FIPS 140–2 Compliance for Database Encryption

Version 2020.3
2021-02-04

InterSystems Corporation 1 Memorial Drive Cambridge MA 02142 www.intersystems.com

FIPS 140–2 Compliance for Database Encryption
InterSystems IRIS Data Platform Version 2020.3 2021-02-04

For Support questions about any InterSystems products, contact:

InterSystems Worldwide Response Center (WRC)
Tel: +1-617-621-0700
Tel: +44 (0) 844 854 2917
Email: support@InterSystems.com

Table of Contents

FIPS 140–2 Compliance for Database Encryption

On specific platforms, InterSystems IRIS® supports FIPS 140–2 compliant cryptography for database encryption. (FIPS 140–2 refers to Federal Information Processing Standard Publication 140-2, which is available at https://csrc.nist.gov/csrc/media/publications/fips/140/2/final/documents/fips1402.pdf.)

1 Supported Platforms

InterSystems IRIS supports FIPS 140-2–compliant cryptography for database encryption on Red Hat Enterprise Linux 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 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

For information about Red Hat support for government standards, see hhttps://access.redhat.com/articles/2918071.

2 Enabling FIPS Support

To enable InterSystems IRIS 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:
   - https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/html/Security_Guide/sect-Security_Guide-Federal_Standards_And_Regulations-Federal_Information_Processing_Standard.html
   - https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/Security_Guide/chap-Federal_Standards_and_Regulations.html

   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 InterSystems IRIS, 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 InterSystems IRIS.

You can then continue performing any activities that involve database encryption and they will be FIPS-compliant.

Note: There is no need to perform any database re-encryption operations when you enable or disable support for the FIPS-compliant libraries. InterSystems IRIS uses the same encryption key and encryption algorithm whether or not it is operating in a FIPS-compliant mode.

For background on encrypted databases, see "Using Encrypted Databases" in the chapter "Managed Key Encryption" in *Security Administration Guide*.

3 Startup Behavior and messages.log

When InterSystems IRIS is started:

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

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

- If **FIPSMode** is 1, InterSystems IRIS 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, InterSystems IRIS writes the following to messages.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, InterSystems IRIS does not start. In this case, messages.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, InterSystems IRIS native cryptography is used, and InterSystems IRIS writes the following to messages.log:

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