RELEASE NOTE

Date: 20-Jun-23

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

Software: Fortanix Data Security Manager

Version: 4.18.2232

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 bug fixes and known issues in the Fortanix Data Security Manager (DSM) SaaS 4.18.2232 release.

NOTE:

- This release is for SaaS only and is not available for on-premises installations.

BUG FIXES

- Fixed an issue where unverified Fortanix DSM users with multi-factor authentication (MFA) configured were not able to log in to DSM using a recovery code after account lockout **(JIRA: PROD-7008)**.
- Fixed an issue where searching for an item without using the search filter in the Fortanix DSM Groups, Apps, and Security Objects table did not show any search results (**JIRA: ROFR: 4214**).

KNOWN ISSUES

- 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 configuration for operations such as attestation (**JIRA: PROD: 3311**).
- Rotating a GCP BYOK virtual key to a Fortanix DSM-backed key (**Rotate to DSM key**) is not supported (**JIRA: PROD: 6722**).

  Workaround: You can manually copy the AES 256 key from a normal DSM group to a GCP-backed group.
- The “Rotate linked key” feature does not work when a Fortanix DSM source key is rotated along with its linked keys by selecting the “**Rotate linked**

keys” check box, where the linked key might belong to a GCP group. In this case rotating the linked key results in rotating the key in GCP as well as generating the new key in GCP (**JIRA: ROFR: 4075**).

Workaround: You must first manually rotate the source key in the normal DSM group and then copy the rotated key to the GCP group.

- An Azure Managed HSM external KMS group now also allows the following security object types to be generated or imported. But the Bring Your Own Key (BYOK) and rotate key functionality does not work for these security object types (**JIRA: ROFR: 4192**).
  - EC
  - AES 128 and AWS 192

  Workaround: Do not generate or import security objects of type EC, AES 128, and AES 192 in an external KMS group of type Azure Managed HSM since the only allowed security object types for an Azure key generated using the Generate or Import key workflows are:
  - RSA key pairs (RSA_2048, RSA_3072, and RSA_4096).
  - AES 256
- For the Azure Managed HSM external KMS group, the following security object types are enabled (**JIRA: ROFR: 4187**).
  - DES
  - DES3
  - EC-KCDSA

  Workaround: Do not generate or import security objects of type EC-KCDSA, DES, or DES3 in an external KMS group of type Azure Managed HSM since the only allowed security object types for an Azure key generated using the Generate or Import key workflows are:
  - RSA key pairs (RSA_2048, RSA_3072, and RSA_4096).
  - AES 256

RELEASE NOTE

Date: 20-Jun-23

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

Software: Fortanix Data Security Manager

Version: 4.18.2232

- If an Azure key is rotated and then soft-deleted, only one version of the key is soft-deleted (**JIRA: PROD: 6947**).

  Workaround: Perform a key scan in DSM to synchronize the key state with Azure.

For a complete list of new features, enhancements to existing features, other improvements, and bug fixes refer to the full description of the DSM 4.18 release note.

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.
- 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.

SUPPORT

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

DISCLAIMERS

RELEASE NOTE

Date: 20-Jun-23

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

Software: Fortanix Data Security Manager

Version: 4.18.2232

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 4.18.2232