

RELEASE NOTE

Date: 14-Jul-22

Subject: Software changes, updates, bug fixes, etc.

Software: Fortanix Data Security Manager

Version: 4.8

OVERVIEW

This document provides an overview of new features, general enhancements, improvements, and resolved issues in the Fortanix Data Security Manager (DSM) 4.8 release.

 **WARNING:**

- It is "REQUIRED" to upgrade Fortanix DSM to version 4.4 or 4.6 before upgrading to version 4.8. If you want to upgrade to 4.8 from an older version, please reach out to the Fortanix Customer Success team.

NEW FUNCTIONALITY / FEATURES

1. Support Load Balancing for FIPS L3 Clustering (JIRA: PROD-3321):

This release allows you to set up your FIPS appliances on a load balancer for the following advantages:

- Connect to a FIPS node based on the region where the request is pushed to the region that is faster to reach, thereby reducing the latency.
- Connect to a healthy FIPS node for crypto operations.

RELEASE NOTE

Date: 14-Jul-22

Subject: Software changes, updates, bug fixes, etc.

Software: Fortanix Data Security Manager

Version: 4.8

For more details, refer to [User's Guide: FIPS DSM Setup as External KMS](#).

2. Support for ARIA Korean Crypto algorithm (JIRA: PROD-2291):

This release adds support for creating a new type of Korean Cryptography security object: ARIA.

RELEASE NOTE

Date: 14-Jul-22

Subject: Software changes, updates, bug fixes, etc.

Software: Fortanix Data Security Manager

Version: 4.8

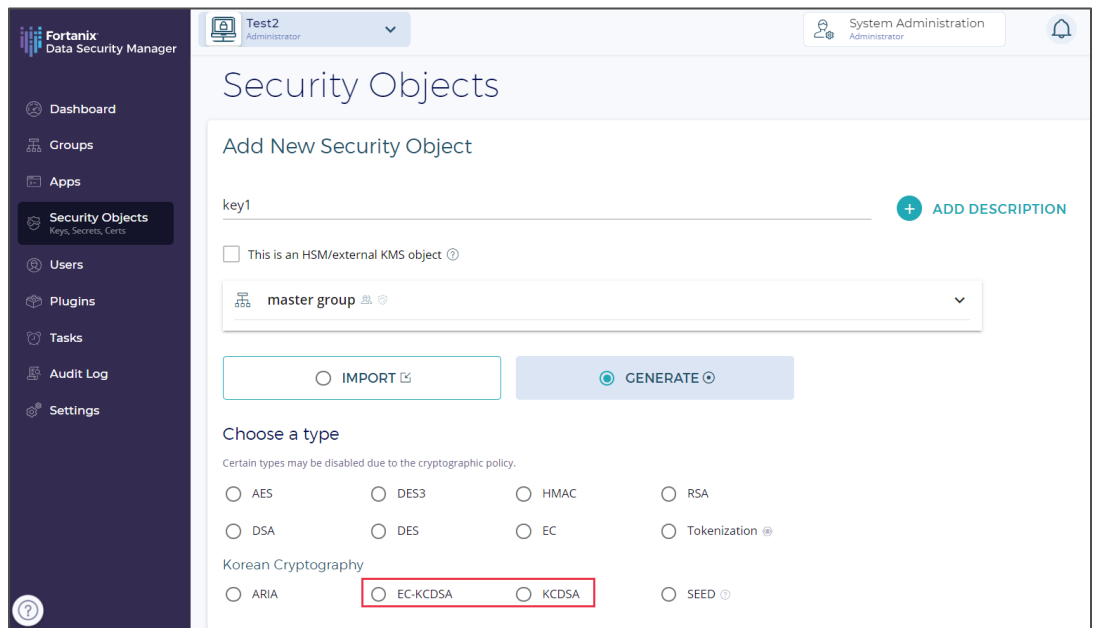
For more details refer to:

[Algorithm support](#)

[User's Guide: Key Lifecycle Management](#)

3. Support for KCDSA/EC-KCDSA Korean Crypto algorithm (JIRA: PROD-4189):

This release adds support for creating a new type of Korean Cryptography security object: KCDSA and EC-KCDSA.



For more details refer to:

[Algorithm support](#)

[User's Guide: Key Lifecycle Management](#)

4. Support for SAP Data Custodian BYOK Plugin (JIRA: PROD-4636):

This release adds support for generating a symmetric and asymmetric key in Fortanix DSM and then BYOK it into SAP Data Custodian.

For more details refer to [User's Guide: Plugin Library](#).

RELEASE NOTE

Date: 14-Jul-22

Subject: Software changes, updates, bug fixes, etc.

Software: Fortanix Data Security Manager

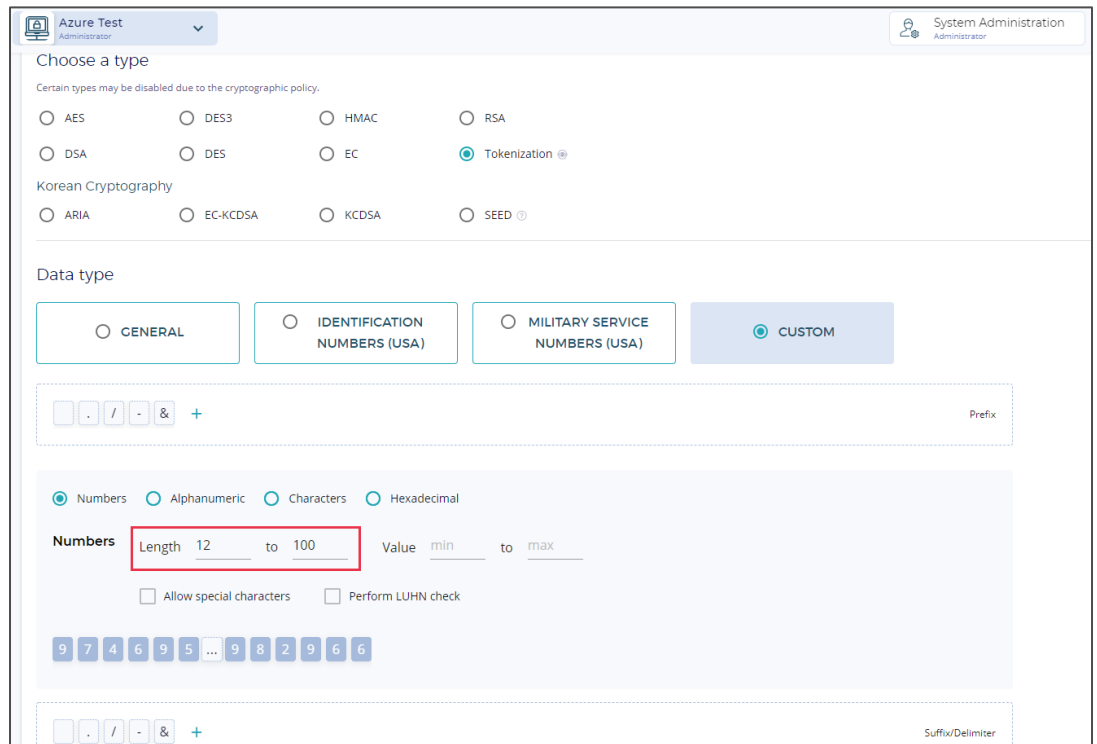
Version: 4.8

ENHANCEMENTS TO EXISTING FEATURES

1. **Support for variable-length for each component of a custom token (JIRA: PROD-3680).**

This release provides the flexibility to users to have minimum and

maximum length for each component of a custom token.



The screenshot shows the 'Choose a type' configuration page in the Fortanix Data Security Manager. The 'Data type' section is set to 'CUSTOM'. Under the 'Numbers' category, the 'Length' is configured as '12 to 100', which is highlighted with a red box. Other options like 'GENERAL', 'IDENTIFICATION NUMBERS (USA)', and 'MILITARY SERVICE NUMBERS (USA)' are also visible. The interface includes a 'Prefix' field and a 'Suffix/Delimiter' field.

For more details, refer to the [User's Guide: Tokenization](#).

2. **Support for PGP encryption and decryption using Bouncy Castle Java API (JIRA: PROD-3975).**

OTHER IMPROVEMENTS

1. **The KMIP provider now accepts all optional headers for all KMIP versions supported (JIRA: PROD-4249).**
2. **U2F is now migrated to WebAuthn (JIRA: PROD-4203).**

RELEASE NOTE

Date: 14-Jul-22

Subject: Software changes, updates, bug fixes, etc.

Software: Fortanix Data Security Manager

Version: 4.8

3. Created a separate job for audit log-only backup that runs on its own schedule and backup destination (JIRA: DEVOPS-2564). *For more details, refer to [Fortanix DSM Backup and Restore Guide](#).*
4. Changed the text from "SDKMS" or "Self-Defending KMS" to "DSM" for external plugins hosted in the Fortanix GitHub repository (JIRA: PROD-4836).
5. Updated UUID dependency to the latest version (JIRA: PROD-4760).
6. Extracted the common duplicate code (`SdkmsAes`, `SdkmsDes`, `SdkmsDsa`, `SdKmsEc`, `SdKmsRsa`) from JCE to a super class (JIRA: PROD-4744).
7. Added response time to sdkms-cli auditlog download (JIRA: PROD-4626).
8. Improvement to the Azure BYOK HSM Plugin (JIRA: PROD-4616).
9. Added support to log errors for the denied keys if the Key Access Justification (KAJ) policy provided by Google does not match the Fortanix DSM App KAJ policy (JIRA: PROD-4572).
10. Handled error scenarios for patterns with varying minimum length and maximum length using delimiters when creating custom tokens (JIRA: ROFR-3245).
11. Added 4200D4 (Offset Items) tag in KMIP code for Racktop integration (JIRA: PROD-4475).
12. Created JCE artifacts for Java 11(JIRA: PROD-4373).
13. Added JCE and Java Clients support for Java 11 (JIRA: PROD-4372).

BUG FIXES

1. Fixed EC-KCDSA: 500 response status code for SecP192K1, SecP224K1, and SecP256K1 curve (JIRA: PROD-4903).
2. Fixed an issue where Rotate key was not working in KCDSA and ECKCDSA (JIRA: PROD-4902).
3. Fixed an issue where the final token pattern is not visible in the detailed view of the security object after the Tokenization security object is created.

RELEASE NOTE

Date: 14-Jul-22

Subject: Software changes, updates, bug fixes, etc.

Software: Fortanix Data Security Manager

Version: 4.8

Also fixed an issue where the minimum length for the token pattern always shows 12 characters long even though it is set to be greater than 12 (**JIRA: ROFR-3273**).

4. Fixed an issue where the cluster creation fails on the Azure/series2 cluster in the `get_csrs` step as the DSM pod crashes in RC build 2273 (**JIRA: PROD-4890**).
5. Fixed an issue where the Plus icon in the "create your own custom token UI" was misaligned (**JIRA: ROFR-3268**).
6. Fixed an error where the "Save Changes" option is enabled by default in the **HSM/KMS** tab after the FIPS Group is created, and the **Network** tab in inspect mode shows "credential" instead of "PIN" when saving with a single API KEY (**JIRA: ROFR-3263**).
7. Fixed an issue where the custom attributes were not showing in the **Attributes/Tags** tab after they were added in the create Security Object form for an AWS group (**JIRA: PROD-4743**).
8. Fixed an issue where when the Workspace CSE APIs return an error, the CORS headers are not set correctly. (**JIRA: PROD-4698**).
9. Fixed an issue where DSM approval request now returns forbidden errors instead of bad requests when access is denied (**JIRA: PROD-4690**).
10. Fixed an issue in the database async code where the client drops its connection and the Future representing the API call is dropped by hyper (**JIRA: PROD-4672**).
11. Fixed Panic in `ImportComponents` API (**JIRA: PROD-4668**).
12. Fixed an issue where using a transient key as a wrapping/unwrapping key, you can create a key in any group regardless of your access to the group using `UnwrapKey` API (**JIRA: PROD-4662**).

RELEASE NOTE

Date: 14-Jul-22

Subject: Software changes, updates, bug fixes, etc.

Software: Fortanix Data Security Manager

Version: 4.8

13. Fixed an issue that can cause problems in some scenarios when using `DEFAULT_CONSISTENCY` for writing to index tables such as `subject_by_name` (**JIRA: PROD-4657**).
14. Fixed an issue where custom attributes that are not AWS tags are shown as AWS tags with the prefix `aws-tag` (**JIRA: ROFR-3208**).
15. Fixed an issue where the `crypto::UnwrapKey` API required `DECRYPT` or `MASKDECRYPT` app permissions (**JIRA: PROD-4654**).
16. Fixed an issue where selecting an account from the account switcher fails with an error (**JIRA: ROFR-3193**).
17. Fixed an issue where the IP whitelist error messages had padding (**JIRA: PROD-4614**).
18. Fixed a GUI issue when sorting audit logs by Type (**JIRA: ROFR-3180**).
19. Fixed panic in Copy API (**JIRA: PROD-4506**).
20. Fixed an issue where the KMIP-Easy-Wizard passes an incorrect certificate, and the ERROR UI navigates to next the page (**JIRA: ROFR-3147**).
21. Fixed an issue where the Oauth screen goes to an account logged in instead of the account the Oauth link was generated for (**JIRA: ROFR-3137**).
22. Fixed an issue where the Secrets rekey operation was sending lots of unnecessary data (**JIRA: ROFR-2642**).

QUALITY ENHANCEMENTS / UPDATES

- Updated Cassandra to version 3.11.13 (**JIRA: DEVOPS-2696**).
- Refactored SPI implementations (Ciphers, keys, signatures, mac, and so on) as per the type and purpose in separate packages (**JIRA: PROD-4801**).
- `sdkms-cli` support extended on Java 11 (**JIRA: PROD-4546**).
- Kubernetes version upgrade from 1.14 to version 1.16 (**JIRA: DEVOPS-1425**).

RELEASE NOTE

Date: 14-Jul-22

Subject: Software changes, updates, bug fixes, etc.

Software: Fortanix Data Security Manager

Version: 4.8

SECURITY FIXES

- Updated aesmd for the May 2022 Intel update (**JIRA: DEVOPS-2489**).
- Updated BIOS for the May 2022 Intel update (**JIRA: DEVOPS-2488**).
- Intel update for BIOS, PSW, and Code Changes (**JIRA: PROD-4447**).

KNOWN ISSUES

- An account could be lost if account tables are inconsistent between nodes. Make sure a backup is successful before proceeding with ANY upgrade (**JIRA: PROD-4234**).
- When a node is removed from a 3-node cluster with build 4.2.2087, and the 2-node cluster is upgraded with build 4.3.xxxx, it is possible that the deploy job is exited and marked completed before cluster upgrade (**JIRA: DEVOPS-2068**).
Workaround: If all the pods are healthy, you can deploy the version again.
- The sync key API returns a “400 status code and response error” due to the short-term access token expiry during the sync key operation of a group linked to AWS KMS (**JIRA: PROD-3903**).
- `exclude` does not work in the `proxy` config for operations such as attestation (**JIRA: PROD: 3311**).

FORTANIX DATA SECURITY MANAGER PERFORMANCE STATISTICS

- **Series 2**

KEY TYPES AND OPERATIONS	THROUGHPUT (Operations/second on a 3-node cluster)
AES 256: CBC Encryption/Decryption	4211/4176
AES 256: GCM Encryption/Decryption	4205/4176
AES 256: FPE Encryption/Decryption	2137/2125

RELEASE NOTE

Date: 14-Jul-22

Subject: Software changes, updates, bug fixes, etc.

Software: Fortanix Data Security Manager

Version: 4.8

KEY TYPES AND OPERATIONS	THROUGHPUT (Operations/second on a 3-node cluster)
AES 256 Key Generation	1127
RSA 2048 Encryption/Decryption	3692/1120
RSA 2048 Key Generation	31
RSA 2048 Sign/Verify	1112/3630
EC NISTP256 Sign/Verify	1040/606
Data Security Manager Plugin (Hello world plugin)	1659 (invocations/second)

- **Azure Standard_DC8_v2**

KEY TYPES AND OPERATIONS	THROUGHPUT (Operations/second on a 3-node [Standard_DC8_v2] cluster)
AES 256: CBC Encryption/Decryption	2993/3152
AES 256: GCM Encryption/Decryption	3069/3086
AES 256: FPE Encryption/Decryption	1709/1765
AES 256 Key Generation	1073
RSA 2048 Encryption/Decryption	2950/1067
RSA 2048 Key Generation	43
RSA 2048 Sign/Verify	1085/2848
EC NISTP256 Sign/Verify	839/527
Data Security Manager Plugin (Hello world plugin)	1584 (invocations/second)

- **Series 2 JCE**

RELEASE NOTE

Date: 14-Jul-22

Subject: Software changes, updates, bug fixes, etc.

Software: Fortanix Data Security Manager

Version: 4.8


KEY TYPES AND OPERATIONS	THROUGHPUT (Operations/second on a 3-node cluster)
AES 256: CBC Encryption/Decryption	3441/3686
AES 256 Key Generation	1234
RSA 2048 Key Generation	31
RSA 2048 Sign/Verify	865/1824
EC NISTP256 Sign/Verify	852/541
Data Security Manager Plugin (Hello world plugin)	1623 (invocations/second)

- Azure Standard_DC8 JCE

KEY TYPES AND OPERATIONS	THROUGHPUT (Operations/second on a 3-node [Standard_DC8 JCE] cluster)
AES 256: CBC Encryption/Decryption	2808/2872
AES 256: GCM Encryption/Decryption	9203/2908
AES 256 Key Generation	1118
RSA 2048 Key Generation	43
RSA 2048 Sign/Verify	807/1604
EC NISTP256 Sign/Verify	670/448
Data Security Manager Plugin (Hello world plugin)	1565 (invocations/second)

BEST PRACTICES

Fortanix, Inc. | 44 Castro St
#305 | Mountain View, CA

94041 |  +1 628.400.2043

 info@fortanix.com

 www.fortanix.com

RELEASE NOTE

Date: 14-Jul-22

Subject: Software changes, updates, bug fixes, etc.

Software: Fortanix Data Security Manager

Version: 4.8

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.
- Utilize strong passwords.
- Monitor logs.
- Restrict physical access to the appliance to trusted administrators.
- Create two System Administrator accounts.
- Enable daily backups for the cluster.

INSTALLATION

To download the DSM SGX (on-prem/Azure) and Software (AWS/Azure/VMWare) packages, click [here](#).

SUPPORT

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.

RELEASE NOTE**Date:** 14-Jul-22**Subject:** Software changes, updates, bug fixes, etc.**Software:** Fortanix Data Security Manager**Version:** 4.8

Copyright © 2022 Fortanix, Inc. All rights reserved.

Fortanix Data Security Manager Release Notes

Release 4.8