Fortanix Data Security Manager Release Notes

RELEASE NOTES

Date: 14-Feb-25

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

Software: Fortanix Data Security Manager

Version: 4.36

OVERVIEW

This document provides an overview of new features, general improvements, and resolved issues in the Fortanix Data Security Manager (DSM) 4.36 release.

This release is superseded by the March 17, 2025, release.

WARNING:

- You are **REQUIRED** to upgrade Fortanix DSM to version 4.31 or 4.34 before upgrading to version 4.36. If you want to upgrade Fortanix DSM to version 4.36 from a version earlier than 4.31, please contact the Fortanix Support team at your earliest to validate the upgrade path.
- Downgrade from 4.36 to any prior version is not supported due to the DCAP migration.

NOTE:

- The Fortanix DSM cluster upgrade must be done with Fortanix Support on call. Please reach out to Fortanix Support if you are planning an upgrade.
- The customer's BIOS version must be checked by Fortanix Support before the Fortanix DSM software upgrade. If required, the BIOS version should be upgraded to the latest version and verified by Fortanix Support for a smooth upgrade.
- If your Fortanix DSM version is 4.31 or later, then the HSM Gateway version must also be 4.31 or later. Similarly, if the HSM Gateway version is 4.31 or later, then your Fortanix DSM version must be 4.31 or later.

NEW FEATURES

- A Fortanix DSM system administrator can now create a replication account on a DSM on-premises destination cluster, sourced from an account on the DSM Software as a Service (SaaS) cluster, to enable

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

RELEASE NOTES

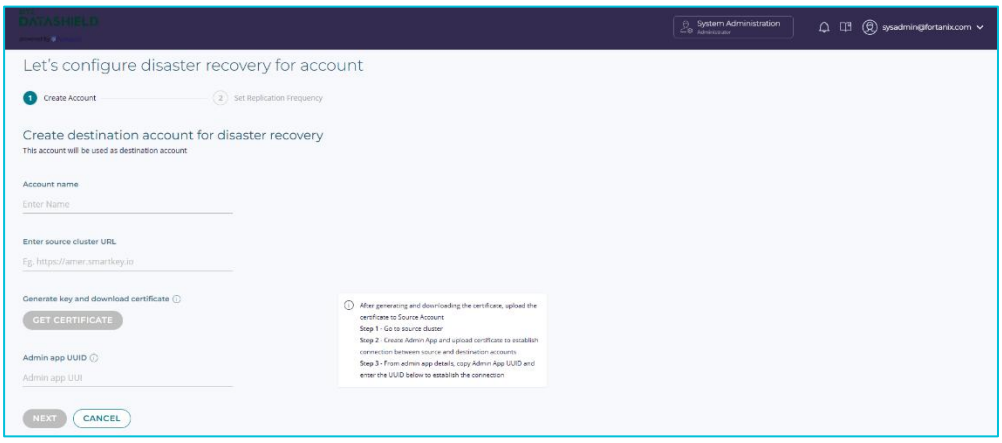
Date: 14-Feb-25

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

Software: Fortanix Data Security Manager

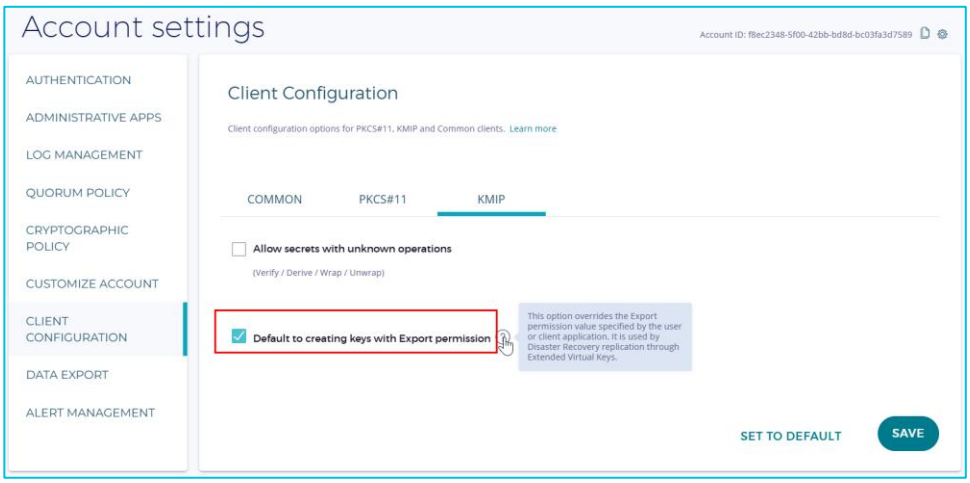
Version: 4.36

disaster recovery. This setup replicates all the account-level attributes, groups, cryptographic applications (apps) (API key, Client Certificate, and Trusted CA), and exportable security objects from the source cluster to the destination cluster **(JIRA: PM-385)**.



For more information, refer to User's Guide: Account Replication.

- Added a new check box "**Default to creating keys with Export permission**" in DSM account **Settings** → **CLIENT CONFIGURATION** → **KMIP** tab for disaster recovery using account replication **(JIRA: PROD-8910)**.



For more information, refer to the following documents:

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

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

RELEASE NOTES

Date: 14-Feb-25

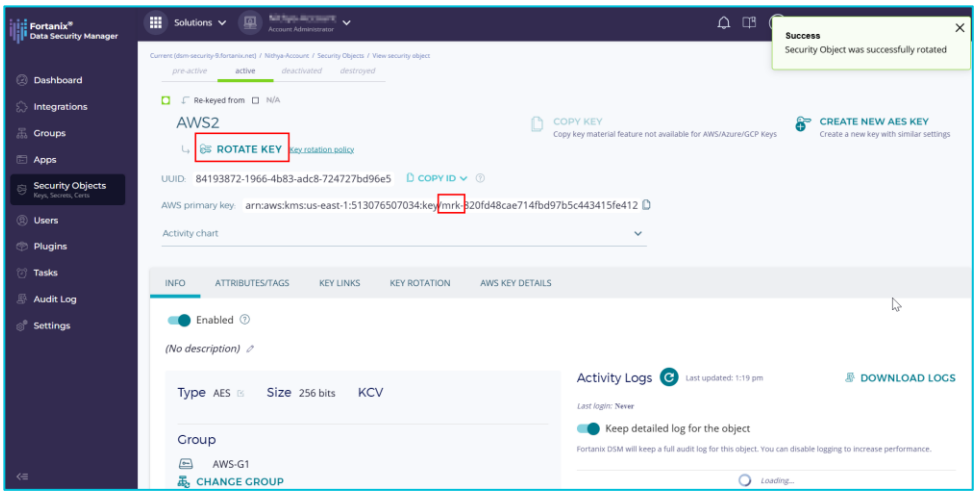
Subject: Software changes, updates, bug fixes, etc.

Software: Fortanix Data Security Manager

Version: 4.36

For details on always enabling key export permission during key creation using Fortanix DSM clients (JCE, PKCS#11, and CNG/EKM), refer to the Section 7: Client Features and Improvements.

- Added support for rotating multi-region Bring Your Own Key (BYOK) keys in Amazon Web Service (AWS) Key Management Service (KMS) **(JIRA: PM-433)**.
  - You can now rotate a multi-region key generated or imported in a AWS KMS externally backed DSM group.



  - You can now rotate a key copied from a normal DSM group to an AWS KMS externally backed DSM group as a multi-region key using linked-key rotation. This will rotate the primary and all replicas in AWS KMS to the new value of the key.

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

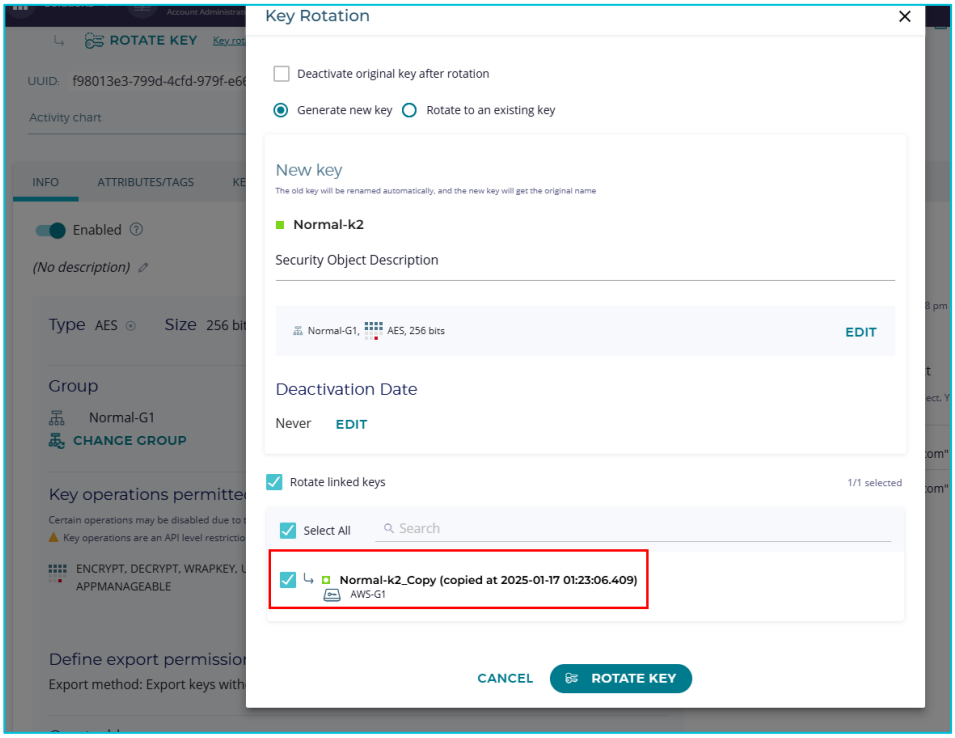
RELEASE NOTES

Date: 14-Feb-25

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

Software: Fortanix Data Security Manager

Version: 4.36



For more information, refer to [Fortanix DSM - AWS KMS BYOK (Bring Your Own Key)](#).

- Added support to enable auto-rotation of keys using the new **AWS KMS auto-rotation** option when generating keys in AWS KMS **(JIRA: PM-434)**.

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

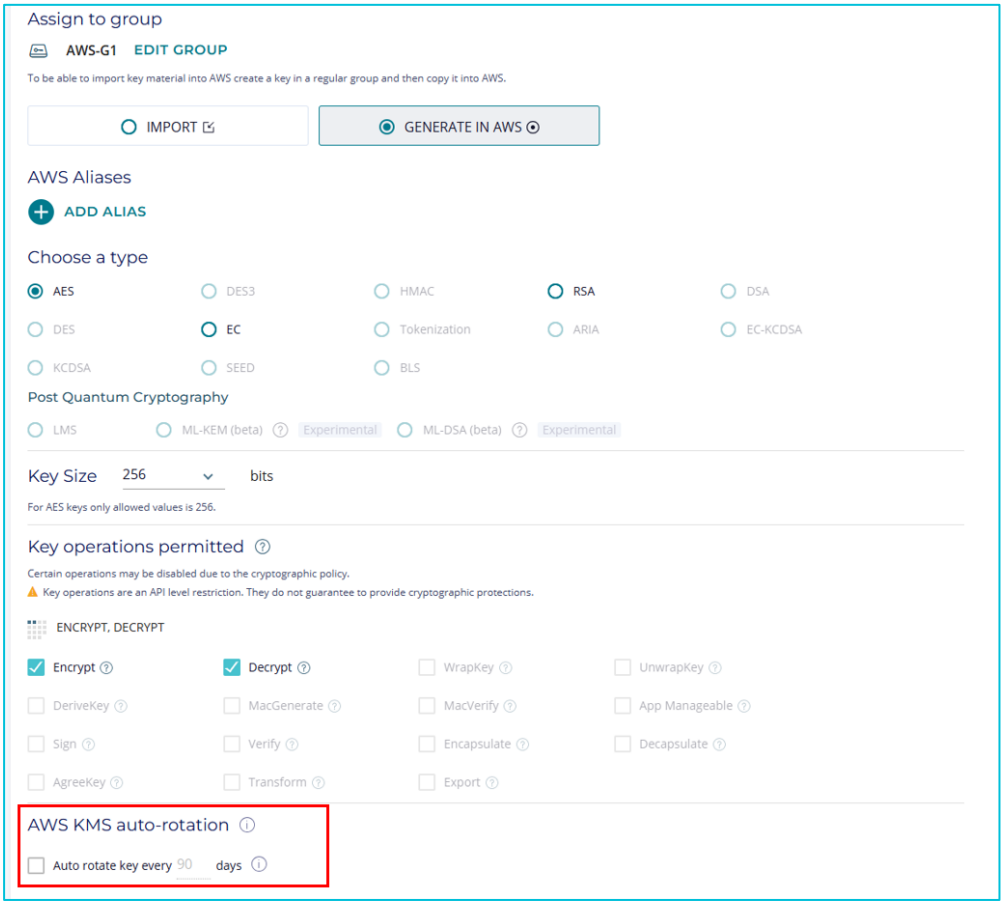
RELEASE NOTES

Date: 14-Feb-25

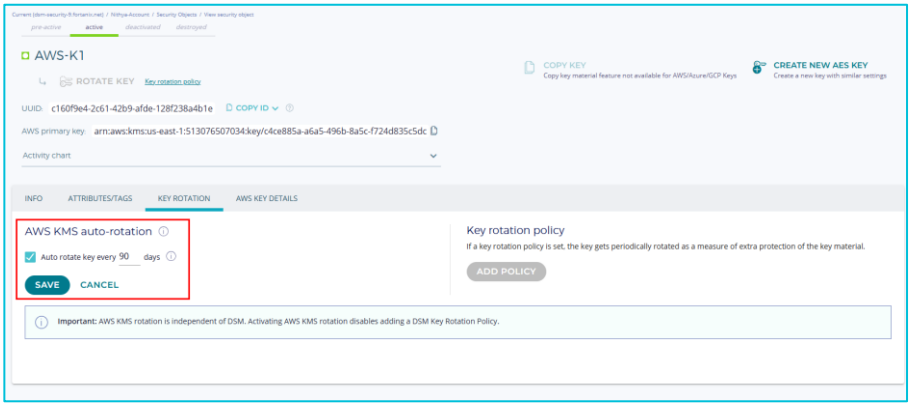
Subject: Software changes, updates, bug fixes, etc.

Software: Fortanix Data Security Manager

Version: 4.36



- You can also configure the auto-rotation policy from the **KEY ROTATION** tab in the detailed view of the AWS KMS virtual key.



- If the auto-rotate feature is active in AWS KMS, the **KEY ROTATION** tab in the detailed view of the AWS KMS virtual key will show the **AWS KMS auto-rotation** as enabled after key sync in Fortanix DSM.

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

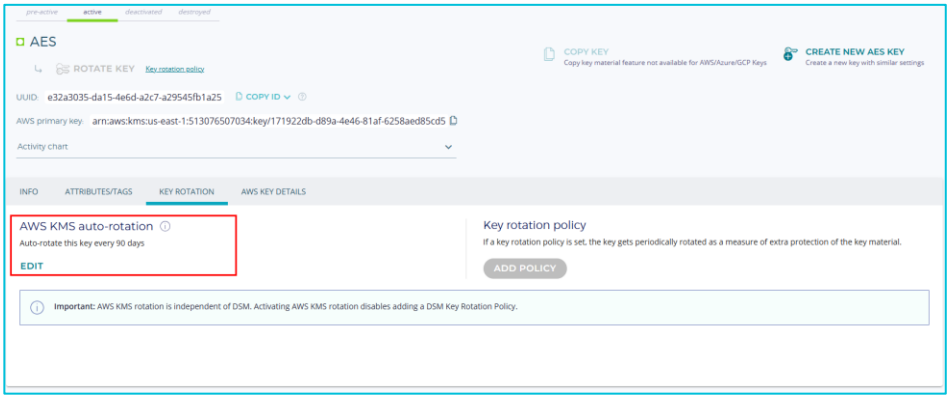
RELEASE NOTES

Date: 14-Feb-25

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

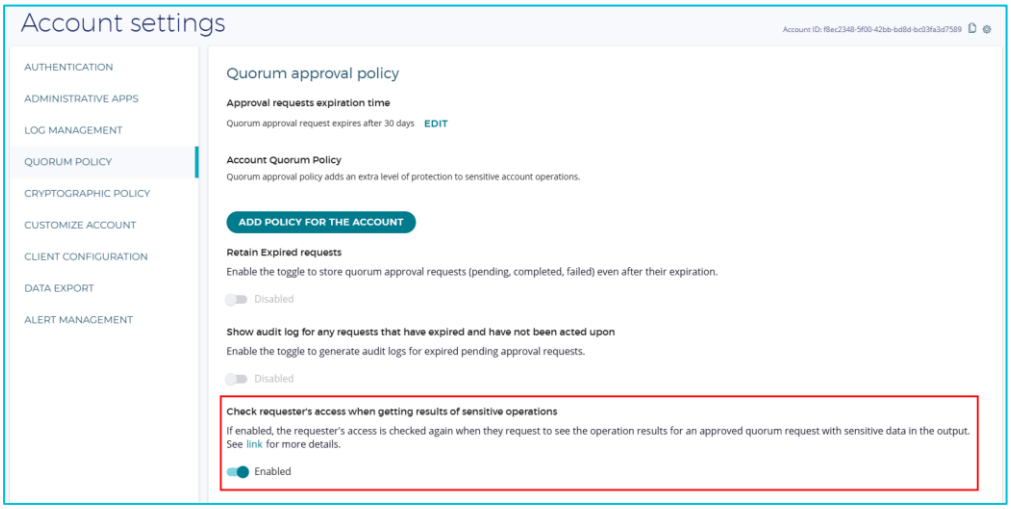
Software: Fortanix Data Security Manager

Version: 4.36



For more information, refer to Fortanix DSM - AWS KMS BYOK (Bring Your Own Key).

- Added a new option **Check requester's access when getting results of sensitive operations** in the Fortanix DSM account **Quorum approval policy** page to specify access control limits on the requester when trying to retrieve the results of an approved quorum approval task with sensitive data in the output **(JIRA: PM-451)**.



For more information, refer to User's Guide: Account Quorum Policy.

- Fortanix DSM now supports ISO 11568-compliant calculation of Key Check Values (KCV) for AES keys (all sizes) and DES3 keys (168-bit only). This is displayed as the **CMAC KCV** field in the detailed view of the key **(JIRA: PM-435)**.

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

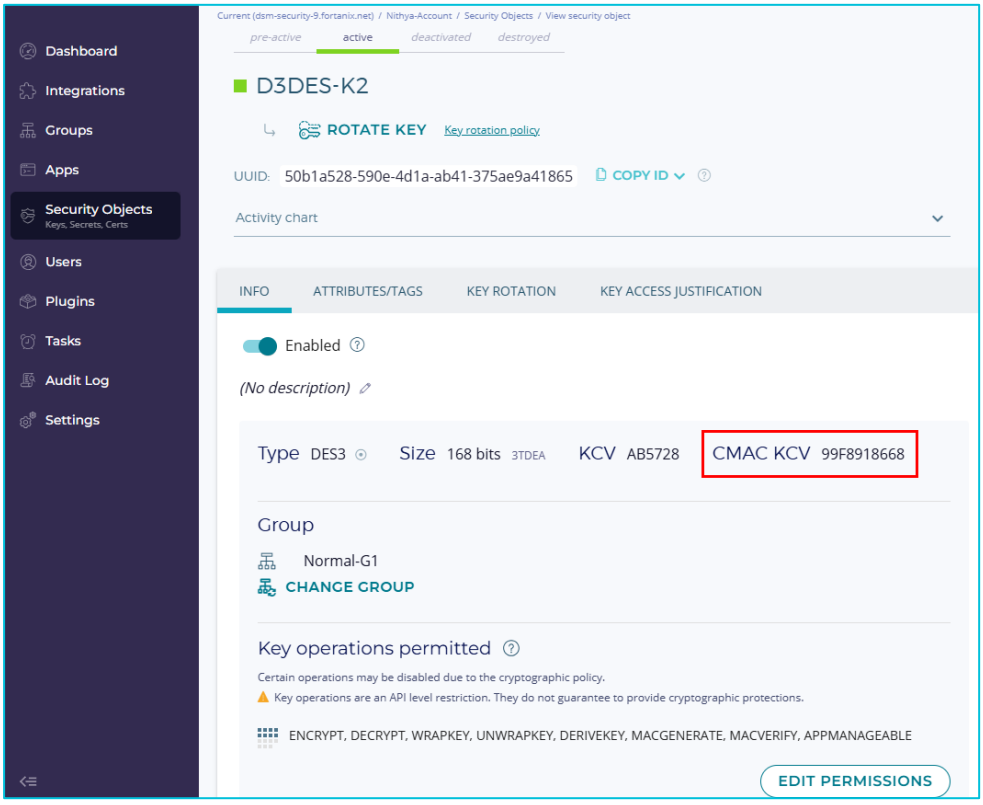
RELEASE NOTES

Date: 14-Feb-25

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

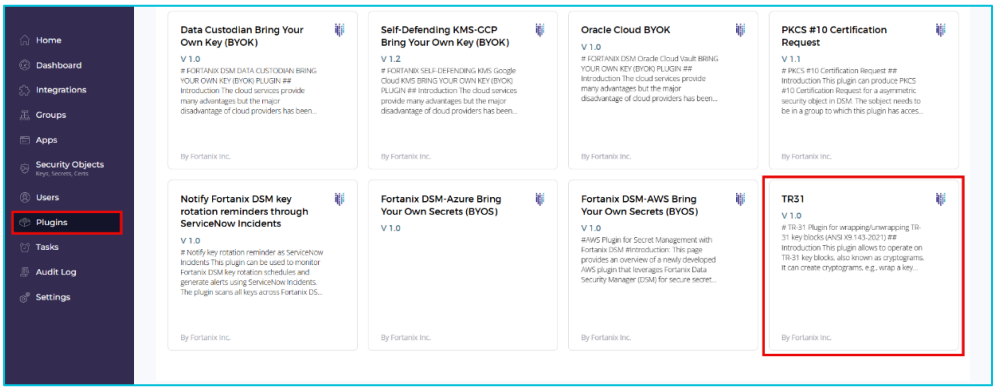
Software: Fortanix Data Security Manager

Version: 4.36



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

- Added support for new **TR31** plugin in the DSM Plugin Library. This plugin can be used to import and export any key types under the American National Standards Institute (ANSI) Technical Report (TR)-31 format (**JIRA: PROD-9300**).



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

IMPROVEMENTS

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

RELEASE NOTES

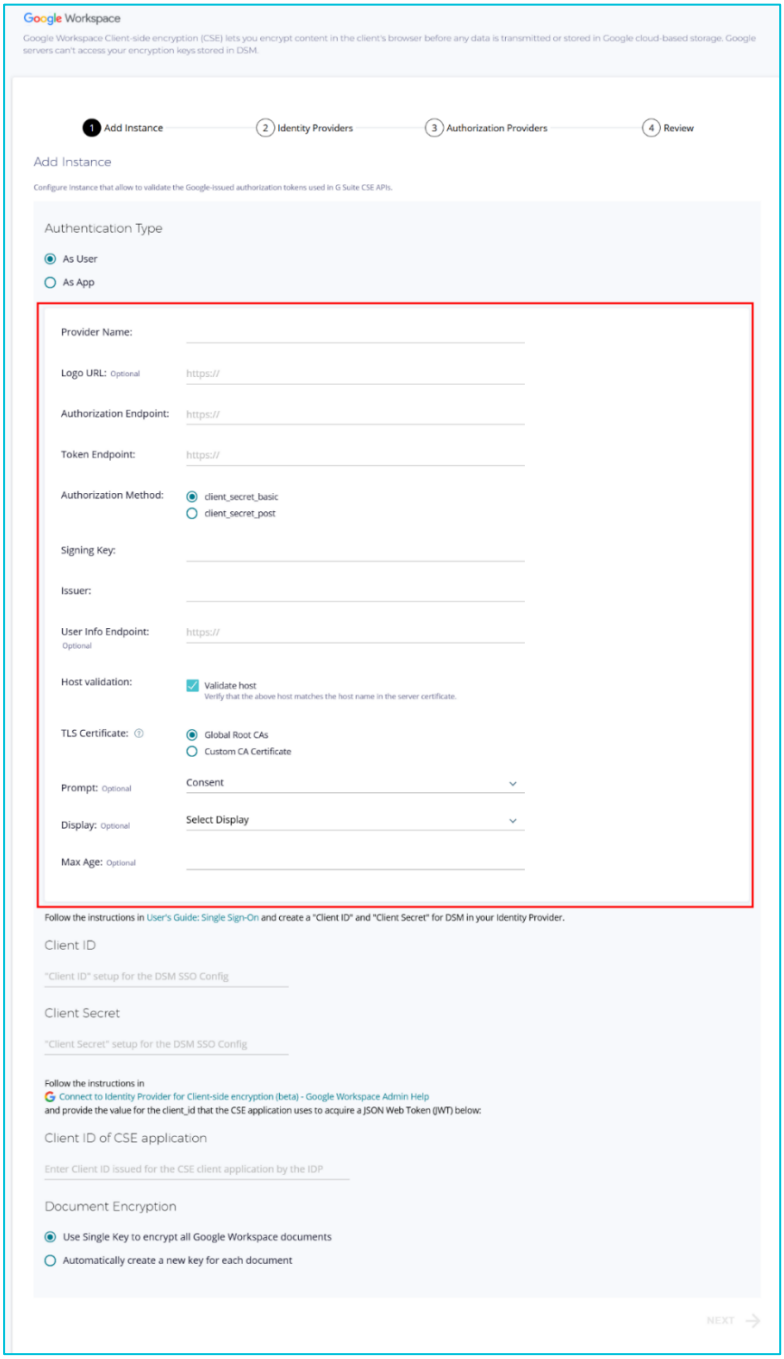
Date: 14-Feb-25

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

Software: Fortanix Data Security Manager

Version: 4.36

- Added support to provide Single Sign-On (SSO) identity provider (IdP) information, along with the necessary configuration details for **Google Workspace**, without requiring remote URL access **(JIRA: ROFR-5097)**.



For more information, refer to Using Fortanix DSM for Google Workspace Client-Side Encryption.

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

RELEASE NOTES

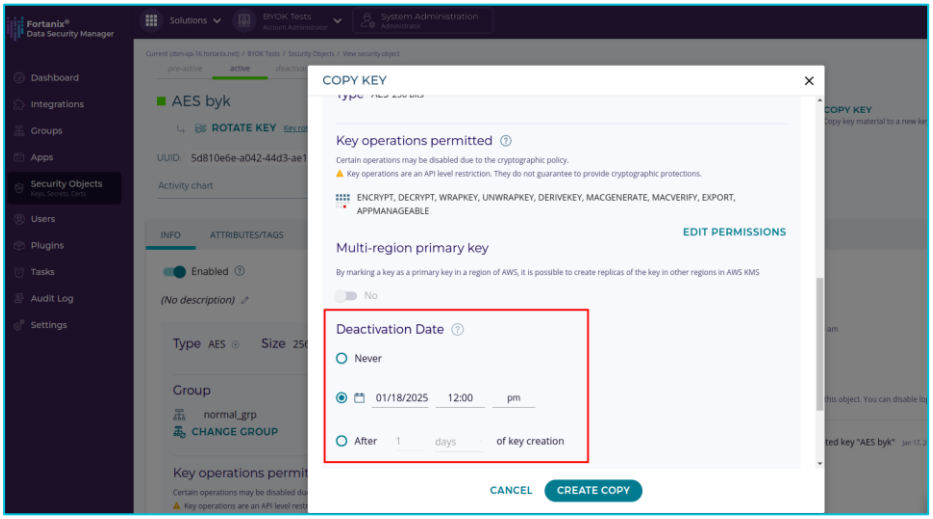
Date: 14-Feb-25

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

Software: Fortanix Data Security Manager

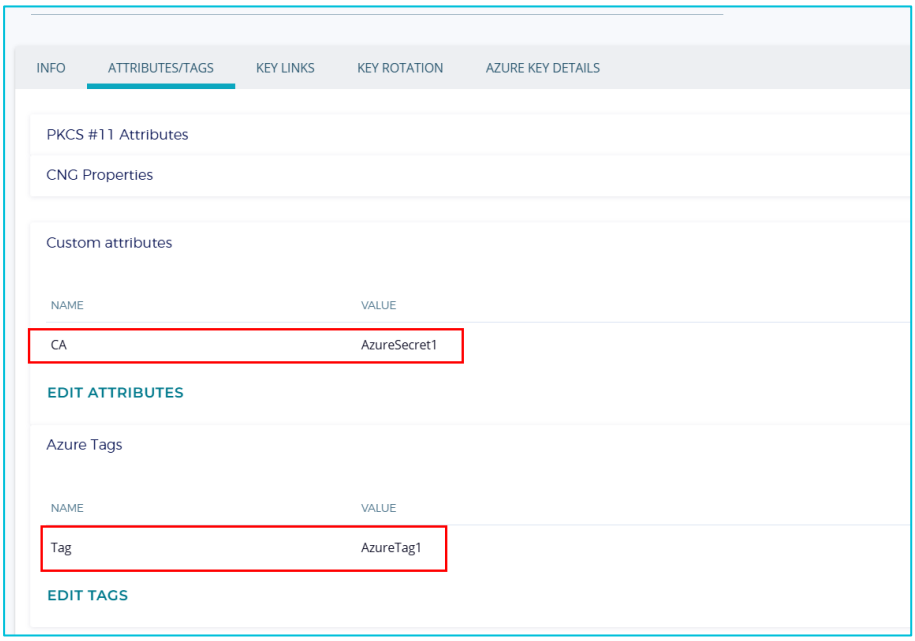
Version: 4.36

- When copying a key with an expiry or deactivation date from a normal DSM group to an externally backed AWS KMS group, the copied key in AWS KMS will retain the same expiry date **(JIRA: PM-232)**.



For more information, refer to Fortanix DSM - AWS KMS BYOK (Bring Your Own Key).

- When a source security object in Fortanix DSM, linked to a copy in externally backed Azure Key Vault (AKV) group, is rotated, the **Azure key name**, **Azure Tags**, and **Custom attributes** on the original key version in AKV are now copied to the new version (**JIRA: PM-437/EXTREQ-1035**).



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

RELEASE NOTES

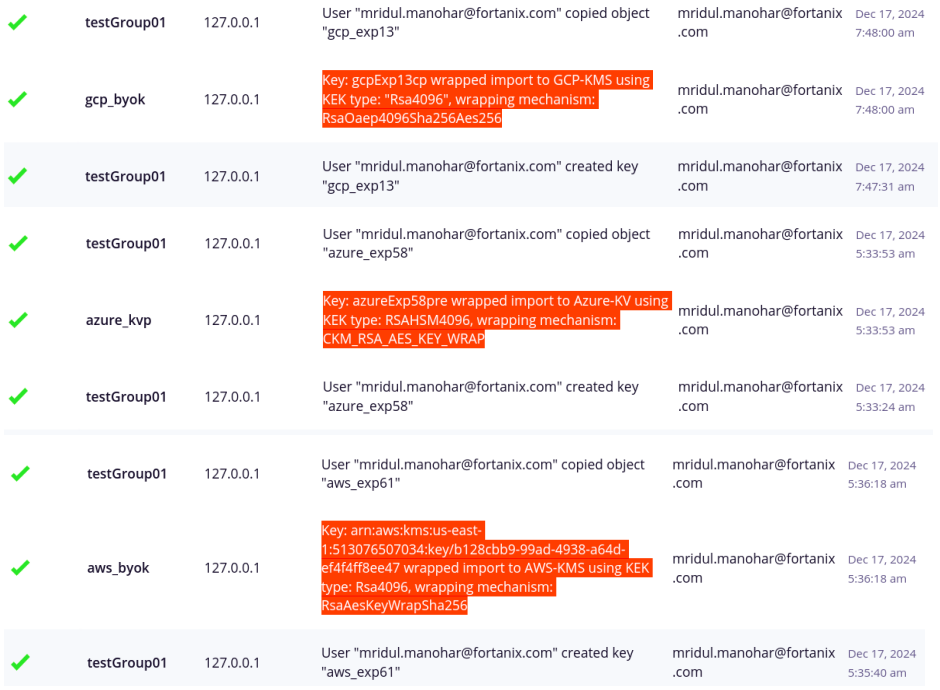
Date: 14-Feb-25

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

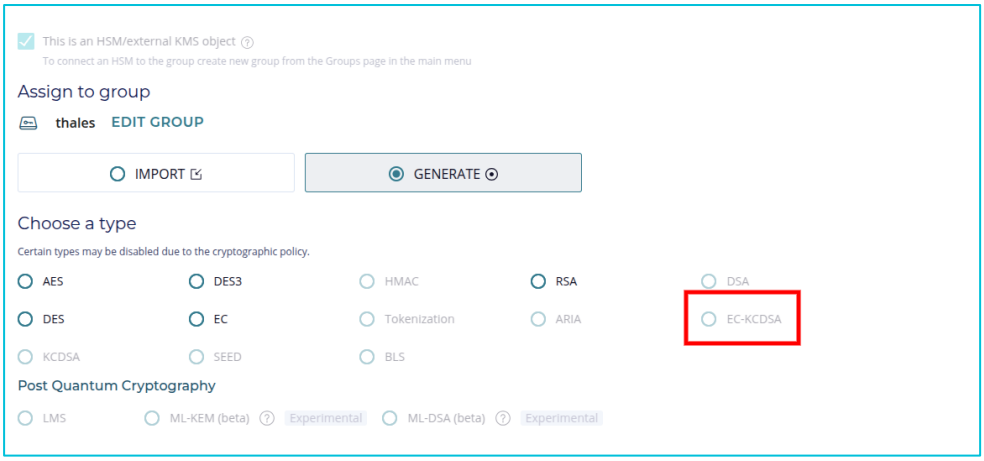
Software: Fortanix Data Security Manager

Version: 4.36

- Fortanix DSM now includes detailed audit log entries when uploading keys to a cloud KMS (AWS, Azure, and GCP) (**JIRA: PM-436**).
  The logs display the key type, key length, and wrapping mechanism used. Additionally, the wrapping mechanism has been upgraded to use RSA 4096 - the longest supported key pair for enhanced protection.



- Disabled generating or importing **EC-KCDSA** key types for **Thales Luna HSM** backed group in Fortanix DSM **(JIRA: ROFR-5011)**.



- Added padding space in **Export key as encrypted key material** tasks approval window (**JIRA: ROFR-4830**).

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

RELEASE NOTES

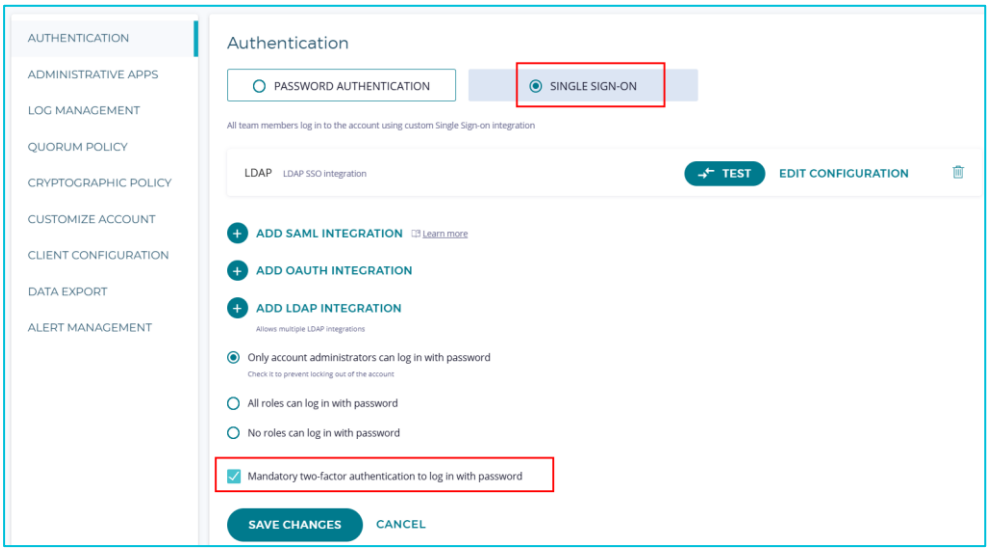
Date: 14-Feb-25

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

Software: Fortanix Data Security Manager

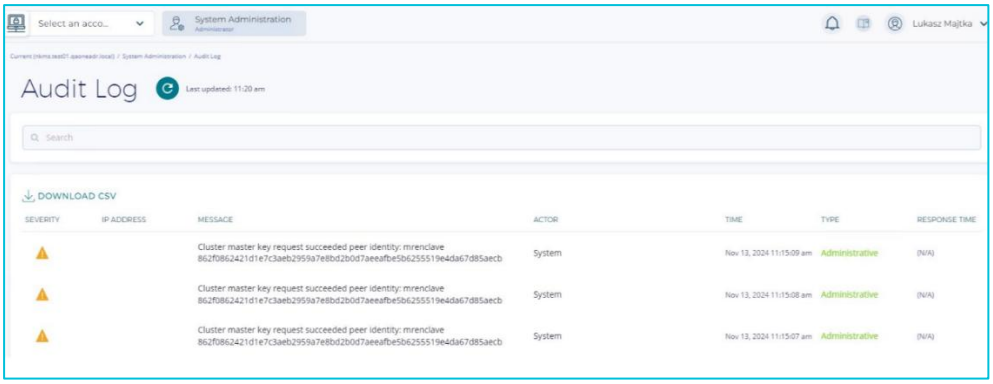
Version: 4.36

- Added support for **Mandatory two-factor authentication to log in with password** when **Only account administrators can log in with password** is selected in the **SINGLE SIGN-ON** tab if **SINGLE SIGN-ON** is enabled **(JIRA: ES-466)**.



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

- Removed Fortanix DSM cluster transparency logs from the Fortanix DSM system administration audit logs **(JIRA: PROD-9612)**.



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

RELEASE NOTES

Date: 14-Feb-25

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

Software: Fortanix Data Security Manager

Version: 4.36

OTHER IMPROVEMENTS

- Fortanix FX2200 appliances now uses Intel Software Guard Extensions (SGX) Data Center Attestation Primitives (DCAP) attestation instead of Intel Attestation Service (IAS) since IAS will be reaching the end of life by April 02, 2025 **(JIRA: PROD-9335)**.

  For more information, refer to Fortanix DSM Installation Guide.
- JSON Web Token (JWT) App authentication to Fortanix DSM now supports app authentication using Microsoft Azure Entra that supports configuring the DSM SaaS domain URL as values for the Audience (`aud`) claim **(JIRA: PM-423)**.

  For more information, refer to User's Guide: Authentication.
- Updated mbedtls dependency to v2.28.9 **(JIRA: PROD-9795)**.
- Improved the DSM REST APIs documentation **(JIRA: PM-285)**.

QUALITY ENHANCEMENTS

- Upgraded fluentd to version 1.18.0 (**JIRA: PROD-9777**).
- Improved Bitcoin Improvement Proposal 32 (BIP32) performance by implementing caching for specific elliptic curve points per key **(JIRA: PROD-9502**).

API UPDATES

- Added support for Disaster Recovery with account recovery and EVKs (**JIRA: PM-385**).
  - Added/updated the following APIs to support the configuration and management of replication accounts and account credentials (**JIRA: PROD-9066**):
    - `POST /sys/v1/accounts`: Updated to include a new `purpose` field, which can be set to configure account replication.

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

RELEASE NOTES

Date: 14-Feb-25

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

Software: Fortanix Data Security Manager

Version: 4.36

- `GET /sys/v1/accounts/{acct-id}/replication/recent_scan_summary`: Added to fetch the information about recent account replication scans.
- `PATCH /sys/v1/accounts/{acct-id}`: Updated to allow converting a replication account to a standard account and configuring replication account settings, with the conversion being irreversible. Regular account update operations are also supported.
- `POST /sys/v1/accounts/{acct_id}/replication/credentials`: Added to create an admin app credential that can be used to perform account replication. Currently, a single replication account can store up to two replication credentials.
- `GET /sys/v1/accounts/{acct_id}/replication/credentials`: Added to retrieve all stored replication credentials under the account.
- `GET /sys/v1/accounts/{acct_id}/replication/credentials/{credential_id}`: Added to retrieve a specified replication credential.
- `PATCH /sys/v1/accounts/{acct_id}/replication/credentials/{credential_id}`: Added to update a specified replication credential. This can be used to associate an app ID with the credential, and/or upload certificate chains for the credential.
- `DELETE /sys/v1/accounts/{acct_id}/replication/credentials/{credential_id}`: Added to delete a specified replication credential.

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

RELEASE NOTES

Date: 14-Feb-25

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

Software: Fortanix Data Security Manager

Version: 4.36

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

    - `POST /sys/v1/accounts/{acct_id}/replication/credentials/{credential_id}/self_signed`: Added to generate a self-signed certificate for a specified replication credential.
  - Added support for key operations override in the KMIP client configuration settings (**JIRA: PROD-9009**).
    - Added support for new `key_ops_override` method with `EXPORT` permission in the following APIs:
      - `POST /sys/v1/accounts`
      - `PATCH /sys/v1/accounts/:acct_id`
      - `POST /sys/v1/groups`
      - `PATCH /sys/v1/groups/:group_id`
- Updated the `AwsKmsInfo` definition to enable auto rotation for AWS KMS keys generated from Fortanix DSM (**JIRA: PM-434**).
  - You can now specify the `aws_key_rotation_status` when creating and updating keys in AWS-backed groups.
  - If key rotation is enabled, you can also specify the `rotation_period_in_days`.
- Added a new field `check_access_for_sensitive_operation_results` in the `ApprovalRequestSettings` to specify access control limits on the requester when trying to retrieve the results of an approved quorum approval task with sensitive data in the output (**JIRA: PM-451**).

  The new field affects the following APIs:
  - `POST /sys/v1/accounts`
  - `GET /sys/v1/accounts`
  - `PATCH /sys/v1/accounts/{acct_id}`
  - `GET /sys/v1/accounts/{acct_id}`
  - `POST /sys/v1/roles`
  - `GET /sys/v1/roles`
  - `GET /sys/v1/roles/{custom_role_id}`
  - `PATCH /sys/v1/roles/{custom_role_id}`

- `POST /sys/v1/approval_requests/{req_id}/approve`

- Added an optional `kcv_cmac` field to APIs that return `Sobject` as part of their response, allowing the display of the Cipher-based Message Authentication Code (CMAC) Key Check Value (KCV) for AES (all sizes) and DES3 keys (168-bit only) (**JIRA: PM-435**).

INTEGRATIONS AND USE CASES

- Added support to integrate Fortanix DSM with the Secrets Store Container Storage Interface (CSI) Driver solution to securely access secrets such as API keys, passwords, and certificates in Kubernetes pods (**JIRA: PM-188**).

  For more details, refer to Fortanix Data Security Manager Using Secret Store CSI Driver.

- Added support to perform Filesystem Encryption (FSE) on a Couchbase cluster using Fortanix DSM to encrypt the data directory used by the Couchbase database to store the user data (**JIRA: TIA-29**).

  For more details, refer to Filesystem Encryption for Couchbase Using Fortanix Data Security Manager.

- Added support for filesystem encryption for virtual machines (VMs) in the Nutanix Acropolis Operating System (AOS) using Fortanix DSM for seamless encryption and management of the entire VM landscape in an Nutanix AOS environment.

  For more details, refer to Filesystem Encryption for Nutanix Using Fortanix Data Security Manager.

- Added support to integrate Fortanix DSM with Dell PowerFlex using CloudLink through Key Management Interoperability Protocol (KMIP) server configuration to simplify key management and protect critical data both at rest and in motion (**JIRA: TIA-19**).

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

RELEASE NOTES

Date: 14-Feb-25

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

Software: Fortanix Data Security Manager

Version: 4.36

For more details, refer to Using Fortanix Data Security Manager with Dell PowerFlex Using CloudLink.

CLIENT FEATURES AND IMPROVEMENTS

- Added support for uploading and retrieving the Transferable Public Keys (TPKs) to Fortanix DSM using the Sequoia DSM (sq-dsm) client (**JIRA: PM-400**).

  For more details, refer to Clients: Sequoa PGP.
- Added support for Fortanix DSM PKCS#11, JCE, and CNG/EKM/CSP clients, allowing users to toggle a flag that automatically includes the `EXPORT` permission in every key creation request. This enhancement ensures proper usage of replicated account) in disaster recovery scenarios (**JIRA: PM-385**).

  For more details, refer to the following:
  - *Clients: PKCS#11 Library*
  - *Clients: Java Cryptography Extension (JCE) Provider*
  - *Clients: Microsoft CNG Key Storage Provider*
- Updated custom logging for the Windows CNG, EKM, and CSP clients separately, providing more specific logging for each client (**JIRA: PROD-9776**).

  For more details, refer to Clients: Microsoft CNG Key Storage Provider.

DSM ACCELERATOR NEW FEATURES

- **DSM Accelerator Webservice**
  - Added support for key wrapping during the export process from Fortanix DSM to the Fortanix DSM Accelerator Webservice, ensuring the secure transfer and protection of sensitive key data (**JIRA: PM-26**).

    For more details, refer to DSM Accelerator Webservice Developer Guide.

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

RELEASE NOTES

Date: 14-Feb-25

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

Software: Fortanix Data Security Manager

Version: 4.36

- **DSM Accelerator JCE Provider**
  - Added support for key wrapping during the export process from Fortanix DSM to Fortanix DSM Accelerator JCE Provider, ensuring the secure transfer and protection of sensitive key data (**JIRA: PM-407**).

    For more details, refer to DSM Accelerator JCE Provider Developer Guide.

BUG FIXES

- Fixed an issue where the option to rotate linked keys was disabled for AWS Multi-Region keys in the Fortanix DSM user interface (UI) (**JIRA: ROFR-5241**).
- Fixed an error that occurred when attempting to rotate a key from an Azure-backed group to DSM group (**JIRA: ROFR-5249**).
- Fixed an issue where FIPS DSM could not be configured as an HSM for a group when using the **Store keys externally** option (**JIRA: ES-454**).
- Fixed an issue where rotating linked keys for an Azure CDC group resulted in missing links (such as "rekeyed to" and "copied from") and an error after the rotation process (**JIRA: ROFR-5248**).
- Fixed an issue where the Admin app was unable to create child or tenant accounts within an account that has a reseller subscription (**JIRA: PROD-6451**).

KNOWN ISSUES

- 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)**.

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

RELEASE NOTES

Date: 14-Feb-25

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

Software: Fortanix Data Security Manager

Version: 4.36

- 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.

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

RELEASE NOTES

Date: 14-Feb-25

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

Software: Fortanix Data Security Manager

Version: 4.36

- 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.

- The DSM upgrade from v4.31 to v4.34 causes `sdkms-join` pods to enter a `CrashLoopBackOff` state due to a TLS certificate validation error **(JIRA: PROD-9782)**.

  Workaround: Perform the following steps to resolve this issue:

  a. Run the following command to edit the `sdkms-join` deployment:

  ```
  kubectl edit deploy sdkms-join
  ```

  b. Add the following environment variables under the `env` section:

  ```
  - name: http_proxy
    value: <customer_proxy_url>
  - name: https_proxy
    value: <customer_proxy_url>
  - name: no_proxy
    value:
  localhost,127.0.0.0/8,127.0.1.1,10.244.0.0/16,
  10.245.0.0/16
  ```

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

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

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

RELEASE NOTES

Date: 14-Feb-25

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

Software: Fortanix Data Security Manager

Version: 4.36

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

FORTANIX DATA SECURITY MANAGER PERFORMANCE STATISTICS

- **Series 2**

KEY TYPES AND OPERATIONS	THROUGHPUT (Operations/second on a 3-node cluster re-using a single TLS session)
AES 256: CBC Encryption/Decryption	7,138/6,894
AES 256: GCM Encryption/Decryption	6,785/6,838
AES 256: FPE Encryption/Decryption	4,956/4,940
AES 256 Key Generation	1,279
RSA 2048 Encryption/Decryption	5,749/1,188
RSA 2048 Key Generation	34
RSA 2048 Sign/Verify	1,169/5,832
RSA 4096 Sign/Verify	388/4,587
EC NISTP256 Sign/Verify	1,810/1,129
Kyber ML-KEM Encapsulation	1,320
Kyber ML-KEM Decapsulation	1,242
LMS Key (Height, Node)	
L1 5, Node 24	220.7
L1 5, Node 32	181.1
L1 10, Node 24	9
L1 10, Node 32	7.2

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

RELEASE NOTES

Date: 14-Feb-25

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

Software: Fortanix Data Security Manager

Version: 4.36

KEY TYPES AND OPERATIONS	THROUGHPUT (Operations/second on a 3-node cluster re-using a single TLS session)
BIP32 Key Derive as Transient Hardened Child Key	765
BIP32 Sign	765
ECDSA: EC SecP256K1 Key Generation	889
ECDSA Sign	889
Data Security Manager Plugin (Hello world plugin)	2,398 (invocations/second)

- **Azure Standard_DC8_v2**

KEY TYPES AND OPERATIONS	THROUGHPUT (Operations/second on a 3-node [Standard_DC8_v2] cluster re-using a single TLS session)
AES 256: CBC Encryption/Decryption	5,386/5,487
AES 256: GCM Encryption/Decryption	5,352/5,409
AES 256: FPE Encryption/Decryption	4,666/4,730
AES 256 Key Generation	1,257
RSA 2048 Encryption/Decryption	5,059/1,384
RSA 2048 Key Generation	44
RSA 2048 Sign/Verify	1,401/5,044
RSA 4096 Sign/Verify	528/4,415
EC NISTP256 Sign/Verify	2,033/1,341

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

KEY TYPES AND OPERATIONS	THROUGHPUT (Operations/second on a 3-node [Standard_DC8_v2] cluster re-using a single TLS session)
Data Security Manager Plugin (Hello world plugin)	2,495 (invocations/second)

- **Series 2 JCE**

KEY TYPES AND OPERATIONS	THROUGHPUT (Operations/second on a 3-node cluster re-using a single TLS session)
AES 256: CBC Encryption/Decryption	6,043/5,773
AES 256 Key Generation	1,322
RSA 2048 Key Generation	33
RSA 2048 Sign/Verify	985/2,902
RSA 4096 Sign/Verify	363/2,583
EC NISTP256 Sign/Verify	1,333/942
Data Security Manager Plugin (Hello world plugin)	2,382 (invocations/second)

- **Azure Standard_DC8 JCE**

KEY TYPES AND OPERATIONS	THROUGHPUT (Operations/second on a 3-node [Standard_DC8 JCE] cluster re-using a single TLS session)
AES 256: CBC Encryption/Decryption	5,026/5,269

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

RELEASE NOTES

Date: 14-Feb-25

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

Software: Fortanix Data Security Manager

Version: 4.36

KEY TYPES AND OPERATIONS	THROUGHPUT (Operations/second on a 3-node [Standard_DC8 JCE] cluster re-using a single TLS session)
AES 256 Key Generation	1,184
RSA 2048 Key Generation	43
RSA 2048 Sign/Verify	1,134/2,705
RSA 4096 Sign/Verify	491/2,532
EC NISTP256 Sign/Verify	1,566/1,101
Data Security Manager Plugin (Hello world plugin)	2,505 (invocations/second)

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

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

ITEM	SPECIFICATION
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	21,434/21,048
AES 256: GCM Encryption/Decryption	21,948/21,866
AES 256: FPE Encryption/Decryption	9,689/9,660

- **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	21,456/21,652
AES 256: CFB Encryption/Decryption	22,022/21,708
AES 256: CTR Encryption/Decryption	21,915/21,723
AES 256: OFB Encryption/Decryption	22,093/21,782

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

RELEASE NOTES

Date: 14-Feb-25

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

Software: Fortanix Data Security Manager

Version: 4.36

KEY TYPES AND OPERATIONS	THROUGHPUT (Operations/second on a 1-node cluster re-using a single TLS session)
AES 256: CCM Encryption/Decryption	21,772/21,597

INSTALLATION

To install the DSM Runtime Encryption® SGX (on-prem/Azure) and Software (AWS/Azure/VMWare) packages, Download Here.

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.

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

RELEASE NOTES

Date: 14-Feb-25

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

Software: Fortanix Data Security Manager

Version: 4.36

Fortanix Data Security Manager Release Notes

Release 4.36

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

✉ info@fortanix.com

🌐 www.fortanix.com