT) binary Flash Protect Key, stored in the 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 uses the Flash Protect Key stored within this file when communicating with a protected MachXO4 or MachXO4 RoT device.
File Protection Password	Password/Password	Encryption passcode	The 8–16 character passcode that is used to secure the *.key* file.

© 2026 Lattice Semiconductor Corp. All Lattice trademarks, registered trademarks, patents, and disclaimers are as listed at www.latticesemi.com/legal.
All other brand or product names are trademarks or registered trademarks of their respective holders. The specifications and information herein are subject to change without notice.

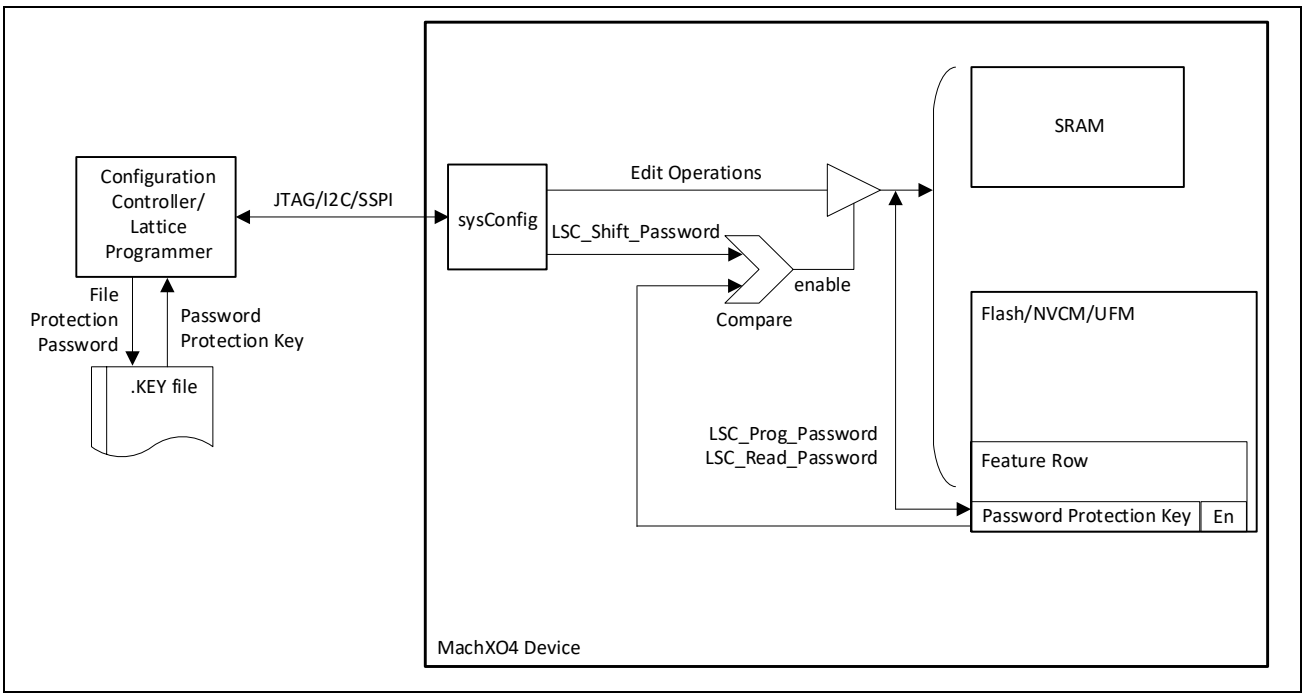


Figure 1.1. Password Security Block Diagram

© 2026 Lattice Semiconductor Corp. All Lattice trademarks, registered trademarks, patents, and disclaimers are as listed at www.latticesemi.com/legal.
All other brand or product names are trademarks or registered trademarks of their respective holders. The specifications and information herein are subject to change without notice.

2. Overview

2.1. Operation

The MachXO4 or MachXO4 RoT device Password feature requires the controller accessing the MachXO4 or MachXO4 RoT device through a sysConfig port (JTAG, SSPI, I2C, or WISHBONE) to 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, user can perform only rudimentary non-configuration operations such as Read Device ID.

The Lattice Radiant™ and Lattice Radiant Programmer software tools support secure generation and use of the Password Protection Key. In addition, for embedded environments, the Deployment tool of the Radiant Programmer supports the generation of 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). 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 or MachXO4 RoT 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 Design Considerations

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. Alternatively, methods using 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* file. Neither the Password Protection Key nor the *.SVF* file itself is 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.

© 2026 Lattice Semiconductor Corp. All Lattice trademarks, registered trademarks, patents, and disclaimers are as listed at www.latticesemi.com/legal.
All other brand or product names are trademarks or registered trademarks of their respective holders. The specifications and information herein are subject to change without notice.

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 or MachXO4 RoT devices is available in the Lattice Radiant software. To enable this security feature, you must also install the Encryption Control Pack available at the Lattice Radiant software web page.

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.

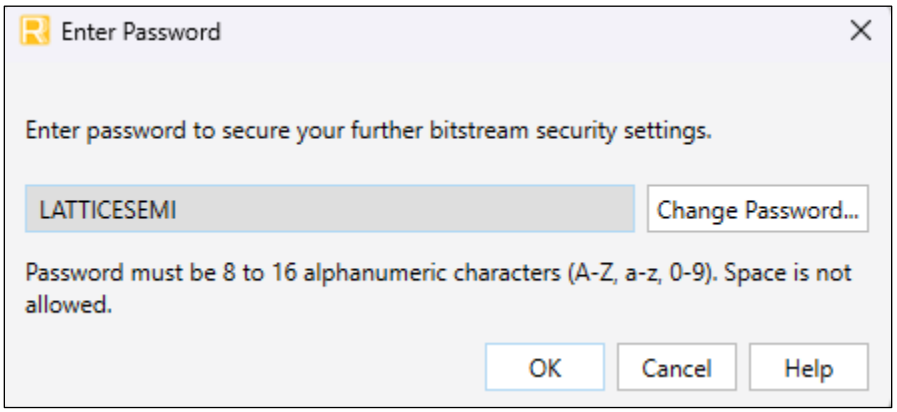


Figure 3.1. Enter Password Dialog Box

2. The new File Protection Password must have 8 to 16 alphanumeric 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**.

© 2026 Lattice Semiconductor Corp. All Lattice trademarks, registered trademarks, patents, and disclaimers are as listed at www.latticesemi.com/legal.
All other brand or product names are trademarks or registered trademarks of their respective holders. The specifications and information herein are subject to change without notice.

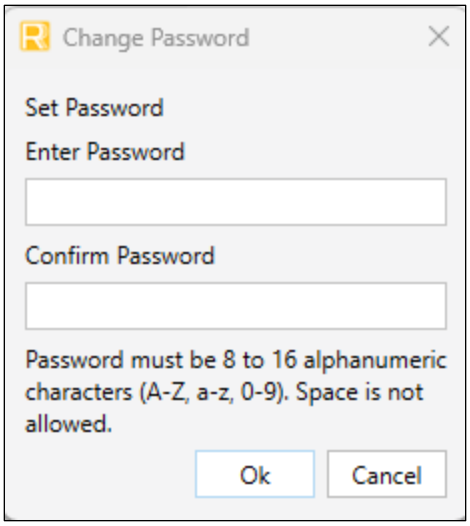


Figure 3.2. Change Password Dialog Box

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.

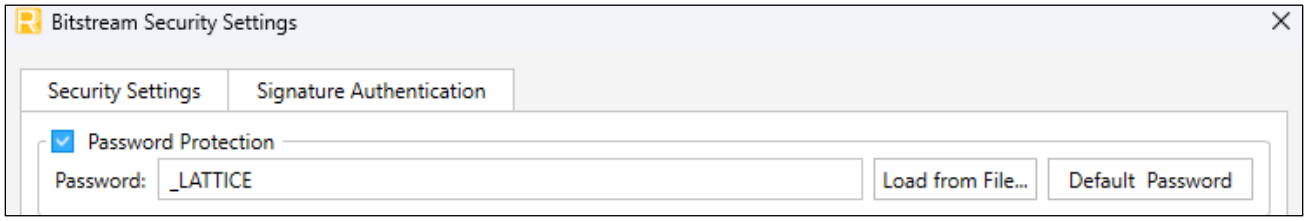


Figure 3.3. Bitstream Security Settings Dialog Box

© 2026 Lattice Semiconductor Corp. All Lattice trademarks, registered trademarks, patents, and disclaimers are as listed at www.latticesemi.com/legal.
All other brand or product names are trademarks or registered trademarks of their respective holders. The specifications and information herein are subject to change without notice.

4. Using Password Protection Keys

4.1. Software Requirements

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

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.

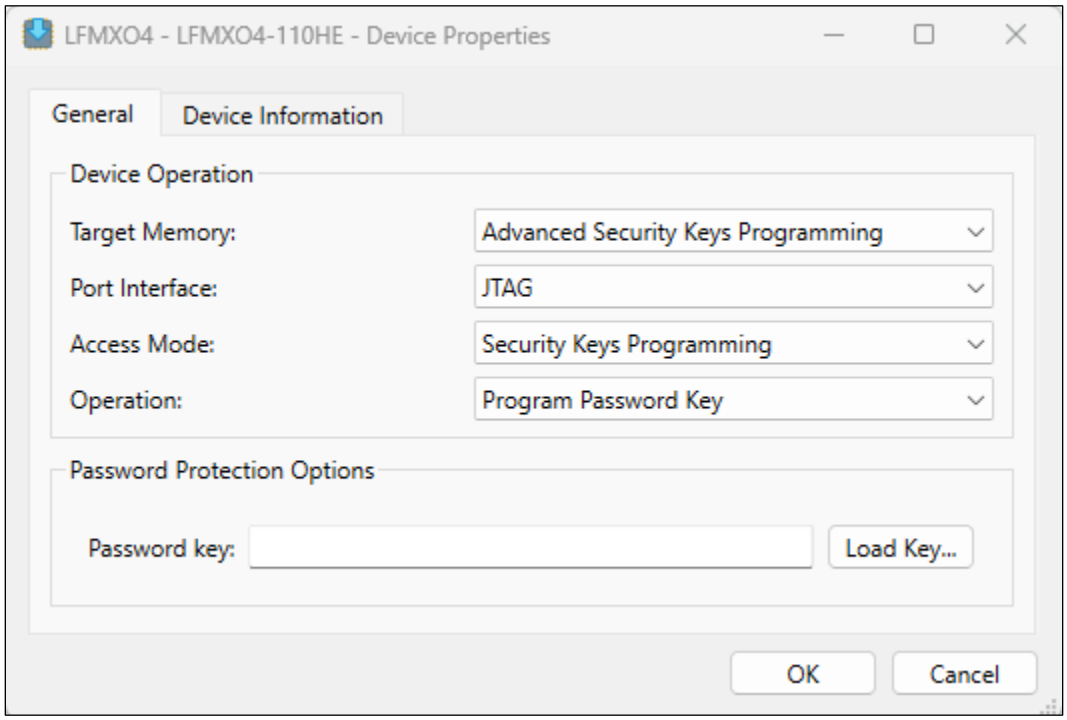


Figure 4.1. Password Key Options

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 (MachXO4) / 128-bit value (MachXO4 RoT) is displayed in ASCII or HEX 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.

© 2026 Lattice Semiconductor Corp. All Lattice trademarks, registered trademarks, patents, and disclaimers are as listed at www.latticesemi.com/legal.
All other brand or product names are trademarks or registered trademarks of their respective holders. The specifications and information herein are subject to change without notice.

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 unprotected MachXO4 device, refer to the following table for access mode and password operations.

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

Access Mode	Operation
Advanced Security Keys Programming	Program Password Key Program Password Key with Lock Erase Feature Row with Password Key Read Password Key (MachXO4 RoT only)

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 or MachXO4 RoT device, the device remains unlocked until the edit mode is exited. Edit modes are canceled 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- MachXO4

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 (MachXO4)
LSC_READ_PASSWORD	0xF2	0xF2 00 00 00	1 byte Opcode + 3 bytes operand + read 64-bit Passcode (MachXO4)
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 (MachXO4)

Table 5.2. Password Protection Key-Related sysConfig Commands – MachXO4 RoT

Command	Op Code	Use	Description
LSC_PROG_PASSWORD	0xF1	0xF1 00 00 00 pp pp pp pp pp pp pp pp pp pp pp pp pp pp pp pp	1 byte Opcode + 3 bytes operand + 128-bit Passcode (MachXO4 RoT).
LSC_READ_PASSWORD	0xF2	0xF2 00 00 00	1 byte Opcode + 3 bytes operand + 128-bit Passcode (MachXO4 RoT).
LSC_SHIFT_PASSWORD	0xBC	0xBC 00 00 00 pp pp pp pp pp pp pp pp pp pp pp pp pp pp pp pp	1 byte Opcode + 3 bytes operand + 128-bit Passcode (MachXO4 RoT).

© 2026 Lattice Semiconductor Corp. All Lattice trademarks, registered trademarks, patents, and disclaimers are as listed at www.latticesemi.com/legal.
All other brand or product names are trademarks or registered trademarks of their respective holders. The specifications and information herein are subject to change without notice.

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 5.3. 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

© 2026 Lattice Semiconductor Corp. All Lattice trademarks, registered trademarks, patents, and disclaimers are as listed at www.latticesemi.com/legal.
All other brand or product names are trademarks or registered trademarks of their respective holders. The specifications and information herein are subject to change without notice.

References

- MachXO4 Family Data Sheet (FPGA-DS-02125)
- MachXO4 Family Root-of-Trust Devices Data Sheet (FPGA-DS-02126)
- 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

© 2026 Lattice Semiconductor Corp. All Lattice trademarks, registered trademarks, patents, and disclaimers are as listed at www.latticesemi.com/legal.
All other brand or product names are trademarks or registered trademarks of their respective holders. The specifications and information herein are subject to change without notice.

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.

© 2026 Lattice Semiconductor Corp. All Lattice trademarks, registered trademarks, patents, and disclaimers are as listed at www.latticesemi.com/legal.
All other brand or product names are trademarks or registered trademarks of their respective holders. The specifications and information herein are subject to change without notice.

Revision History

Revision 1.1, September 2026

Section	Change Summary
All	• Performed minor editorial edits. • Updated the device name to include MachXO4 RoT.
Abbreviations in This Document	Added the following abbreviations—ECIES, HEX, JTAG, RoT, and SSPI.
Introduction	• Updated the introduction to include more details about using the Password Security feature in RoT devices. • Updated Table 1.1. Password Security Feature Terminology Used in This Document.
Overview	• Updated the Operation section. • Updated the section title for *Security Limitations* to Security Design Considerations.
Creating and Securing the Password Protection Key	Updated the Lattice Radiant web page link in the Software Requirements section.
Using Password Protection Keys	• Updated the Programming the Device Using Programmer section to include MachXO4 RoT-specific Password Protection Key details. • Updated Table 4.1. Access Mode and Password Operations for the Password Feature to include Read Password Key operation for MachXO4 RoT.
Low-Level Implementation	Added Table 5.2. Password Protection Key-Related sysConfig Commands – MachXO4 RoT to include MachXO4 RoT-specific Password Protection Key length references and sysConfig commands.
References	Added the following reference: • MachXO4 Family RoT Data Sheet (FPGA-DS-02126).

Revision 1.0, December 2025

Section	Change Summary
All	Initial release

© 2026 Lattice Semiconductor Corp. All Lattice trademarks, registered trademarks, patents, and disclaimers are as listed at www.latticesemi.com/legal.
All other brand or product names are trademarks or registered trademarks of their respective holders. The specifications and information herein are subject to change without notice.



www.latticesemi.com