Fortanix Data Security Manager- Accelerator Release Notes

RELEASE NOTE

Date: 10-Nov-23

Subject: New features, bug fixes, etc.

Software: Fortanix Data Security Manager-Accelerator

Version: 4.23

OVERVIEW

This document provides an overview of general improvements and resolved issues in the Fortanix Data Security Manager (DSM)-Accelerator 4.23 release.

NEW FEATURES/IMPROVEMENTS

- **DSM-Accelerator JCE Provider:**
  - **Added support for DSM-Accelerator JCE for Windows (JIRA: PM-123)**. *For more details, refer to the Developer's Guide: Fortanix DSM-Accelerator JCE Provider*.

BUG FIXES

- The retry mechanism does not work as expected in the DSM-Accelerator Webservice (**JIRA: PROD-7068**).

FORTANIX DATA SECURITY MANAGER – ACCELERATOR PERFORMANCE STATISTICS

- **Runtime Environment**

NOTE:

- The following table lists the standard recommended runtime environment. You can choose a higher configuration for better performance.
- DSM-Accelerator was run in the runtime environment listed below for performance testing.

ITEM	SPECIFICATION
Number of Cores	4
CPU	Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz
RAM	16 GiB

Fortanix, Inc. | 3910 Freedom Circle | Suite 104 | Santa Clara, CA 95052 | +1 650.943.2484
info@fortanix.com
www.fortanix.com

RELEASE NOTE

Date: 10-Nov-23

Subject: New features, bug fixes, etc.

Software: Fortanix Data Security Manager-Accelerator

Version: 4.23

ITEM	SPECIFICATION
Docker Runtime Configuration	`docker run -d --network host --memory=4g --memory-swap=6g --log-opt max-size=100m`

- **DSM-Accelerator Webservice**

NOTE: The performance numbers below are captured with a single node; if you need higher performance or throughput, then we recommend adding multiple nodes.

KEY TYPES AND OPERATIONS	THROUGHPUT (Operations/second on a 1-node cluster)
AES 256: CBC Encryption/Decryption	16,575/16,918
AES 256: GCM Encryption/Decryption	16,445/16,910
AES 256: FPE Encryption/Decryption	4,923/4,974

- **Additional Modes**

KEY TYPES AND OPERATIONS	THROUGHPUT (Operations/second on a 1-node cluster)
AES 256: CBCNOPAD Encryption/Decryption	16,663/17,018
AES 256: CFB Encryption/Decryption	16,664/17,081
AES 256: CTR Encryption/Decryption	16,668/17,051
AES 256: OFB Encryption/Decryption	16,967/17,385
AES 256: CCM Encryption/Decryption	16,355/16,697

BEST PRACTICES

Because our quality assurance process includes continuous security testing, Fortanix recommends keeping all Fortanix products updated with the latest

Fortanix, Inc. | 3910 Freedom Circle | Suite 104 | Santa Clara, CA 95052 | ☎ +1 650.943.2484
✉ info@fortanix.com
🌐 www.fortanix.com

releases as soon as possible. As an overall strategy to reduce risk exposure, customers are encouraged to follow best practices, which include:

- Always keep the product version up to date.
- Only issue accounts to trusted administrators.
- Monitor logs.
- Create two or more System Administrator accounts.

DOWNLOADS

To download the DSM-Accelerator Webservice, or PKCS#11 client or Java SDK packages, click here.

SUPPORT

For any questions regarding this release note, please contact support@fortanix.com

DISCLAIMERS

Fortanix Data Security Manager Release Notes

Release 4.22

RELEASE NOTE

Date: 10-Nov-23

Subject: New features, bug fixes, etc.

Software: Fortanix Data Security Manager-Accelerator

Version: 4.23

Fortanix, Inc. | 3910 Freedom Circle | Suite 104 | Santa Clara, CA 95052 | ☎ +1 650.943.2484

✉ info@fortanix.com

🌐 www.fortanix.com