RELEASE NOTES

Date: 2-Jul-24

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

Software: Fortanix Data Security Manager SaaS

Version: 4.30

OVERVIEW

This document provides an overview of new features, general improvements, and resolved issues in the Fortanix Data Security Manager (DSM) SaaS 4.30 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 support to rotate keys in a Google Cloud Key Management Service (KMS) group in Fortanix DSM. The following scenarios are supported:
    - Fortanix DSM can now rotate Google Cloud KMS keys to new versions uploaded from DSM by rotating the linked source security object **(JIRA: PM-312)**.

      For more details, refer to the User's Guide: Google Cloud KMS.

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

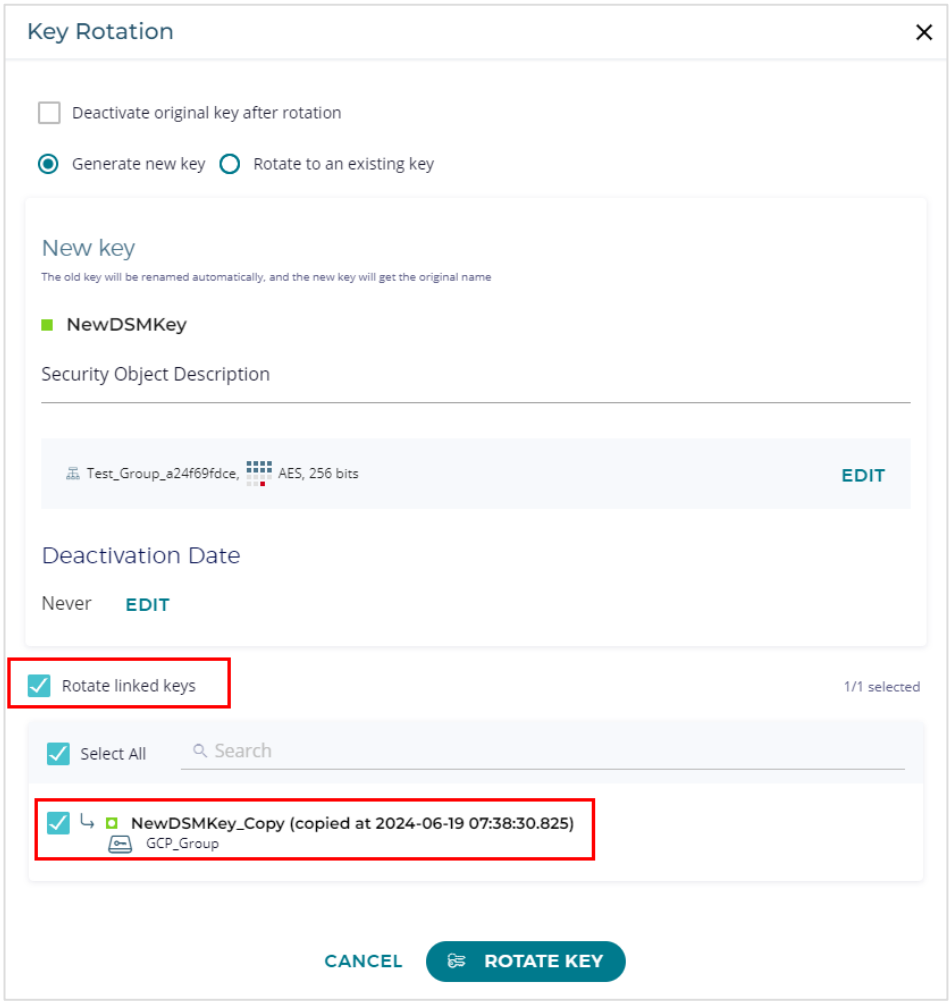
RELEASE NOTES

Date: 2-Jul-24

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

Software: Fortanix Data Security Manager SaaS

Version: 4.30



- Google KMS keys can now be rotated to a value of an existing Fortanix DSM security object by selecting the **Rotate to DSM key** check box **(JIRA: PM-208)**.

  For more details, refer to the User's Guide: Google Cloud KMS.

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

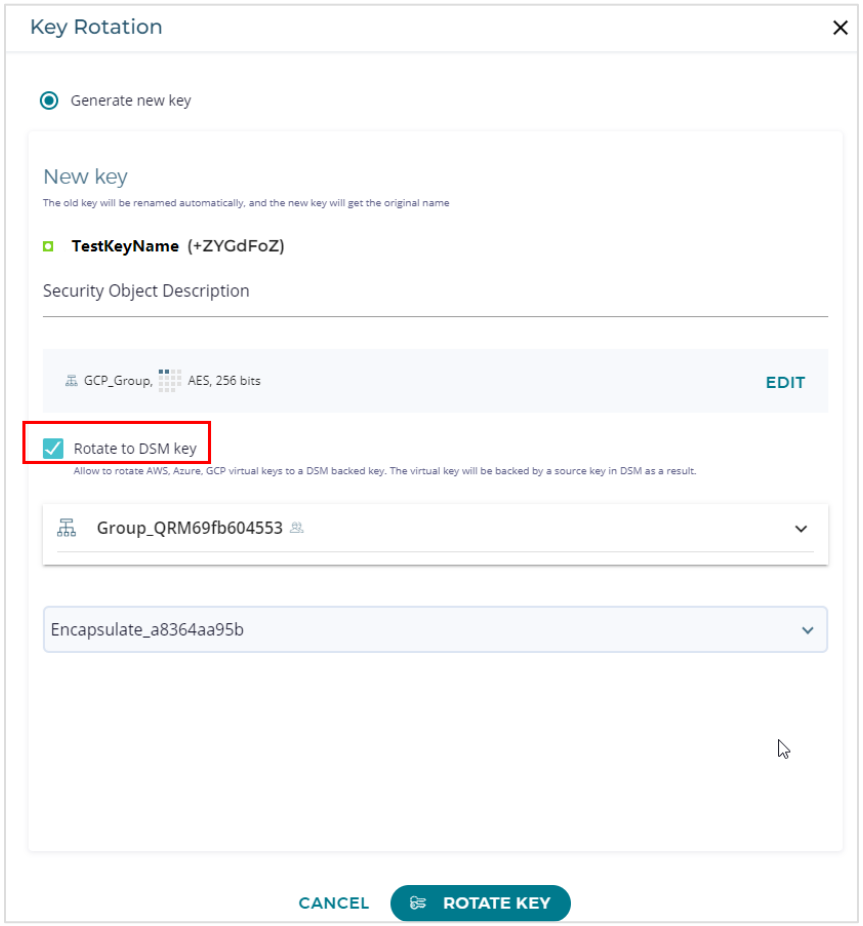
RELEASE NOTES

Date: 2-Jul-24

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

Software: Fortanix Data Security Manager SaaS

Version: 4.30



ENHANCEMENTS TO EXISTING FEATURES

- Fortanix DSM can now generate and import Elliptic Curve (EC) keys over curve **SecP256K1** in premium Azure Key Vaults through the DSM user interface (UI) **(JIRA: ROFR-4873)**.

  For more details, refer to the Fortanix DSM - Azure Key Vault BYOK (Bring Your Own Key) and Fortanix DSM - Azure Key Vault Cloud Native Key Management.

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

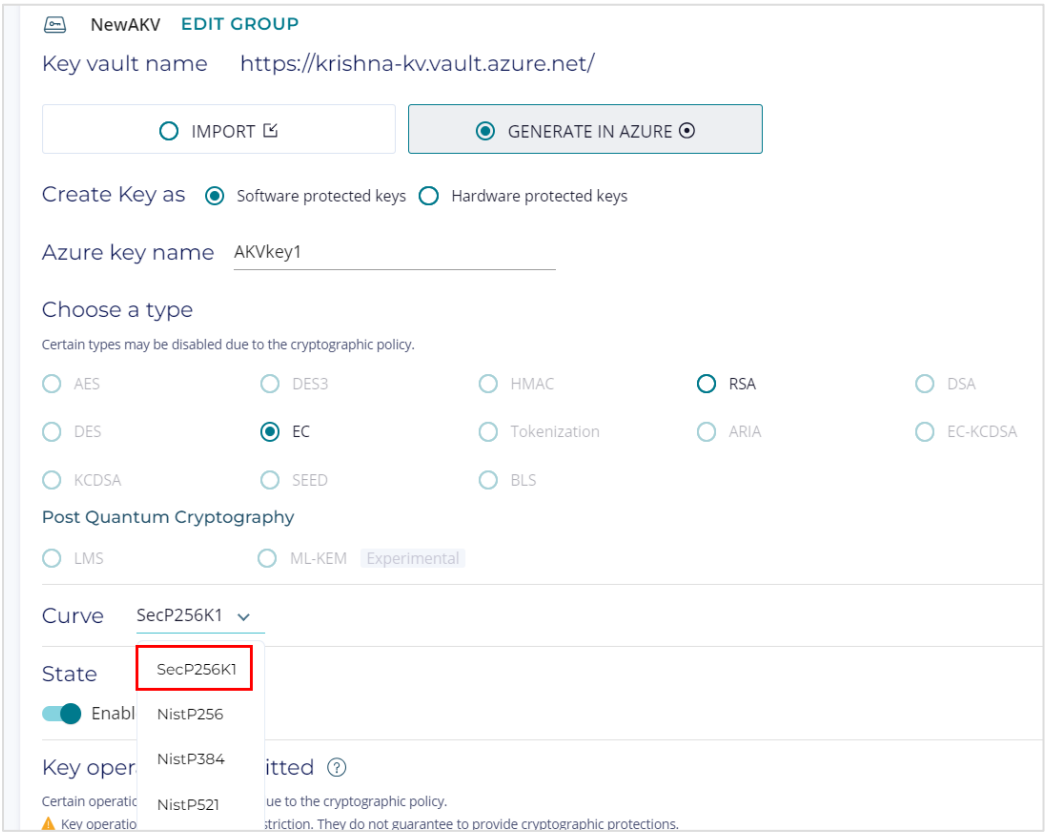
RELEASE NOTES

Date: 2-Jul-24

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

Software: Fortanix Data Security Manager SaaS

Version: 4.30



- New AWS Regions have been added as target to upload Customer Managed Keys to AWS KMS: Asia Pacific (Hyderabad), Asia Pacific (Jakarta), Asia Pacific (Melbourne), Canada West (Calgary), Europe (Spain), Europe (Zurich), Israel (Tel Aviv), and Middle East (UAE) **(JIRA: EXTREQ-1072)**.

  For more details, refer to the Fortanix DSM - AWS Key Management Service CDC Group Setup.

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

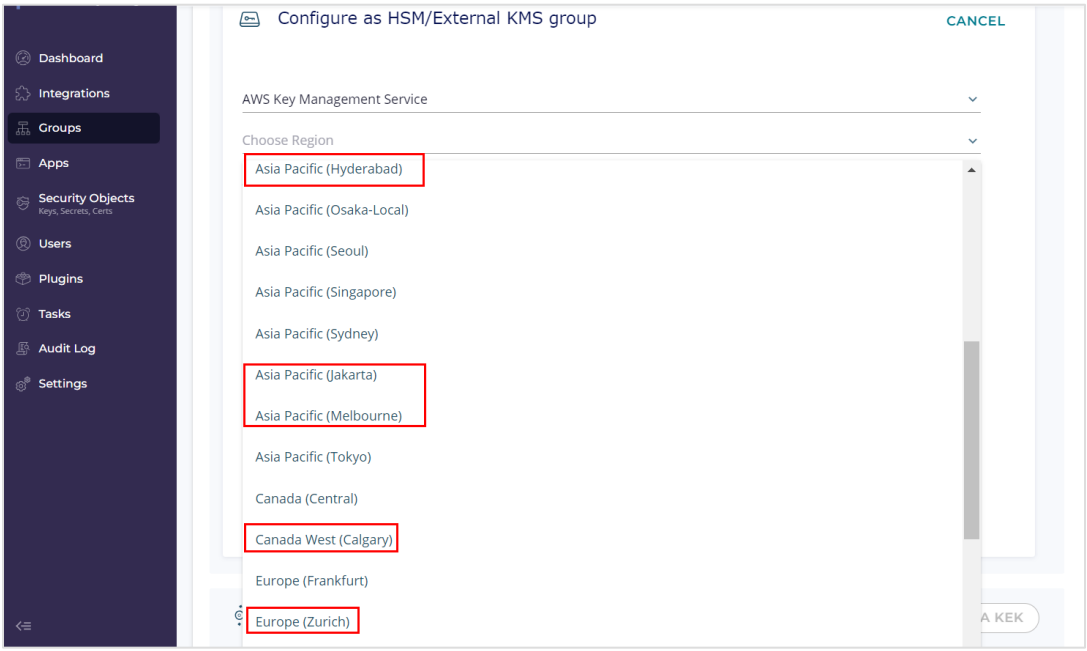
RELEASE NOTES

Date: 2-Jul-24

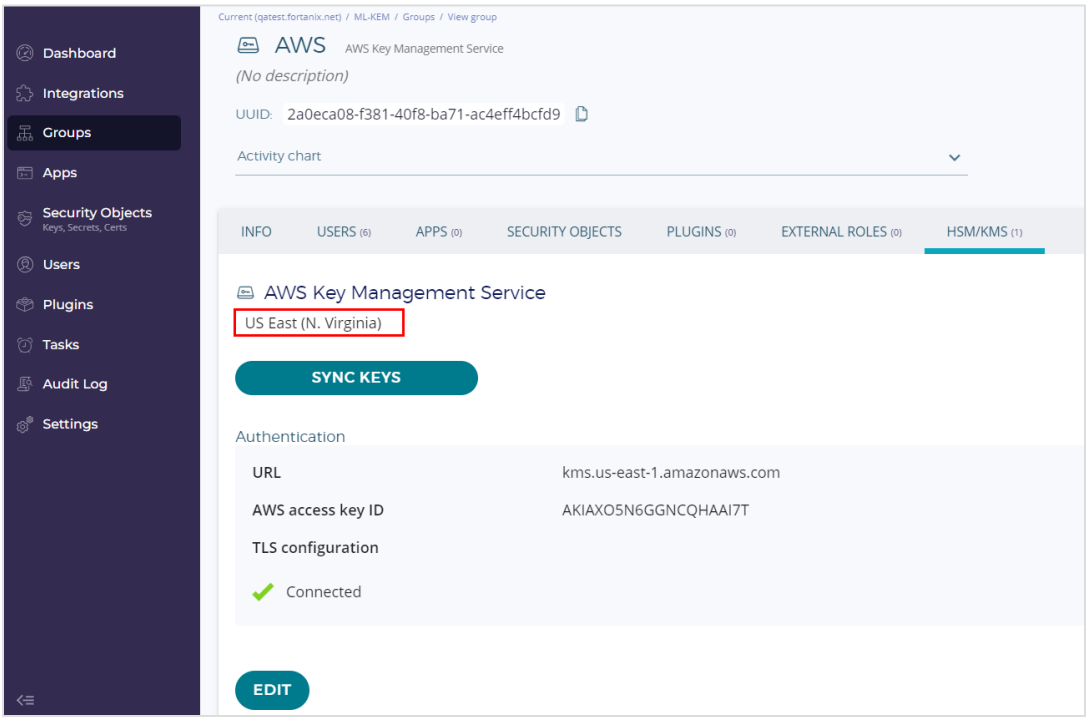
Subject: Software changes, updates, bug fixes, etc.

Software: Fortanix Data Security Manager SaaS

Version: 4.30



- The AWS region name is now shown in the detailed view of an AWS KMS group under the **HSM/KMS** tab in the Fortanix DSM **(JIRA: ROFR-3099)**.



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

RELEASE NOTES

Date: 2-Jul-24

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

Software: Fortanix Data Security Manager SaaS

Version: 4.30

CLIENT IMPROVEMENTS

- Added quorum policy approval support for the Fortanix DSM CNG client (**JIRA: PM-68**).

  For more details, refer to the Clients: Microsoft CNG Key Storage Provider.
- The Fortanix DSM 32-bit version of the CNG Provider client now supports sign and verify operations (**JIRA: PM-332**).
- The Fortanix DSM Windows PKCS#11 client now supports configuring the log file location (**JIRA: PM-245**).

  For more details, refer to the Clients: PKCS#11 Library.

DSM ACCELERATOR IMPROVEMENTS AND BUG FIXES

- **DSM Accelerator Webservice:**
  - Improved the Fortanix DSM Accelerator Webservice performance for highly transactional applications, by removing the bearer token check in the Fortanix DSM Accelerator Webservice so that it does not reach out to Fortanix DSM for authentication when processing locally cached keys (**JIRA: PM-351**).
- **DSM Accelerator JCE Provider:**
  - Improved the Fortanix DSM Accelerator JCE Provider performance for highly transactional applications, by removing the bearer token check in the Fortanix DSM Accelerator JCE Provider so that it does not reach out to Fortanix DSM for authentication when processing locally cached keys (**JIRA: PM-351**).
  - The path to copy the library `libdsmaccelerator.so` in Linux can now be configured using the environment variable `FORTANIX_TEMP_DIR` **(JIRA: PROD-8500)**.

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

RELEASE NOTES

Date: 2-Jul-24

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

Software: Fortanix Data Security Manager SaaS

Version: 4.30

- The path to copy the library `dsmaccelerator.dll` in Windows can now be configured using the environment variable `FORTANIX_TEMP_DIR` **(JIRA: PROD-8576)**.
  For more details, refer to the *DSM Accelerator JCE Provider Developer Guide*.

INTEGRATIONS AND USE CASES

- Added support to use the 32-bit version of Microsoft SignTool with the 32-bit version of Fortanix DSM CNG Provider to sign and verify Microsoft Office macro files (**JIRA: PM-332**).
  For more details, refer to the Using Fortanix Data Security Manager with 32-Bit SignTool for Signing and Verifying Microsoft Office Macro Files.

QUALITY IMPROVEMENTS

- Upgraded the `fluent-bit` package to the latest version (v3.0.6) for Observe's host agent monitoring **(JIRA: DEVOPS-4862)**.

BUG FIXES

- Fixed an issue where the user could not import an RSA key in Fortanix DSM UI (**JIRA: ES-353**).

KNOWN ISSUES

- Having empty fields for groups, users, or processes in the File Decryption Policy would result in an incorrect policy (**JIRA: ROFR-4954**).
  Workaround: If you want to create a policy where all groups, users, or processes are allowed, then update the policy using the agent instead of the Fortanix DSM user interface (UI).
- Unable to copy EC - **SecP256K1** keys with export permission from a normal group to an Azure Key Vault group in Fortanix DSM (**JIRA: ROFR-4955**).

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

RELEASE NOTES

Date: 2-Jul-24

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

Software: Fortanix Data Security Manager SaaS

Version: 4.30

Workaround: Perform the copy operation using the Fortanix DSM REST API.

- 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. Please make sure 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).
- After downgrading Fortanix DSM to version 4.25, it still shows the **Node size** field with a null value for LMS keys that were added in DSM version 4.26, even though the Node size is not a supported parameter in the older version (**JIRA: PROD-8278**).
- Unable to create an LMS key with the following height combinations of 20 (**JIRA: PROD-8248**).
  - 5, 20, and vice versa.
- 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**).

- 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.

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

RELEASE NOTES

Date: 2-Jul-24

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

Software: Fortanix Data Security Manager SaaS

Version: 4.30

- `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.

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

RELEASE NOTES

Date: 2-Jul-24

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

Software: Fortanix Data Security Manager SaaS

Version: 4.30

Fortanix Data Security Manager SaaS Release Notes

Release 4.30

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

✉ info@fortanix.com

🌐 www.fortanix.com