Fortanix Data Security Manager Release Notes

RELEASE NOTES

Date: 28-Mar-25

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

Software: Fortanix Data Security Manager

Version: 4.37

OVERVIEW

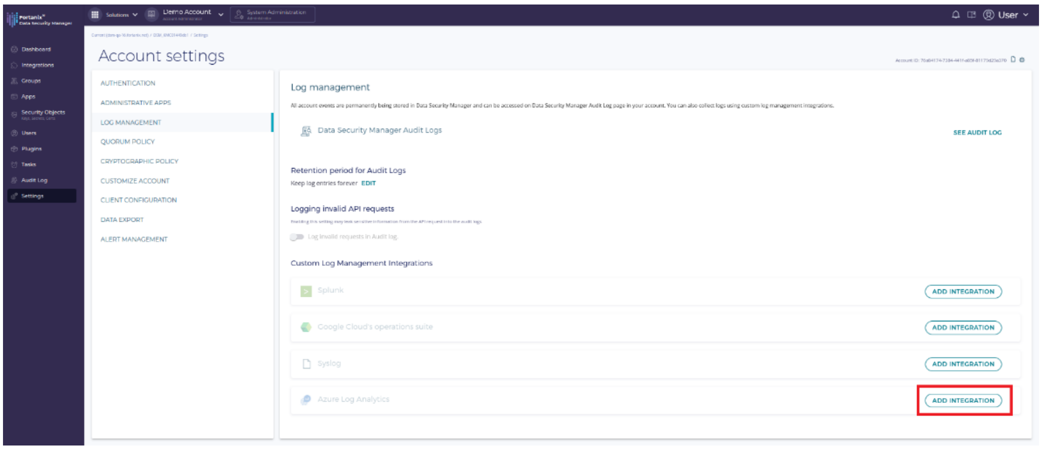
This document provides an overview of new features, general improvements, and resolved issues in the Fortanix Data Security Manager (DSM) SaaS 4.37 release.

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

- Fortanix DSM can now be configured to send audit log entries to Azure Log Analytics for centralized monitoring **(JIRA: PM-112)**.



All account events are permanently being stored in Data Security Manager and can be accessed on Data Security Manager Audit Log page in your account. You can also collect logs using custom log management integrations.

Keep log entries forever

Log invalid requests in Audit log

For more information, refer to [User's Guide: Logging](#).

- Fortanix DSM now supports the generation of a new post-quantum cryptography (PQC) key type called eXtended Merkle Signature Scheme (XMSS) key, which can be used for signature generation and verification **(JIRA: PM-103)**.

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

✉ info@fortanix.com

www.fortanix.com

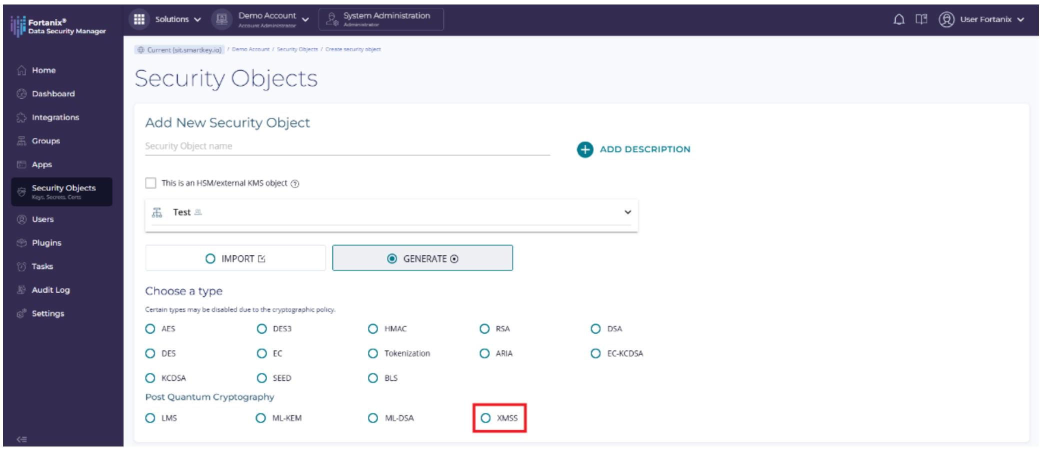
RELEASE NOTES

Date: 28-Mar-25

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

Software: Fortanix Data Security Manager

Version: 4.37



Add New Security Object

Security Object name

□ This is an HSM/external KMS object

Test

○ IMPORT ● GENERATE

Choose a type

Certain types may be disabled due to the cryptographic policy.

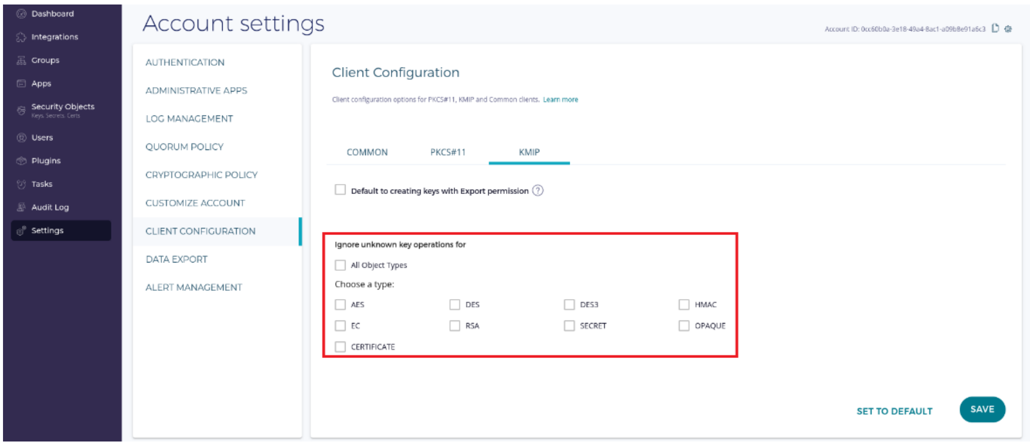
○ AES ○ DES3 ○ HMAC ○ RSA ○ DSA
○ DES ○ EC ○ Tokenization ○ ARIA ○ EC-KCDSA
○ KCDSA ○ SEED ○ BLS

Post Quantum Cryptography

○ LMS ○ ML-KEM ○ ML-DSA ○ XMSS

For more information, refer to [User's Guide: Fortanix Data Security Manager Key Lifecycle Management](#).

- Fortanix DSM now supports the option to disallow keys with unknown operations in the Key Management Interoperability Protocol (KMIP) client configuration settings. This enhancement provides system administrators with greater flexibility in filtering keys so that the unsupported operations for those selected key types are ignored during processing the KMIP request. This feature can be enabled by navigating to the **CLIENT CONFIGURATION** → **KMIP** tab and selecting the required keys in the **Ignore unknown key operations for** section **(JIRA: PM-408)**.



Account ID: 0cc60b0a-3e18-49a4-8ac1-a09b8e91a6c3

Client Configuration

Client configuration options for PKCS#11, KMIP and Common clients. Learn more

□ Default to creating keys with Export permission

Ignore unknown key operations for

□ All Object Types

Choose a type:

□ AES □ DES □ DES3 □ HMAC
□ EC □ RSA □ SECRET □ OPAQUE
□ CERTIFICATE

Additionally, the existing **Allow secrets with unknown operations** check box has been removed to allow users to select multiple security object types for unknown operations.

For more information, refer to the following guides:

RELEASE NOTES

Date: 28-Mar-25

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

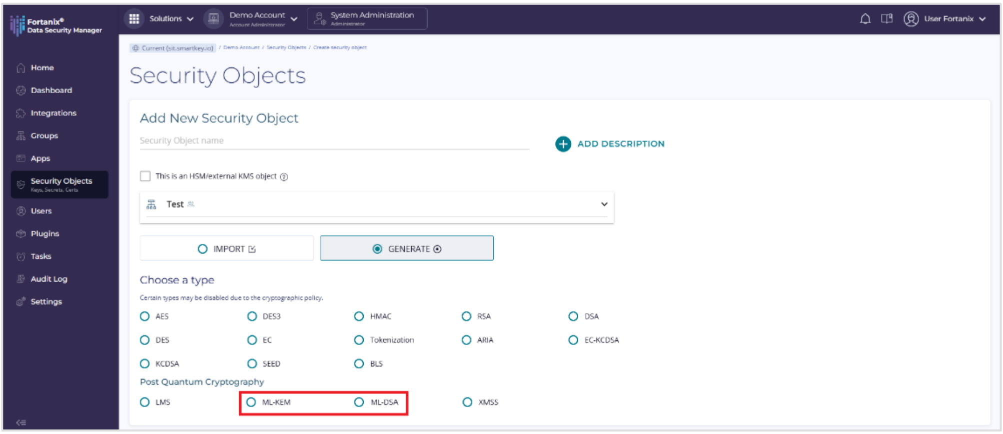
Software: Fortanix Data Security Manager

Version: 4.37

- *User's Guide: Account Client Configurations*
- *User's Guide: Group Client Configurations*

IMPROVEMENTS

- Fortanix DSM now supports the standard algorithms for Module-Lattice-Based Digital Signature Algorithm **(ML-DSA)** and Module-Lattice-Based Key Encapsulation Mechanism **(ML-KEM)** as the Post-Quantum Cryptography (PQC) methods and they replace the previously available ML-DSA (beta) and ML-KEM (beta) security objects. Additionally, the **Experimental** tag has been removed **(JIRA: PM-413)**.



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

- When performing normal rotation, linked key rotation, or rotate to DSM key in Azure Key Vault or GCP KMS, specifying the Azure key name or GCP key ID is optional as they are automatically inherited from the previous key version **(JIRA: PM-475)**.

  For more information, refer to the following guides:

  - *Fortanix DSM - Azure Key Vault BYOK (Bring Your Own Key)*
  - *Fortanix DSM - Google Cloud Platform BYOK (Bring Your Own Key)*

- Fortanix DSM can now generate Elliptic Curve (EC) keys over curve **X448** through the DSM user interface (UI) **(JIRA: ROFR-5247)**.

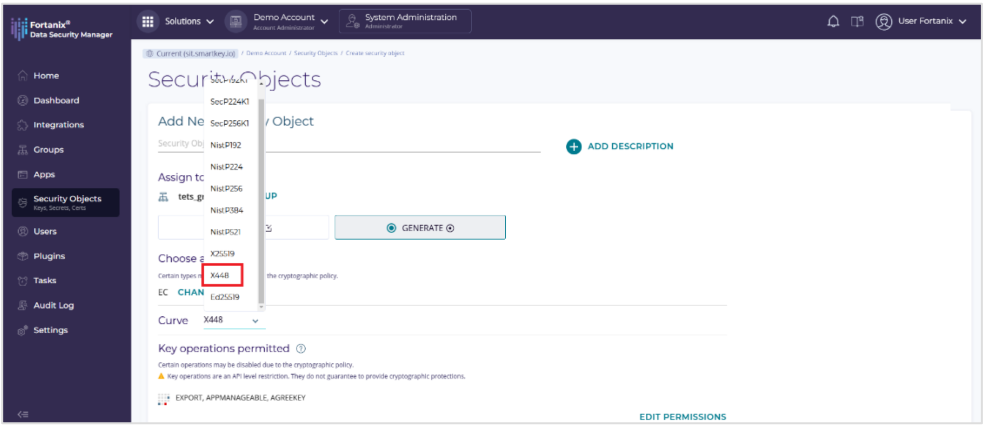
RELEASE NOTES

Date: 28-Mar-25

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

Software: Fortanix Data Security Manager

Version: 4.37



Certain types n the cryptographic policy.

Curve X448

Key operations permitted

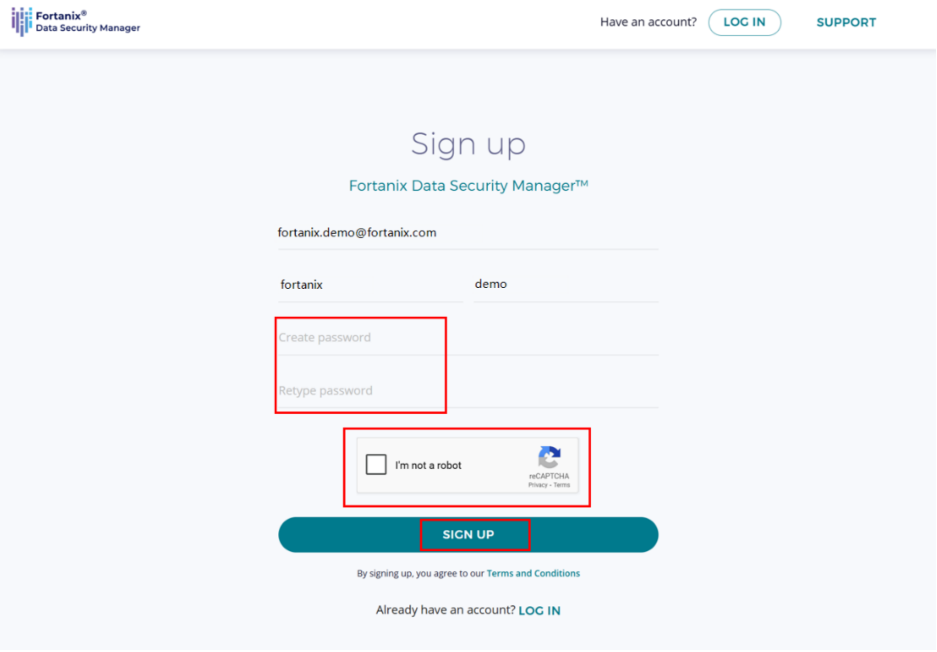
Certain operations may be disabled due to the cryptographic policy.

⚠ Key operations are an API level restriction. They do not guarantee to provide cryptographic protections.

EXPORT, APPMANAGEABLE, AGREEKEY

For more information, refer to [User's Guide: Fortanix Data Security Manager Key Lifecycle Management](#).

- Added support for reCAPTCHA verification when resetting your forgotten password using the **Forgot your password?** link on Fortanix DSM UI during sign-in **(JIRA: PM-370)**.



fortanix.demo@fortanix.com

fortanix demo

By signing up, you agree to our Terms and Conditions

Already have an account? LOG IN

For more information, refer to [User's Guide: Sign Up for Fortanix Data Security Manager SaaS](#).

- The users with host administration permissions can now create, configure, and manage Fortanix DSM Filesystem Encryption policies for Windows clients using the **FILE DECRYPTION POLICY** tab in DSM UI to

RELEASE NOTES

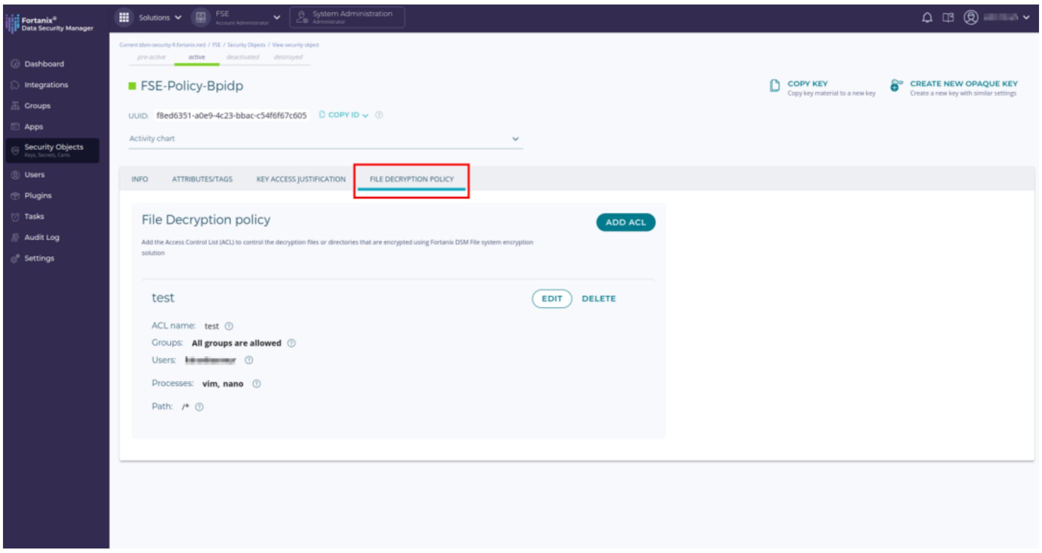
Date: 28-Mar-25

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

Software: Fortanix Data Security Manager

Version: 4.37

manage and control access to services, users, processes, and groups on the Windows client effectively **(JIRA: FSE-132)**.



Fortanix® Data Security Manager
Solutions
FSE Account Administrator
System Administration Administrator
Dashboard
Integrations
Groups
Apps
Security Objects Keys, Secrets, Certs
Users
Plugins
Tasks
Audit Log
Settings
Current (dsm-security-9.fortanix.net) / FSE / Security Objects / View security object
pre-active
active
deactivated
destroyed
COPY KEY
Copy key material to a new key
CREATE NEW OPAQUE KEY
Create a new key with similar settings
COPY ID
Activity chart
INFO
ATTRIBUTES/TAGS
KEY ACCESS JUSTIFICATION
FILE DECRYPTION POLICY
ADD ACL
EDIT
DELETE

■ FSE-Policy-Bpidp

UUID: f8ed6351-a0e9-4c23-bbac-c54f6f67c605

File Decryption policy

Add the Access Control List (ACL) to control the decryption files or directories that are encrypted using Fortanix DSM File system encryption solution

test

ACL name: test

Groups: All groups are allowed

Users: [redacted]

Processes: vim, nano

Path: /*

For more information, refer to [Filesystem Encryption for Windows as a Service Using Fortanix Data Security Manager - Setup and Usage]().

OTHER IMPROVEMENTS

- Fortanix DSM now supports cookie as the transport mechanism for session tokens during authentication **(JIRA: PM-184)**.

  Instead of storing session tokens in local storage, Fortanix DSM utilizes secure, HTTP-only cookies, enhancing security and ensuring better protection against unauthorized access.

  NOTE: Users who were logged in before the Fortanix DSM 4.37 release will be logged out and may receive an unauthorized access message. They must log in again to initiate a new session.

  For more information, refer to [User's Guide: Authentication]().

API UPDATES

- Added an additional enum variant for Azure Log Analytics to the `LoggingConfig` and `LoggingConfigRequest`, which in turn affects the `add_logging_configs`, `mod_logging_configs`, and `del_logging_configs` in the `patch`

`"/sys/v1/accounts/:acct_id"` (update account) API, supporting Azure Log Analytics integration in Fortanix DSM (**JIRA: PM-112**).

- After finalizing the ML-KEM (FIPS 203) and ML-DSA (FIPS 204) specifications, Fortanix DSM deprecated the `MlKemBeta` and `MlDsaBeta` key types and replaced them with `MlKem` and `MlDsa`, which correspond to the FIPS 203 and FIPS 204 specifications, respectively (**JIRA: PM-413**).

CLIENT IMPROVEMENTS

- Added support to specify a target group when creating or importing a key in the Sequoia-PGP client (**JIRA: PM-402**).

  For more information, refer to Clients: Sequoia PGP.
- Added support for adding custom metadata when creating or importing a key in the Sequoia-PGP client (**JIRA: PM-403**).

  For more information, refer to Clients: Sequoia PGP.
- Added support for publishing the Windows signed binary to the Chocolatey package manager in the Sequoia-PGP client (**JIRA: PM-453**).

  For more information, refer to Sequoia-PGP.
- Updated the SAP Data Custodian (DC) BYOK plugin to enhance validation, improve parameter handling, and provide better clarity in the key import process (**JIRA: PM-420**).
- The SAP Data Custodian BYOK plugin now supports importing Fortanix DSM keys (AES and RSA) into Data Custodian groups or rotating them if they are already imported in AWS and non-AWS keystore providers (**JIRA: PM-426**).

  For more information, refer to User's Guide: Plugin Library.

DSM ACCELERATOR NEW FEATURES AND BUG FIXES

- **DSM Accelerator Webservice:**

  - Added support for encryption and decryption using the RSA keys in Fortanix DSM Accelerator Webservice (**JIRA: PM-395**).

    For more information, refer to [DSM Accelerator Webservice Developer Guide](#).
  - Resolved a performance issue in Fortanix DSM Accelerator Webservice for AWS Nitro, where one node in the cluster issued export requests more frequently even when the cache Time-To-Live (TTL) is configured longer (**JIRA: PROD-10043**).
  - Fixed an issue in Fortanix DSM Accelerator Webservice for AWS Nitro where, in cluster mode, it failed to export security objects if the locally cached bearer token had expired (**JIRA: PROD-10051**).
- **DSM Accelerator JCE Provider:**
  - Added support for encryption and decryption using the RSA keys in Fortanix DSM Accelerator JCE Provider (**JIRA: PM-395**).

    For more information, refer to [DSM Accelerator JCE Provider Developer Guide](#).

BUG FIXES

- Fixed an issue where the rotation of Secret-type security object failed when the **Deactivation date** was set in the group's **Key metadata policy (JIRA ES-382)**.

KNOWN ISSUES

- The `create` operation for security object creation does not work for the Azure Managed HSM plugin **(JIRA: PROD-7078)**.
- The **COPY KEY** dialog box does not filter the HSM/External KMS groups as expected when **Import key to HSM/External KMS** check box is selected, if there are more than 1,000 groups in the account **(JIRA: ROFR-5167)**.

- Unable to delete a user who was invited to an account with a "Custom account role" that includes an "All Groups Role" along with group membership assigned explicitly in the invite user workflow if the invited user has not accepted the invitation **(JIRA: PROD-9409)**.

  Workaround: To delete the invited user, contact Fortanix Support or perform the following steps:

  - If you have already assigned explicit group memberships, perform the following steps to remove them and delete the user:
    - Change the user's account role to "Account Member".
    - Remove the group memberships one by one using the user interface.
    - Delete the user.
- The `sudo get_csrs --rotate` command does not support changing the hostname of the service URL. For example, if your service main URL is dsm.fortanix.net, you cannot change this main URL hostname **(JIRA: PROD-9542)**.
- When you run `sudo get_csrs --rotate` command to create a new certificate pair for cluster and UI, it does not remove the old certificate pair from the sdkms pod resulting in two certificate pairs which can lead to unexpected results **(JIRA: PROD-9570)**.
- Deleting replica keys in groups with key history policies only results in a soft-delete of the keys **(JIRA: PROD-9925)**.

  Workaround: Users should avoid deleting keys that are associated with a key-undo policy.
- When creating a group-level Quorum approval policy, users with the “Custom account roles permissions” are not listed in the user list **(JIRA: ROFR-5253)**.

  Workaround: Assign the **Get External Roles** permission to allow the users to be listed in the quorum policy.

RELEASE NOTES

Date: 28-Mar-25

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

Software: Fortanix Data Security Manager

Version: 4.37

- Unable to save Account Cryptographic policy with below permissions **(JIRA: ROFR-5254)**.

  ```
  "Create Account Security Object Policies",
  "Set Approval Request Expiry",
  "Get All Users"
  ```

  Workaround: Add the `Update Account Security Object Policies` permission to the Custom account role to enable saving the Account Cryptographic policy.

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 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.

RELEASE NOTES

Date: 28-Mar-25

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

Software: Fortanix Data Security Manager

Version: 4.37

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 4.37