RELEASE NOTES

Date: 7-Oct-24

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

Software: Fortanix Data Security Manager SaaS

Version: 4.33

OVERVIEW

This document provides an overview of new features, general improvements, and resolved issues in the Fortanix Data Security Manager (DSM) SaaS 4.33 release.

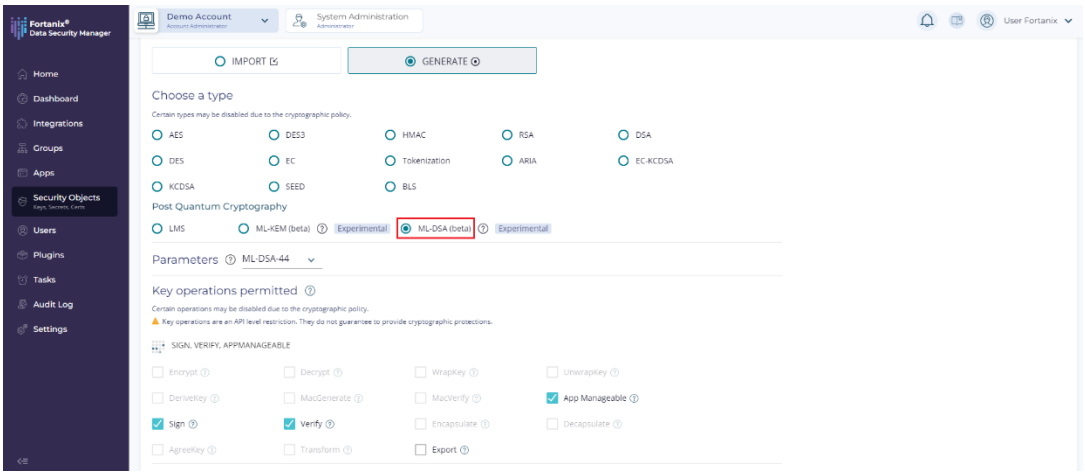
NOTE:

- This release is for **SaaS only** and is not available for on-premises installations. Updates in this release will be part of a future on-premises release.

NEW FEATURES

- Added Module-Lattice-Based Digital Signature Algorithm (ML-DSA) (Crystals-Dilithium) (beta) algorithm support in Fortanix DSM **(JIRA: PM-106)**.

  With this feature, a user can now select ML-DSA (beta) as a new Post Quantum Cryptography (PQC) algorithm when generating and importing a new security object.



For more details, refer to User's Guide: Fortanix Data Security Manager Key Lifecycle Management.

RELEASE NOTES

Date: 7-Oct-24

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

Software: Fortanix Data Security Manager SaaS

Version: 4.33

- Added support for the X25519Kyber768Draft00 TLS 1.3 CipherSuite for both browser and web services connections to Fortanix DSM **(JIRA: PM-194)**.

ENHANCEMENTS TO EXISTING FEATURES

- Enhanced the **Export Key** flow with lazy loading for wrapping keys to resolve the issues related to key export **(JIRA: ROFR-4999)**.

OTHER IMPROVEMENTS

- Enhanced Fortanix DSM to fetch the cryptography policy compliance status only for the groups currently displayed in the user interface (UI) **(JIRA: PM-364)**.
- Enhanced the REST API to lazily fetch compliance status for Fortanix DSM groups **(JIRA: ROFR-5067)**.
- The Fortanix DSM UI now immediately reflects the changes or deletions of the security objects in the cryptography policy compliance status **(JIRA: EXTREQ-958)**.

DSM ACCELERATOR NEW FEATURES

- **DSM Accelerator Webservice:**
    - Added support for setting up Fortanix DSM Accelerator Webservice on Nitro using Fortanix CCM. This feature simplifies and accelerates the deployment of Fortanix DSM Accelerator Webservice in Nitro environments (**JIRA: PM-389**).
        - Added support to configure quorum policy approval for Fortanix DSM Accelerator Webservice on Nitro (**JIRA: PROD-9105**).

RELEASE NOTES

Date: 7-Oct-24

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

Software: Fortanix Data Security Manager SaaS

Version: 4.33

- Added support to retrieve the server-side Transport Layer Security (TLS) key and certificate for Fortanix DSM Accelerator Webservice on Nitro, directly from Fortanix DSM (**JIRA: PM-390**).

For more details, refer to DSM Accelerator Webservice for Nitro with CCM Setup Guide.

- Introduced Bearer Token authentication support for Fortanix DSM Accelerator Webservice Rust Webservice API requests (**JIRA: PM-391**).

BUG FIXES

- Fixed an issue where LDAP users logging into Fortanix DSM using account member role were facing high latency when navigating the DSM menu items **(JIRA: ES-356)**.
- Fixed an issue in a DSM Azure Key Vault group where the users were unable to restore a purged key to enabled state with the key material successfully reimported into Azure Key Vault **(JIRA: ES-383)**.
- Fixed an issue where the users encountered the error "This operation requires an account to be selected first" **(JIRA: ES-427).**
- Fixed an issue where a quorum approval request for rotating a key using Batch API does not work as expected **(JIRA: ES-380)**.
- Fixed an issue that prevented users from removing the ML-KEM key from the allowed security objects in an account or group using the cryptographic policy (**JIRA: ES-364**).
- Fixed issues where the Fortanix DSM UI had a default limitation of displaying only 3000 groups and the performance of a DSM page decreased when there are over 1000 groups in a DSM account **(JIRA: ROFR-5047 and ROFR-4997)**.

RELEASE NOTES

Date: 7-Oct-24

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

Software: Fortanix Data Security Manager SaaS

Version: 4.33

- Fixed an issue where copying AES and RSA keys from a regular DSM group to an Amazon Web Service (AWS) Cloud Data Control (CDC) group failed due to exceeding the Key Management Service (KMS) API rate limit **(JIRA ES-435)**.
- Fixed an issue where users were unable to create an LMS key with a height combination of 5 and 20, or vice versa **(JIRA: PROD-8248)**.

KNOWN ISSUES

- A Fortanix DSM account, whether normal or system administrator, with the "No Roles Can Login with Password" role selected, may experience issues when attempting to log in using a password. If the users select such an account and enter the SSO credentials, they will be logged out instead of accessing the account **(JIRA: ROFR-4998)**.

  Workaround: The users should log in directly with SSO after the "No Roles Can Login with Password" role is set to access the account.
- When you edit the starting time of a Key rotation policy for a security object with the value as single digit time, for example: 01:00 am, it shows an error “Invalid date/time selected. Ensure that you filled in a valid 12-hour time” **(JIRA: ROFR-4786)**.

  Workaround: Re-enter the rotate start time by removing the “0” before the single digit time and enter a new time (for example, 01:00 am to 2:00 am).
- The hyperlink color for the field “**Follow the instructions in**” in the “**Add Instance**” form for Google Workspace Client-Side Encryption (CSE) still reflects the old link color value (**JIRA: ROFR-4789**).

RELEASE NOTES

Date: 7-Oct-24

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

Software: Fortanix Data Security Manager SaaS

Version: 4.33

- The sync key API returns a "400 status code and response error" if its short-term access token expires during the synchronization of a group linked to AWS KMS (**JIRA: PROD-3903**).

  Workaround: increase the timeout of the temporary session token beyond the expected duration of the sync key operation.
- `exclude` does not work in the `proxy` configuration for operations such as attestation (**JIRA: PROD-3311**).
- 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.
- The `create` operation for security object creation does not work for the Azure Managed HSM plugin (**JIRA: PROD-7078**).
- Copying an RSA or EC key from a normal DSM group to an AWS KMS-backed DSM group does not work as expected and results in an error (**JIRA: PROD-7787**).

  Workaround: Export the RSA or EC key from the normal DSM group and import it into the AWS KMS-backed DSM group.
- The admin applications (apps) cannot retrieve the details for `GET /users/{uuid}` and instead returns the error "Inappropriate authorization for the requested operation" **(JIRA: PROD-9212)**.

  Workaround: Use `GET /users/{uuid}` using the system administrator credentials to retrieve the user ID details.

RELEASE NOTES

Date: 7-Oct-24

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

Software: Fortanix Data Security Manager SaaS

Version: 4.33

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.

SUPPORT

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

DISCLAIMERS

Fortanix Data Security Manager SaaS Release Notes

Release 4.33