FIPS

- What is FIPS 140?
- Why FIPS compliance matters
- How Docker Hardened Images support FIPS compliance
- Identify images that support FIPS
- Use a FIPS variant
- View the FIPS attestation

{{< summary-bar feature_name="Docker Hardened Images" >}}

What is FIPS 140?

FIPS 140 is a U.S. government standard that defines security requirements for cryptographic modules that protect sensitive information. It is widely used in regulated environments such as government, healthcare, and financial services.

FIPS certification is managed by the NIST Cryptographic Module Validation Program (CMVP), which ensures cryptographic modules meet rigorous security standards.

Why FIPS compliance matters

FIPS 140 compliance is required or strongly recommended in many regulated environments where sensitive data must be protected, such as government, healthcare, finance, and defense. These standards ensure that cryptographic operations are performed using vetted, trusted algorithms implemented in secure modules.

Using software components that rely on validated cryptographic modules can help organizations:

- Satisfy federal and industry mandates, such as FedRAMP, which require or strongly recommend FIPS 140-validated cryptography.

- Demonstrate audit readiness, with verifiable evidence of secure, standards-based cryptographic practices.
- Reduce security risk, by blocking unapproved or unsafe algorithms (e.g., MD5) and ensuring consistent behavior across environments.

How Docker Hardened Images support FIPS compliance

While Docker Hardened Images are available to all, the FIPS variant requires a paid Docker Hardened Images subscription.

Docker Hardened Images (DHIs) include variants that use cryptographic modules validated under FIPS 140. These images are intended to help organizations meet compliance requirements by incorporating components that meet the standard.

- FIPS image variants use cryptographic modules that are already validated under FIPS 140.
- These variants are built and maintained by Docker to support environments with regulatory or compliance needs.
- Docker provides signed test attestations that document the use of validated cryptographic modules. These attestations can support internal audits and compliance reporting.
- Entropy sources (random number generation for cryptographic operations) vary by base image. Debian-based images use the OpenSSL entropy source, while Alpine-based images source entropy from the host kernel.

> [!NOTE]
>
> Using a FIPS image variant helps meet compliance requirements but does not make an application or system fully compliant. Compliance depends on how the image is integrated and used within the broader system.

Identify images that support FIPS

Docker Hardened Images that support FIPS are marked as **FIPS** compliant in the Docker Hardened Images catalog.

To find DHI repositories with FIPS image variants, search the catalog and:

- Use the **Compliance** filter on the catalog page and select **FIPS**

- Look for **FIPS** compliant on individual image listings

These indicators help you quickly locate repositories that support FIPS-based compliance needs. Image variants that include FIPS support will have a tag ending with `-fips`, such as `3.13-fips`.

Use a FIPS variant

To use a FIPS variant, you must mirror the repository and then pull the FIPS image from your mirrored repository.

View the FIPS attestation

The FIPS variants of Docker Hardened Images contain a FIPS attestation that lists the actual cryptographic modules included in the image.

You can retrieve and inspect the FIPS attestation using the Docker Scout CLI:

```
$ docker scout attest get \
  --predicate-type https://docker.com/dhi/fips/v0.1 \
  --predicate \
  dhi.io/<image>:<tag>
```

For example:

```
$ docker scout attest get \
  --predicate-type https://docker.com/dhi/fips/v0.1 \
  --predicate \
  dhi.io/python:3.13-fips
```

The attestation output is a JSON array describing the cryptographic modules included in the image and their compliance status. For example:

```
[
  {
    "certification": "CMVP #4985",
    "certificationUrl": "https://csrc.nist.gov/projects/cryptographic-module-validation-
program/certificate/4985",
    "name": "OpenSSL FIPS Provider",
    "package": "pkg:dhi/openssl-provider-fips@3.1.2",
```

```
    "standard": "FIPS 140-3",
    "status": "active",
    "sunsetDate": "2030-03-10",
    "version": "3.1.2"
  }
]
```

□□□ #2
□ □□□ □□□ 2026-10-31 19:15:35 UTC
□ □□□ □□□ 2026-10-31 19:15:37 UTC