

## RELEASE NOTE

**Date:** 5-Jan-23

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

**Software:** Fortanix Data Security Manager

**Version:** 4.13

## OVERVIEW

This document provides an overview of new features, general enhancements, improvements, and resolved issues in the Fortanix Data Security Manager (DSM) 4.13 release.

This release is superseded by [February 15, 2023 release](#).



### WARNING:

- It is "REQUIRED" to upgrade Fortanix DSM to version 4.9 or 4.11 before upgrading to version 4.13. If you want to upgrade to 4.13 from an older version, please reach out to the Fortanix Support team.
- Once upgraded to version 4.13, Fortanix DSM can **NO LONGER** be downgraded to any prior version. This is due to limitations of common infrastructure components such as Docker and Kubernetes.



### NOTE:

- The Fortanix DSM cluster upgrade must be done with Fortanix Support on call. Please reach out to Fortanix Support if you are planning an upgrade.
- The customer's BIOS version must be checked by Fortanix Support prior to the Fortanix DSM software upgrade. If required, the BIOS version should be upgraded to the latest version and verified by Fortanix Support for a smooth upgrade.
- The Fortanix DSM Dashboard's performance is significantly improved in this release. With this improvement, the dashboard will take no more than 2-3 seconds to load the last six months of data after aggregation is complete for a specific account. However, you may observe more latency during the account aggregation, which is a one-time activity.

## RELEASE NOTE

**Date:** 5-Jan-23

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

**Software:** Fortanix Data Security Manager

**Version:** 4.13

- If your Fortanix DSM version is 4.13 or later, then the HSM gateway version must also be 4.13 or later. Similarly, if the HSM Gateway version is 4.13 or later, then your Fortanix DSM version must be 4.13 or later.

## NEW FUNCTIONALITY / FEATURES

### 1. Extended Virtual Keys – Key Caching and Automatic Key Scan (JIRA: ROFR-3462).

- **Added support to specify scheduled scans (JIRA: PROD-5544).**

This release adds support to store the cached key material of the DSM source keys in the DSM destination group using DSM-backed group configuration so that the keys are replicated across cloud and on-prem environments. This way applications can fall back to a different cluster if one is down.

- You can also perform automatic scheduled scans to scan the source group for new keys.

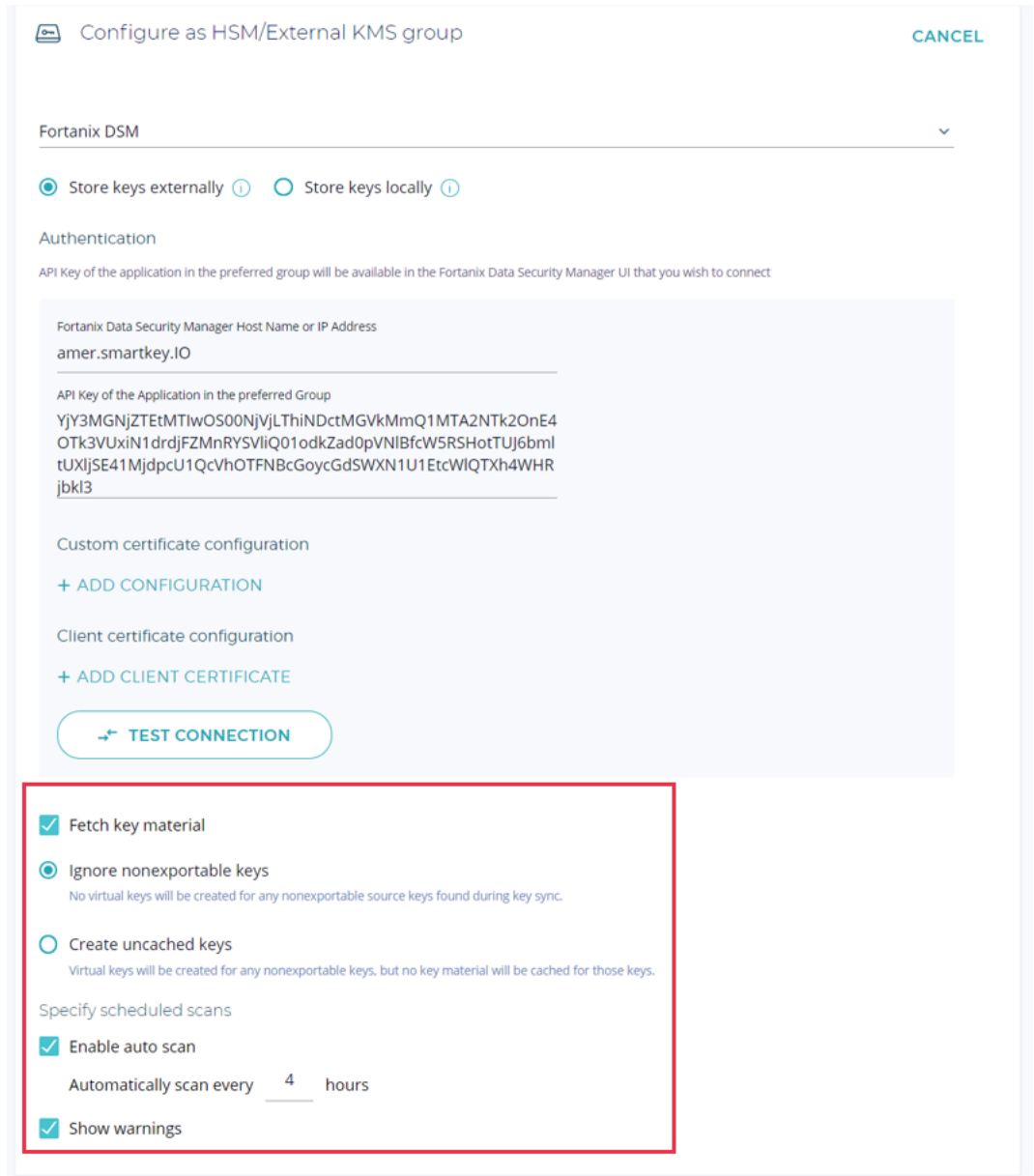
## RELEASE NOTE

**Date:** 5-Jan-23

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

**Software:** Fortanix Data Security Manager

**Version:** 4.13



Configure as HSM/External KMS group CANCEL

Fortanix DSM ▼

☒ Store keys externally ⓘ ☐ Store keys locally ⓘ

Authentication

API Key of the application in the preferred group will be available in the Fortanix Data Security Manager UI that you wish to connect

Fortanix Data Security Manager Host Name or IP Address  
amer.smartkey.io

API Key of the Application in the preferred Group  
YjY3MGNjZTETMTIwOS00NjVjLThtNDctMGVhMmQ1MTA2NTk2OnE4OTk3VUxiN1drdJFZMnRYSVliQ01odkZad0pVNIBfcW5RSHotTUIj6bmltUXIjSE41MjdpcU1QcVhOTFNbcGoycGdSWXN1U1EtcWIQTxh4WHRjbkl3

Custom certificate configuration  
[+ ADD CONFIGURATION](#)

Client certificate configuration  
[+ ADD CLIENT CERTIFICATE](#)

[TEST CONNECTION](#)

☒ Fetch key material

☒ Ignore nonexportable keys  
No virtual keys will be created for any nonexportable source keys found during key sync.

☐ Create uncached keys  
Virtual keys will be created for any nonexportable keys, but no key material will be cached for those keys.

Specify scheduled scans

☒ Enable auto scan  
Automatically scan every  hours

☒ Show warnings

For more details, refer to [Fortanix Extended Virtual Keys Guide](#).

## 2. Added a new sub-section for “Post-Quantum Cryptography (PQC)” key types in the security object form (JIRA: ROFR-3702).

- **Support for LMS key type (JIRA: ROFR-1616).**

This release adds support for generating a new key type called LMS key that can only be used for signature generation and verification.

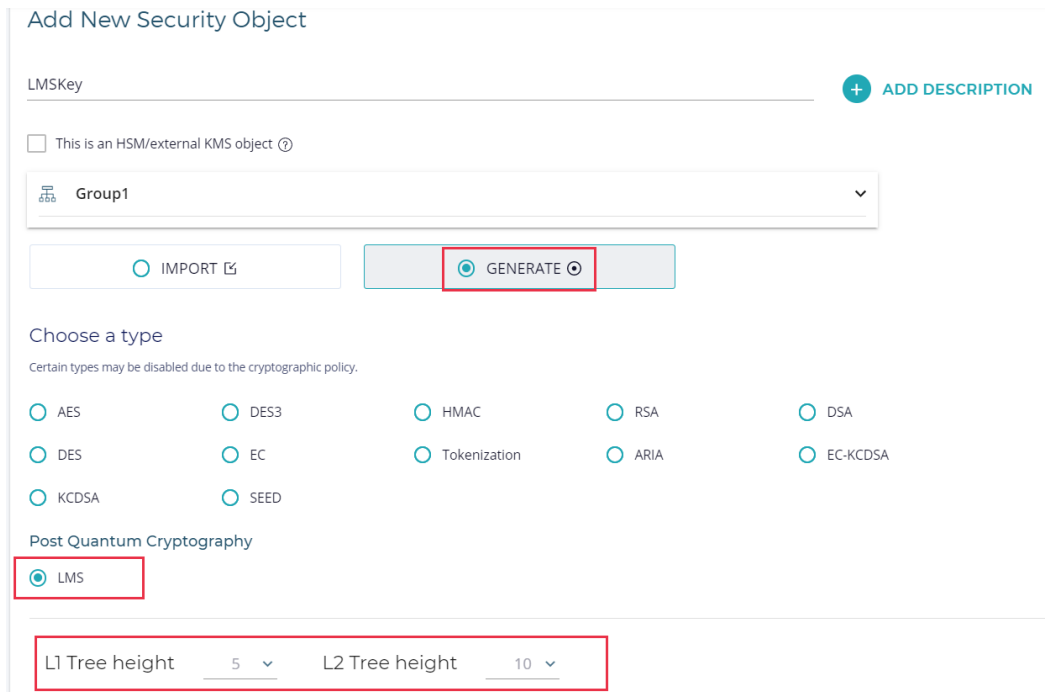
## RELEASE NOTE

**Date:** 5-Jan-23

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

**Software:** Fortanix Data Security Manager

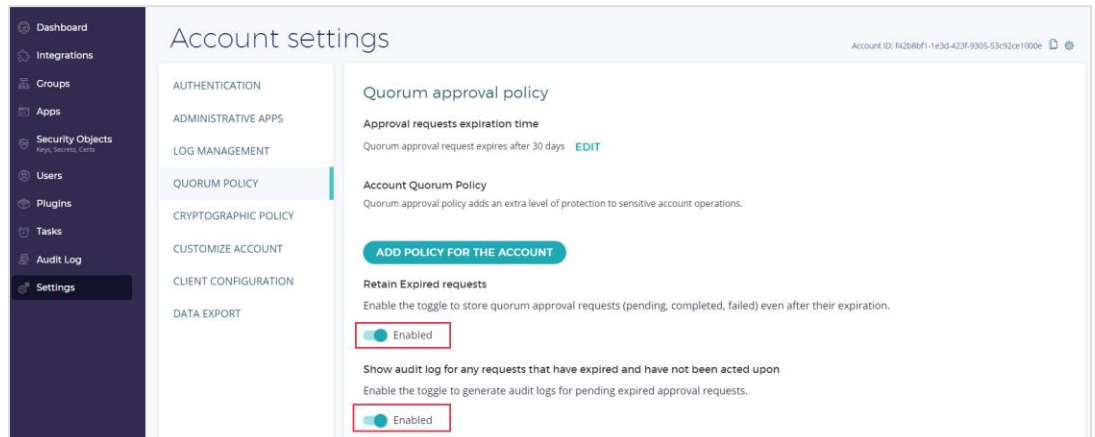
**Version:** 4.13



For more details refer to the [User's Guide: Key Lifecycle Management](#).

### 3. Show expired Quorum approval requests in the DSM UI (JIRA: ROFR-3755).

This release adds a new feature in the Quorum approval request **Account Settings** page, that allows you to retain expired approval requests in the **Tasks** pane and you can also generate audit logs for expired approval requests.



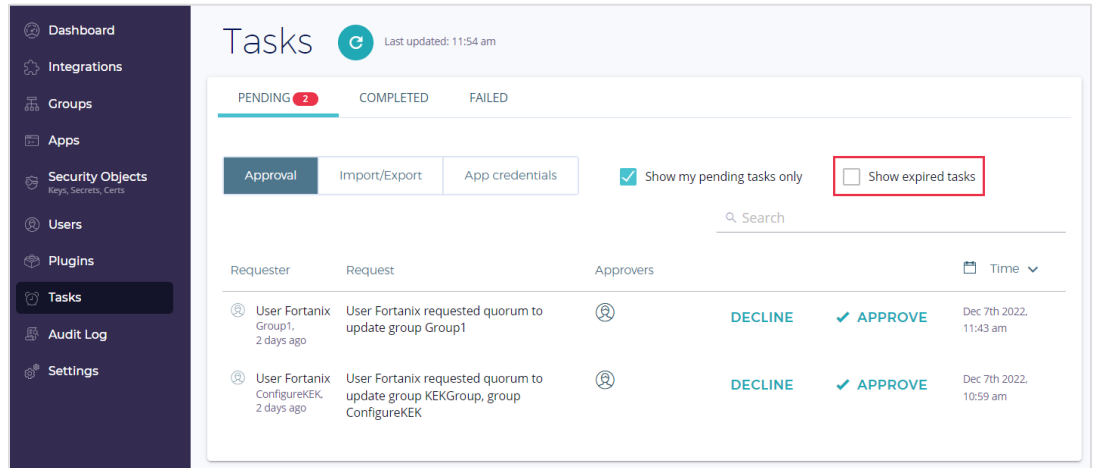
## RELEASE NOTE

**Date:** 5-Jan-23

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

**Software:** Fortanix Data Security Manager

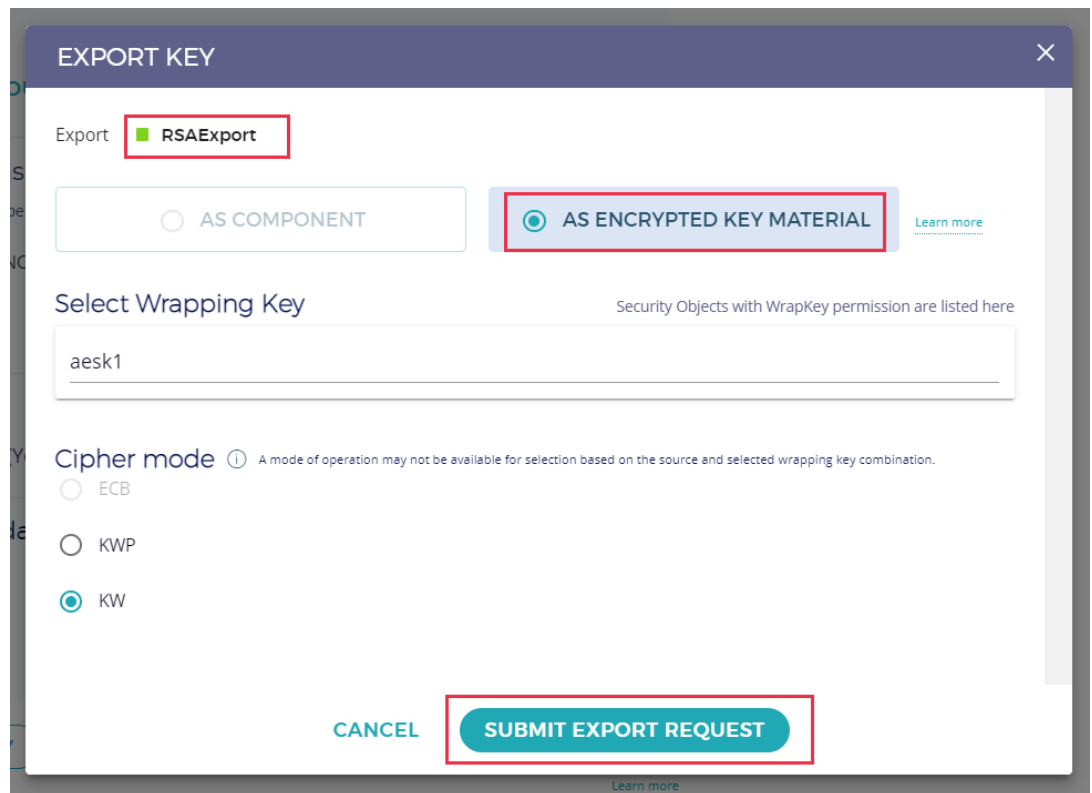
**Version:** 4.13



For more details refer to the [User's Guide: Quorum Policy](#).

### 4. Allow exporting RSA/EC keys as encrypted key material (JIRA: ROFR-3015).

This release adds support to export RSA/EC keys as encrypted key material and wrap with an AES key.



## RELEASE NOTE

**Date:** 5-Jan-23

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

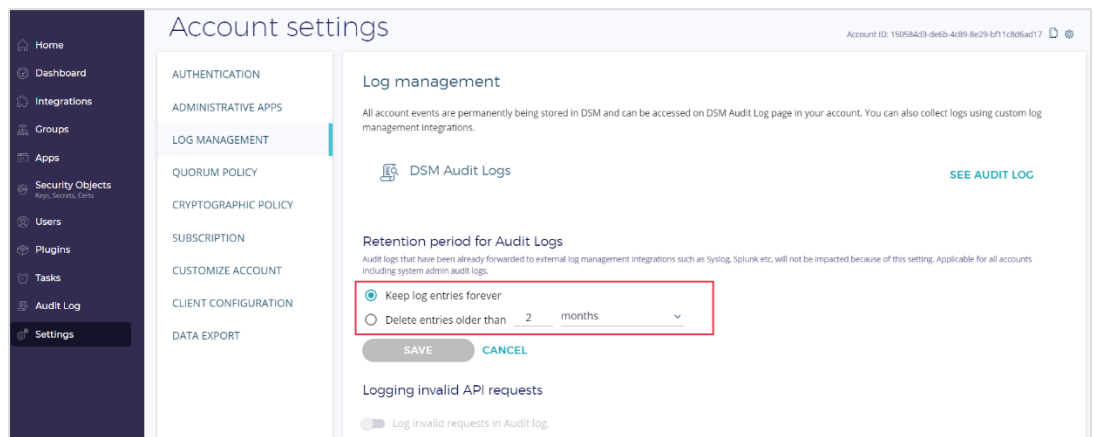
**Software:** Fortanix Data Security Manager

**Version:** 4.13

For more details refer to the [User's Guide: Export Key](#).

### 5. Time-based policy to purge audit logs (JIRA: PROD-4115).

This release adds the ability to set the retention period of audit logs for each account. Purging older logs will help keep log performance and search functions robust. Please ensure that any logs needed for long-term retention are off-boarded through the DSM Log Management feature before enabling log purge.



For more details refer to the [User's Guide: Logging](#).

- **The Audit logs list now only shows logs for a 30-day range using the Time filter (JIRA: ROFR-3780).**
  - Added support to search audit logs using the “Time” filter in the Search Bar to search audit logs for any 30-day period.
  - Added notifications to show the end of the list and when the audit log table is empty.

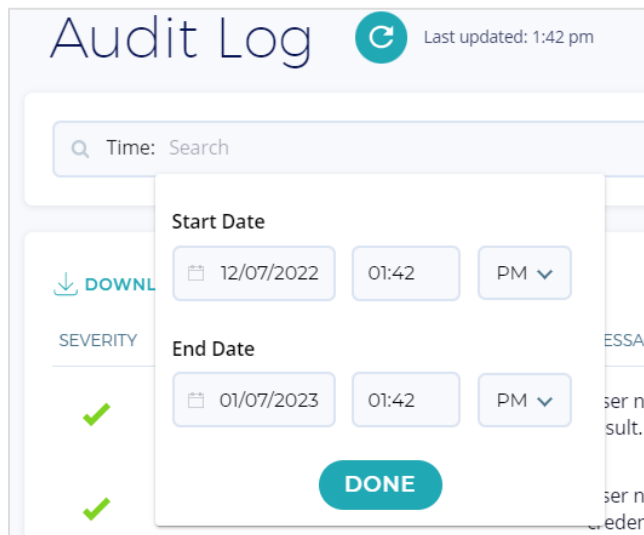
## RELEASE NOTE

**Date:** 5-Jan-23

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

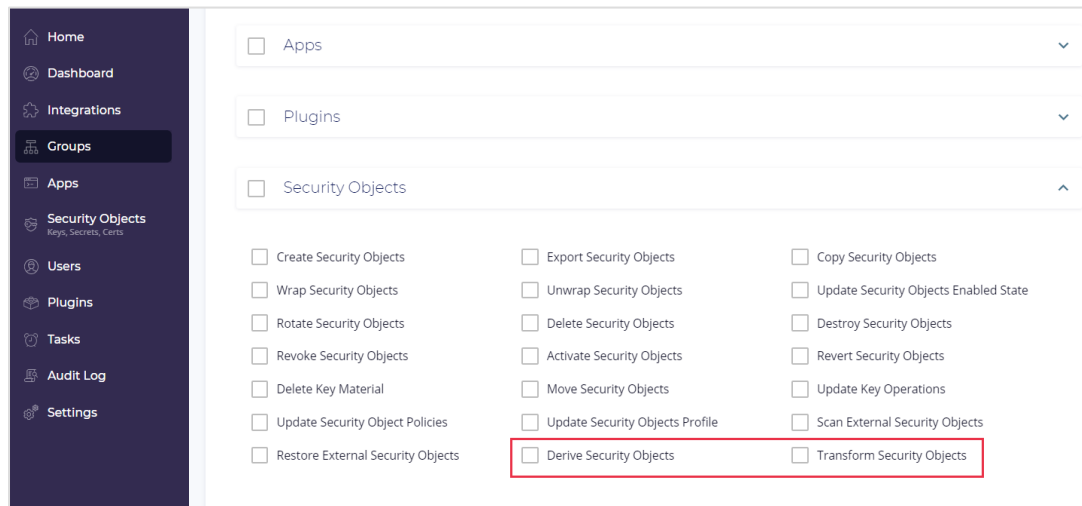
**Software:** Fortanix Data Security Manager

**Version:** 4.13



### 6. Added new Custom Group Role Security Objects permissions (JIRA: ROFR-3683).

The **Security Objects** permissions in a Custom Group Role now include the **Derive** and **Transform** permissions.



## RELEASE NOTE

**Date:** 5-Jan-23

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

**Software:** Fortanix Data Security Manager

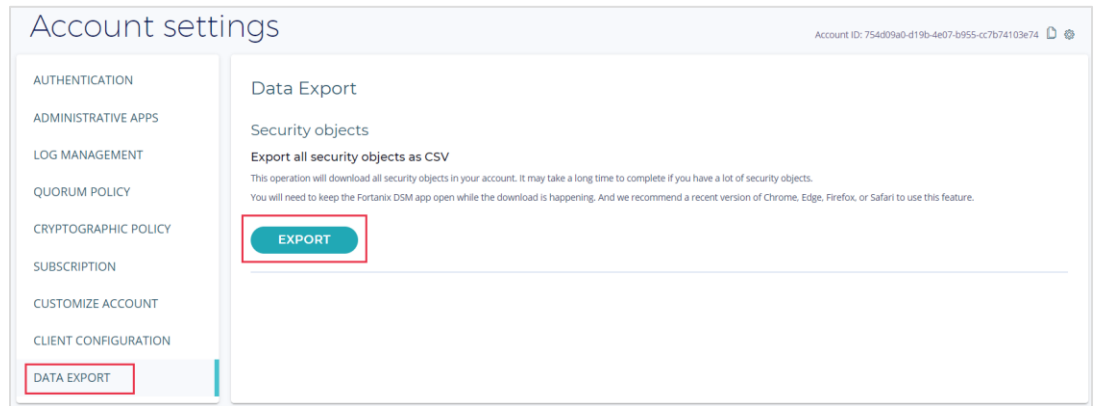
**Version:** 4.13

### 7. Added a new **DATA EXPORT** page to export all security objects as a CSV (JIRA: ROFR-3491).

This release adds a new tab called **DATA EXPORT** in the DSM **Account settings** page to export all the security objects in that DSM account as a CSV file.



**NOTE:** This feature exports only the key metadata, not the actual key material.



For more details, refer to the [User's Guide: Data Export](#).

### 8. Support for AWS External Key Stores (JIRA: PROD-3914).

Support is now generally available for AWS External Key Stores (XKS), enabling DSM to be a Root of Trust for the AWS Key Management Service. Please contact Fortanix support for instructions on how to enable this feature on your installation.

For more details, refer to the [AWS External Key Store Concepts](#).

## ENHANCEMENTS TO EXISTING FEATURES

### 1. Cryptographic policy improvements for DES3 key (JIRA: ROFR-3715).

You can now select the key length for DES3 keys in the Cryptographic policy for security objects at the DSM account and group levels.



## RELEASE NOTE

**Date:** 5-Jan-23

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

**Software:** Fortanix Data Security Manager

**Version:** 4.13



### Cryptographic policy for security objects

Restrict adding certain types of security objects to the group, set minimum key sizes, and manage permitted key operations for all objects.

⚠ The disabled options are restricted by the account cryptographic policy.

#### Allowed object types for the group:

At least one object type must be permitted.

<input checked="" type="checkbox"/> AES	<input checked="" type="checkbox"/> DES3	<input checked="" type="checkbox"/> HMAC	<input checked="" type="checkbox"/> Opaque	<input checked="" type="checkbox"/> RSA
<input checked="" type="checkbox"/> DSA	<input checked="" type="checkbox"/> DES	<input checked="" type="checkbox"/> EC	<input checked="" type="checkbox"/> Secret	<input checked="" type="checkbox"/> Certificate 
<input checked="" type="checkbox"/> BIP32	<input checked="" type="checkbox"/> EC-KCDSA	<input checked="" type="checkbox"/> KCDSA	<input checked="" type="checkbox"/> SEED 	<input checked="" type="checkbox"/> ARIA

#### Allowed key sizes:

AES ☒ 128 bits ☒ 192 bits ☒ 256 bits

[EDIT](#)

DES3 ☒ 112 bits ☒ 168 bits

[SAVE](#)

HMAC 112 bits minimum For HMAC key choose size from 112 to 8192

[EDIT](#)

## 2. Google Workspace CSE easy wizard integration improvements (JIRA: ROFR-2815).

You can now configure a new Google Workspace CSE instance using the **Integrations** tab that supports the following:

- Auto-generate the Key Service URL using the Add Instance wizard.
- Auto-generate and Google CSE group and an AES key to encrypt the Google Workspace CSE documents.
- Ability to edit an instance (**JIRA: ROFR-3718**).
- Ability to delete an instance (**JIRA: ROFR-3718**).

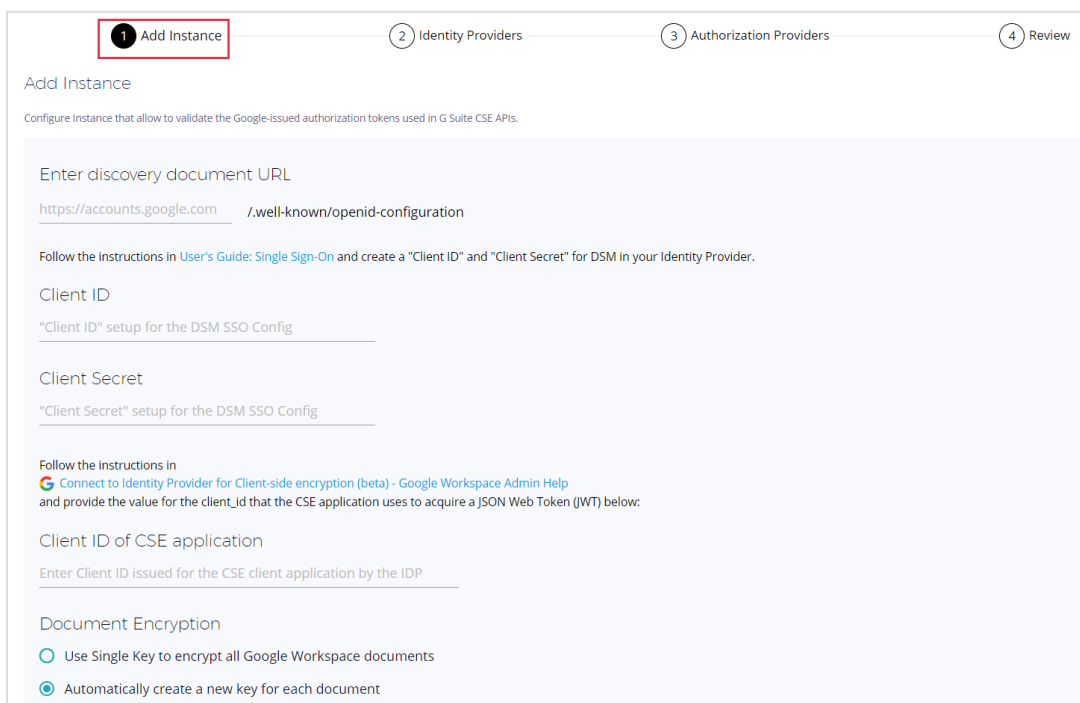
## RELEASE NOTE

**Date:** 5-Jan-23

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

**Software:** Fortanix Data Security Manager

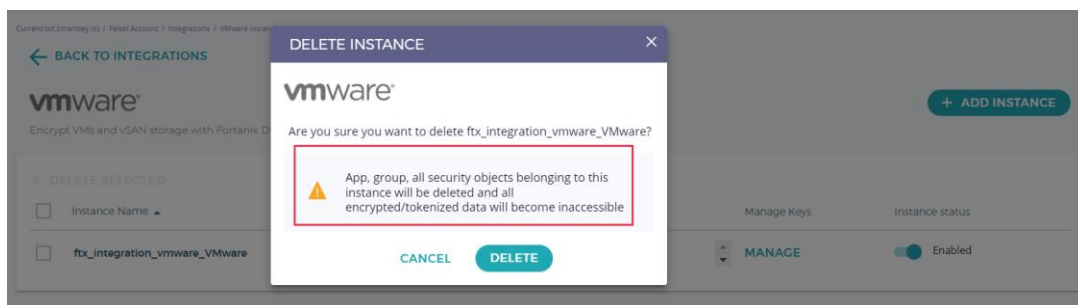
**Version:** 4.13



For more details, refer to the [Integration Guide: DSM with Google Workspace CSE](#).

### 3. VMware Easy Wizard improvements

- Improved the delete instance message for VMware easy wizard (JIRA: ROFR-3694).



- Updated the VMware easy wizard interface type to KMIP (JIRA: ROFR-3693).

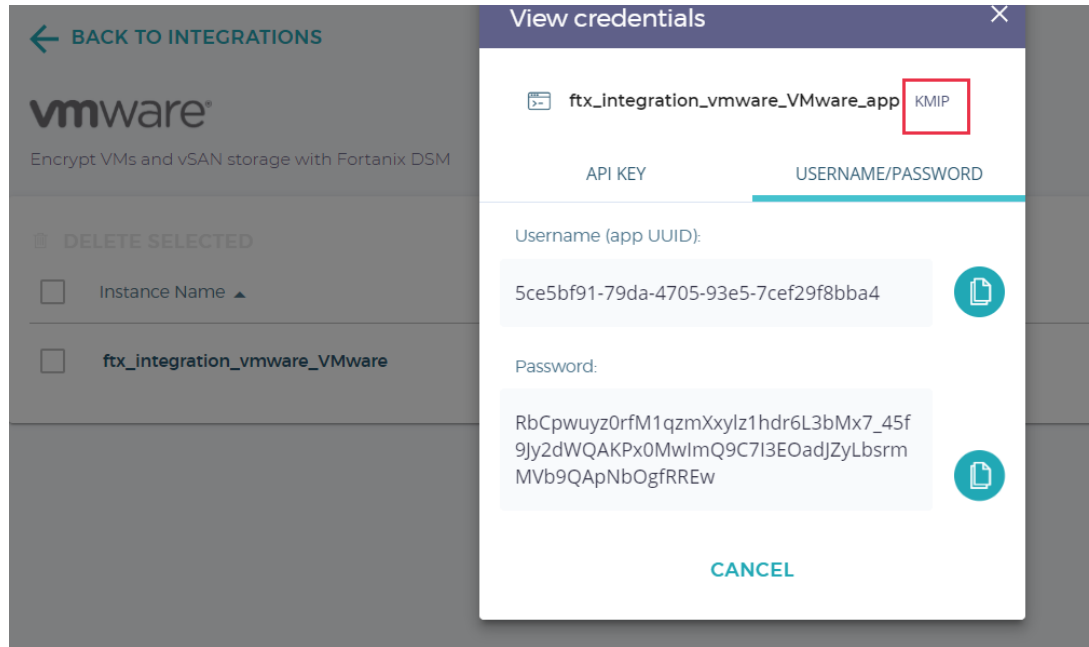
## RELEASE NOTE

**Date:** 5-Jan-23

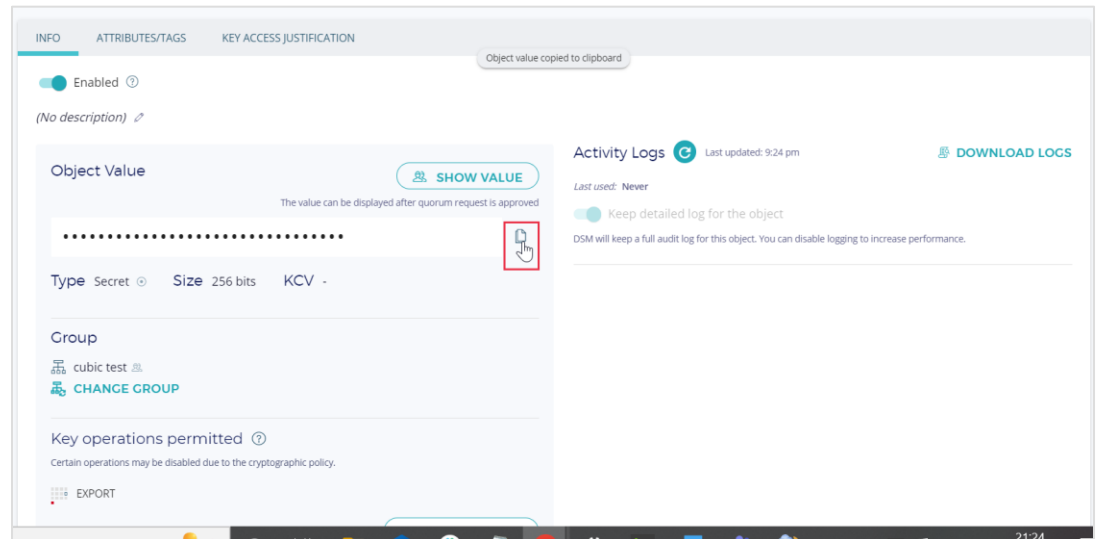
**Subject:** Software changes, updates, bug fixes, etc.

**Software:** Fortanix Data Security Manager

**Version:** 4.13



4. Added the ability to copy a secret value without showing the value on screen (JIRA: ROFR-3655).



5. Added "Business Email" instead of "Email" in the DSM On-prem Signup and Login form (JIRA: ROFR-3636):

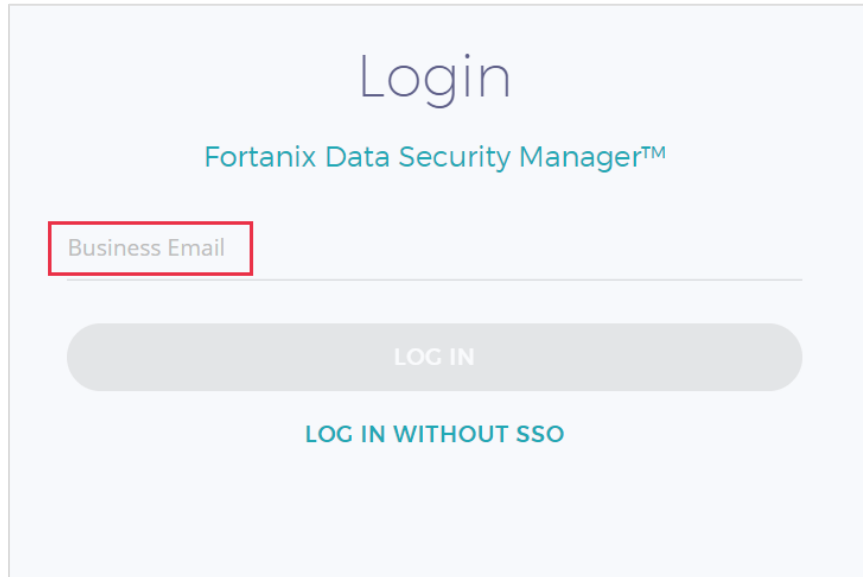
## RELEASE NOTE

**Date:** 5-Jan-23

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

**Software:** Fortanix Data Security Manager

**Version:** 4.13



### 6. Improvements to the labels for the “mode of operation” when unwrapping a security object with RSA key (JIRA: ROFR-3624).

Certain types may be disabled due to the cryptographic policy.

<input checked="" type="radio"/> AES	<input type="radio"/> DES3	<input type="radio"/> HMAC	<input type="radio"/> RSA	<input type="radio"/> DSA
<input type="radio"/> DES	<input type="radio"/> EC	<input type="radio"/> Tokenization	<input type="radio"/> ARIA	<input type="radio"/> EC-KCDSA
<input type="radio"/> KCDSA	<input type="radio"/> SEED			

☒ The key has been encrypted  
To import an encrypted key in a file or as a blob, select the corresponding KEK that was previously used to encrypt your target key.

Select Key Encryption Key

RSAExport

Padding Scheme ⓘ

☐ PKCS1v15

☒ OAEP Hashing Algorithm

Key Check Value (KCV) En

Place value here or import f

SHA1  
SHA224  
SHA256  
SHA384  
SHA512

### 7. Improved the options for Minimum password length in the System Administration Policies settings (JIRA: ROFR-3596).

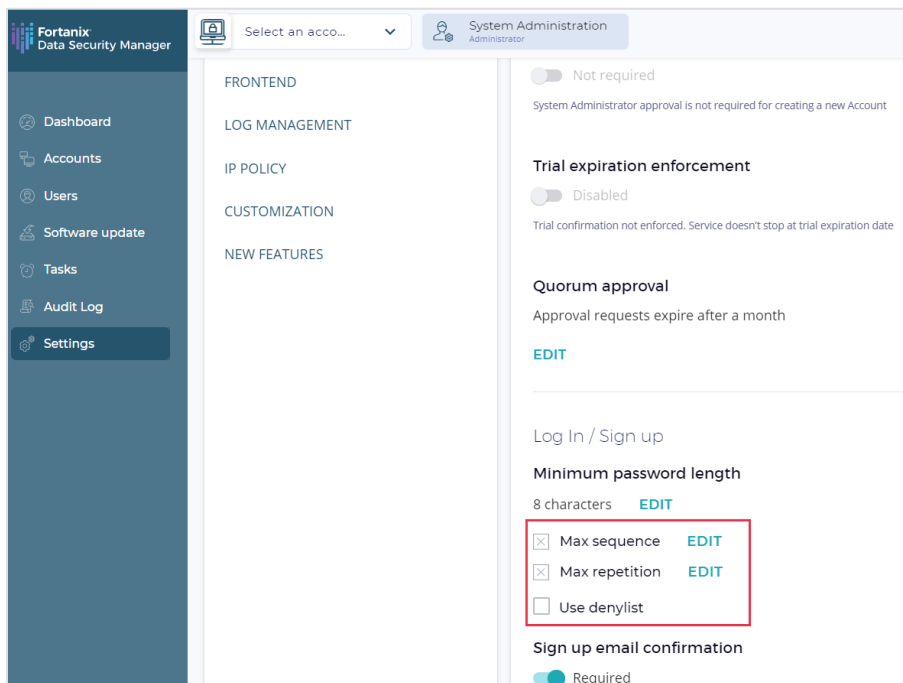
## RELEASE NOTE

**Date:** 5-Jan-23

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

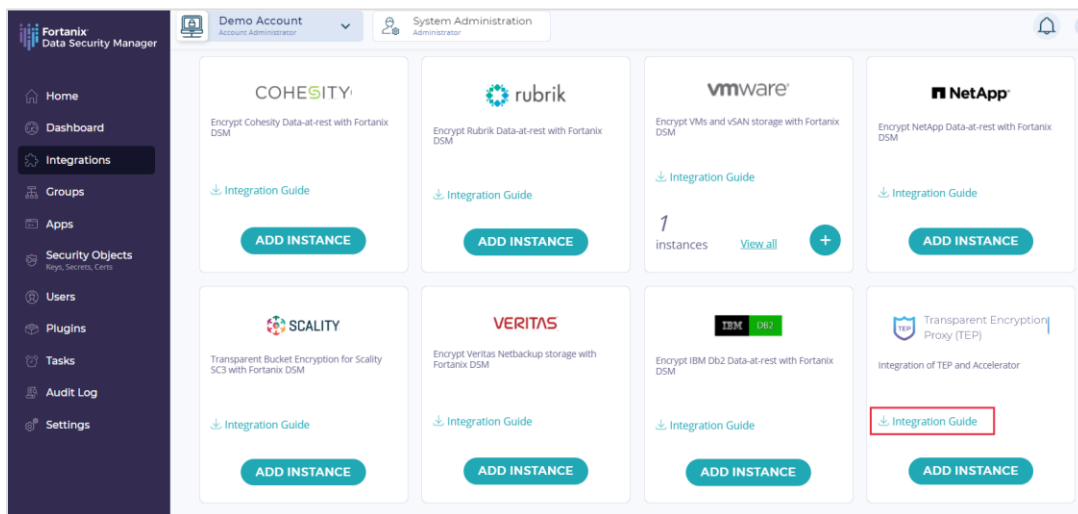
**Software:** Fortanix Data Security Manager

**Version:** 4.13



For more details, refer to the [System Administration Guide: Policies](#).

## 8. Added documentation link for Transparent Encryption Proxy (TEP) in the easy wizard integration for TEP (JIRA: ROFR-3595).



## RELEASE NOTE

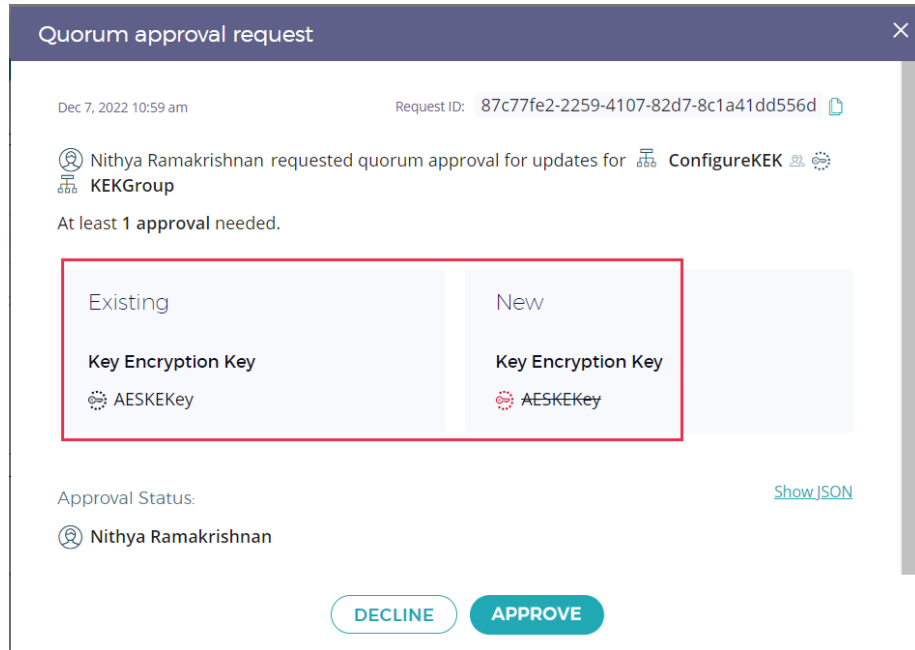
**Date:** 5-Jan-23

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

**Software:** Fortanix Data Security Manager

**Version:** 4.13

9. Implemented a human-readable view for Quorum approval requests related to the Group Key Encryption Key (KEK) feature (JIRA: ROFR-3321).



10. This release allows updating the app-level Client Configuration KMIP settings using the DSM REST API and after you set it, a read-only view of the setting will be visible in the detailed view of the app in the DSM UI (JIRA: ROFR-3081).

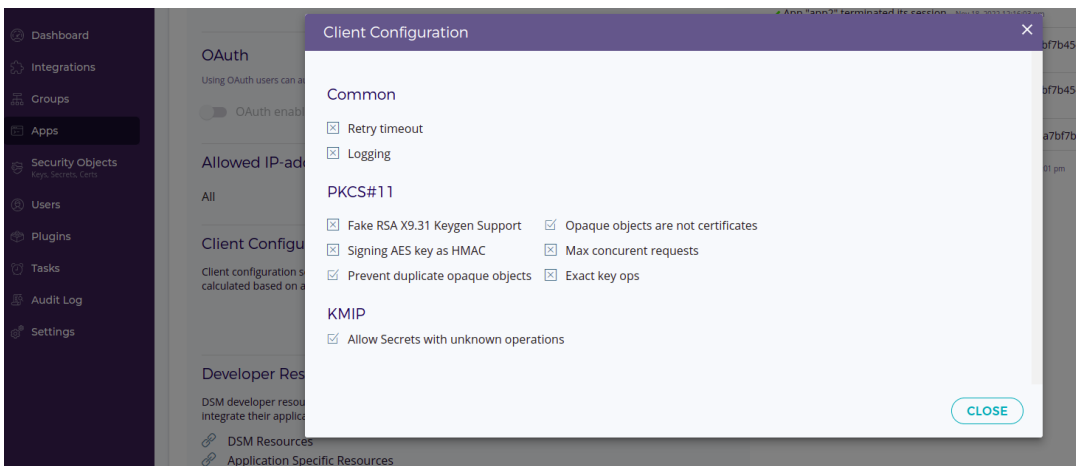
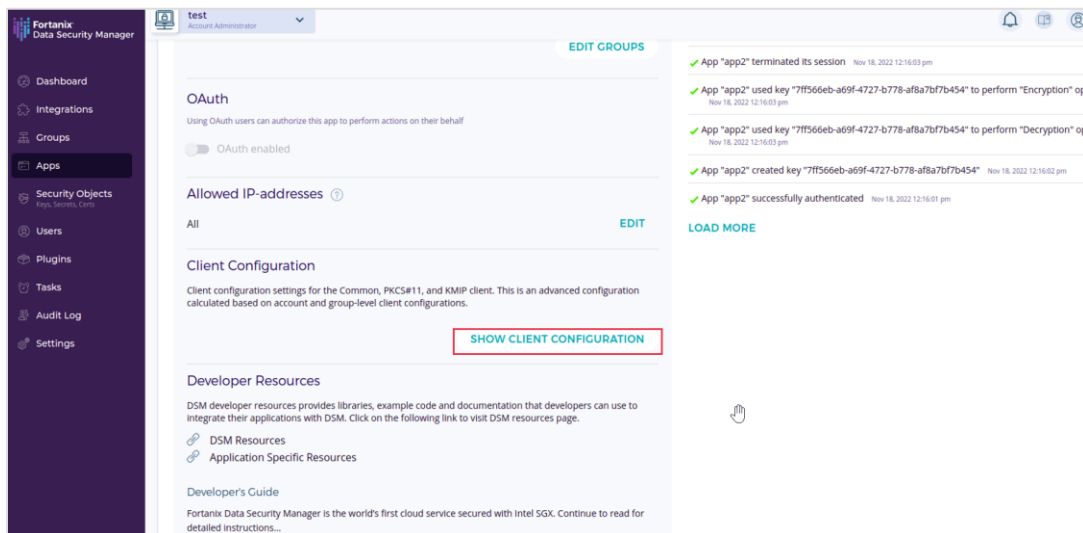
## RELEASE NOTE

**Date:** 5-Jan-23

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

**Software:** Fortanix Data Security Manager

**Version:** 4.13



### 11. Improvements to the User Profile page in the DSM UI (JIRA: ROFR-2955):

- The User icon is consistent with Fortanix iconography.
- Added "Created" and "Last login" information.
- Enabled email confirmation.
- Ability to view and copy your user ID.

## RELEASE NOTE


**Date:** 5-Jan-23

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

**Software:** Fortanix Data Security Manager

**Version:** 4.13

### My Profile


User Fortanix

User ID: c3d05d40-907d-426b-9651-066c0b76a5e0

E-mail: user.fortanix@fortanix.com

Password:

CHANGE PASSWORD

Two-step Authentication:

Off

ENABLE

Created: Oct 25th 2022, 11:43 am

Last Login: Dec 7th 2022, 9:03 am

## 12. Improved the audit logs section in the DSM app detailed view (JIRA: ROFR-2792):

If the audit log list in the DSM app detailed view exceeds more than “N”, you can see the complete logs using the **LOAD MORE** button which redirects to the Audit logs list page.

Dashboard

Integrations

Groups

Apps

Security Objects

Users

Plugins

Tasks

Audit Log

Settings

#### API Key

SDK provides tools, compilers, headers, libraries, code samples, and a new help system that developers can use to create applications.

COPY API KEY

REGENERATE

Change authentication method

#### Groups

DSMA-Demo-Group-QP-dvm06mp9jd Default group

App permissions

EDIT GROUPS

#### OAuth

Using OAuth users can authorize this app to perform actions on their behalf

OAuth enabled

#### Allowed IP-addresses

All

EDIT

#### Developer Resources

DSM developer resources provides libraries, example code and documentation that developers can use to integrate their applications with DSM. Click on the following link to visit DSM resources page.

DSM Resources

Developer's Guide

Fortanix Data Security Manager is the world's first cloud service secured with Intel SGX. Continue to read for detailed instructions...

#### Activity Logs

Last login: November 15, 2022, 12:56 pm

App "DSMA-APP-6qqu31mg18q" used key "DSMA-50-yyslq8lwd" to perform "Encryption" operation	Nov 15, 2022 12:38:02 pm
App "DSMA-APP-6qqu31mg18q" used key "DSMA-50-yyslq8lwd" to perform "Encryption" operation	Nov 15, 2022 12:38:00 pm
App "DSMA-APP-6qqu31mg18q" used key "DSMA-50-yyslq8lwd" to perform "Encryption" operation	Nov 15, 2022 12:37:58 pm
App "DSMA-APP-6qqu31mg18q" used key "DSMA-50-yyslq8lwd" to perform "Encryption" operation	Nov 15, 2022 12:37:56 pm
App "DSMA-APP-6qqu31mg18q" used key "DSMA-50-yyslq8lwd" to perform "Encryption" operation	Nov 15, 2022 12:37:54 pm
App "DSMA-APP-6qqu31mg18q" used key "DSMA-50-yyslq8lwd" to perform "Encryption" operation	Nov 15, 2022 12:37:52 pm
App "DSMA-APP-6qqu31mg18q" used key "DSMA-50-yyslq8lwd" to perform "Encryption" operation	Nov 15, 2022 12:37:50 pm
App "DSMA-APP-6qqu31mg18q" used key "DSMA-50-yyslq8lwd" to perform "Encryption" operation	Nov 15, 2022 12:37:48 pm
App "DSMA-APP-6qqu31mg18q" used key "DSMA-50-yyslq8lwd" to perform "Encryption" operation	Nov 15, 2022 12:37:46 pm
App "DSMA-APP-6qqu31mg18q" used key "DSMA-50-yyslq8lwd" to perform "Encryption" operation	Nov 15, 2022 12:37:44 pm

LOAD MORE



## RELEASE NOTE

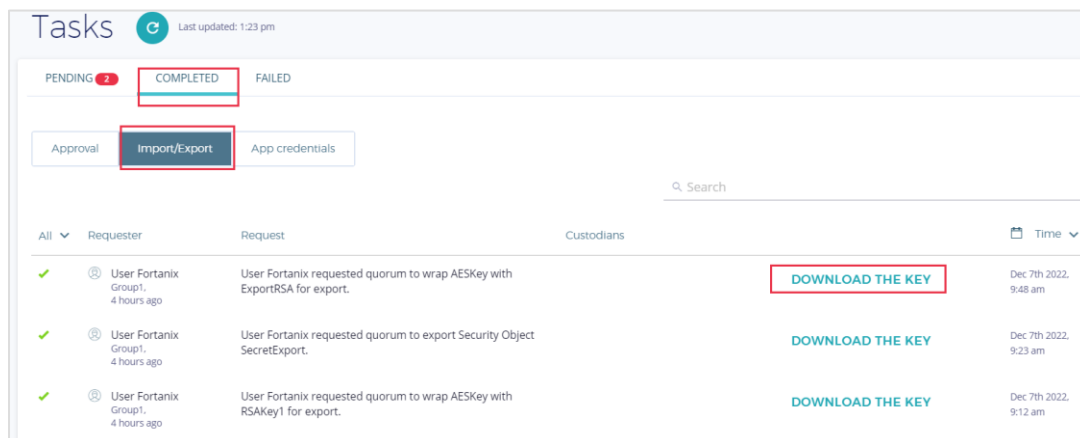
**Date:** 5-Jan-23

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

**Software:** Fortanix Data Security Manager

**Version:** 4.13

### 13. Improved the Quorum approval workflow by updating the status of an exported key after it is downloaded (JIRA: PROD-2507).



For more details, refer to the [User's Guide: Export Key](#).

### 14. Improved audit logs for denied key access due to Key Access

**Justification (KAJ) policy at key level (JIRA: PROD-5069):**

The audit log for denied key access now shows:

- The Key ID and Key Name of the key that was denied access.
- The KAJ reason due to which the key access was restricted.

### 15. Applied the updated "Pending Changes" text in the System

**Administration Policies Settings for Sign up email confirmation (JIRA: ROFR-3595).**

### 16. Added "HIGHVOLUME" in the filter for key operations for Server-Side Table Processing (JIRA: ROFR-3582).

### 17. The RSA/ ECB/OAEPADDING is now supported for OAEP\_MGF1\_SHA256, OAEP\_MGF1\_SHA384, OAEP\_MGF1\_SHA512 modes (JIRA: PROD-5576).

### 18. Support to show audit logs for scheduled key rotation (JIRA: PROD-5318).

### 19. Audit logs are now restricted to the last 30-day range (JIRA: ROFR-3780).

## RELEASE NOTE

**Date:** 5-Jan-23

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

**Software:** Fortanix Data Security Manager

**Version:** 4.13

You can now view audit logs for the last 30-day period. To view older logs you need to use the “Time” filter in the search bar.

**20. Support to wrap an AES key with an RSA key in a FIPS-backed group (JIRA: PROD-5823).**

**21. Removed the “Last Run” column for the Plugins list view table (JIRA: ROFR-3654).**

**22. Improved the description for purging an Azure soft-deleted key in the section **Purge deleted key in Azure key vault** in the **Azure Key Details** tab (JIRA: ROFR-3650).**

**23. Added “read-only mode” for all UI screens for a System Operator role in the System Administration settings view (JIRA: ROFR-3711).**

As system operators do not have permissions to add/modify any System Administration settings, a read-only view is created for this role so that they can view but not edit the settings.

**24. DSM SaaS improvements:**

- **Improved the Trial Expiration logic for DSM SaaS (JIRA: ROFR-3699).**  
The trial expiration logic is now simplified to always use `trial_expires_at` field instead of `expires_at` field in account details for information regarding trial expiry.
- **Improved the signup error message when trying to sign up using a sign-up URL if you are restricted from signing up (JIRA: ROFR-3684).**

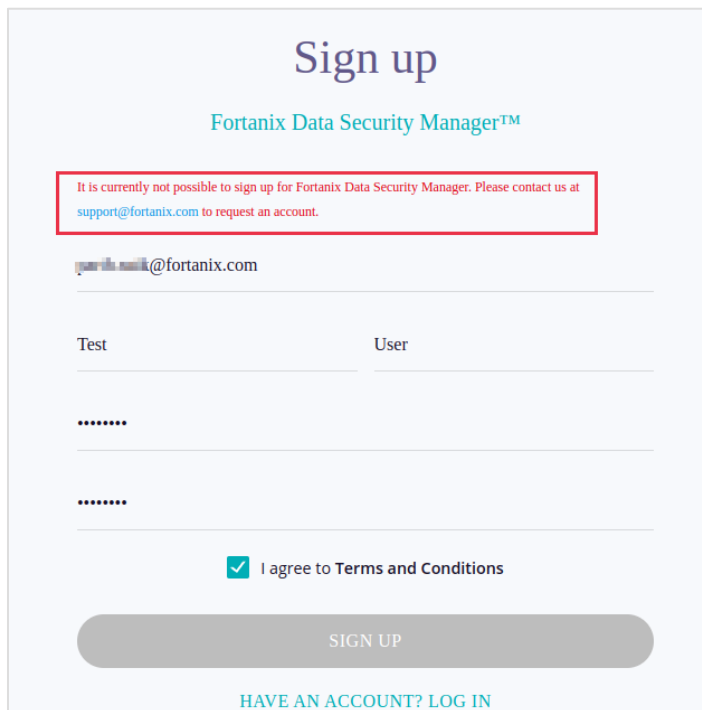
## RELEASE NOTE

**Date:** 5-Jan-23

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

**Software:** Fortanix Data Security Manager

**Version:** 4.13



## CLIENT FEATURES AND ENHANCEMENTS

### 1. KMIP Client Enhancements:

- a. Added support for modifying custom X attributes (**JIRA: PROD-5457**).

### 2. JCE Client Enhancements:

- a. The RSA/ ECB/OAEPADDING is now supported for all the standard combinations of SHA-series hash and MGF1 padding - OAEP\_MGF1\_SHA256, OAEP\_MGF1\_SHA384, OAEP\_MGF1\_SHA512 (**JIRA: PROD-4446**).

### 3. Terraform Provider Enhancements:

- a. Added support to assign multiple groups to a single app with an authentication method as "Google Service Account" (**JIRA: DEVOPS-3299**).
- b. Added support to import keys and upload the signed certificate and private key. (**JIRA: PROD-4714**).
- c. Added support for managing existing groups (**JIRA: DEVOPS-3325**).

## RELEASE NOTE

**Date:** 5-Jan-23

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

**Software:** Fortanix Data Security Manager

**Version:** 4.13

d. Added support for uploading custom security objects (**JIRA: PROD-5983**).

e. Added support to rotate a security object of type "Secret" (**JIRA: DEVOPS-2910**).

For more details refer to, <https://support.fortanix.com/docs/clients-terraform-provider>.

## OTHER IMPROVEMENTS

1. Google Stackdriver now sends logs in batches for better performance (**JIRA: PROD-5890**).

2. Improved sdkms-cli error messages (**JIRA: PROD-5183**).

### 3. REST API improvements:

a. Improvements to the API for short-term DSM password policies (**JIRA: PROD-5742**).

b. Refactored security object creation flow by adding new components:

- Added new components to refactor security object size (**JIRA: ROFR-3666**).
- Added new components to refactor security object creation type (**JIRA: ROFR-3666**).
- Added new components to refactor security object group selection (**JIRA: ROFR-3664**).
- Added a new component to refactor security object type selection (**JIRA: ROFR-3663**).

c. Improved the slowdown caused by the `check_access()` API (**JIRA: PROD-5565**).

4. Added new custom attributes for VMware Vsphere (**JIRA: PROD-5709**).

5. Improved the System Administration UI by ignoring the pods that are in the "Completed" state but showing as unhealthy in the UI (**JIRA: ROFR-2080**).

## RELEASE NOTE

**Date:** 5-Jan-23

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

**Software:** Fortanix Data Security Manager

**Version:** 4.13

## BUG FIXES

- Fixed a page crash issue when creating security objects in an Azure or HSM-backed group (**JIRA: ROFR-3770**).
- Fixed bad templating of the cleanup job that cleans the leftover security objects from deleted accounts (**JIRA: PROD-5927**).
- Fixed an issue where the **CHANGE GROUP** button in the detailed view of a security object flickers on hover (**JIRA: ROFR-3759**).
- Fixed an issue where the **Use denylist** option in the **Minimum password length** section of the System Administration Policies settings does not get updated when selected (**JIRA: ROFR-3757**).
- Fixed an issue where Quorum approval API requests were failing and returning a 500 error code (**JIRA: PROD-5888**).
- Fixed an issue where the backend changes for PKCS#11 client configuration variable `prevent_duplicate_opaque_objects` were not reflecting on the DSM UI (**JIRA: ROFR-3748**).
- Fixed an issue where the **System Administration** tab on the DSM UI was getting disabled when navigating to the **Settings** page (**JIRA: ROFR-3747**).
- Fixed an issue where exporting a Secret key shows **AS ENCRYPTED KEY MATERIAL** option on the modal window in a disabled state (**JIRA: ROFR-3743**).
- Fixed wrong text in the Key deactivation tooltip in the Copy key modal window when copying a key from a normal group to an AWS-backed group (**JIRA: ROFR-3741**).
- Fixed a UI crash in the **Tasks->Pending** tab when importing an AES key using Key Components (**JIRA: ROFR-3732**).
- Removed an extra character present in the **Client Configuration (Advanced)** section in the group detailed view (**JIRA: ROFR-3729**).

## RELEASE NOTE

**Date:** 5-Jan-23

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

**Software:** Fortanix Data Security Manager

**Version:** 4.13

- Fixed the label for the **CANCEL CHANGES** button in the Pending Changes box in the System Administration Policies page (**JIRA: ROFR-3717**).
- Fixed an issue where the create security object flow shows additional key types even though the account-level Cryptographic policy was updated to support only certain keys (**JIRA: ROFR-3716**).
- Fixed an issue that did not allow users to create a group quorum policy when Derive and Transform operations were present (**JIRA: ROFR-3710**).
- Fixed an issue where the user was unable to create Admin Apps with a Custom account role (**JIRA: ROFR-3709**).
- Fixed an issue where removing key permission using the **Restrict Key Permissions** dialog box resulted in some buttons being enabled even before the permission update operation was completed (**JIRA: ROFR-3707**).
- Fixed a panic in the account selection page when an invited user logs in and tries to select an account that still shows as “pending” (**JIRA: ROFR-3706**).
- Fixed an issue where the **COPY KEY** modal window does not filter external and normal groups (**JIRA: ROFR-3705**).
- Fixed styling issue on the DSM homepage (**JIRA: ROFR-3703**).
- Fixed an issue where the Cryptography `intersectTypes` function was missing the logic for new key types (**JIRA: ROFR-3701**).
- Fixed an issue that allowed a user to click the **Delete** button multiple times to delete a Cryptographic policy (**JIRA: ROFR-3698**).
- Fixed a font issue on the Cryptographic policy page (**JIRA: ROFR-3697**).
- Fixed missing Audit Log breadcrumb on the Audit Log list page (**JIRA: ROFR-3695**).
- Fixed unnecessary characters getting appended to the AWS alias in the response of the POST API call during the import key operation (**JIRA: PROD-5792**).

## RELEASE NOTE

**Date:** 5-Jan-23

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

**Software:** Fortanix Data Security Manager

**Version:** 4.13

- Fixed unnecessary characters getting appended to the AWS alias in the response of the GET call during the scan key operation (**JIRA: PROD-5784**).
- Fixed an issue where users were not able to log in using the Microsoft Edge browser when U2F is enabled (**JIRA: ROFR-3685**).
- Fixed missing icon to identify an AWS multi-region key (**JIRA: ROFR-3681**).
- Fixed an issue that shows an error notification when you double-click the **Save** button when creating a plugin from the Plugin library (**JIRA: ROFR-3679**).
- Fixed an issue where the values in the **Select Value** drop down were cut off in the Custom Attribute section of a security object (**JIRA: ROFR-3678**).
- Fixed a mismatch in the Trial Expiration enforcement setting between the UI and backend in the DSM SaaS System Administration account (**JIRA: ROFR-3674**).
- Fixed issues in the BIP32 index boundary values and derive hard child index value (**JIRA: ROFR-3671**).
- Fixed an issue that does not send "GCPBYOK" in the payload when a System Administrator updates the subscription from Trial to Custom (**JIRA: ROFR-3661**).
- Fixed broken service topology specification for `redistributeExternalTraffic` during Kubernetes upgrade to version 1.19 (**JIRA: DEVOPS-3268**).
- Fixed the label for the check box "List previous versions" when publishing a public key (**JIRA: ROFR-3653**).
- Fixed an issue where the URL of a public key has spaces (**JIRA: ROFR-3652**).
- Fixed the validation for AWS Aliases (**JIRA: ROFR-3643**).
- Fixed an issue for BIP32 keys where deriving hard and weak child results in error (**JIRA: ROFR-3644**).

## RELEASE NOTE

**Date:** 5-Jan-23

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

**Software:** Fortanix Data Security Manager

**Version:** 4.13

- Fixed an issue where the **CUSTOM ACCOUNT ROLES** tab was missing on some pages (**JIRA: ROFR-3615**).
- Fixed an issue in the PKCS#11 Client Configuration settings where, updating a specific feature to `true` converts all features to `true` (**JIRA: ROFR-3614**).
- Fixed an issue where AWS aliases allowed invalid characters (**JIRA: PROD-5620**).
- Fixed an issue that now validates if the image uploaded for an Account logo is a valid base64-encoded image (**JIRA: ROFR-3611**).
- Fixed an issue where custom attributes of the source key were not added to a DSM-backed group (**JIRA: ROFR-3610**).
- Fixed an issue where the keytool cert request was not working as expected in Java (**JIRA: PROD-5562**).
- Fixed an issue where the **Credentials** column component for an AWS XKS app was inconsistent in the detailed app view and app table view (**JIRA: ROFR-3600**).
- Fixed a broken documentation link in the app detailed view (**JIRA: ROFR-3599**).
- Fixed an issue where Key compromise action sends an incorrect request body (**JIRA: ROFR-3598**).
- Fixed missing option to enter AWS alias in the dialog box for AWS virtual key rotate to DSM key (**JIRA: ROFR-3594**).
- Fixed an issue where the GCP Key Ring name was not visible when you create a KEY in a GCP-backed group (**JIRA: ROFR-3591**).
- Fixed an issue where the **Home** dashboard on DSM SaaS required a hard refresh to update data (**JIRA: ROFR-3571**).
- Removed key deactivation and activation option from the DSM UI for AWS KMS virtual keys (**JIRA: ROFR-3566**).



## RELEASE NOTE

**Date:** 5-Jan-23

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

**Software:** Fortanix Data Security Manager

**Version:** 4.13

- Fixed an issue that now handles null UUIDs for the audit log entries gracefully (**JIRA: ROFR-3538**).
- Fixed an issue where a user was created even when the invite user flow was canceled (**JIRA: ROFR-3506**).
- Added warning in the UI when a compromised key is enabled and copied to a new group (**JIRA: ROFR-3498**).
- Fixed an issue where the Key undo policy and Key custodian policy icons were not visible on the security object detailed view next to the Group name (**JIRA: ROFR-3498**).
- Fixed an issue where the **Key Management** permissions for a group Quorum policy were displayed in an incorrect format (**JIRA: ROFR-3490**).
- Fixed following issues for a BIP32 key (**JIRA: ROFR-3463**):
  - a. Detailed view of a BIP32 key must not have **CREATE NEW BIP32 KEY** option in the **NEW OBJECT** drop down.
  - b. The **Path** field must not have commas and spaces.
- Fixed an incorrect error message when a security object is deleted from a group that has a Quorum approval policy configured (**JIRA: ROFR-3431**).
- Fixed alignment of the plus icon for the **ADD SCHEMA** option in the **Configure Schema** section in the Add TEP instance screen (**JIRA: ROFR-3408**).
- Fixed an issue where a disabled check box could be selected in the Quorum approval policy group settings (**JIRA: ROFR-3407**).
- Fixed an issue where the check box for the entries in the **USERS, APPS, or PLUGINS** tab was disabled when you click **MANAGE** from the TEP instance table (**JIRA: ROFR-3405**).
- Fixed an issue where TEP supports limited cipher modes, but the error message lists all cipher modes (**JIRA: ROFR-3402**).

## RELEASE NOTE

**Date:** 5-Jan-23

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

**Software:** Fortanix Data Security Manager

**Version:** 4.13

- Fixed an issue where more than one Quorum approval request gets generated for enabling or disabling plugins (**JIRA: ROFR-3401**).
- Fixed an issue that did not allow navigating back to the TEP instance from the DSM KEY (**JIRA: ROFR-3391**).
- Fixed an issue that lists only AES for selecting the wrapping key (**JIRA: ROFR-3294**).
- Fixed an issue in which double-clicking the **Enable** option for **Two-step Authentication** on the user's profile page does not create the U2F key (**JIRA: ROFR-3280**).
- Fixed an issue where even if the Key metadata policy is added to a group, the Key metadata icon is not displayed next to the group name (**JIRA: ROFR-3149**).
- Fixed an issue where the System Administrator Operator role shows extra privileges (**JIRA: ROFR-3119**).
- Fixed a page crash issue due to `getAwsRegionFromSubject` failure to parse the region from the URL (**JIRA: ROFR-3808**).

## QUALITY ENHANCEMENTS / UPDATES

- Created a Cron job for audit log purge (**JIRA: DEVOPS-3472**).
- Updated the Docker CE version from 18.06.3 to 19.03.11 (**JIRA: DEVOPS-3148**).

## KNOWN ISSUES

- An account could be lost if account tables are inconsistent between nodes. Make sure a backup is successful before proceeding with ANY upgrade (**JIRA: PROD-4234**).

## RELEASE NOTE

**Date:** 5-Jan-23

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

**Software:** Fortanix Data Security Manager

**Version:** 4.13

- When a node is removed from a 3-node cluster with build 4.2.2087, and the 2-node cluster is upgraded with build 4.3.xxxx, it is possible that the deploy job is exited and marked completed before cluster upgrade (**JIRA: DEVOPS-2068**).

Workaround: If all the pods are healthy, you can deploy the version again.

- The sync key API returns a "400 status code and response error" due to the short-term access token expiry during the sync key operation of a group linked to AWS KMS (**JIRA: PROD-3903**).
- `exclude` does not work in the `proxy` config for operations such as attestation (**JIRA: PROD-3311**).
- Unable to perform Local encrypt/decrypt operation in Fortanix DSM-Accelerator using DES3 algorithm in CBC/ECB mode with the key size 112 (**JIRA: PROD-5598**).
- When a quorum approval is generated and the request expires, clicking the group that triggered the quorum approval results in a 500 error if the "Retain expired requests" toggle is enabled in the Account quorum policy settings (**JIRA: PROD-6038**).
- In the Google Workspace CSE easy wizard integration, the **Review** page has the Key Service URL hardcoded to the AMER cluster by error (**JIRA: ROFR-3810**).

`https://{amer_url}/crypto/v1/keys/{key_uuid}/integrations/gsuite`

**Workaround:** Copy the correct Key Service URL from the security objects detailed view page.

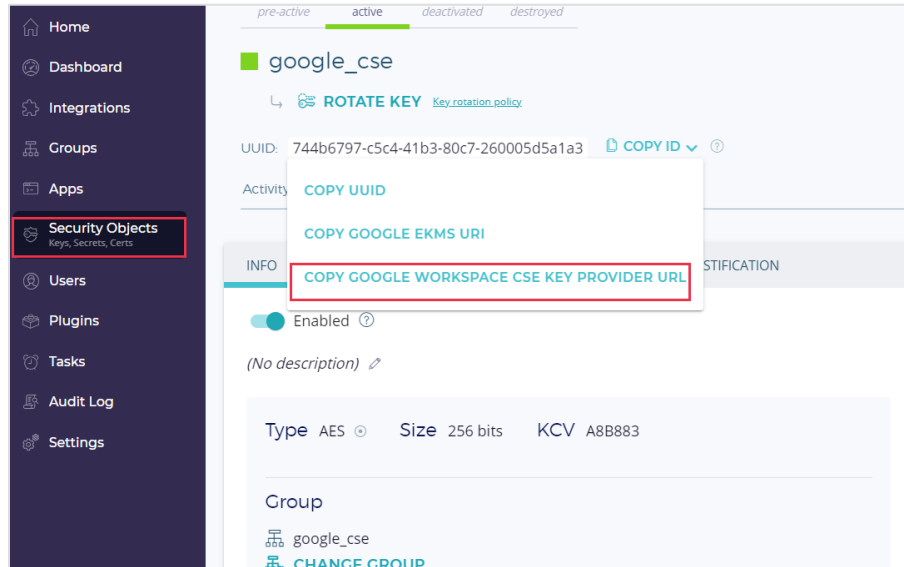
## RELEASE NOTE

**Date:** 5-Jan-23

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

**Software:** Fortanix Data Security Manager

**Version:** 4.13



## FORTANIX DATA SECURITY MANAGER PERFORMANCE STATISTICS

### • Series 2

KEY TYPES AND OPERATIONS	THROUGHPUT (Operations/second on a 3-node cluster)
AES 256: CBC Encryption/Decryption	3878/4017
AES 256: GCM Encryption/Decryption	4033/4089
AES 256: FPE Encryption/Decryption	2110/2092
AES 256 Key Generation	1201
RSA 2048 Encryption/Decryption	3948/1048
RSA 2048 Key Generation	30
RSA 2048 Sign/Verify	1039/3769
EC NISTP256 Sign/Verify	1002/568
Data Security Manager Plugin (Hello world plugin)	1700 (invocations/second)

## RELEASE NOTE

**Date:** 5-Jan-23

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

**Software:** Fortanix Data Security Manager

**Version:** 4.13

- **Azure Standard\_DC8\_v2**

KEY TYPES AND OPERATIONS	THROUGHPUT (Operations/second on a 3-node [Standard_DC8_v2] cluster)
AES 256: CBC Encryption/Decryption	3318/3423
AES 256: GCM Encryption/Decryption	3233/3335
AES 256: FPE Encryption/Decryption	1744/1746
AES 256 Key Generation	1083
RSA 2048 Encryption/Decryption	2993/1080
RSA 2048 Key Generation	41
RSA 2048 Sign/Verify	1074/3155
EC NISTP256 Sign/Verify	824/502
Data Security Manager Plugin (Hello world plugin)	1639 (invocations/second)

- **Series 2 JCE**

KEY TYPES AND OPERATIONS	THROUGHPUT (Operations/second on a 3-node cluster)
AES 256: CBC Encryption/Decryption	3476/3649
AES 256 Key Generation	1180
RSA 2048 Key Generation	30
RSA 2048 Sign/Verify	815/1793
EC NISTP256 Sign/Verify	825/509
Data Security Manager Plugin (Hello world plugin)	1678 (invocations/second)

## RELEASE NOTE

**Date:** 5-Jan-23

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

**Software:** Fortanix Data Security Manager

**Version:** 4.13

- **Azure Standard\_DC8 JCE**

KEY TYPES AND OPERATIONS	THROUGHPUT (Operations/second on a 3-node [Standard_DC8 JCE] cluster)
<b>AES 256: CBC Encryption/Decryption</b>	3047/3208
<b>AES 256 Key Generation</b>	1078
<b>RSA 2048 Key Generation</b>	41
<b>RSA 2048 Sign/Verify</b>	806/1716
<b>EC NISTP256 Sign/Verify</b>	659/438
<b>Data Security Manager Plugin (Hello world plugin)</b>	1597 (invocations/second)

## FORTANIX DATA SECURITY MANAGER – ACCELERATOR PERFORMANCE STATISTICS

- **Runtime Environment**



**NOTE:**

- The following table lists the standard recommended runtime environment. You can choose a higher configuration for better performance.
- DSM-Accelerator was run in the runtime environment listed below for performance testing.

## RELEASE NOTE

**Date:** 5-Jan-23

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

**Software:** Fortanix Data Security Manager

**Version:** 4.13

ITEM	SPECIFICATION
Number of Cores	4
CPU	Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz
RAM	32 GiB

### • DSM-Accelerator Webservice



**NOTE:** The performance numbers below are captured with a single node; if you need higher performance or throughput, then we recommend adding multiple nodes.

KEY TYPES AND OPERATIONS	THROUGHPUT (Operations/second on a 1-node cluster)
AES 256: CBC Encryption/Decryption	9926/9560
AES 256: GCM Encryption/Decryption	9810/9690
AES 256: FPE Encryption/Decryption	2930/2918

### • Additional Modes

KEY TYPES AND OPERATIONS	THROUGHPUT (Operations/second on a 1-node cluster)
AES 256: CBCNOPAD Encryption/Decryption	9626/9560
AES 256: CFB Encryption/Decryption	9810/9690
AES 256: CTR Encryption/Decryption	9810/9810
AES 256: OFB Encryption/Decryption	9750/9722

## RELEASE NOTE

**Date:** 5-Jan-23

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

**Software:** Fortanix Data Security Manager

**Version:** 4.13

## 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.
- Restrict physical access to the appliance to trusted administrators.
- Create two or more System Administrator accounts.
- Enable daily backups for the cluster.

## INSTALLATION

To download the DSM SGX (on-prem/Azure) and Software (AWS/Azure/VMWare) packages, click [here](#).

## SUPPORT

For any questions regarding this release note, please contact [support@fortanix.com](mailto: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.



## RELEASE NOTE

**Date:** 5-Jan-23

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

**Software:** Fortanix Data Security Manager

**Version:** 4.13

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 © 2022 Fortanix, Inc. All rights reserved.

Fortanix Data Security Manager Release Notes

Release 4.13