Fortanix® Data Security Manager- Accelerator Release Note

RELEASE NOTE

Date: 20-Jul-23

Subject: New features, bug fixes, etc.

Software: Fortanix Data Security Manager-Accelerator

Version: 4.19

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

✉ info@fortanix.com

🌐 www.fortanix.com

OVERVIEW

This document provides an overview of new features, general improvements, and resolved issues in the Fortanix Data Security Manager (DSM)-Accelerator 4.19 release.

NEW FEATURES/IMPROVEMENTS

o **Added Guidelines to persist logs for DSM-Accelerator Webservice (JIRA: PROD-5641).**

   For more details, refer to the Administration Guide: Fortanix DSM-Accelerator Webservice External logging Setup Guide.

o **Improved log messages for detailed logging of encryption and decryption operations in the DSM-Accelerator Webservice (JIRA: PM-12).**

o **Added support for Batch Sign and Batch Verify operations in DSM-Accelerator Webservice (JIRA: PROD-6849).**

   For more details, refer to the Developer's Guide: Fortanix DSM-Accelerator Webservice.

BUG FIXES

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

KNOWN ISSUES

• When the Batch Sign operation is performed for **Curve Ed25519/X25519** in DSM-Accelerator Webservice, the status code is showing as 500 instead of 400 (**JIRA: PROD-7007**).

RELEASE NOTE

Date: 20-Jul-23

Subject: New features, bug fixes, etc.

Software: Fortanix Data Security Manager- Accelerator

Version: 4.19

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	32 GiB

- **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	12,848/12,834
AES 256: GCM Encryption/Decryption	13,228/13,235
AES 256: FPE Encryption/Decryption	4,850/4,806

RELEASE NOTE

Date: 20-Jul-23

Subject: New features, bug fixes, etc.

Software: Fortanix Data Security Manager-Accelerator

Version: 4.19

- **Additional Modes**

KEY TYPES AND OPERATIONS	THROUGHPUT (Operations/second on a 1-node cluster)
AES 256: CBCNOPAD Encryption/Decryption	11,528/11,421
AES 256: CFB Encryption/Decryption	13/491/13,458
AES 256: CTR Encryption/Decryption	13,444/13,550
AES 256: OFB Encryption/Decryption	13,490/12,631

BEST PRACTICES

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

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

✉ info@fortanix.com

⊕ www.fortanix.com

RELEASE NOTE

Date: 20-Jul-23

Subject: New features, bug fixes, etc.

Software: Fortanix Data Security Manager-Accelerator

Version: 4.19

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

DISCLAIMERS

Fortanix and the Fortanix logo are registered trademarks of Fortanix, Inc. in the United States and other countries. All other trademarks are the property of their respective owners.

Fortanix assumes no responsibility for any inaccuracies in this document. Fortanix reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Fortanix Data Security Manager Release Notes

Release 4.19

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

✉ info@fortanix.com

🌐 www.fortanix.com