

## RELEASE NOTES

**Date:** 1-Sep-23

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

**Software:** Fortanix Data Security Manager SaaS

**Version:** 4.21

## OVERVIEW

This document provides an overview of new features, general improvements, and resolved issues in the Fortanix Data Security Manager (DSM) SaaS 4.21 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

1. **The Fortanix DSM SaaS cluster now issues key attestation statements that attest that a security object was generated in Fortanix Data Security Manager (DSM) and is not exportable (JIRA: PM-119).** *For more details, refer to the [Fortanix DSM – Issuing Key Attestation Statements guide](#).*
2. **Added support for certificate-based authentication for Azure Key Vault external KMS (JIRA: PM-4).**

You can now authenticate Azure Key Vault (AKV) Bring Your Own Key (BYOK) connections using a client certificate and private key to sign authentication tokens instead of a client secret. In addition, you can still use a client certificate and key for TLS connection authentication.

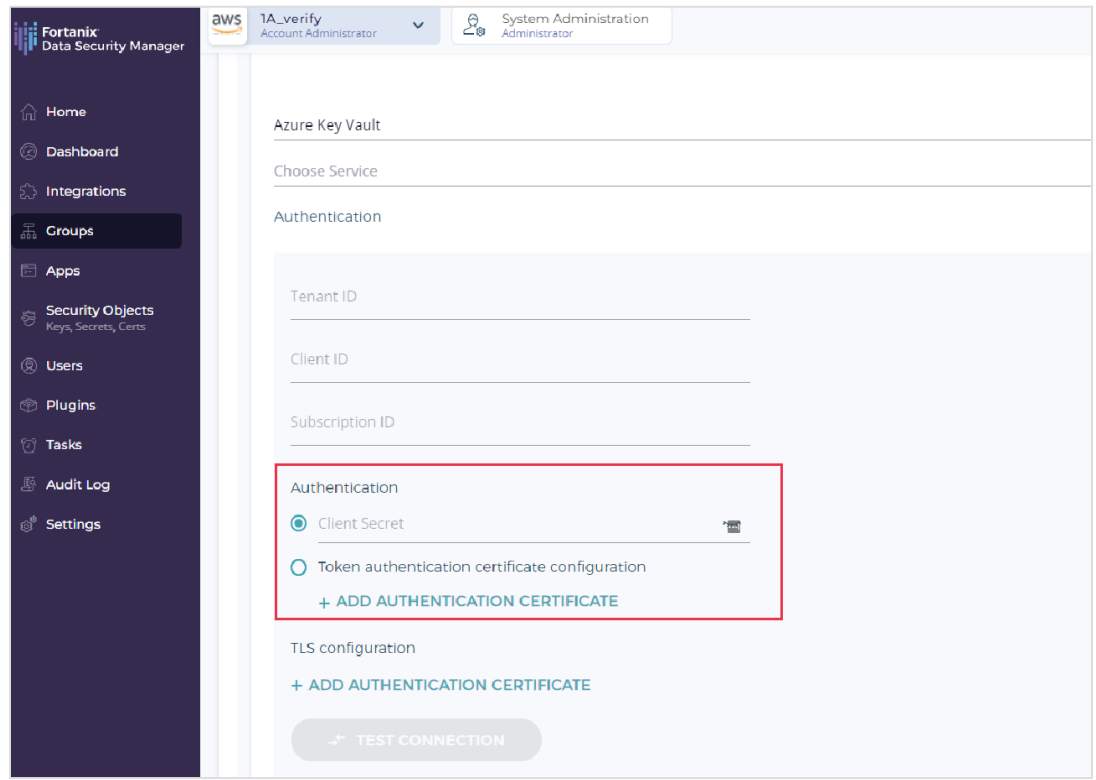
## RELEASE NOTES

**Date:** 1-Sep-23

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

**Software:** Fortanix Data Security Manager SaaS

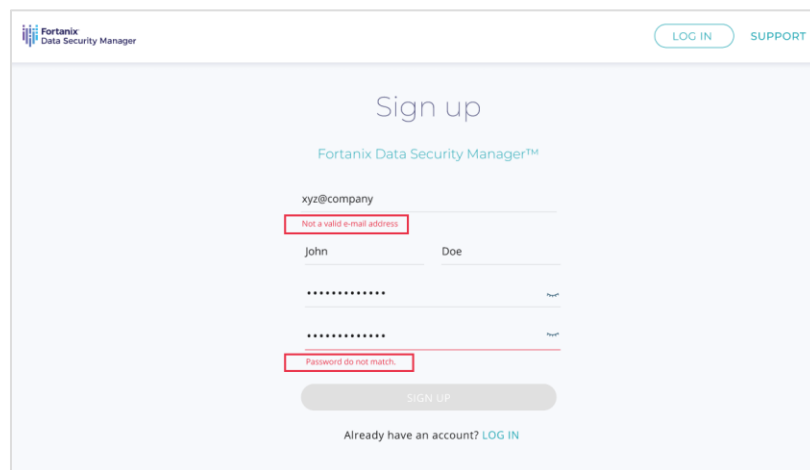
**Version:** 4.21



For more details, refer to [User's Guide: Azure Key Vault CDC Group Setup](#).

### 3. Improved the DSM SaaS sign-up flow validation (JIRA: ROFR-4106).

- Improved the message for incorrect user email format.
- Improved the message for password mismatch.



## RELEASE NOTES

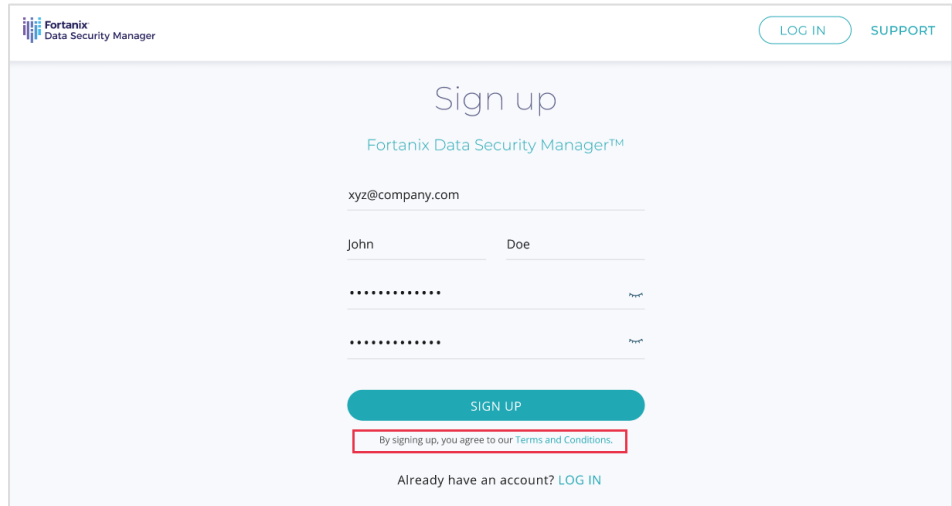
**Date:** 1-Sep-23

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

**Software:** Fortanix Data Security Manager SaaS

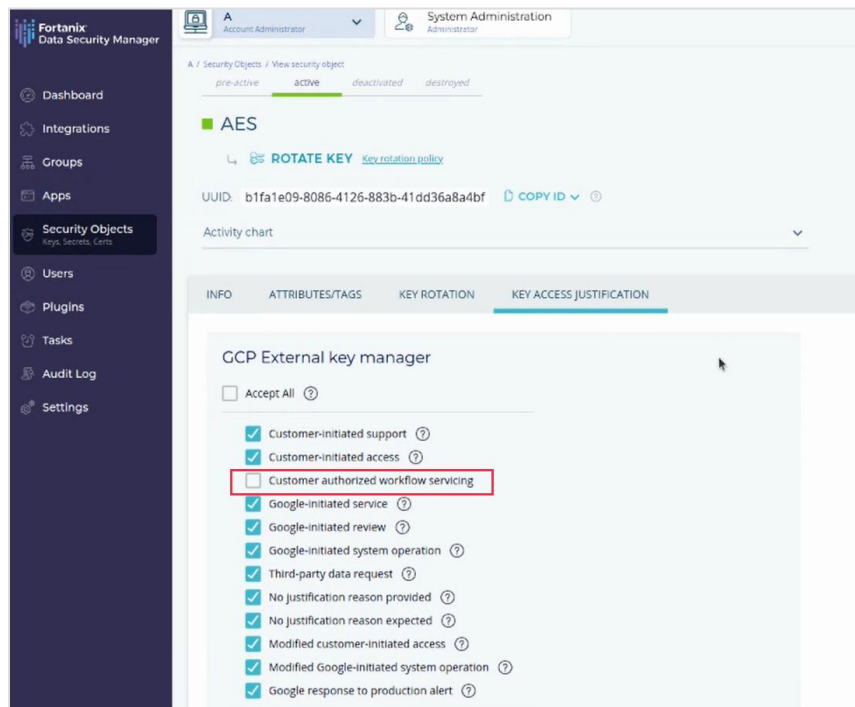
**Version:** 4.21

- Converted the Terms and Conditions check box to a message format.



## 4. Added new Google- Key Access Justification (KAJ) reason for Workflow Servicing in Fortanix DSM app creation workflow (JIRA: ROFR-4103).

The Fortanix DSM app of type **Google Service Account** now has a new KAJ reason - **CUSTOMER\_AUTHORIZED\_WORKFLOW\_SERVICING**.



## RELEASE NOTES

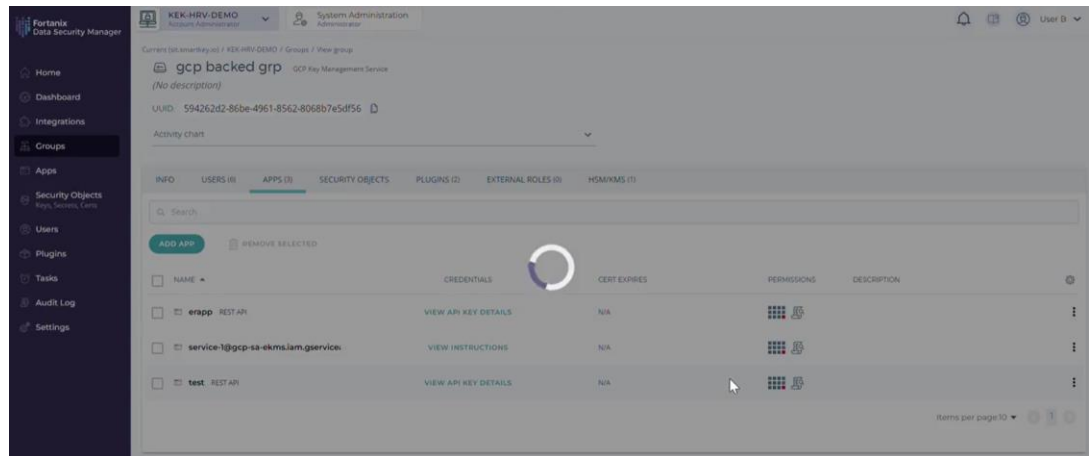
**Date:** 1-Sep-23

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

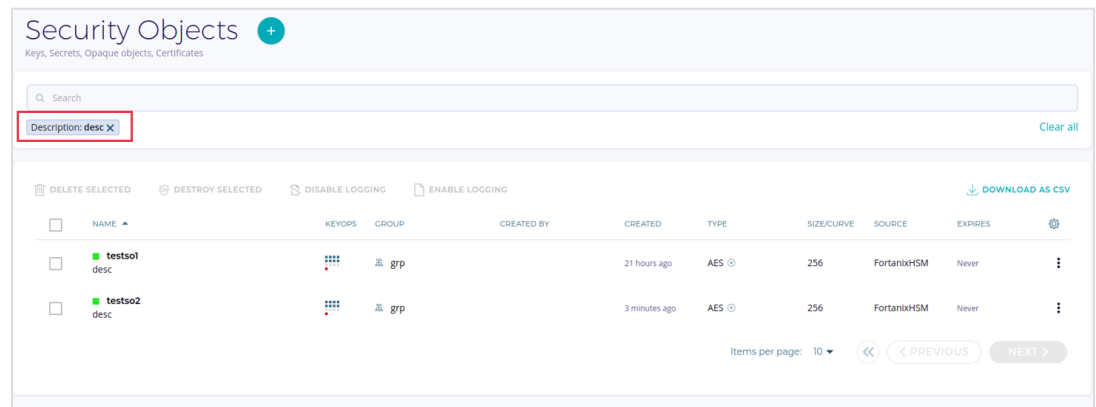
**Software:** Fortanix Data Security Manager SaaS

**Version:** 4.21

- The modal window for VIEW API KEY DETAILS for an app now shows a loading state while the data for the app is being fetched (JIRA: ROFR-4320).



- You can now filter security objects with “Description” in the table view (JIRA: ROFR-4239).



- Implemented Generic Batch API for quorum approval requests while performing rotate linked key operation for a security object in the UI (JIRA: ROFR-4255).

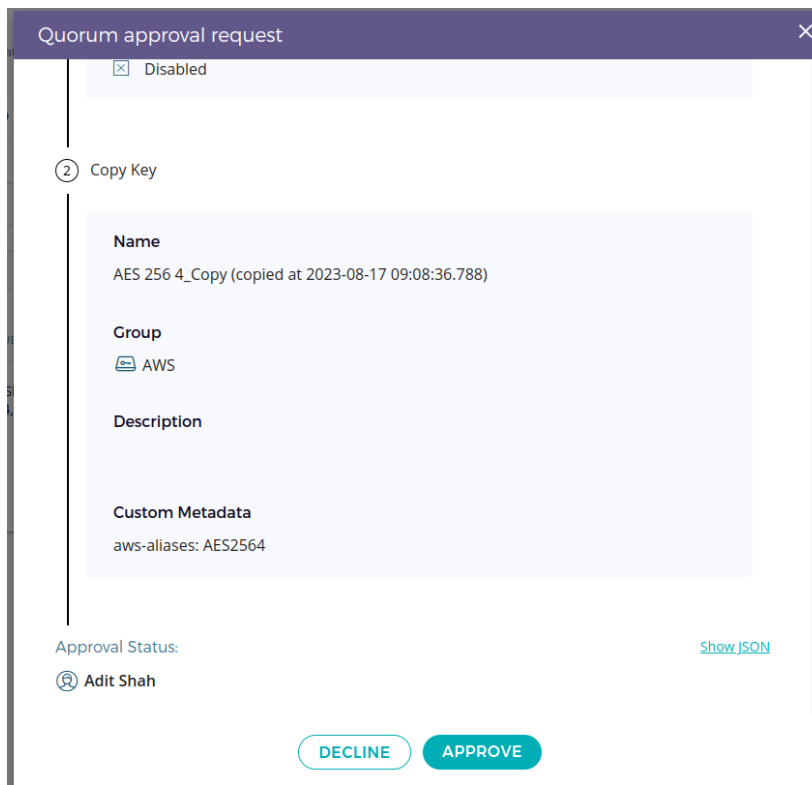
## RELEASE NOTES

**Date:** 1-Sep-23

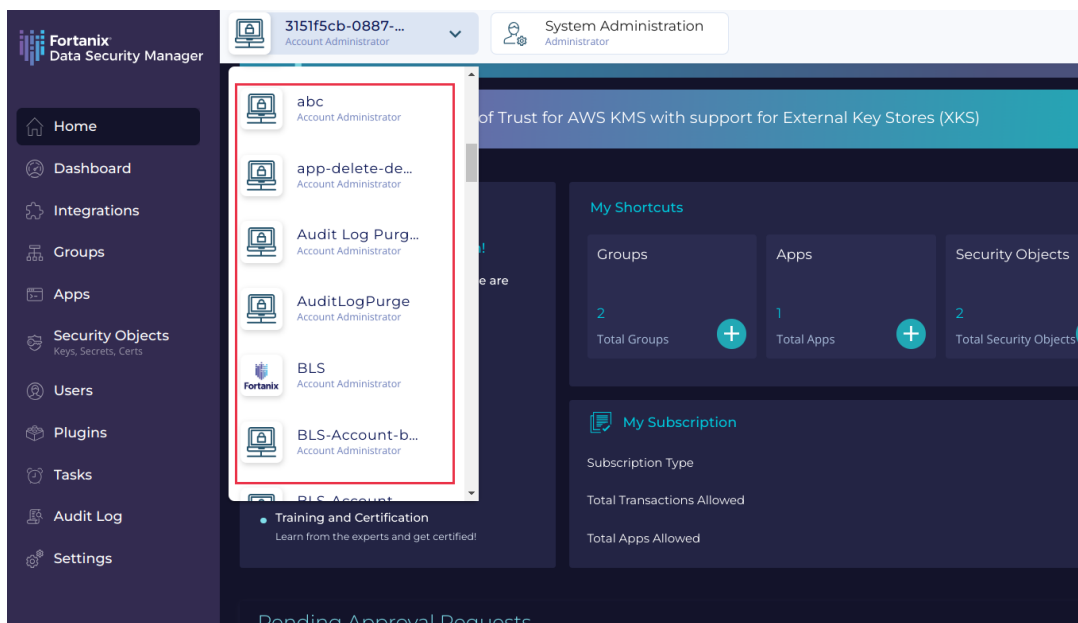
**Subject:** Software changes, updates, bug fixes, etc.

**Software:** Fortanix Data Security Manager SaaS

**Version:** 4.21



8. The DSM account names under the “Accounts” drop down in the DSM UI top pane now shows a loading indicator until all the accounts are loaded (JIRA: ROFR-4119).



## RELEASE NOTES

**Date:** 1-Sep-23

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

**Software:** Fortanix Data Security Manager SaaS

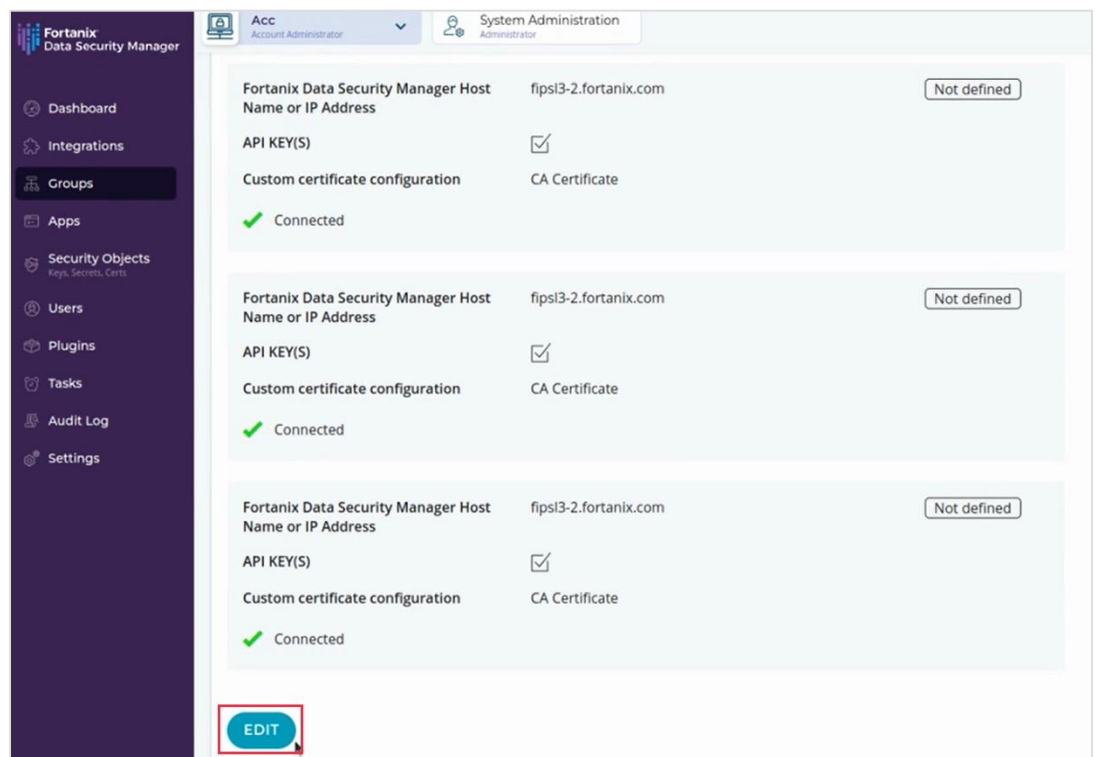
**Version:** 4.21

### 9. Improvements to the Google Workspace CSE easy wizard implementation (JIRA: ROFR-4322).

In the section for “**Document Encryption**”:

- When the user selects “**Use single key to encrypt all Google Workspace documents**”, an additional item called `encryption_type` with value `single_key` is created with `custom_metadata` with value `__dsm_google_cse_single_key` for the security object `google_cse`. This will ensure the correct `kid` is picked for the security object.
- When the user selects “**Automatically create a new key for each document**”, an additional item called `encryption_type` with value `new_key` is created.

### 10. Added view and edit modes for the “HSM/KMS” tab in the detailed view of an external KMS group (JIRA: ROFR-3821).



## RELEASE NOTES

**Date:** 1-Sep-23

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

**Software:** Fortanix Data Security Manager SaaS

**Version:** 4.21

## OTHER IMPROVEMENTS

- If a user does not have the `GET_ADMIN_APPS` permission, then they will be unable to fetch the admin apps (JIRA: ROFR-3925).
- Improved the LMS key sizes by implementing speed or memory tradeoffs (JIRA: PROD-5961)
- Upgraded the generator for OpenAPI to version 3.1 (JIRA: PROD-6905).

## INTEGRATIONS/USE CASES

- Added support for Fortanix DSM integration with IDcentral key management (JIRA: IX-46). For more details, refer to [DSM with IDcentral key management integration guide](#).
- The DSM PKCS#11 library now integrates with Docker Notary (JIRA: PROD-6517). For more details, refer to [Fortanix DSM with Docker Notary for PKCS#11 guide](#).

## CLIENT IMPROVEMENTS

- Added support for tokenization key generation in the DSM JCE Provider and Java SDK (JIRA: PROD-7001).
- Consolidated the DSM Java SDK and JCE provider and published API documentation for consolidated DSM Java client (JCE and Java SDK) (JIRA: PM-70).

## DSM-ACCELERATOR IMPROVEMENTS

- **DSM-Accelerator JCE Provider:**
  - Added support for encrypt operation using a key name for DSM-Accelerator JCE Provider (JIRA: PROD-7178).
  - Added support for tokenization key generation in the DSM-Accelerator JCE Provider (JIRA: PROD-7064).

## RELEASE NOTES

**Date:** 1-Sep-23

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

**Software:** Fortanix Data Security Manager SaaS

**Version:** 4.21

- Consolidated the DSM-Accelerator JCE provider and Java SDK and published API documentation for consolidated DSM Java client (JCE and Java SDK) (**JIRA: PM-70**).

For more details, refer to [Developer's Guide: DSM-Accelerator JCE Provider](#) and [DSM-Accelerator JCE Download](#).

- **DSM-Accelerator Webservice:**

- Added support for encrypt operation using a key name for DSM-Accelerator Webservice (**JIRA: PROD-7192**).

For more details, refer to [Developer's Guide: DSM-Accelerator Webservice](#).

## BUG FIXES

- Fixed an issue where the user was unable to copy an LMS security object (**JIRA: PROD-7336**).
- Fixed an issue where the “**Client Secret**” value was visible after editing from the detailed view of an Azure Key Vault or Azure Managed HSM group (**JIRA: ROFR-4337**).
- Fixed an issue where the “**AWS\_SECRET\_ACCESS\_KEY**” value was visible after editing from the detailed view of an AWS External KMS group (**JIRA: ROFR-4336**).
- Fixed a page crash when the user was trying to add a Custom CA certificate configuration when creating an External HSM/KMS group (**JIRA: ROFR-4335**).
- Fixed an issue where the current DSM account selected was not displayed as the selected account in the account drop down (**JIRA: ROFR-4329**).



## RELEASE NOTES

**Date:** 1-Sep-23

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

**Software:** Fortanix Data Security Manager SaaS

**Version:** 4.21

- Fixed an issue where the modal window for linked key rotation was not displayed when the source DSM key was rotated with the “Rotate linked key” check box selected (**JIRA: ROFR-4324**).
- Fixed an issue where the user gets logged out when invited to a non-SSO-based account when the user was not part of any other DSM account (**JIRA: ROFR-4319**).
- Fixed an issue where the DSM-Accelerator Webservice did not work as expected when a rotated key that was deactivated before `cache_ttl` expiry was still able to perform encrypt and decrypt operations after `cache_ttl` expiry (**JIRA: PROD-7241**).
- Fixed rendering issues in the security object detailed view for DSM custom tokens (**JIRA: ROFR-4313**).
- Fixed an issue where a certificate was converted to base64 format during upload (**JIRA: ROFR-4288**).
- Fixed incorrect “Last login date” in the activity log for DSM apps (**JIRA: ROFR-4275**).
- Fixed an error when a new user invited to a DSM account clicks “JOIN” to join the account (**JIRA: ROFR-4309**).
- Fixed an issue where the description for the Quorum approval task was missing for a FIPS-backed (**JIRA: ROFR-4253**).
- Fixed an issue where the user saw a "Not a HSM group" error message while deleting the HSM/KMS from a FIPS-backed group (**JIRA: ROFR-4245**).
- Fixed a missing pop-up error message when a user who does not have 2FA configured tries to log in to a DSM account with the setting “**Mandatory two-factor authentication for all team members**” (**JIRA: ROFR-4238**).
- Fixed an issue where the **SUBMIT** button was not disabled when no keys were selected or when all keys were disabled after selecting the “Rotate Linked Key” option (**JIRA: ROFR-4233**).

## RELEASE NOTES

**Date:** 1-Sep-23

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

**Software:** Fortanix Data Security Manager SaaS

**Version:** 4.21

- Fixed an issue where the DSM UI shows a success message even when the API call fails (**JIRA: ROFR-4221**).
- Fixed an issue where the search bar in the DSM **Integration** tab did not allow a case-sensitive search to be performed (**JIRA: ROFR-4219**).
- Fixed an issue where the status code for DSM-Accelerator Webservice showed 500 instead of 400 for batch sign Curve Ed25519/X25519 which is not supported (**JIRA: PROD-7007**).
- Fixed an issue where even if all the options under the **Padding policy** section were not selected it still allows the operations (**JIRA: ROFR-4206**).
- Fixed an incorrect definition for `WrappingKeyName` in the Open API version 3 specification (**JIRA: PROD-6977**).
- Fixed an incorrect definition for `TepSchemVariant` in the Open API version 3 specification (**JIRA: PROD-6901**).
- Fixed an issue where the **COPY KEY** option was not disabled for a key in a FIPS-backed group (**JIRA: ROFR-4200**).
- Fixed an issue where the check boxes in the “Regenerate API Key” form when the user clicks the **REGENERATE** button were selected by default in the detailed view of an app (**JIRA: ROFR-4195**).
- Fixed an issue where the user was unable to create a DSM group after canceling the Quorum policy creation for the group (**JIRA: ROFR-4146**).
- Fixed an issue where DSM Dashboard data did not refresh when the user clicked the Refresh icon (**JIRA: ROFR-3986**).

## KNOWN ISSUES

- The DSM login page is shown briefly after performing an SSO login (**JIRA: ROFR-4148**).
- 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

## RELEASE NOTES

**Date:** 1-Sep-23

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

**Software:** Fortanix Data Security Manager SaaS

**Version:** 4.21

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.

- 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.

- Increasing the “**Retention period for Audit Logs**” setting at the account level duplicates the “purge audit log” message in the audit logs (**JIRA: PROD-7031**).

- 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**).

## RELEASE NOTES

**Date:** 1-Sep-23

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

**Software:** Fortanix Data Security Manager SaaS

**Version:** 4.21

- When a key is soft-deleted from the DSM Azure Key Vault Cloud Data Control (CDC) group, the “Purge deleted key” button is not visible in the UI (**JIRA: PROD-7202**).
- Error during DSM login in a new or existing cluster (**JIRA: ROFR-4370**).  
**Workaround:** In the browser developer tools, clear the **auth.accountId** field from Local storage.
- After logging in to Fortanix DSM, you will see an additional region mentioned in the DSM UI breadcrumbs navigation (**JIRA: ROFR-4390**).

## 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](mailto:support@fortanix.com)

## DISCLAIMERS

## RELEASE NOTES

**Date:** 1-Sep-23

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

**Software:** Fortanix Data Security Manager SaaS

**Version:** 4.21

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 4.21