

RELEASE NOTES

Date: 25-Sep-25

Subject: Software changes, updates, bug fixes, and so on.

Software: Fortanix Data Security Manager

Version: 5.3

OVERVIEW

This document provides an overview of new features and general improvements in the Fortanix Data Security Manager (DSM) SaaS 5.3 release.

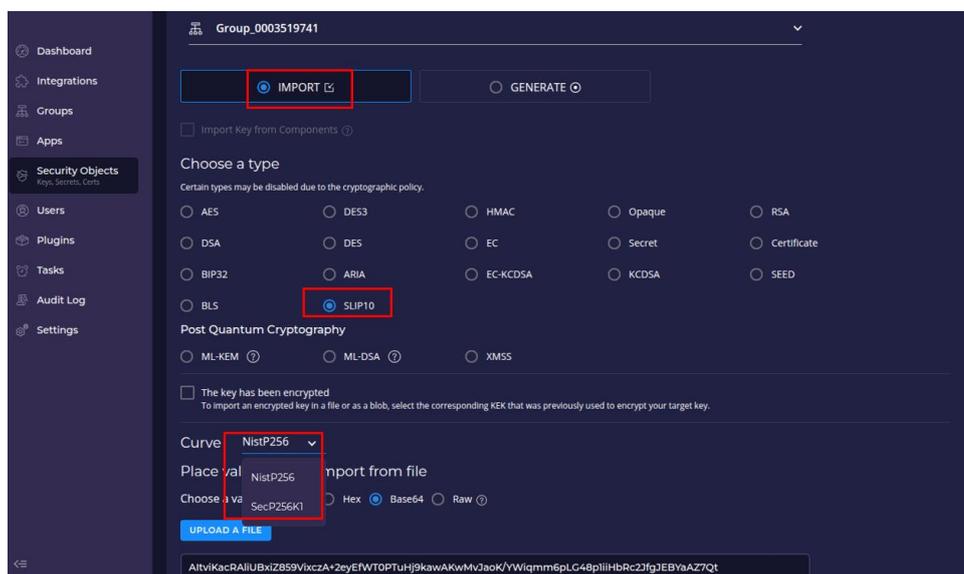


NOTE:

- 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 now supports SLIP10 wallet key derivation using NIST P-256 curves (**JIRA: EXTREQ-1463**).



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

- Fortanix DSM now supports managing RSA keys in Google Cloud Platform (GCP) Key Management System (KMS) (**JIRA: EXTREQ-1255**).
 - Generate, import, and copy keys (Bring Your Own Key) into GCP KMS.

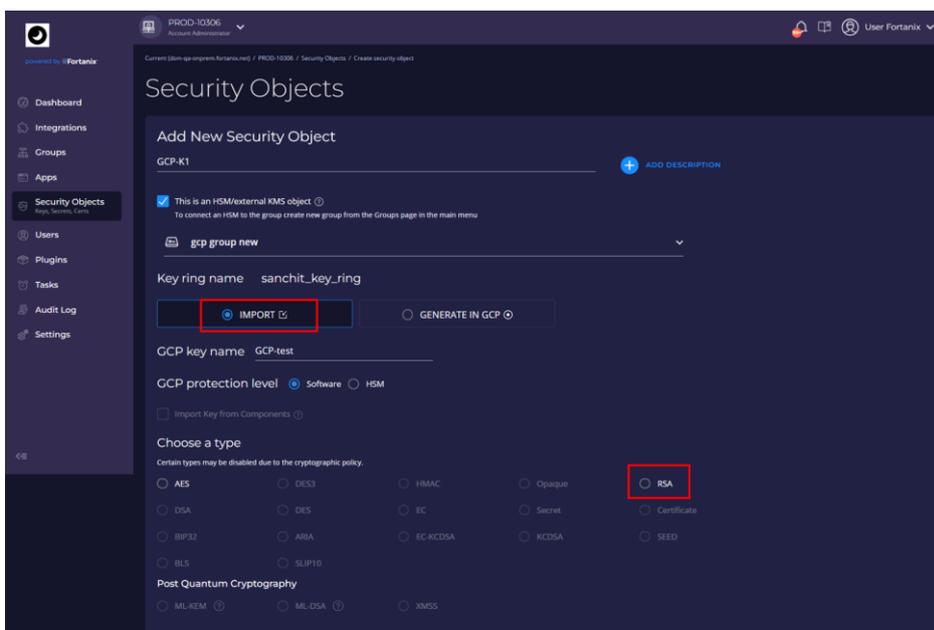
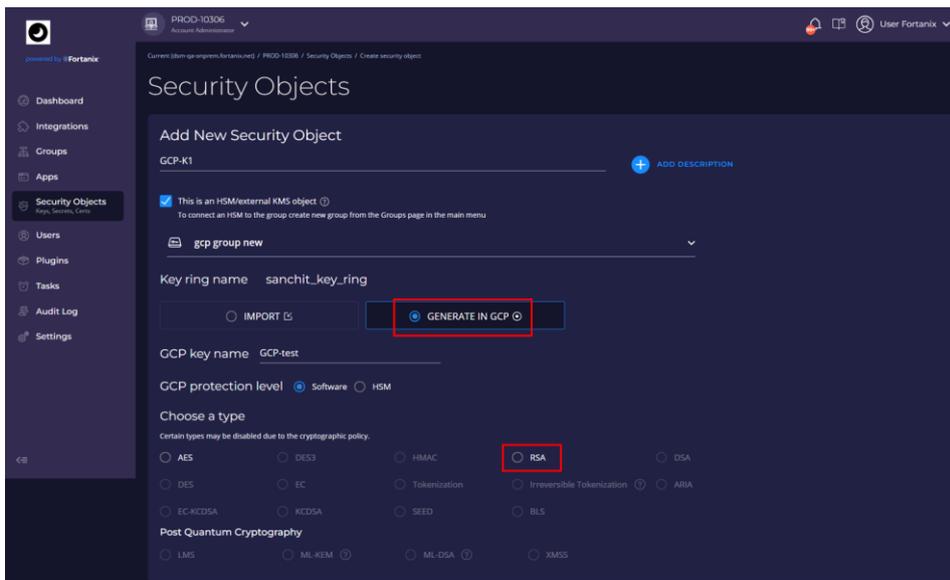
RELEASE NOTES

Date: 25-Sep-25

Subject: Software changes, updates, bug fixes, and so on.

Software: Fortanix Data Security Manager

Version: 5.3



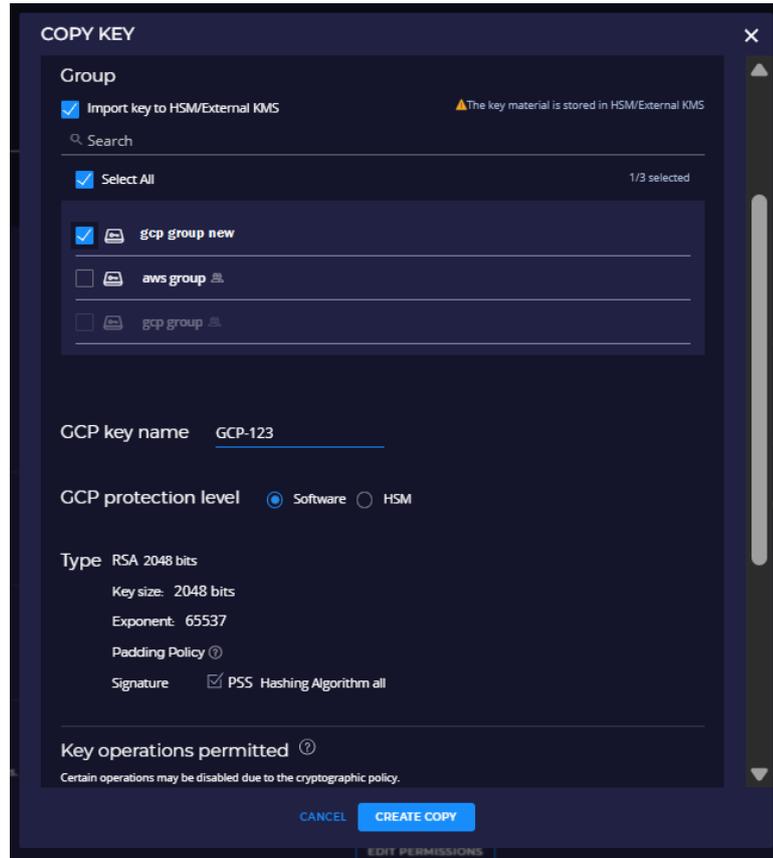
RELEASE NOTES

Date: 25-Sep-25

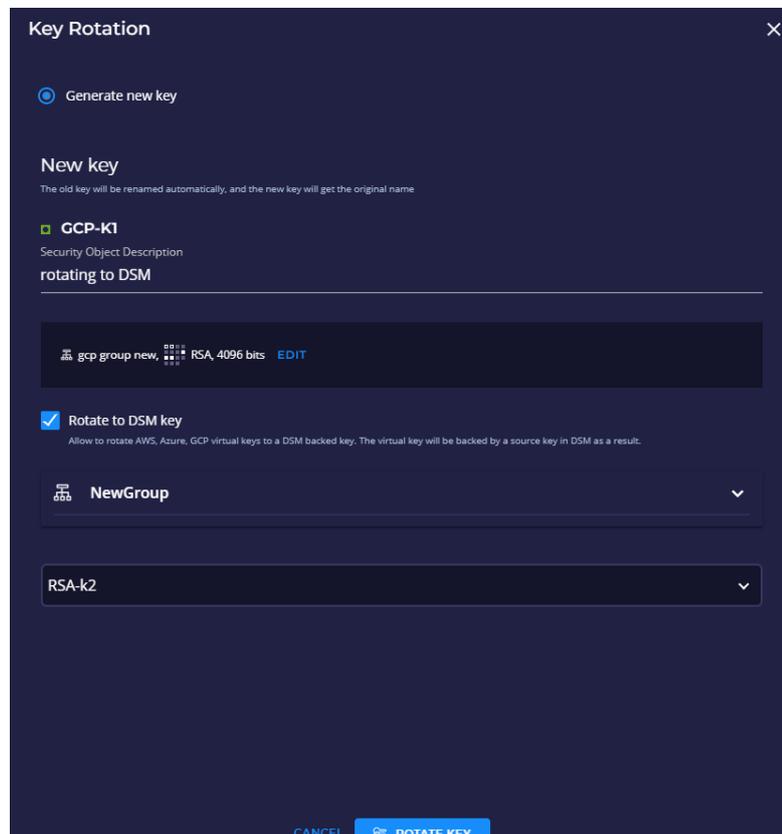
Subject: Software changes, updates, bug fixes, and so on.

Software: Fortanix Data Security Manager

Version: 5.3



- Rotate keys in GCP KMS.



RELEASE NOTES

Date: 25-Sep-25

Subject: Software changes, updates, bug fixes, and so on.

Software: Fortanix Data Security Manager

Version: 5.3

For more information, refer to the following guides:

- [Fortanix Data Security Manager GCP KMS Bring Your Own Key User Guide](#)
- [Fortanix Data Security Manager GCP KMS Cloud Native Key Management User Guide](#)
- Fortanix DSM now adds additional authentication failure logs for Key Management Interoperability Protocol (KMIP) to the system log. **(JIRA:EXTREQ-972)**.
- Added **Learn Mode** toggle in the **FILE DECRYPTION POLICY** tab of Fortanix DSM for Filesystem Encryption Windows and Linux. This feature allows temporary access to guarded paths while capturing detailed audit logs to help administrators refine security policies **(JIRA: FSE-488)**.

For more information, refer to the following guides:

- [Filesystem Encryption for Linux Using Fortanix Data Security Manager - Policies](#)
- [Filesystem Encryption for Windows as a Service Using Fortanix Data Security Manager - Policies](#)

IMPROVEMENTS

- Improved the account name visibility where the full account names are now displayed on hover, making it easier to identify and select the correct account **(JIRA: EXTREQ-1197)**.

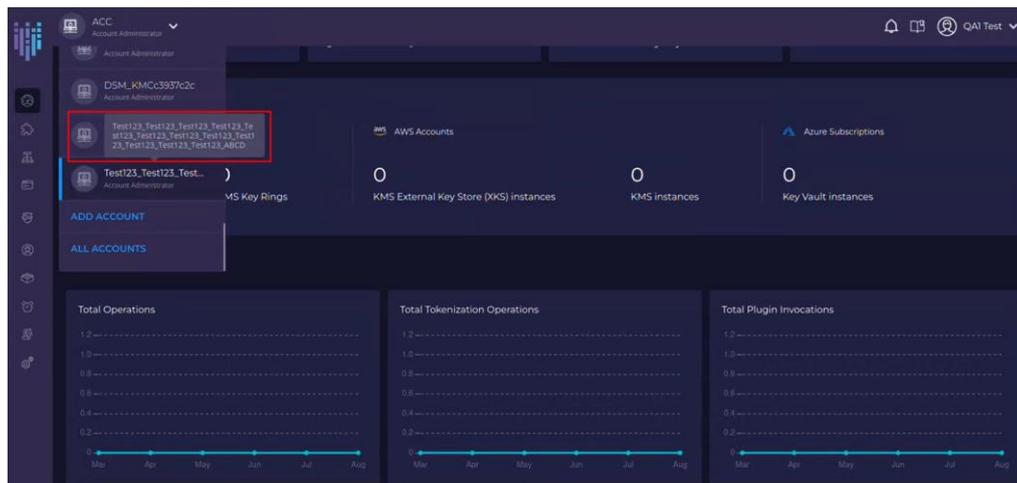
RELEASE NOTES

Date: 25-Sep-25

Subject: Software changes, updates, bug fixes, and so on.

Software: Fortanix Data Security Manager

Version: 5.3



API UPDATES

- Added support for RSA keys in Google Cloud Platform (GCP) Bring Your Own Key (BYOK), allowing you to specify the `key_protection_level` (for example, `Software` or `HSM`) as part of the key's `custom_metadata` (**JIRA: EXTREQ-1255**).
 - This enhancement applies to all APIs involving `SubjectRequest` and `SubjectResponse`, specifically for `Subjects` in Cloud Data Control (CDC) GCP-backed groups that are part of the GCP BYOK setup.
- Added support for SLIP10 hierarchical deterministic keys through `slip10` subjects in Fortanix DSM, in addition to existing BIP32 keys. You can now derive SLIP10 keys (master, hardened, and non-hardened) on NistP256 and SecP256K1 curves, and import or export them in SLIP-32 format, as well as sign and verify with them (**JIRA: EXTREQ-1463**).

This enhancement affects the following APIs:

- Derive a new key from an existing key: `POST /crypto/v1/derive`
- Transform an existing key into a new one: `POST /crypto/v1/transform`
- Sign with a private key: `POST /crypto/v1/sign`
- Verify a signature with a public key: `POST /crypto/v1/verify`

RELEASE NOTES

Date: 25-Sep-25

Subject: Software changes, updates, bug fixes, and so on.

Software: Fortanix Data Security Manager

Version: 5.3

- Get the details and value of a particular exportable security object: `POST /crypto/v1/keys/export`
- Import a security object: `PUT /crypto/v1/keys`

CLIENT IMPROVEMENTS

- Implemented an automatic retry mechanism in Sequoia DSM (**JIRA: ES-532**).
- Added support for additional Linux platforms in Sequoia DSM, including RHEL 9 and SUSE 15 (**JIRA: PROD-10574**).

DSM ACCELERATOR NEW FEATURES

- **DSM Accelerator Webservice SGX**
 - Added support for running Fortanix DSM Accelerator Webservice on Intel® Software Guard Extensions (SGX) (**JIRA: PM-16**).

For more information, refer to the following guides:

- [DSM Accelerator Webservice on SGX](#)
- [DSM Accelerator Webservice on SGX Deployment Guide](#)

KNOWN ISSUES

- Deriving SLIP10 keys fails if a Cryptographic policy is set at the Fortanix DSM account or group level. Additionally, copying SLIP10 keys is currently not supported (**JIRA: PROD-10767**).

Workaround: To derive a SLIP10 key, temporarily delete the account- or group-level Cryptographic policy, perform the key derivation, and then reapply the Cryptographic policy.

- After upgrading Fortanix DSM to version 5.0, Network Time Protocol (NTP) checks in Sensu may fail even if NTP is correctly synchronized across the cluster (**JIRA: RODE-168**).



NOTE: Use the following command to override the alert:

RELEASE NOTES

Date: 25-Sep-25

Subject: Software changes, updates, bug fixes, and so on.

Software: Fortanix Data Security Manager

Version: 5.3

```
check-ntp.rb -u ok -w ${WARN_LEVEL} -c ${CRITICAL_LEVEL}" \
```

- 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: RODE-97**).
- Deleting replica keys in groups with key history policies only results in a soft-delete of the keys (**JIRA: PROD-9925**).

RELEASE NOTES

Date: 25-Sep-25

Subject: Software changes, updates, bug fixes, and so on.

Software: Fortanix Data Security Manager

Version: 5.3

Workaround: Users should avoid deleting keys that are associated with a key-undo policy.

- The Audit Log page in Fortanix DSM does not display recent “Select Account” events when the log retention period is set to 1 day (**JIRA: PROD-10441**).

Workaround: Set the retention period to 2 days or longer under **Settings** → **LOG MANAGEMENT** → **Retention period for Audit Logs** to ensure recent audit log entries are visible.

- Unable to perform Kubernetes CA rotation successfully (**JIRA: RODE-62**).

Workaround: To perform CA rotation in DSM versions 4.36 and higher, contact the Fortanix Support team.

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

RELEASE NOTES

Date: 25-Sep-25

Subject: Software changes, updates, bug fixes, and so on.

Software: Fortanix Data Security Manager

Version: 5.3

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.

Copyright © 2025 Fortanix, Inc. All rights reserved.

Fortanix Data Security Manager Release Notes

Release 5.3