Oracle Linux 9

Installing and Configuring FIPS Mode

F60598-04
March 2024

Oracle Linux 9 Installing and Configuring FIPS Mode,

F60598-04

Contents

Preface

Oracle Linux 9: Installing and Configuring FIPS Mode describes how to enable FIPS mode on Oracle Linux 9 systems.

Documentation License

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at https://www.oracle.com/corporate/accessibility/.

Access to Oracle Support for Accessibility

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit https://www.oracle.com/corporate/accessibility/learning-support.html#support-tab.

Diversity and Inclusion

Oracle is fully committed to diversity and inclusion. Oracle respects and values having a diverse workforce that increases thought leadership and innovation. As part of our initiative to build a more inclusive culture that positively impacts our employees, customers, and partners, we are working to remove insensitive terms from our products and documentation. We are also mindful of the necessity to maintain compatibility with our customers' existing technologies and the need to ensure continuity of service as Oracle's offerings and industry standards evolve. Because of these technical constraints, our effort to remove insensitive terms is ongoing and will take time and external cooperation.

1 About the Federal Information Processing Standard Publication 140-3

The Federal Information Processing Standard (FIPS) Publication 140-3 is a computer security standard developed by the U.S. Government and industry working group for the protection of sensitive but unclassified data. See the official FIPS publications at NIST Computer Security Resource Center.

The FIPS 140-3 standard identifies security requirements and specifies tests to validate that cryptographic algorithms have been implemented correctly. See the full FIPS 140-3 standard at FIPS PUB 140-3 for further details and other specifications of the FIPS standard.

The instructions in this document show how to enable Oracle Linux 9 in FIPS mode to use FIPS-compliant algorithms and protocols. For more information about the current status of FIPS certifications, see Oracle Security Evaluations.

2
FIPS 140-3 Compliance in Oracle Linux 9

Oracle Linux provides a set of cryptographic libraries, services, and user-level cryptographic applications that are compliant with the Federal Information Processing Standard (FIPS) Publication 140-3.

FIPS Publication 140-3, Security Requirements for Cryptographic Modules, specifies the security requirements that must be satisfied by a cryptographic module that's used within a security system to protect sensitive, but unclassified information. The NIST/CSE Cryptographic Module Validation Program (CMVP) validates cryptographic modules to FIPS 140-3. Validated products are accepted by the Federal agencies of both the USA and Canada for the protection of sensitive or designated information.

3

Configuring FIPS Mode in Oracle Linux 9

FIPS mode can be configured during the initial installation of Oracle Linux 9 or after installation, as described in the following sections.

Installing Oracle Linux 9 in FIPS Mode

Add `fips=1` to the kernel command line during system installation to automatically configure a new Oracle Linux 9 system to run in FIPS mode from the first boot.

The main benefit of setting FIPS mode during the installation stage is that Oracle Linux 9 generates all system keys by using FIPS compliant algorithms and continuous monitoring tests.

To verify that FIPS mode is enabled, run the following command after Oracle Linux 9 has been installed:

```
sudo fips-mode-setup --check
```

Enabling and Disabling FIPS Mode for Existing Oracle Linux 9 Installations

You can configure a preexisting Oracle Linux 9 installation to run in FIPS mode by using the `fips-mode-setup` utility, which changes the system-wide cryptographic policy, installs the FIPS dracut module, regenerates the system ramdisk, and updates the kernel boot parameters.

> **Note:**
>
> To enable FIPS mode in Oracle Linux containers, see the Managing Containers chapter in the Oracle Linux: Podman User's Guide.

1. Enable FIPS mode:

   ```
   sudo fips-mode-setup --enable
   ```

   The following output is displayed:

   ```
   Kernel initramdisks are being regenerated. This might take some time.
   Setting system policy to FIPS
   Note: System-wide crypto policies are applied on application start-up.
   It is recommended to restart the system for the change of policies
   to fully take place.
   FIPS mode will be enabled.
   Please reboot the system for the setting to take effect.
   ```

   You must reboot the system for the setting to take effect.

2. Verify that FIPS mode has been enabled correctly:

   ```
   sudo fips-mode-setup --check
   ```

   The following output is displayed:

   ```
   FIPS mode is enabled.
   ```

3. To disable FIPS mode:

   ```
   sudo fips-mode-setup --disable
   ```

   The following output is displayed:

   ```
   Setting system policy to DEFAULT
   Note: System-wide crypto policies are applied on application start-up.
   It is recommended to restart the system for the change of policies
   to fully take place.
   FIPS mode will be disabled.
   Please reboot the system for the setting to take effect.
   ```

   You must reboot the system for the setting to take effect.

For more information, see the `fips-mode-setup(8)` manual pages.

4 FIPS 140-3 Validated Modules in Oracle Linux 9

The following sections describe how to review FIPS 140-3 certifications and install FIPS 140-3 validated cryptographic modules in Oracle Linux 9.

Information About Modules That Have Received FIPS 140-3 Validation

The Oracle FIPS Certifications website provides the following information for each module:

- Name and description of the module.
- Status of the FIPS 140-3 validation process.

> **Important:**
>
> To achieve compliance with FIPS Publication 140-3, you must use the package version that the Security Policy document specifies for each respective module only. You can't install and use other versions of the cryptographic modules.

- Package version for the module.
- Certificate number for the module.

After NIST completes its review for each cryptographic module, the status moves from "Review Pending" or "In Progress" to "Validated." You can then click the certificate number for each cryptographic module to review its associated FIPS certificate, and each FIPS certificate links to the relevant Security Policy document for that module. See the "Life-Cycle Assurance" section of those Security Policy documents for details about each module, and instructions with which the Cryptographic officer can verify their installation and configuration.

Installing FIPS Validated Cryptographic Modules for Oracle Linux 9

After you enable FIPS mode on Oracle Linux 9, you can then install FIPS validated cryptographic modules, as required. For information about the software channels that provide packages containing FIPS validated cryptographic modules, see Where Packages for FIPS Validated Cryptographic Modules for Oracle Linux 9 Can Be Found.

The following information applies to systems that are running a fully patched Oracle Linux 9 release that can install and enable FIPS cryptographic modules.

To install FIPS validated cryptographic modules, see the "Life-Cycle Assurance" section of the Security Policy document for the FIPS module that you plan to install.

The Security Policy document explains how to verify that the package is FIPS 140-3 validated, and how to configure the module for FIPS mode. See FIPS Validated Cryptographic Modules for Oracle Linux 9 for the certificate number, which includes a link to the NIST FIPS 140-3 validation page. This page provides details about FIPS certification and the Security Policy document.

FIPS Validated Cryptographic Modules for Oracle Linux 9

The following table describes Oracle's FIPS 140-3 Level 1 certifications for cryptographic components that reside within Oracle Linux 9 for the x86_64 and AARCH64 platforms.

The package versions that are listed reflect information that's found in the logical cryptographic boundary for the specific module. The epoch for packages with the `_fips` suffix is set to `10`, so they supersede any versions of the same package without the `_fips` suffix .

Cryptographic Module Name	Package Version	Certificate Number
Oracle Linux 9 OpenSSL Cryptographic Module	`openssl-libs-3.0.7-24.0.3.el9_fips`	In Progress
Oracle Linux 9 libgcrypt Cryptographic Module	`libgcrypt-1.10.0-10.0.1.el9_2_fips`	In Progress
Oracle Linux 9 NSS Cryptographic Module	`nss-softokn-3.90.0-3.0.1.el9_2_fips`	In Progress
Oracle Linux 9 GnuTLS Cryptographic Module	`gnutls-3.7.6-21.0.1.el9_2_fips`	In Progress
Oracle Linux 9 Kernel Crypto API Cryptographic Module	In Progress	In Progress
Oracle Linux Unbreakable Enterprise Kernel (UEK 7) Cryptographic Module	`kernel-uek-5.15.0-101.103.2.1.el9uek`	In Progress

Where Packages for FIPS Validated Cryptographic Modules for Oracle Linux 9 Can Be Found

The following are the dedicated Unbreakable Linux Network (ULN) channels and yum repository containing FIPS validated cryptographic modules for Oracle Linux 9:

x86_64 Platform:

- `ol9_x86_64_u3_security_validation` ULN channel
- `ol9_u3_security_validation` yum repository

aarch64 Platform:

- `ol9_aarch64_u3_security_validation` ULN channel
- `ol9_u3_security_validation` yum repository

Note that the `ol9_u3_security_validation` yum repository is a common repository name for the x86_64 and aarch64 platforms. This repository contains FIPS validated packages for both platforms and security updates for those packages.

Security updates for the UEK7 cryptographic module are available in the corresponding yum repository and ULN channel. For more information, see the Unbreakable Enterprise Kernel documentation.

For more information about how to manage yum repositories and ULN channels, see Oracle Linux: Managing Software on Oracle Linux.

For specific instructions on installing FIPS validated cryptographic modules, see Installing FIPS Validated Cryptographic Modules for Oracle Linux 9.