FIPS 140–2 Compliance for Database Encryption

Version 2019.4
2020-01-28

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

FIPS 140–2 Compliance for Database Encryption
InterSystems IRIS Data Platform Version 2019.4 2020-01-28
Copyright © 2020 InterSystems Corporation
All rights reserved.

InterSystems, InterSystems IRIS, InterSystems Caché, InterSystems Ensemble, and InterSystems HealthShare are registered trademarks of InterSystems Corporation.

All other brand or product names used herein are trademarks or registered trademarks of their respective companies or organizations.

This document contains trade secret and confidential information which is the property of InterSystems Corporation, One Memorial Drive, Cambridge, MA 02142, or its affiliates, and is furnished for the sole purpose of the operation and maintenance of the products of InterSystems Corporation. No part of this publication is to be used for any other purpose, and this publication is not to be reproduced, copied, disclosed, transmitted, stored in a retrieval system or translated into any human or computer language, in any form, by any means, in whole or in part, without the express prior written consent of InterSystems Corporation.

The copying, use and disposition of this document and the software programs described herein is prohibited except to the limited extent set forth in the standard software license agreement(s) of InterSystems Corporation covering such programs and related documentation. InterSystems Corporation makes no representations and warranties concerning such software programs other than those set forth in such standard software license agreement(s). In addition, the liability of InterSystems Corporation for any losses or damages relating to or arising out of the use of such software programs is limited in the manner set forth in such standard software license agreement(s).

THE FOREGOING IS A GENERAL SUMMARY OF THE RESTRICTIONS AND LIMITATIONS IMPOSED BY INTERSYSTEMS CORPORATION ON THE USE OF, AND LIABILITY ARISING FROM, ITS COMPUTER SOFTWARE. FOR COMPLETE INFORMATION REFERENCE SHOULD BE MADE TO THE STANDARD SOFTWARE LICENSE AGREEMENT(S) OF INTERSYSTEMS CORPORATION, COPIES OF WHICH WILL BE MADE AVAILABLE UPON REQUEST.

InterSystems Corporation disclaims responsibility for errors which may appear in this document, and it reserves the right, in its sole discretion and without notice, to make substitutions and modifications in the products and practices described in this document.

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 1

1 Supported Platforms 1

2 Enabling FIPS Support 1

3 Startup Behavior and messages.log 2

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 http://csrc.nist.gov/publications/fips/fips140-2/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 https://www.redhat.com/en/technologies/industries/government/standards.

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.
6. Enable and configure encrypted databases as outlined in "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.
  ```