Fortanix Data Security Manager Accelerator Release Notes

RELEASE NOTE

Date: 2-Jul-24

Subject: New features, bug fixes, etc.

Software: Fortanix Data Security Manager Accelerator

Version: 4.30

OVERVIEW

This document provides an overview of the resolved issues in the Fortanix Data Security Manager (DSM) Accelerator 4.30 release.

BUG FIXES

- **DSM Accelerator Webservice:**
  - Improved the Fortanix DSM Accelerator Webservice performance for highly transactional applications, by removing the bearer token check in the Fortanix DSM Accelerator Webservice so that it does not reach out to Fortanix DSM for authentication when processing locally cached keys. (**JIRA: PM-351**).
- **DSM Accelerator JCE Provider:**
  - Improved the Fortanix DSM Accelerator JCE Provider performance for highly transactional applications, by removing the bearer token check in the Fortanix DSM Accelerator JCE Provider so that it does not reach out to Fortanix DSM for authentication when processing locally cached keys. (**JIRA: PM-351**).
  - The path to copy the library `libdsmaccelerator.so` in Linux can now be configured using the environment variable `FORTANIX_TEMP_DIR` **(JIRA: PROD-8500)**.
  - The path to copy the library `dsmaccelerator.dll` in Windows can now be configured using the environment variable `FORTANIX_TEMP_DIR` **(JIRA: PROD-8576)**.

    For more details, refer to the Developer's Guide: DSM Accelerator JCE Provider.

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

RELEASE NOTE

Date: 2-Jul-24

Subject: New features, bug fixes, etc.

Software: Fortanix Data Security Manager Accelerator

Version: 4.30

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	2 GiB
VM Type	Standard D4ds v4 Azure VM
Docker Runtime Configuration	`sudo docker run -d --network host --memory=1g --memory-swap=2g --log-driver json-file --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 re-using a single TLS session)
AES 256: CBC Encryption/Decryption	20,907/20,557
AES 256: GCM Encryption/Decryption	21,274/21,267
AES 256: FPE Encryption/Decryption	9,456/9,417

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

RELEASE NOTE

Date: 2-Jul-24

Subject: New features, bug fixes, etc.

Software: Fortanix Data Security Manager Accelerator

Version: 4.30

- **Additional Modes**

KEY TYPES AND OPERATIONS	THROUGHPUT (Operations/second on a 1-node cluster re-using a single TLS session)
AES 256: CBCNOPAD Encryption/Decryption	20,777/21,075
AES 256: CFB Encryption/Decryption	21,488/21,279
AES 256: CTR Encryption/Decryption	21,398/21,197
AES 256: OFB Encryption/Decryption	21,480/ 21,137
AES 256: CCM Encryption/Decryption	21,076/ 21,172

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.

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

RELEASE NOTE

Date: 2-Jul-24

Subject: New features, bug fixes, etc.

Software: Fortanix Data Security Manager Accelerator

Version: 4.30

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 4.30

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

✉ info@fortanix.com

🌐 www.fortanix.com