ORACLE
Linux

Ten Simple Steps to Enabling FIPS 140-2 Mode in Oracle Linux

Oracle Linux Technical Brief

December 2020

About FIPS 140

The Federal Information Processing Standard (FIPS) 140 is a cryptographic standard developed by the National Institute of Standards and Technology (NIST) in the US for the protection of sensitive but unclassified data. FIPS 140 specifies security requirements for cryptographic modules that encrypt and decrypt data, securely generate cryptographic keys, perform hashing, execute key agreement using industry standard protocols, and generate or verify digital signatures.

The Cryptographic Module Validation Program (CMVP) was established by NIST and the Canadian Centre for Cyber Security (CCCS) of the Government of Canada in July 1995 to oversee testing results of cryptographic modules by accredited third party laboratories. NIST published the first cryptographic standard called FIPS 140-1 in 1994. The current version of the FIPS 140 standard is FIPS 140-2 and was issued in 2001. In March 2019, FIPS 140-3 was announced and is available for testing as of September of 2020. FIPS 140-3 maps to the international standard ISO/IEC 19790:2012. Currently vendors can test to both FIPS 140-2 and FIPS 140-3 however as of September 22nd of 2021, vendors will only be able to test to FIPS 140-3.

FIPS 140 validation is mandatory for vendors selling cryptography into the US and Canadian governments. A number of industry-specific regulations and standards make reference to the FIPS 140-2 requirements. These include Payment Card Industry Security Standards Council (PCI SSC) standards for credit card data processing, Health Insurance Portability and Accountability Act (HIPAA) in the healthcare industry, Joint Interoperability Command (JITC) in the U.S. Military, etc. US Federal Risk and Authorization Management Program (FedRAMP) requirements interpret "approved cryptographic techniques" as the set of cryptographic modules validated per FIPS 140.

As a pre-requisite to performing CMVP validations, Cryptographic Algorithm Validation Program (CAVP) conformance testing is done to validate FIPS-approved and NIST-recommended cryptographic algorithms.

Within the Cryptographic Module Validation Program (CMVP) there are three main phases which are represented by lists on the CMVP website: Implementation Under Test (IUT), Modules in Process (MIP) and Validated Modules.

The IUT list includes modules where the vendor is under contract with an accredited laboratory to perform the validation testing, but nothing has been submitted to the CMVP. Vendors have 18 months to complete testing or be removed from the IUT list.

The Modules in Process List includes modules where laboratories submitted testing results to the CMVP, and the validation process is in one of these phases:

- Review pending—testing has completed at the laboratory and the report has been submitted to the CMVP
- In review—the submission has been assigned and is being reviewed by a CMVP reviewer
- Coordination—an iterative phase where the CMVP reviewer submits report comments back to the laboratory who responds to them with input from the vendor. This phase continues until the CMVP reviewer has closed off all the comments
- Finalization—documents are finalized and a certificate number is assigned

The Validated Modules list includes modules which completed validations against the FIPS 140 standard. Modules are considered active for five years from their validated date.

For Oracle specific CMVP module listings, please see oracle.com/corporate/security-practices/assurance/development/external-security-evaluations/fips/certifications.html. For additional information on Oracle's FIPS 140 status and participation, please email seceval_us@oracle.com.

Why FIPS 140-2?

Encryption products purchased by US and Canadian government agencies are required by law to undergo the FIPS 140-2 validation. These products are validated against FIPS 140-2 at security levels ranging from level 1 (lowest) to level 4 (highest). The testing and validation of products against the FIPS 140-2 criteria is performed by NIST and CSEC-approved and accredited certification laboratories.

FedRAMP-authorized cloud solutions that use encryption as a mechanism to meet a security requirement, must be FIPS 140-2 validated under the CMVP.

Oracle's Commitment to FIPS 140

Oracle is committed to the FIPS 140 standards as these standards reflect global market demand, as well as procurement and regulatory requirements. Since 1999, Oracle has been increasing the number of validations performed against the FIPS 140 standard. Oracle's validation approach includes a combination of FIPS 140 validated open source cryptographic libraries and proprietary 3rd party cryptographic modules.

Oracle includes FIPS 140-2 Level 1 validated cryptography included in distributions of Oracle Linux 6 and Oracle Linux 7 on x86-64 containing Red Hat Compatible Kernel and Oracle's Unbreakable Enterprise Kernel. Oracle "vendor affirms" that the FIPS validation will be maintained on all other x86-64 equivalent hardware. Oracle Linux 8 cryptographic module validation was in progress when this paper was published.

Oracle does perform regular maintenance of its FIPS 140 validations to bring its validation status in line with the latest security updates. However it takes a long time to go through the FIPS 140 validation process, and it is impossible to do validation updates to every patch release so maintenance of FIPS 140 validations are strategically targeted. The re-validations are also partially dependent upon the package releases of the Linux open source community.

Oracle Linux FIPS 140-2 Level 1 Certified Packages

The FIPS 140 validation process is an expensive and time-consuming process. Vendors must hire a third-party lab to do the validation; most vendors also hire consultants to write documentation that is required as a part of the process. The validation process for FIPS 140-2 requires that vendors prove they have implemented their crypto correctly against the FIPS 140 Standard requirements. This proof is accomplished via the independent 3rd party labs that validate each cryptographic module is correctly implementing the FIPS 140 requirements as defined in FIPS PUB 140 Standard.

Oracle's FIPS 140 strategy is to certify the cryptographic components only that execute on a general purpose computing platform with no specific physical requirements at Security Level 1. This is because most customer use cases only require FIPS 140 Level 1. This allows Oracle to port these cryptographic components to other similar general purpose computing platforms and maintain "Vendor Affirmation" compliance to the FIPS 140 standard without undergoing re-validations. FIPS 140 re-validation is required if the cryptographic components significantly change..

In order to be FIPS 140-2 compliant, customers must start by running the specific FIPS certified packages on the hardware that was specified for the FIPS 140-2 validation or on "Vendor Affirmed" Hardware. Oracle recommends customers enable security updates as the systems get patched regularly to address bugs and security updates even though they may fall out of FIPS 140 compliance. It is more desirable to maintain a strong security posture than seek full FIPS compliance. As updates to Oracle Linux evolve, Oracle is committed to ensuring that its FIPS 140 compliance maps as closely as possible to the latest security update release of the product.

Oracle Linux FIPS Certified packages can be obtained from Oracle Linux yum servers:

- Oracle Linux 7: https://yum.oracle.com/repo/OracleLinux/OL7/security/validation/x86_64/index.html
- Oracle Linux 6: https://yum.oracle.com/repo/OracleLinux/OL6/security/validation/x86_64/index.html

Oracle Linux 7 FIPS 140-2 Level 1 consists of the following certificates and package versions:

- 3616 - Oracle Linux 7 NSS Cryptographic Module
    - nss-softokn-3.36.0-5.0.1.el7_5.x86_64.rpm
- 3604 - Oracle Linux 7 libgcrypt Cryptographic Module
    - libgcrypt-1.5.3-14.el7.x86_64.rpm
- 3590 - Oracle Linux 7 OpenSSH Server Cryptographic Module
    - openssh-server-7.4p1-16.el7.x86_64.rpm
- 3582 - Oracle Linux 7 OpenSSH Client Cryptographic Module
    - openssh-clients-7.4p1-16.el7.x86_64.rpm
- 3474 - Oracle Linux 7.5 and 7.6 OpenSSL Cryptographic Module
    - openssl-libs-1.0.2k-12.0.3.el7.x86_64 and openssl-libs-1.0.2k-16.0.1.el7.x86_64
- 3348 - Oracle Linux 7.3 Unbreakable Enterprise Kernel (UEK 4)
    - kernel-uek-4.1.12-124.16.4.el7uek.x86_64
- 3342 - Oracle Linux 7.3 Kernel Crypto API
    - kernel-3.10.0-862.3.3.0.1.el7.x86_64
- 3215 - Oracle Linux 7.3 libgcrypt Cryptographic Module
    - libgcrypt-1.5.3-13.el7_3.1.x86_64
- 3169 - Oracle Linux 7.3 GnuTLS Cryptographic Module
    - gnutls-3.3.24-1.0.3.el7.x86_64.rpm, gmp-6.0.0-12.el7_1.x86_64.rpm, nettle-2.7.1-8.el7.x86_64.rpm
- 3168 - Oracle Linux 7.3 Libreswan Cryptographic Module
    - libreswan-3.15-8.0.1.el7.x86_64
- 3143 - Oracle Linux 7.3 NSS Cryptographic Module
    - nss-softokn-3.16.2.3-14.4.0.1.el7.x86_64
- 3032 - Oracle Linux 7.3 OpenSSH Client Cryptographic Module
    - openssh-clients-6.6.1p1-35.el7_3.x86_64
- 3028 - Oracle Linux 7.3 OpenSSH Server Cryptographic Module
    - openssh-server-6.6.1p1-35.el7_3.x86_64
- 3017 - Oracle Linux 7.3 OpenSSL Cryptographic Module
    - openssl-1.0.1e-60.0.1.el7_3.1.x86_64

Oracle Linux 6 FIPS 140-2 Level 1 consists of the following certificates and package versions:

- 3421 - Oracle Linux 6.9 Kernel Crypto API
  - kernel-2.6.32-754.3.5.0.1.el6.x86_64
- 3348 - Oracle Linux 6.9 Unbreakable Enterprise Kernel (UEK 4)
  - kernel-uek-4.1.12-124.16.4.el6uek.x86_64
- 3170 - Oracle Linux 6.9 Libreswan Cryptographic Module
  - libreswan-3.15-7.5.0.1.el6_9.x86_64
- 3111 - Oracle Linux 6.9 NSS Cryptographic Module
  - nss-softokn-3.14.3-23.3.0.1.el6_8.x86_64
- 3031 - Oracle Linux 6.9 OpenSSH Server Cryptographic Module
  - openssh-server-5.3p1-122.el6.x86_64
- 3030 - Oracle Linux 6 OpenSSH Client Cryptographic Module
  - openssh-clients-5.3p1-122.el6.x86_64
- 3017 - Oracle Linux 6 OpenSSL Cryptographic Module
  - openssl-1.0.1e-57.0.1.el6.x86_64

Enabling FIPS 140-2 Mode

Installing and enabling any of the FIPS 140-2 validated kernels requires the correct versions of the kernel and all the package versions it depends on.

Once the packages are installed, you can enable FIPS mode by following the Oracle Linux documentation:

- Oracle Linux 7
- Oracle Linux 6

The instructions below are using Oracle Linux 7. To enable FIPS mode, do the following:

1. Ensure the system is at Oracle Linux 7 Update 6.
2. Ensure your system is registered with the Unbreakable Linux Network (ULN) and that the `ol7_x86_64_security_validation` and `ol7_x86_64_latest` channels are enabled.

   Alternatively, you can enable the ol7_latest channel as follows:

   ```
   # yum-config-manager --enable ol7_x86_64_latest
   ```
3. Install the required packages.
   a. Install `hmaccalc`.

      ```
      # yum install hmaccalc-0.9.13-4.el7.x86_64
      ```
   b. The dracut-fips package provides the modules to build a dracut initramfs file system that performs an integrity check.

      ```
      # yum install dracut-fips-033-463.0.2.el7.x86_64 dracut-config-rescue-033-463.0.2.el7.x86_64 dracut-network-033-463.0.2.el7.x86_64
      ```

c. If the system CPU supports AES New Instructions (AES-NI), install the dracut-fips-aesni package.

```
# yum install dracut-fips-aesni-033-463.0.2.el7.x86_64
```

d. Install the OpenSSL cryptographic module.

```
# yum install openssl-1.0.1e-60.0.1.el7_3.1.x86_64
```

e. Install the OpenSSH cryptographic modules.

```
# yum install openssh-server-6.6.1p1-35.el7_3.x86_64 openssh-clients-
  6.6.1p1-35.el7_3.x86_64
```

4. Choose the kernel you are going to run. Either the Unbreakable Enterprise Kernel (UEK) or Red-Hat Compatible Kernel (RHCK).

5. Recreate the initramfs file system.

```
# dracut -f
```

6. Configure the boot loader so that the system boots into FIPS mode.

a. Identify the boot partition and the UUID of the partition, for example:

```
# df /boot
Filesystem     1K-blocks   Used Available Use% Mounted on
/dev/sda1         508588 294476    214112  58% /boot
# blkid /dev/sda1
/dev/sda1: UUID="6046308a-75fc-418e-b284-72d8bfad34ba" TYPE="xfs"
```

b. As the root user, open `/etc/default/grub` for editing.

c. If /boot or /boot/efi reside on a separate partition to the root partition, add the `boot=UUID=`***`boot_UUID`*** line to the boot loader configuration. This step ensures that the system can identify the appropriate boot device.

```
GRUB_CMDLINE_LINUX="vconsole.font=latarcyrheb-sun16 rd.lvm.lv=ol/swap
  rd.lvm.lv=ol/root crashkernel=auto vconsole.keymap=uk rhgb quiet
  boot=UUID=6046308a-75fc-418e-b284-72d8bfad34ba
```

d. Add the `fips=1` option to the boot loader configuration.

e. Save your changes and then close `/etc/default/grub`.

```
GRUB_CMDLINE_LINUX="vconsole.font=latarcyrheb-sun16 rd.lvm.lv=ol/swap
  rd.lvm.lv=ol/root crashkernel=auto vconsole.keymap=uk rhgb quiet
  boot=UUID=6046308a-75fc-418e-b284-72d8bfad34ba fips=1
```

7. Rebuild the GRUB configuration.

- On BIOS-based systems, run the following command:

```
# grub2-mkconfig -o /boot/grub2/grub.cfg
```

- On UEFI-based systems, run the following command:

```
# grub2-mkconfig -o /boot/efi/EFI/redhat/grub.cfg
```

8. Oracle Linux 7 doesn't ship with prelink enabled, but if you have prelink enabled, you must disable it and remove all existing prelinked binaries.
    a. As the root user, open `/etc/sysconfig/prelink` for editing.
    b. Set `PRELINKING=no`.
    c. Save your changes and then close `/etc/sysconfig/prelink`.
    d. Run the following command to remove all existing prelinking:

```
# prelink -u -a
```

9. Reboot the system.
10. Verify that FIPS is enabled, as follows:

```
# cat /proc/sys/crypto/fips_enabled
1
```

Upon completion of these technical steps, the system is running in FIPS 140-2 mode.

Conclusion

Your organization may be required to operate systems with FIPS 140 because of regulatory or other organizational requirements. Oracle includes FIPS 140-2 Level 1 validated cryptography included in distributions of Oracle Linux 6 and Oracle Linux 7 on x86-64 containing Red Hat Compatible Kernel and Oracle's Unbreakable Enterprise Kernel. Building an Oracle Linux system with FIPS-140 mode enabled can be done in just 10 easy steps.

For more information about Oracle Linux, please visit oracle.com/linux.