# Table of Contents

FIPS 140–2 Compliance for Caché Database Encryption.................................................. 1

1 Supported Platforms ........................................................................................................ 1
2 Enabling FIPS Support ..................................................................................................... 1
3 Startup Behavior and cconsole.log .................................................................................. 2
FIPS 140–2 Compliance for Caché Database Encryption


1 Supported Platforms

Caché supports FIPS 140-2–compliant cryptography for database encryption on Red Hat Enterprise Linux 6.6 (or later minor versions) and Red Hat Enterprise Linux 7.1 (or later minor versions) for x86-64. For each supported version, Red Hat has a certificate of validation for the OpenSSL libcrypto.so and libssl.so libraries; this certificate is available at the site listed below.

Red Hat 6.6, 7.1, 7.2, and 7.3

- The libraries are libcrypto.so.1.0.1e and libssl.so.1.0.1e
- The certificate is https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/2441

Red Hat 7.4 and later

- The libraries are libcrypto.so.1.0.2k and libssl.so.1.0.2k
- The certificate is https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/3016


2 Enabling FIPS Support

To enable Caché support for FIPS 140–2 compliant cryptography for database encryption, do the following:

1. Download and install the openssl package from the RedHat repository (rhel-6-server-rpms or rhel-7-server-rpms, depending on which version of Red Hat Enterprise Linux for x86-64 you are using).

2. Enable FIPS mode for the operating system. For information, see one of the following:

   Be sure to reboot and to check that FIPS mode is enabled.

3. Check the directory /usr/lib64 for the following symbolic links. If these do not exist, create them:
• The symbolic link `libssl.so` should point to the appropriate file (such as `libssl.so.1.0.2k`), in the same directory.
• The symbolic link `libcrypto.so` should point to the appropriate file (such as `libcrypto.so.1.0.2k`), in the same directory.

4. In Caché, specify the **FIPSMode** CPF parameter as **True** (1). To do so:
   a. Open the Management Portal.
   b. Select **System Administration > Configuration > Additional Settings > Startup**.
      Here you will see a row for **FIPSMode**.
   c. Specify the value for **FIPSMode** as **True** and save your change.

5. Restart Caché.


### 3 Startup Behavior and cconsole.log

When Caché is started:

• If **FIPSMode** is 0, Caché native cryptography is used, including optimized assembly code using Intel AES-NI hardware instructions, if supported by the CPU. In this mode, Caché writes the following to `cconsole.log` upon startup:

  FIPS 140-2 compliant cryptography for database encryption is not configured in cache.cpf

• If **FIPSMode** is 1, Caché attempts to resolve references to functions in the `/usr/lib64/libcrypto.so` FIPS-validated library, and then attempts to initialize the library in FIPS mode. If these steps are successful, Caché writes the following to `cconsole.log`:

  FIPS 140-2 compliant cryptography for database encryption is enabled for this instance.

• If **FIPSMode** is 1, but the initialization of the library is unsuccessful, Caché does not start. In this case, `cconsole.log` contains the following message:

  FIPS 140-2 compliant cryptography for database encryption initialization failed. Aborting.

• On platforms other than lnxrhx64, if **FIPSMode** is 1, Caché native cryptography is used, and Caché writes the following to `cconsole.log`:

  FIPS 140-2 compliant cryptography for database encryption is not supported on this platform.