TuxCare

Guide

Simplifying FIPS Compliance on AlmaLinux

A PRACTICAL & MODERNIZED APPROACH

Achieving FIPS 140-3 compliance is a critical step for organizations handling sensitive government and enterprise data, ensuring that the cryptography they use for processing this data meets strict security standards. However, the FIPS certification process can be complex, costly, and time-consuming. This guide breaks down everything you need to know about achieving FIPS compliance – what it entails, why it matters, what it looks like for AlmaLinux users, and how you can streamline the process with the most innovative technologies on the market.

In this guide, you'll learn how you can bypass lengthy re-certifications, keep your systems secure without breaking compliance, accelerate your time-to-market, and ensure your Linux environment meets stringent US and Canadian security standards while reducing operational overhead and compliance headaches.

What Is FIPS?

The **Federal Information Processing Standards (FIPS)** are a set of security requirements established by the **National Institute of Standards and Technology (NIST)** to ensure the confidentiality and integrity of sensitive data in government and regulated industries.

Specifically, **FIPS 140-3** defines the security standards for **cryptographic modules**, setting strict guidelines for how encryption is implemented, validated, and maintained.

Cryptographic modules are hardware, software, or firmware components that perform encryption and other cryptographic functions such as key management, authentication, and digital signing. These modules can exist in various forms, from hardware security modules (HSMs) and trusted platform modules (TPMs) to software-based encryption libraries. They serve as the foundation for securing sensitive data, ensuring that cryptographic operations meet rigorous security standards and resist potential attacks.

FIPS 140-3 Compliance Is Required for:

- U.S. and Canadian federal agencies
- government contractors
- companies providing services to the U.S. federal government.

FIPS compliance is a requirement for many organizations that fit into the requirements listed above, but it's also recommended for companies in industries like finance, healthcare, and critical infrastructure – where data security is paramount.

> **Meeting FIPS standards ensures that the cryptographic modules used in an organization's systems are rigorously tested and approved, reducing the risk of security breaches and regulatory non-compliance.**

However, achieving and maintaining FIPS compliance can be complex. Certification is time consuming and costly, and once a system is validated, applying security updates without breaking compliance becomes a challenge.

Why Should You Care About FIPS 140-3 Compliance?

FIPS 140-3 isn't just another security standard – it's a requirement for organizations handling sensitive government data and a critical benchmark for industries prioritizing strong encryption.

Whether mandated by regulation or necessary for business opportunities, FIPS compliance ensures your cryptographic security meets the highest standards. In the following section, we'll explore the compliance frameworks and industries where FIPS 140-3 is required or strongly recommended.

FIPS 140-3 is required or recommended under multiple compliance regimes, including:

- FedRAMP — Federal Risk and Authorization Management Program
- FISMA — Federal Information Security Modernization Act
- Cybersecurity Maturity Model Certification — Cybersecurity Maturity Model Certification
- DISA — Defense Information Systems Agency Security Technical Implementation Guide
- HIPAA Compliance — Health Insurance Portability and Accountability Act
- PCI Security Standards Council — Payment Card Industry Data Security Standard
- CJIS — Criminal Justice Information Services Security Policy
- Common Criteria — The Common Criteria for Information Technology Security Evaluation
- ITAR — International Traffic in Arms Regulation
- Gramm-Leach-Bliley Act Compliant — Gramm–Leach–Bliley Act

Patching for FIPS Compliance

Maintaining FIPS 140-3 compliance isn't just about meeting the initial certification – staying compliant over time presents its own set of challenges. From strict update controls to revalidation requirements, organizations must carefully navigate a landscape where security and compliance don't always align.

Why is patching for FIPS compliance such a challenge?

Tightly Controlled Security Updates

Cryptographic implementations require strict maintenance, ensuring that all encryption functions remain validated and uncompromised.

Mandatory Revalidation for Certain Updates

Any change affecting a cryptographic module's security boundaries requires costly and time-consuming revalidation by NIST-approved laboratories.

Balancing Security & Compliance

Organizations must carefully manage patching policies to stay secure while avoiding compliance violations.

Strict Version Lock-in

Organizations must often use older, certified versions of cryptographic modules, limiting the ability to quickly adopt security improvements.

Complex Certification Process

Navigating FIPS certification requires extensive documentation, testing, and coordination with accredited labs, adding delays and administrative burdens.

Working With Legacy Software

If you are coming from an older ecosystem like CentOS 7 or use Active Directory, you may find problems with FIPS mode denying access to deprecated algorithms like SHA1 or DES.

How to Make FIPS Compliance Painless

Fortunately, TuxCare's **Extended Security Updates for AlmaLinux** makes the FIPS compliance process effortless by providing you with pre-certified cryptographic FIPS packages and ongoing security updates that ensure ongoing security and stability for your regulated workloads – saving you time and resources while ensuring peace of mind.

Extended Security Updates (ESU)

part of TuxCare's Enterprise Support for AlmaLinux

Extended Security Updates (ESU) for AlmaLinux extend the lifecycle of specific AlmaLinux minor versions by delivering both prolonged security updates for High and Critical vulnerabilities as well as FIPS-compliant security patches, enabling greater stability and security for AlmaLinux deployments.

Ensure Painless FIPS 140-3 Compliance

Meet stringent US and Canadian government security standards with our FIPS-validated components, protecting against legal and financial penalties and making your products eligible for government contracts.

Accelerate Deployment and Cut Costs

Bypass the lengthy and expensive certification process by implementing pre-certified AlmaLinux FIPS packages. This speeds up your time-to-market and reduces overall project costs, giving you a competitive edge.

Maintain Compliance-Preserving Security

Keep your certified deployments secure with FIPS-compliant updates that fix vulnerabilities without altering validated cryptography, ensuring fast re-certification if a cryptographic vulnerability arises.

24/7/365 Technical Support Access

Get round-the-clock access to our technical support engineers.

Our ESU support includes assistance with:

- ESU repository setup issues
- Package update problems (package conflicts, missing dependencies)
- AlmaLinux FIPS and CVE-related questions
- ePortal issues
- AlmaLinux kernel crash issues (root cause analysis)

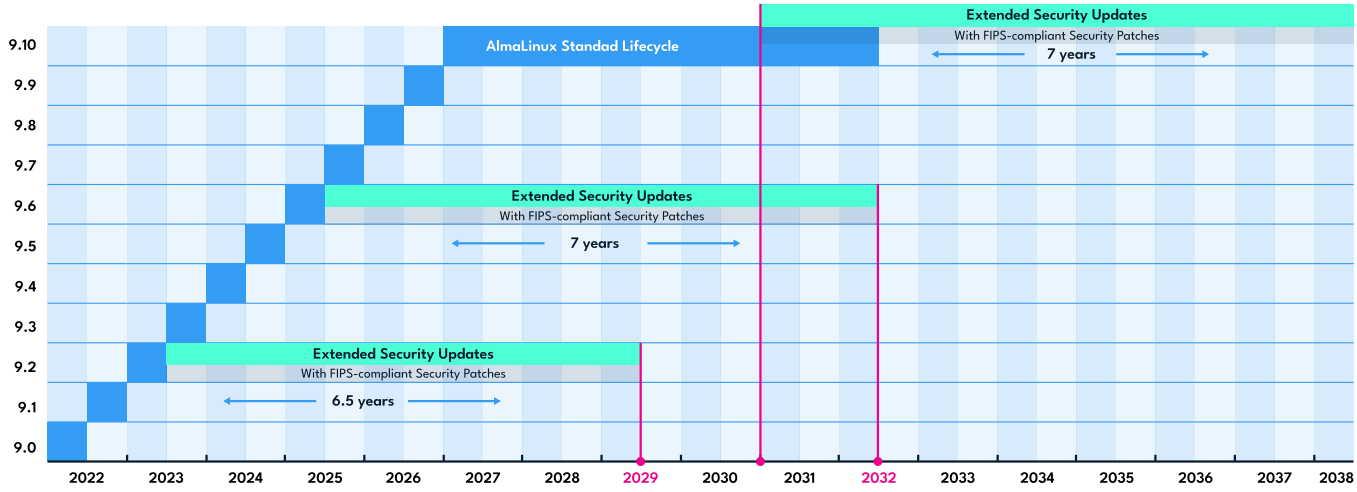
Keeping Up with the FIPS Security Lifecycle, Made Easy with ESU from TuxCare

AlmaLinux provides a 10-year lifecycle with a new minor release arriving every 6 months, bringing new features until the fifth year. Each of the minor releases is supported for 6 months. Customers who want to remain with the specific AlmaLinux minor release for years instead of months can opt for Extended Security Updates (ESU).

TuxCare's Extended Security Updates (ESU) delivers an extended period of security fixes for critical and high-risk vulnerabilities for select AlmaLinux minor versions, as well as the full suite of five FIPS-validated modules (kernel, openssl, libcrypt, nss and gnutls) and FIPS-compliant security patches for FIPS-certified AlmaLinux deployments. The product also unlocks commercial use of the FIPS-validated packages.

Long-Term Security and Compliance for FIPS-Certified AlmaLinux Deployments

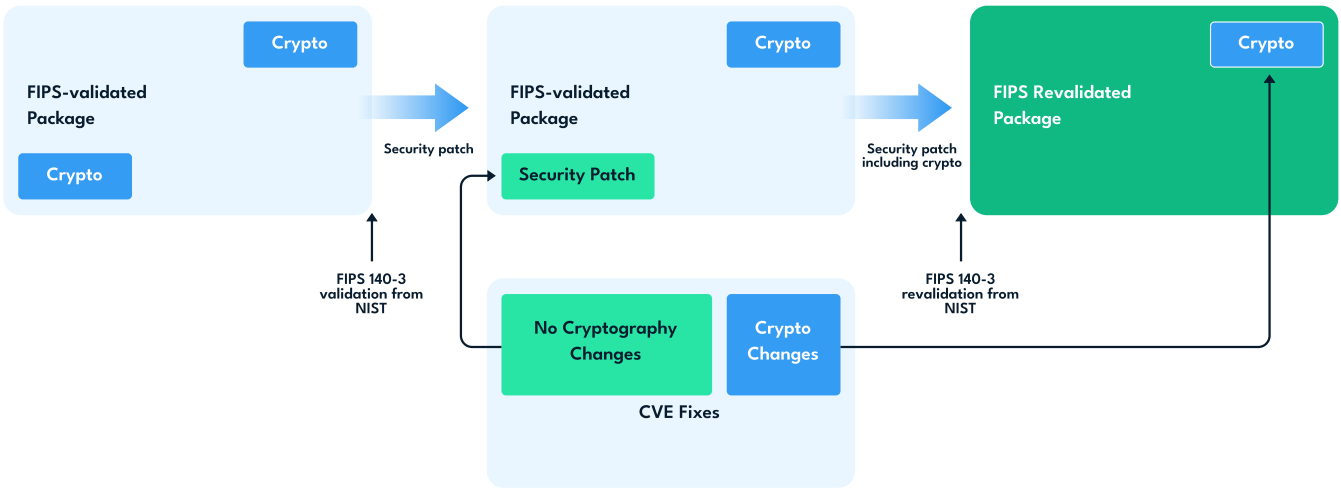
Extended Security Updates provide high and critical security fixes to extend the AlmaLinux lifecycle, so you can stay on a FIPS-validated AlmaLinux minor release (currently 9.2, 9.6 and 9.10) for over six years with at least a year overlap between each ESU release.



Extended Security Updates are currently available for AlmaLinux 9.2 and have planned support for AlmaLinux 9.6 and 9.10. Each ESU release includes at least a one-year overlap with the previous one to ensure a smooth transition. Since a FIPS certificate, once obtained, is valid for five years, we strive to ensure that our customers receive FIPS-compliant patches until the certificate's expiration date.

Prevent Unpatched CVEs from Compromising Your AlmaLinux Security Baseline Established by FIPS

Cryptographic modules are specific parts of FIPS-certified packages. Most vulnerabilities do not affect these modules, allowing you to maintain AlmaLinux FIPS 140-3 compliance with our FIPS-compliant security patches. If a cryptographic vulnerability arises, we will deliver a re-certified package.



FIPS 140-3 Validated Packages for AlmaLinux 9.2

The following list contains information about the current validation statuses for FIPS-validated AlmaLinux packages available with Extended Security Updates. Cryptographic modules that are on the Modules In Process list have passed all lab testing, have received intermediate CAVP and ESV certificates, and the report has been submitted to NIST to issue the final certificates.

Cryptographic Module	Version String	Associated Packages	Validation Status	Certificate
Kernel Crypto API	5.14.0-284.11.1.el9_2.tuxcare.5 5.14.0-284.11.1.el9_2.tuxcare.6 libkcapi 1.3.1-3.el9	kernel-5.14.0-284.11.1.el9_2.tuxcare.5 kernel-5.14.0-284.11.1.el9_2.tuxcare.6 libkcapi-1.3.1-3.el9.x86_64 libkcapi-hmaccalc-1.3.1-3.el9.x86_64	Active	#4750 (ESV/CAVP)
OpenSSL	3.0.7-1d2bd88ee26b3c90	openssl-3.0.7-20.el9_2.tuxcare.1 openssl-libs-3.0.7-20.el9_2.tuxcare.1	Active	#4823 (ESV/CAVP)
NSS	3.90.0-b84457b0165f79bf	nss-softokn-3.90.0-6.el9_2.tuxcare.1 nss-softokn-freebl-3.90.0-6.el9_2.tuxcare.1	Review Pending	TBA (ESV/CAVP)
Libgcrypt	1.10.0-19b8f37bc86846fe	libgcrypt-1.10.0-10.el9_2.tuxcare.3	Review Pending	TBA (ESV/CAVP)
GnuTLS	1.10.0-19b8f37bc86846fe	gnutls-3.7.6-23.el9_2.tuxcare.3 nettle-3.8-3.el9_2.tuxcare.1	Review Pending	TBA (ESV/CAVP)