

RELEASE NOTES

Date: 31-Jan-24

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

Software: Fortanix Data Security Manager SaaS

Version: 4.25

OVERVIEW

This document provides an overview of new features, general improvements, and resolved issues in the Fortanix Data Security Manager (DSM) SaaS 4.25 release.

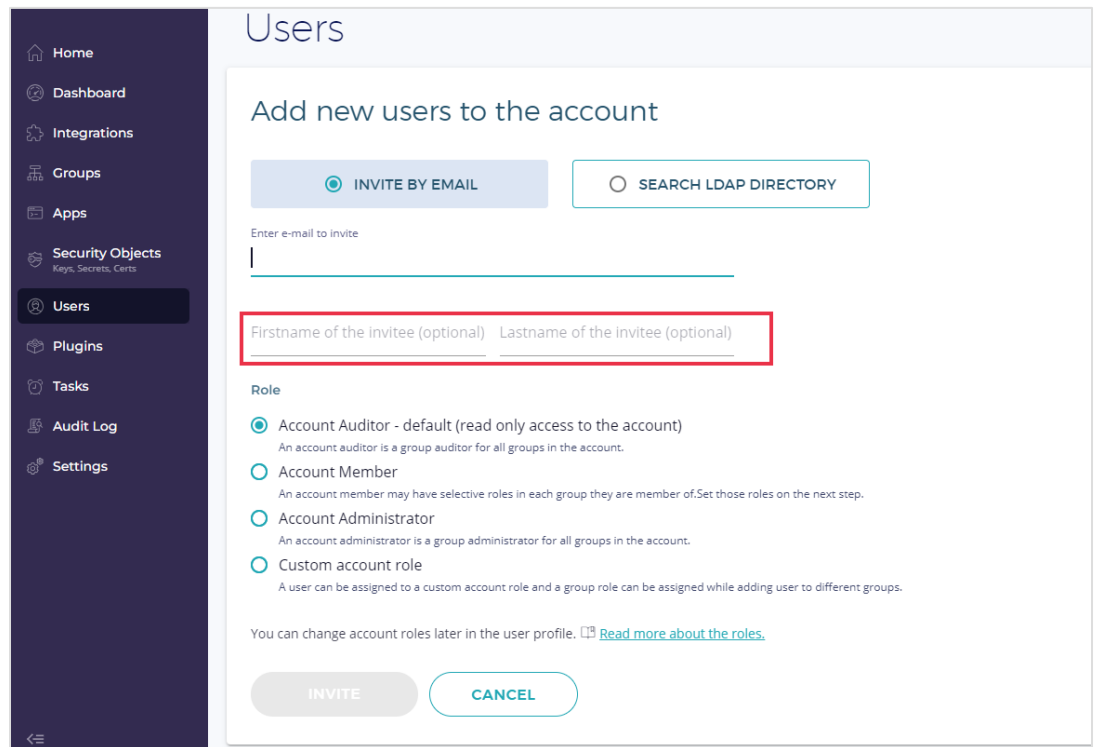


NOTE:

- 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.

ENHANCEMENTS TO EXISTING FEATURES

- Added “Firstname” and “Lastname” fields in the DSM Invite User form instead of a single “Name of the invitee” field (JIRA: ROFR-4578).



RELEASE NOTES

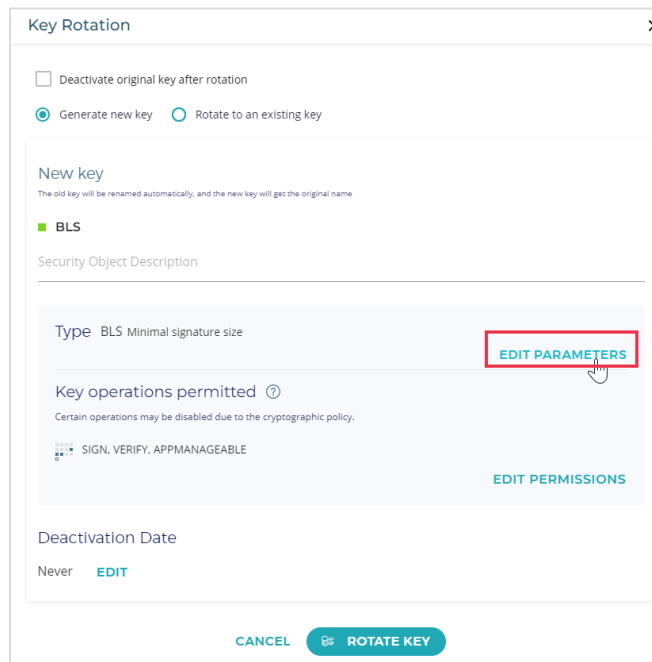
Date: 31-Jan-24

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

Software: Fortanix Data Security Manager SaaS

Version: 4.25

- The BLS key variant type can now be updated from the Fortanix DSM UI while rotating the BLS key (JIRA: ROFR-4574).



Key Rotation

☐ Deactivate original key after rotation

☒ Generate new key ☐ Rotate to an existing key

New key

The old key will be renamed automatically, and the new key will get the original name

■ BLS

Security Object Description

Type: BLS Minimal signature size [EDIT PARAMETERS](#)

Key operations permitted ⓘ

Certain operations may be disabled due to the cryptographic policy.

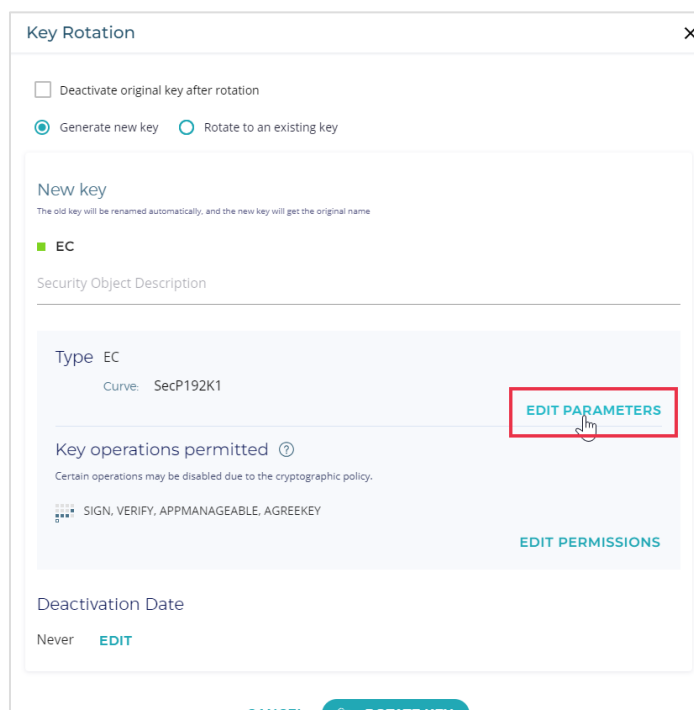
■ SIGN, VERIFY, APPMANAGEABLE [EDIT PERMISSIONS](#)

Deactivation Date

Never [EDIT](#)

[CANCEL](#) [ROTATE KEY](#)

- The EC curve can now be updated from the Fortanix DSM UI while rotating the EC-KCDSA key (JIRA: ROFR-4576).



Key Rotation

☐ Deactivate original key after rotation

☒ Generate new key ☐ Rotate to an existing key

New key

The old key will be renamed automatically, and the new key will get the original name

■ EC

Security Object Description

Type: EC

Curve: SecP192K1 [EDIT PARAMETERS](#)

Key operations permitted ⓘ

Certain operations may be disabled due to the cryptographic policy.

■ SIGN, VERIFY, APPMANAGEABLE, AGREEKEY [EDIT PERMISSIONS](#)

Deactivation Date

Never [EDIT](#)

[CANCEL](#) [ROTATE KEY](#)

RELEASE NOTES

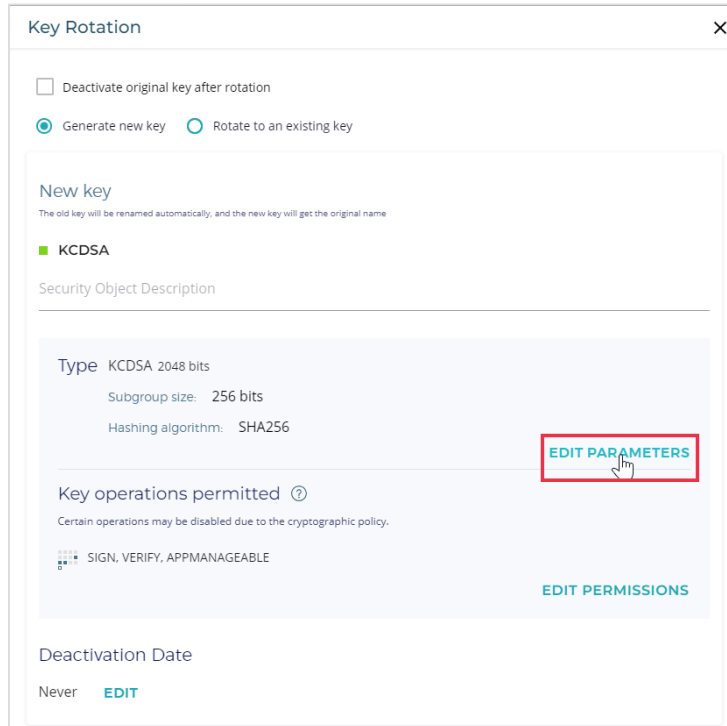
Date: 31-Jan-24

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

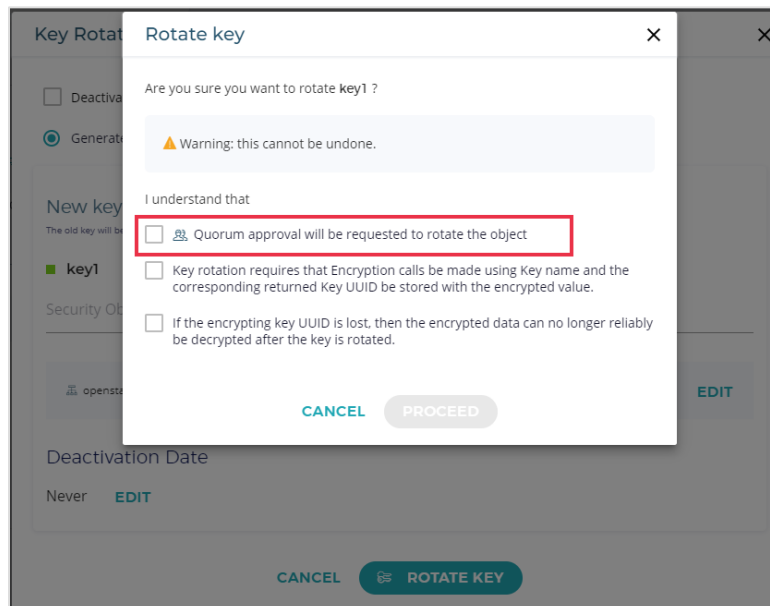
Software: Fortanix Data Security Manager SaaS

Version: 4.25

- The KCDSA subgroup size can now be updated from the Fortanix DSM UI while rotating the KCDSA key (JIRA: ROFR-4575).



- Added the “Quorum approval will be requested to rotate the object” option in the Rotate Key window (JIRA: ROFR-4518).



RELEASE NOTES

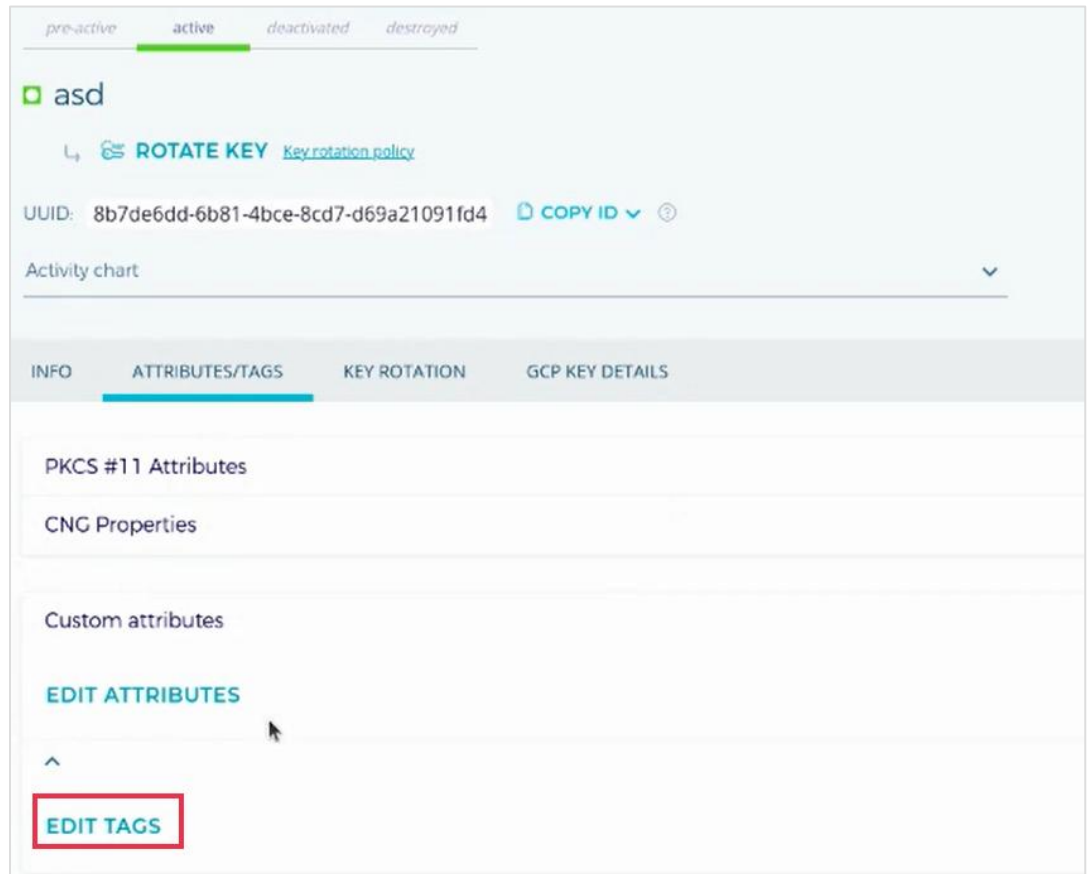
Date: 31-Jan-24

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

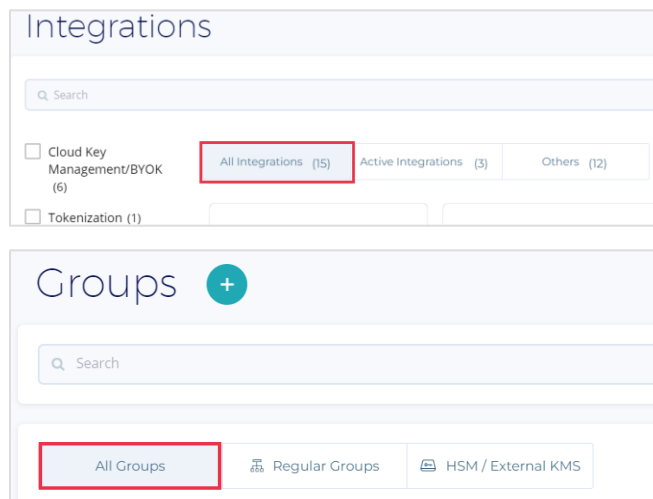
Software: Fortanix Data Security Manager SaaS

Version: 4.25

- Removed the "EDIT TAGS" option in the "ATTRIBUTES/TAGS" tab in the detailed view of a GCP BYOK key (JIRA: ROFR-4514).



- Updated the switcher component in the DSM UI to follow consistent coloring (JIRA: ROFR-4680).



RELEASE NOTES

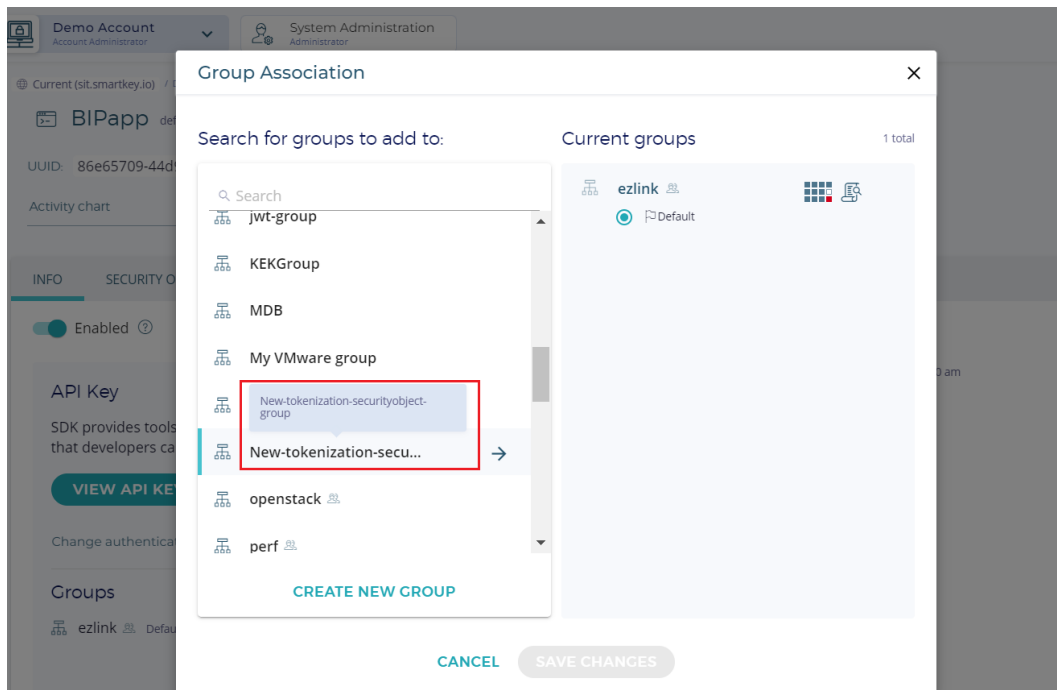
Date: 31-Jan-24

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

Software: Fortanix Data Security Manager SaaS

Version: 4.25

- Added tooltips to show the full names in multi-assigner views (JIRA: ROFR-4646).



OTHER IMPROVEMENTS

- DSM now supports TLS 1.3 protection for API clients and browser access (JIRA: PM-185).
- Added support for adding custom roles for DSM administrative applications using the API (JIRA: PM-100).
- De-duplicated the error messages returned from the Google Workspace CSE access control check and combined the error returned for the PrivateKeySign and PrivateKeyDecrypt methods (JIRA: PROD-7902).
- The Key Check Value (KCV) now appears only for keys of type AES, DES, and DES3 (JIRA: ROFR-4616).
- API clients can now perform HMAC operations with an AES key in DSM (JIRA: PM-224).

RELEASE NOTES

Date: 31-Jan-24

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

Software: Fortanix Data Security Manager SaaS

Version: 4.25

DSM INTEGRATIONS

- **Fortanix DSM now integrates with Skyhigh Secure Web Gateway (SWG) to deliver Hardware Security Module (HSM) capabilities (JIRA: EXTREQ-485).** For more details, refer to the integration guide: [Using DSM with Skyhigh SWG](#).
- **Fortanix DSM now integrates with Veeam Backup and Replication to enable backup encryption (JIRA: EXTREQ-981).** For more details, refer to the integration guide: [Using DSM for Veeam backup encryption](#).

DSM ACCELERATOR IMPROVEMENTS

- **DSM Accelerator JCE Provider:**
 - **Added support for authenticating DSM applications with client certificates when using the DSM Accelerator unified JCE Provider (JIRA: PM-140).** For more details, refer to [Developer's DSM Accelerator JCE Provider](#).
- **DSM Accelerator Webservice:**
 - **Validated Snowflake integration with DSM Accelerator Webservice deployed in Amazon Web Service (AWS) Elastic Kubernetes Service (EKS) environment (JIRA: ROQA-4476).**

BUG FIXES

- Fixed a confusing iconography in the DSM Key Metadata Policy where the **Accept** option was showing red and the **Forbid to use** option was showing green (**JIRA: ROFR-4400**).
- Fixed an issue where the Quorum approval request was not generated when deriving a BIP32 child (**JIRA: ROFR-4630**).
- Fixed multiple issues in the Add LDAP Users flow (**JIRA: ROFR-4618**).

RELEASE NOTES

Date: 31-Jan-24

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

Software: Fortanix Data Security Manager SaaS

Version: 4.25

- Fixed an issue where the user could not sort the columns in the LDAP table containing LDAP users.
 - Fixed an issue where the placement of the **Add Users to the Account** button was changing.
 - Fixed an issue where the page limit value was changing.
 - Fixed an issue where the total number of rows was sometimes shown and sometimes not shown.
- Fixed an issue where the user was unable to paste or type the necessary key URL in step 3 of the Workspace CSE Integration workflow (**JIRA: ROFR-4614**).
- Fixed an issue where the security object deactivation date in edit mode was not displaying the old value but instead displayed the current date (**JIRA: ROFR-4610**).
- Fixed broken styling for radio buttons on **Settings** → **Authentication** → **SSO** page (**JIRA: ROFR-4601**).
- Fixed an issue where the input field for the **Max concurrent requests** option in **Account** → **Settings** → **Client Configuration** → **PKCS#11** was "X bytes" instead of "No. of connections." (**JIRA: ROFR-4857**).
- Fixed an issue where the user was able to update the padding policy of a security object during the DSM rotate key operation using the API, but the user was unable to do the same using the DSM UI (**JIRA: ROFR-4570**).
- Fixed an issue where the Fortanix DSM UI wrongly parses the padding policy response for a key (**JIRA: ROFR-4569**).
- Fixed an issue where the exponent value of RSA keys was not displayed on the key details page (**JIRA: ROFR-4562**).
- Fixed an issue where the "**Download certificate**" button on the security object details page causes issues for small screen sizes (**JIRA: ROFR-4559**).

RELEASE NOTES

Date: 31-Jan-24

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

Software: Fortanix Data Security Manager SaaS

Version: 4.25

- Fixed an issue where SSO authentication integrations were displayed as configured even if the user failed to configure them due to an error (**JIRA: ROFR-4557**).
- Fixed an issue where the user could not rotate a security object for the second time when the group had a quorum policy configured (**JIRA: ROFR-4551**).
- Fixed an issue where "Using second-factor security key is required to approve requests" is enabled by default and non-editable when configuring quorum policy for a DSM group (**JIRA: ROFR-4545**).
- Fixed an issue where, when editing the Key Rotation policy for a DSM group, the **SAVE** button at the bottom was enabled even though no edits were made (**JIRA: ROFR-4540**).
- Fixed an issue when rotating a security object in the group with a quorum policy configured does not redirect the user to the security object list page after the rotation (**JIRA: ROFR-4538**).
- Fixed a typo in the DSM LDAP configuration page (**JIRA: ROFR-4529**).
- Fixed an issue where the response body of the batch API for key rotation reported the operation as successful even though the second API failed (**JIRA: ROFR-4508**).
- Fixed an issue where, after publishing the public key using the "**Public key published**" toggle in the detailed view of a DSA, EC-KCDSA, and KCDSA keys, the **URL of the API endpoint** value is not displayed (**JIRA: ROFR-4710**).
- Fixed an issue where adding SAML integration in the DSM **Account Settings** → **AUTHENTICATION** → **SINGLE SIGN-ON** results in an error (**JIRA: ROFR-4707**).
- Fixed a page issue when adding groups on the Fortanix DSM Groups page (**JIRA: ROFR-4693**).

RELEASE NOTES

Date: 31-Jan-24

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

Software: Fortanix Data Security Manager SaaS

Version: 4.25

- Fixed an issue where the **SAVE CHANGES** button was enabled when adding an app from the detailed view of a DSM group even though no changes were added (**JIRA: ROFR-4692**).
- Fixed an issue where the **LOG IN** button changes color even when in a disabled state (**JIRA: ROFR-4659**).
- Fixed an issue where even though the user failed to save tags when creating an AWS key using the HSM/External KMS workflow in DSM, the key was successfully created (**JIRA: PROD-7932**).
- Fixed an issue where the Fortanix DSM UI does not give an option for deleting key material and reimporting the key material for the imported BYOK keys (**JIRA: ROFR-4656**).
- Fixed non-functional vertical scroll bar in all DSM UI pages (**JIRA: ROFR-4643**).

KNOWN ISSUES

- 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**).
- Rotating a GCP BYOK key to a pre-existing Fortanix DSM-hosted key (**Rotate to DSM key**) is not supported (**JIRA: PROD-6722**).

Workaround: You can manually copy an existing AES 256 key from a normal DSM group to a GCP-backed group. This key automatically becomes the currently active crypto key version in the GCP key ring.

RELEASE NOTES

Date: 31-Jan-24

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

Software: Fortanix Data Security Manager SaaS

Version: 4.25

- The “Rotate linked key” feature fails with an error for keys in an externally backed group where the external entity is a Google Cloud Platform key ring (**JIRA: PROD-6828**).
Workaround: You must first manually rotate the source key in the regular DSM group and then copy the rotated key to the GCP group.
- 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**).
- The retry mechanism does not work as expected in the DSM Accelerator Webservice (**JIRA: PROD-7068**).
- 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.

RELEASE NOTES

Date: 31-Jan-24

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

Software: Fortanix Data Security Manager SaaS

Version: 4.25

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.

Copyright © 2023 Fortanix, Inc. All rights reserved.
Fortanix Data Security Manager SaaS Release Notes
Release 4.25