FIPS Compliance Guide

Version 1.0

December 2023

Contents

Introduction

FIPS is a complex topic with many interrelated aspects. This guide attempts to introduce the concepts and how they apply to the Pyramid platform to configure the platform for FIPS compliance.

Disclaimers

BETA: As of version 2023.10 Pyramid offers the ability to run the platform in 'FIPS' mode. However, this is a **beta implementation** of the capability, and it should not be used in production until it is formally released.

The guide is by no means an exhaustive treatise on the FIPS topic, and we would encourage any organization considering or requiring their Pyramid installation to be FIPS compliant to conduct their own research and reading on the topic in order to address their own particular concerns and scenarios.

While Pyramid Analytics makes every effort to support a range of operating systems, databases and authentication providers, certain combinations or versions of these third-party components may preclude the support of Pyramid running in FIPS mode. Please consult the Appendix of this document where known restrictions are listed before embarking on implementing Pyramid in FIPS mode.

Definition of Terms

The terms "FIPS 140-2 compliant," "FIPS 140-2 compliance," and "FIPS 140-2-compliant mode" are defined here for use and clarity. These terms are not recognized or defined government terms. The United States and Canadian governments recognize the validation of cryptographic modules against standards like FIPS 140-2 instead of using cryptographic modules in a specified or conformant manner.

In this guide, we use FIPS 140-2-compliant, FIPS 140-2 compliance, and FIPS 140-2-compliant mode to mean that Pyramid 2023.10 and later versions can be configured to use only FIPS 140-2-validated instances of algorithms and hashing functions in all instances in which encrypted or hashed data is imported to or exported from Pyramid 2023.10 and later versions. Additionally, this means that Pyramid 2023.10 and later versions will manage keys in a secure manner, as is required of FIPS 140-2-validated cryptographic modules. The key-management process also includes both key generation and key storage.

We use "certified" here to mean that the instance of the algorithm is FIPS 140-2 validated or that the operating system contains FIPS140-2-validated instances of algorithms.

What is FIPS?

Federal Information Processing Standard (FIPS) is a standard developed by the following two government bodies:

- The National Institute of Standards and Technology (NIST) in the United States
- The Communications Security Establishment (CSE) in Canada

FIPS standards are either recommended or mandated for use in federal government-operated IT systems in the United States and Canada.

What is FIPS 140-2?

FIPS 140-2 is a statement that's titled "Security Requirements for Cryptographic Modules." It specifies which encryption algorithms and which hashing algorithms can be used and how encryption keys are to be generated and managed. Some hardware, software, and processes that contain the algorithms can be considered FIPS 140-2 certified, and other hardware, software, and processes that call the correct algorithms can be considered FIPS 140-2 compliant.

Compliant

Pyramid from version 2023.10 onward can be configured to run in a manner that is compliant with FIPS 140-2. To configure Pyramid 2023.10 and later versions in this manner, it must run on an operating system that is itself FIPS 140-2 compliant or that provides cryptographic modules that are certified. The difference between compliance and certification is not subtle. Algorithms can be certified. It is insufficient to use an algorithm just because it is listed on the approved lists in FIPS 140-2. Instead, you must use an instance of such an algorithm that is certified. This means the instance is government-validated. Certification requires testing and verification by a U. S. or Canadian government-approved evaluation lab. Windows Server 2012 and later versions, and Windows 8 and later versions contain the certified instance of each allowed algorithm. Most importantly, a call to each of these algorithms provides only the certified instance.

We detail the requirements for enabling FIPS mode for RedHat8 below, but of course other Pyramid supported distributions of Linux also offer FIPS mode support. Please consult the respective installation or configuration requirements for the version of Linux being used.

All applications that perform encryption or hashing and that run on a certified version of Windows or Linux can be compliant by using only the certified instances of the approved algorithms and by complying with the key-generation and key-management requirements. This requires either using the OS function for key generation and key management or complying with key-generation and key-management requirements within the application. Areas in a FIPS-compliant application may exist where noncompliant algorithms or processes are enabled. For example, some internal processes that stay in the system and some external data that's slated to be additionally encrypted by a certified algorithm instance are allowed.

Pyramid FIPS Compliance Overview

Pyramid 2023.10 and later versions can be FIPS 140-2 compliant because it can be configured to run with FIPS 140-2-certified algorithm instances.

Windows

Installing Pyramid 2023.10 and later versions on a host that's running Windows Server 2016 or later from one of the following list of Windows servers.

Windows Requirements

The FIPS mode must be set before Pyramid 2023.10 or a later version is started. To set the FIPS mode, follow these steps:

1. Log on to Windows as a Windows system administrator.
2. Select Start.
3. Select Control Panel.
4. Select Administrative Tools. (You may have to switch to large Icons for the next step.)
5. Select Local Security Policy. The Local Security Settings window appears.
6. In the navigation pane, select Local Policies > Security Options.
7. In the pane on the right, double-click System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing.
8. In the dialog box that appears, select Enabled > Apply.
9. Select OK.
10. Close the Local Security Settings window.

Linux

Each distribution of Linux will have its own subtle differences in how to enable or install in FIPS mode. In this document we will use RedHat8 as an example, but the installation requirements for FIPS mode for the Linux distribution you are using, if not RedHat8, should be consulted in detail.

Installing RedHat8 in FIPS mode

Starting the installation in FIPS mode is the recommended method if you aim for FIPS compliance.

To ensure that your RHEL system generates and uses all cryptographic keys only with FIPS-approved algorithms, you must switch RHEL to FIPS mode.

You can enable FIPS mode by using one of the following methods:

- Starting the installation in FIPS mode
- Switching the system into FIPS mode after the installation

If you aim for FIPS compliance, start the RedHat installation in FIPS mode. This avoids cryptographic key material regeneration and re-evaluation of the compliance of the resulting system associated with converting already deployed systems.

Important: Only enabling FIPS mode during the RHEL installation ensures that the system generates all keys with FIPS-approved algorithms and continuous monitoring tests in place.

FIPS Installation Procedure

- Add the fips=1 option to the kernel command line during the system installation.
- During the software selection stage, do not install any third-party software.
- After the installation, the system starts in FIPS mode automatically.

FIPS Verification

After the system starts, check that FIPS mode is enabled:

```
$ fips-mode-setup --check

FIPS mode is enabled.
```

To operate a FIPS-compliant system, create all cryptographic key material in FIPS mode. Furthermore, the cryptographic key material must never leave the FIPS environment unless it is securely wrapped and never unwrapped in non-FIPS environments.

Switching the system to FIPS mode by using the fips-mode-setup tool does not guarantee compliance with the FIPS 140 standard. Re-generating all cryptographic keys after setting the system to FIPS mode may not be possible. For example, in the case of an existing IdM realm with users' cryptographic keys you cannot re-generate all the keys. If you cannot start the installation in FIPS mode, always enable FIPS mode as the first step after the installation, before you make any post-installation configuration steps or install any workloads.

The fips-mode-setup tool also uses the FIPS system-wide cryptographic policy internally. But on top of what the update-crypto-policies --set FIPS command does, fips-mode-setup ensures the installation of the FIPS dracut module by using the fips-finish-install tool, it also adds the fips=1 boot option to the kernel command line and regenerates the initial RAM disk.

Furthermore, enforcement of restrictions required in FIPS mode depends on the contents of the /proc/sys/crypto/fips_enabled file. If the file contains 1, RHEL core cryptographic components switch to mode, in which they use only FIPS-approved implementations of cryptographic algorithms. If /proc/sys/crypto/fips_enabled contains 0, the cryptographic components do not enable their FIPS mode.

The FIPS system-wide cryptographic policy helps to configure higher-level restrictions. Therefore, communication protocols supporting cryptographic agility do not announce ciphers that the system refuses when selected. For example, the ChaCha20 algorithm is not FIPS-approved, and the FIPS cryptographic policy ensures that TLS servers and clients do not announce the TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 TLS cipher suite, because any attempt to use such a cipher fails.

If you operate RHEL in FIPS mode and use an application providing it’s own FIPS-mode-related configuration options, ignore these options and the corresponding application guidance. The system running in FIPS mode and the system-wide cryptographic policies enforce only FIPS-compliant cryptography. For example, the Node.js configuration option --

enable-fips is ignored if the system runs in FIPS mode. If you use the --enable-fips option on a system not running in FIPS mode, you do not meet the FIPS-140 compliance requirements.

Pyramid FIPS Configuration

Installing a new instance of Pyramid in FIPS compliance mode

The Pyramid full installer gives the option to install Pyramid in FIPS mode. Currently, only new, clean installations are supported through this mechanism. By choosing FIPS mode at the start of the installation process, this enforces the creation of a secure connection to the database running the Pyramid repository. It is advisable to have the required components and certificates to hand to create this secure connection before starting the FIPS enabled installation process.

Upgrading and existing Pyramid installation to FIPS compliance mode

Pyramid does not currently offer an automated process for upgrading and existing instance of Pyramid to support FIPS mode.

A documented, manual, step by step guide for upgrading to FIPS compliance will be available shortly.

Pyramid Repository

For FIPS compliance, a secure connection is required to the database acting as the Pyramid Repository. As noted earlier, when installing in FIPS compliant mode, the installation process will enforce an encrypted connection to the Pyramid Repository.

After installation

As mentioned previously, to maintain FIPS compliance, any data source to be accessed by users needs to be accessed via a secure connection.

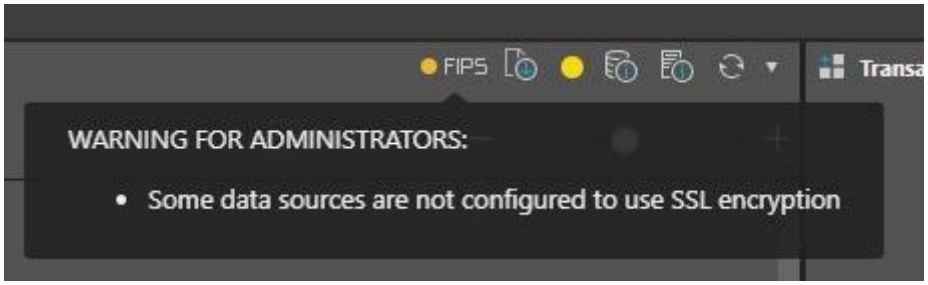
Again, as stated previously, this does not necessarily imply FIPS compliance, that must be provided by the vendor of the database or data source concerned.

There are also other factors to consider providing full FIPS compliance. As well as enforcing secure connection to the database running the Pyramid Repository, encrypted network traffic between Pyramid services is also enforced. Running in FIPS mode will also ensure that FIPS certified encryption algorithms are used to encrypt the data in flight.

Other, non data source connections must also be encrypted, for example, the connection to the authentication engine that Pyramid is using like Active Directory.

As Pyramid is a dynamic environment, where connections to other data sources may be created or dropped, an indicator is offered to assess the current state of FIPS compliance.

This can be found on the Diagnostics Dashboard in the Admin Hub. An indicator is provided to show the degree of FIPS compliance that is currently in place. This has three modes:



- Green - all data sources and features secured.
- Amber – at least one data source has an unsecured connection.
- Red – More than one feature not secured, e.g. LDAP as well as data.

See Pyramid Help for more details on the Diagnostics Dashboard.

Additionally, to aid in determining which data source connections are encrypted or not, the Data Source listing page in Admin shows a column where the row is checked if the data connection is encrypted. This can be sorted to show all encrypted connections grouped together at the top or bottom of the list, or alphabetically sorted by connection name or type.

See Pyramid Help for more information on Data Source listings.

FIPS and connection to eternal data sources

The nature of the Pyramid platform means that it will be connecting to data sources not under the control of Pyramid. To conform to FIPS compliance, these connections must be secure. Pyramid provides mechanisms for creating, managing, and maintaining secure connections to a variety of data sources.

However, establishing a secure connection to a data source does not automatically imply that the data source itself is FIPS compliant. This must be established from the vendor of the data storage mechanism being accessed by Pyramid.

Pyramid running in FIPS compliant mode does NOT enforce secure connections to data. It is up to the administrator for the Pyramid system to decide and enforce if all connections are to be secured or not.

Certificate manager

When establishing secure connections to data sources, those data sources may not provide a security certificate signed by a security certificate authority, but may provide their own, self-signed or root, certificates for secure connections.

In this case, these certificates must be managed within the Pyramid platform. The Certificate Manager available in the Admin Hub provides a mechanism for managing these types of

certificates and must be used when connection to those data sources that do not provide a certificate authority issued security certificate.

See Pyramid Help for further details on accessing and using the Pyramid Certificate Manager.

Encrypted Connection to IMDB

Pyramid provides an in memory, column store relational database, IMDB, as part of the Pyramid platform. This is often used for adhoc, ephemeral business models, but also in some instances for significant production systems.

To ensure FIPS compliance, if the IMDB database is to be used, then the connection to IMDB must also be secured. Details of how to achieve this are available in Pyramid Help.

Appendix

As noted in previous sections of this guide, FIPS compliance is a complex undertaking involving many interrelated components from multiple vendors.

In the process of developing a FIPS compliant version of the Pyramid Platform, a number of caveats have become apparent in particular installation scenarios, operating system versions, Pyramid repository database versions and restrictions in third party software components.

This appendix lists these restrictions and will be continually updated as we progress from the beta release of FIPS support to full production support.

Operating System Specific Considerations

Windows

- When the FIPS flag is on in the group policy, PostgreSQL is only supported from version 10 and above, with the hashing algorithm set to SCRAM SHA-256. It's on by default from version 14, and you need to change old passwords to migrate if you change from MD5 to SCRAM. A tool for batch password changes will be provided in the future.
- When the FIPS flag is on in the group policy, Puppeteer is not supported on Windows servers before version 2022. Puppeteer is a third-party component based on the Chromium engine that provides printing services in a Pyramid installation.
- OLEDB, ADOMD, AMO/TMO are by default encrypted, but no evidence of FIPS compliance exists.
- SharePoint is not FIPS compliant.
- Active Directory must be configured to LDAPS and used with a certificate inside Pyramid to be FIPS compliant.

Linux

- IMDB with SSL encryption does not currently work in all versions of Ubuntu with FIPS mode enabled in the OS.
- Ubuntu supports FIPS mode, but only if you have a pro subscription. Detailed installation instructions can be found here
- Oracle 7 supports FIPS mode. Detailed installation instructions can be found here.
- Oracle 8 supports FIPS mode: Detailed installation instructions can be found here.

Other Considerations

- Pyramid Import Export (PIE) files are only supported if they were created on Pyramid version 2023.00 and above. A tool for converting old PIE files will be provided in the near future. This is due to a FIPS compliant Pyramid installation not supporting the older non FIPS compliant PIE encryption algorithm. A separate utility to convert older PIE files to FIPS compliance may be supplied in the future.
- Licenses issued prior to Pyramid 2023.00 which are not enterprise licenses and also contain a machine key are not supported.

- SAML is not FIPS compliant and cannot be made FIPS compliant.
- Kubernetes client is not FIPS compliant.