

RELEASE NOTES

Date: 10-Oct-23

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

Software: Fortanix Data Security Manager SaaS

Version: 4.22

OVERVIEW

This document provides an overview of new features, general improvements, and resolved issues in the Fortanix Data Security Manager (DSM) SaaS 4.22 release.

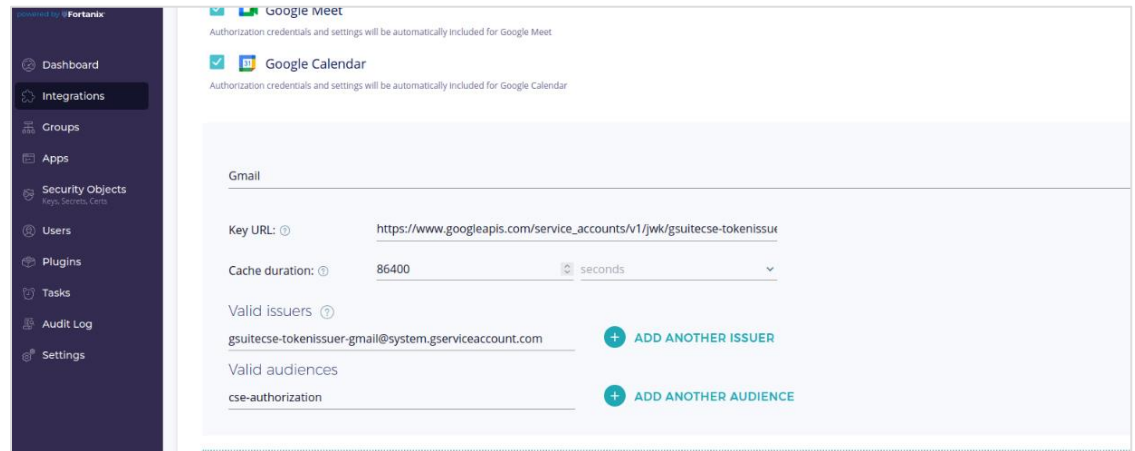


NOTE:

- 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

1. As the Security Administrator of an organization that uses Google Workspace, you can now use Google Workspace CSE to wrap Private Keys and Certificates, so that the Workspace CSE users can encrypt and sign messages in Gmail (**JIRA: PM-43**).



For more details, refer to the [Using Fortanix DSM for Google Workspace Client-Side Encryption](#).

RELEASE NOTES

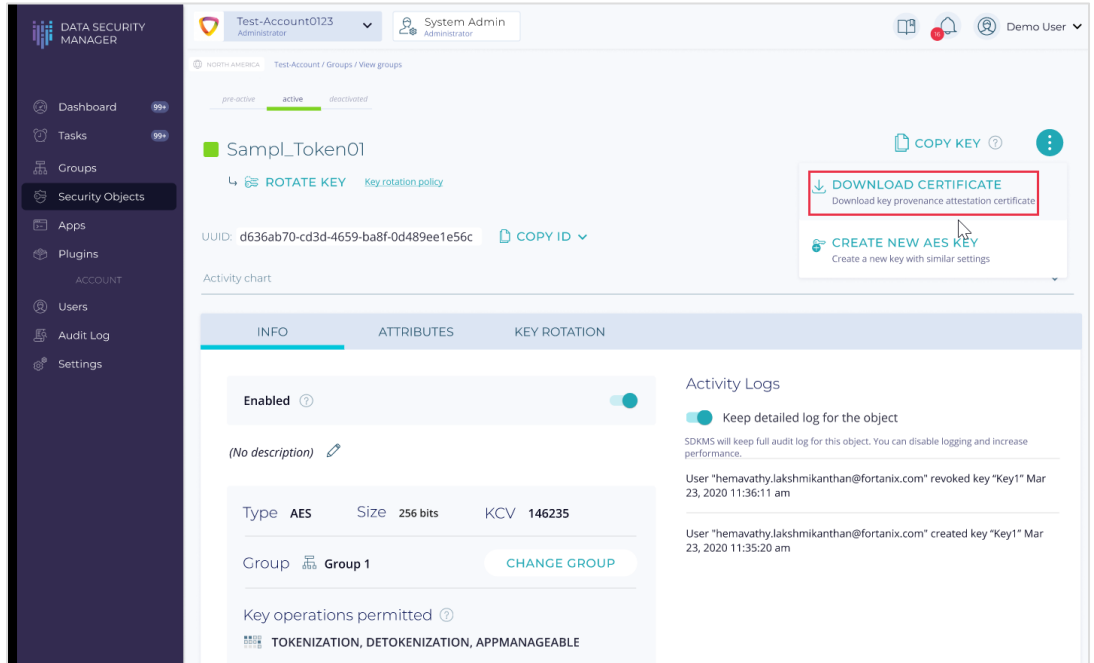
Date: 10-Oct-23

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

Software: Fortanix Data Security Manager SaaS

Version: 4.22

2. Provided download capability for the Key Attestation Statement when a key was generated in DSM and the Key Attestation Certificate was available (JIRA: ROFR-3973).



For more details, refer to the [Fortanix DSM – Issuing Key Attestation Statements guide](#).

3. Added new fine-grained “Manage” permissions for the Fortanix DSM app (JIRA: ROFR-4240).

For more details, refer to [User's Guide: Security Controls for Fortanix Data Security Manager Applications](#).

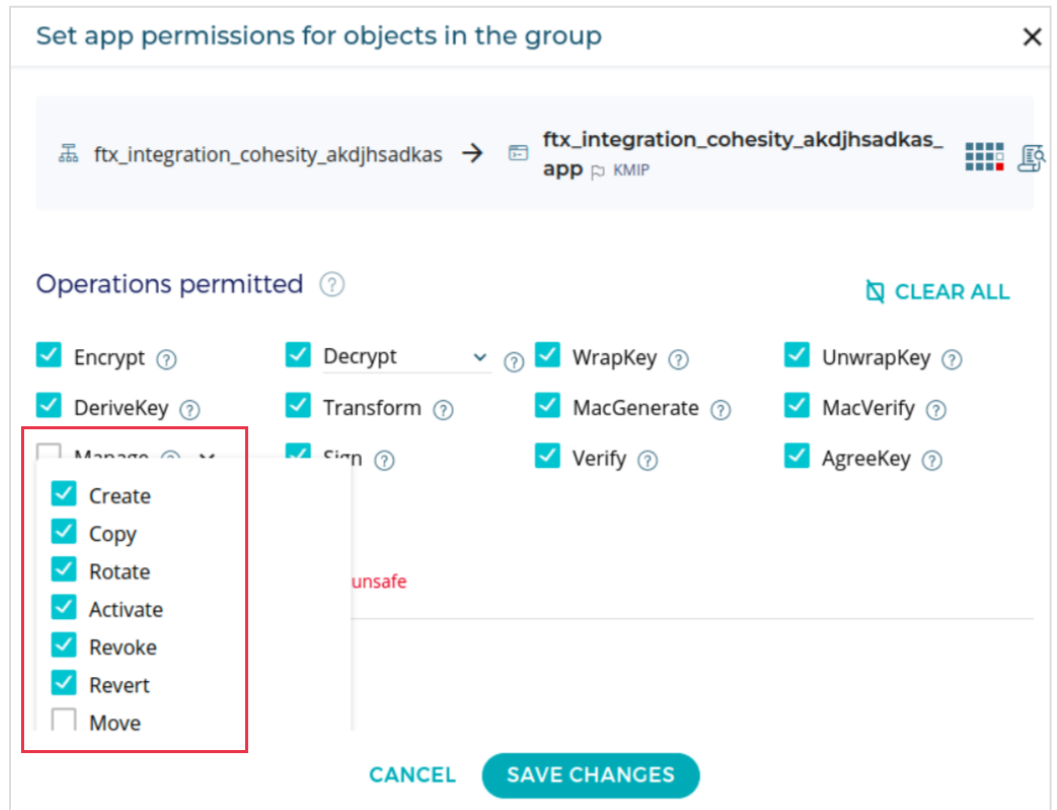
RELEASE NOTES

Date: 10-Oct-23

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

Software: Fortanix Data Security Manager SaaS

Version: 4.22



ENHANCEMENTS TO EXISTING FEATURES

- Added support to restrict the domains that are allowed to use cross-origin MFA iframe/popup (JIRA: ROFR-4339).
- Added a description for the option "Logging invalid API requests" in the DSM Account Settings → Log Management to indicate that enabling this setting may leak sensitive information from the API request into the audit logs (JIRA: ROFR-4327).
- Added support to edit a DSM user's description (JIRA: ROFR-4310).
- Added support to add/edit Key Access Justification policies for a DSM group (JIRA: ROFR-4249).

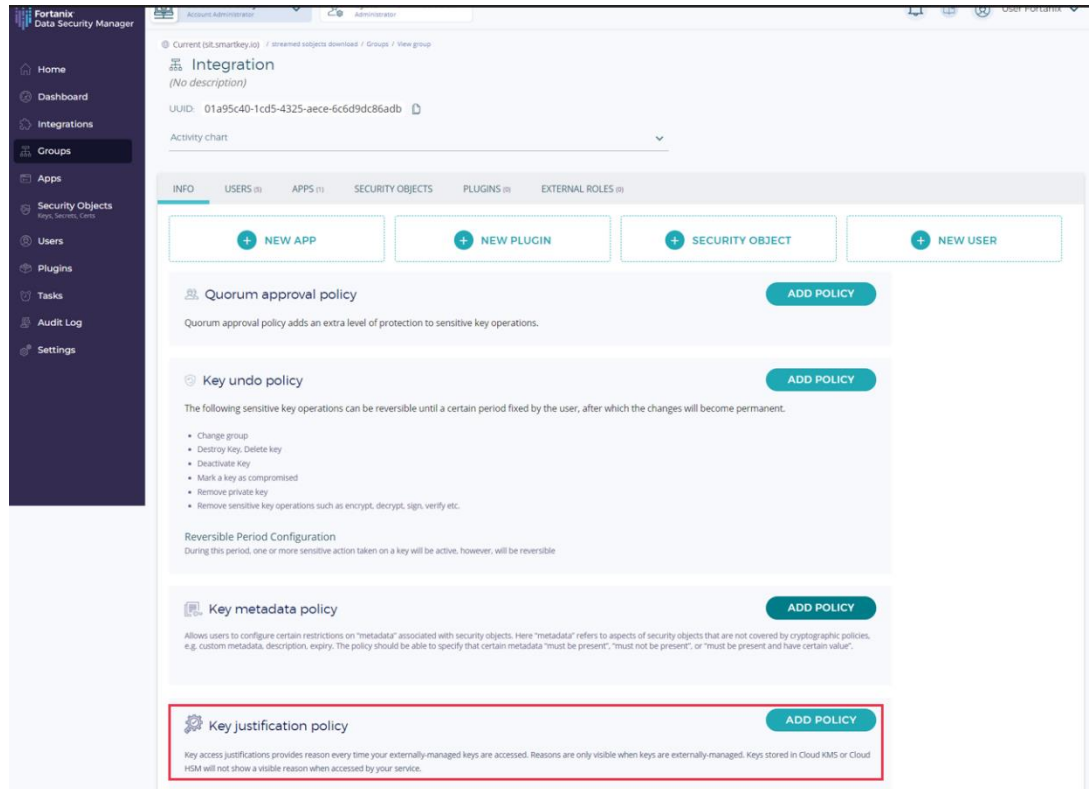
RELEASE NOTES

Date: 10-Oct-23

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

Software: Fortanix Data Security Manager SaaS

Version: 4.22



CLIENT IMPROVEMENTS

- **Migrated the Swagger Java SDK from `javax` binding to `jakarta` binding (JIRA: PROD-7306).**
- **Implemented TLS and UI cert key rotation in Fortanix DSM CLI (JIRA: PM-135)**

DSM-ACCELERATOR IMPROVEMENTS

- **DSM-Accelerator Webservice:**
 - Added support for using key name in DSM-Accelerator Webservice for the cryptographic operations decrypt, sign, verify, batch sign, and batch verify (**JIRA: PROD-7176**). *For more details, refer to [Developer's Guide: DSM-Accelerator Webservice](#)*

RELEASE NOTES

Date: 10-Oct-23

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

Software: Fortanix Data Security Manager SaaS

Version: 4.22

- Added support for AWS Lambda Serverless deployment for DSM-Accelerator Webservice (**JIRA: PM-22**). For more details, refer to [Deploying DSM-Accelerator Webservice on AWS Lambda](#).

INTEGRATIONS/USE CASES

- **Added support for Fortanix DSM integration with Delinea Secret Server (JIRA: IX-36)**. For more details, refer to [DSM with Delinea Secret Server](#).

BUG FIXES

- Fixed a page crash while enabling the **OAuth** option for DSM apps (**JIRA: ROFR-4439**).
- Fixed an issue in LMS where, when creating a key with different heights, it still freezes to l1=5 and l2=10 heights (**JIRA: ROFR-4427**).
- Fixed a page crash when adding a Key Metadata policy in a Fortanix DSM group (**JIRA: ROFR-4416**).
- Fixed an issue when clicking on "**Authorization enabled**" toggle results in "Oops!" Page error in the DSM **Account Settings** → **Authentication** → **Single Sign-On** → **LDAP** configuration (**JIRA: ROFR-4412**).
- Fixed a null pointer exception in the DSM-Accelerator JCE SDK when creating a tokenization security object (**JIRA: PROD-7481**).
- Fixed an issue where, after logging in to Fortanix DSM, an additional region was mentioned in the DSM UI breadcrumbs navigation (**JIRA: ROFR-4390**).
- Fixed DSM login error, on a new or existing cluster (**JIRA: ROFR-4370**).
- Fixed an issue where the **Assign** role was not set even after adding/ or updating the **Assign** role in the DSM **Account Settings** → **Authentication** → **Single Sign-On** → **LDAP** configuration (**JIRA: ROFR-4367**).

RELEASE NOTES

Date: 10-Oct-23

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

Software: Fortanix Data Security Manager SaaS

Version: 4.22

- Fixed an issue where the type of authentication was missing in the detailed view of AWS or Azure Key Vault backed group with Certificate-based authentication (**JIRA: ROFR-4365**).
- Fixed an issue in the Azure Managed HSM backed group where the test connection operation failed (**JIRA: ROFR-4362**).
- Fixed an issue in an Azure Key Vault backed group where the Client Secret value overlaps with the Authentication parameter (**JIRA: ROFR-4361**).
- Fixed an issue where a user could create an Azure Backed group without selecting the service (**JIRA: ROFR-4358**).
- Fixed an issue where creating and assigning a new group in the Fortanix DSM app detailed view page does not show any notification in the UI about the update (**JIRA: ROFR-4352**).
- Fixed an issue where the user was unable to import a SECRET key in a group with the Key Metadata policy configured (**JIRA: ROFR-4342**).
- Fixed an issue where, while creating a security object using Admin Apps, the app name was not visible in the '**Created by**' column in the security object list view (**JIRA: ROFR-4338**).
- Fixed an issue where the flannel interface was deleted after network restart (**JIRA: DEVOPS-4195**).
- Fixed an issue with the flannel configmap that needed an update during the upgrade (**JIRA: DEVOPS-4244**).
- Fixed an issue where a DSM user gets logged out when logging in with SSO and navigating to the **Profile** page (**JIRA: ROFR-4334**).
- Fixed an issue in the DSM **Integrations** page where searching for an integration with space does not filter the correct results (**JIRA: ROFR-4333**).
- Fixed an issue where lazy loading was still seen even if the accounts count was 1 or 2 (**JIRA: ROFR-4330**).

RELEASE NOTES

Date: 10-Oct-23

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

Software: Fortanix Data Security Manager SaaS

Version: 4.22

- Fixed an issue where the **SAVE CHANGES** button was not disabled when editing or adding a new OAuth configuration in an app (**JIRA: ROFR-4301**).
- Fixed an issue where the **SAVE CHANGES** button was not greyed out when multiple nodes were added in a FIPS-backed group (**JIRA: ROFR-4300**).
- Fixed an issue where the Azure OAuth login fails for the first time and displays the login page again (**JIRA: ROFR-4298**).
- Fixed an issue where creating a new EC key does not work as expected and changes the curve type to the default value (**JIRA: ROFR-4266**).
- Fixed an issue where the key rotation operation in an external group calls the `copy` API that fails instead of calling the `approval_requests` API (**JIRA: ROFR-4343**).
- Fixed a number of issues with the “Let’s get Started!” walkthrough UI (**JIRA: ROFR-3557**).

KNOWN ISSUES

- Custom value cannot be selected from the drop down when there are more than two options in the drop down (**JIRA: ROFR-4429**).
- 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**).

RELEASE NOTES

Date: 10-Oct-23

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

Software: Fortanix Data Security Manager SaaS

Version: 4.22

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**).
- 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**).

- Page crashes when an app is created using API without the `app_type` parameter and modified from UI later (**JIRA: ROFR-4383**).

- The user gets an “OOPS” page when trying to associate an existing plugin with other DSM groups (**JIRA: ROFR-4468**).

Workaround: To associate an existing plugin to another DSM group:

1. Navigate to the **Plugins** page and open that plugin.

RELEASE NOTES

Date: 10-Oct-23

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

Software: Fortanix Data Security Manager SaaS

Version: 4.22

2. In the detailed view of the plugin, in the **INFO** tab, click the **EDIT GROUPS** button.
3. In the “Groups Association” form, add the necessary groups for the plugin and click **SAVE CHANGES** to save the changes.

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.

Copyright © 2023 Fortanix, Inc. All rights reserved.

RELEASE NOTES

Date: 10-Oct-23

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

Software: Fortanix Data Security Manager SaaS

Version: 4.22

Fortanix Data Security Manager SaaS Release Notes

Release 4.22