Gentran Integration Suite™

Federal Information Processing Standards

Version 4.3

Sterling Commerce
An IBM Company

Federal Information Processing Standards (FIPS) 140-2

To conform to the security requirements of FIPS 200, applications must use cryptographic modules certified by the Cryptographic Module Validation Program and compliant with FIPS 140-1 or 140-2. The minimum requirements for the use of validated cryptography by applications are:

- All cryptographic operations, including key generation, must be performed by validated cryptographic modules.
- Only approved security functions are permitted.
- Only approved key establishment techniques are permitted.

FIPS 140-2 with Application

The Certicom Government Service Edition (GSE) is a FIPS 140-2 Level 1 certified cryptographic module distributed with Application. GSE is a low-level cryptographic toolkit written in Java that implements a variety of security functions, including unapproved security functions.

When in FIPS mode, Application performs the following tasks:

- Enables the GSE FIPS state machine and invokes power-on self-tests.
- Funnels cryptographic function calls from the core system to the GSE.

Installing FIPS

During a new installation, when asked if you want to run in FIPS mode, select TRUE.

Enabling and Disabling FIPS Mode

You can enable FIPS mode during the installation process or manually after the install.

To manually enable FIPS mode:

1. In the install_dir/properties directory, locate the security.properties file.
2. Open the security.properties file in a text editor.
3. Specify the following configurations:
   FIPSMode=true
4. Save and close the security.properties file.
5. Restart the server.
   This is necessary for the changes to be recognized in the system.

Note: If you make changes to the security.properties file, be sure to make the same changes to the security.properties.in file. This will prevent your customized settings from being overwritten. You should use the security property file to customize FIPS rather than editing Application property files directly.

To manually disable FIPS mode:

1. In the install_dir/properties directory, locate the security.properties file.

2. Open the security.properties file in a text editor.
3. Specify the following configurations:
   FIPSMode=false
4. Save and close the security.properties file.
5. Restart the server.
   This is necessary for the changes to be recognized in the system.

Verifying Licenses

You should verify that you have a license for operating in FIPS mode before it is enabled. The Application will check your license at start up and will not start if FIPS mode is enabled but not licensed.