

## RELEASE NOTE

**Date:** 16-May-23

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

**Software:** Fortanix Data Security Manager SaaS

**Version:** 4.17

## OVERVIEW

This document provides an overview of new features, general enhancements, improvements, and resolved issues in the Fortanix Data Security Manager (DSM) SaaS 4.17 release.



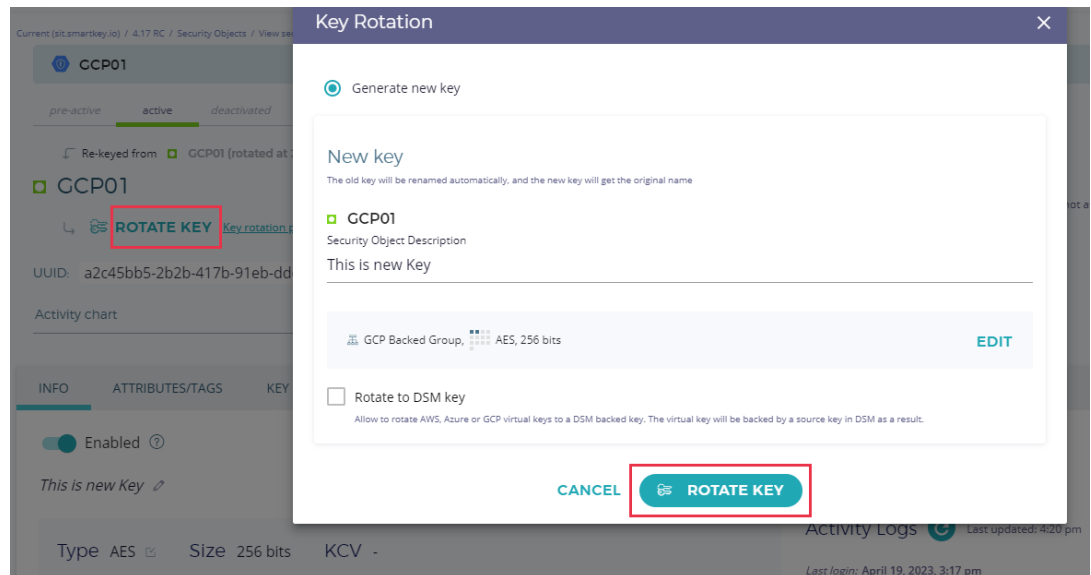
### NOTE:

- This release is for **SaaS only** and not available for On-Prem installations.
- If you are installing Fortanix DSM for the first time (fresh install), then the nodes should be at 5.4.0-26-generic, Kernel before installation.

## NEW FUNCTIONALITY / FEATURES

### 1. Support key rotation for GCP BYOK security objects (JIRA: PM-28):

This release adds support to rotate a GCP BYOK native key with another native key.



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

## ENHANCEMENTS TO EXISTING FEATURES

## RELEASE NOTE

**Date:** 16-May-23

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

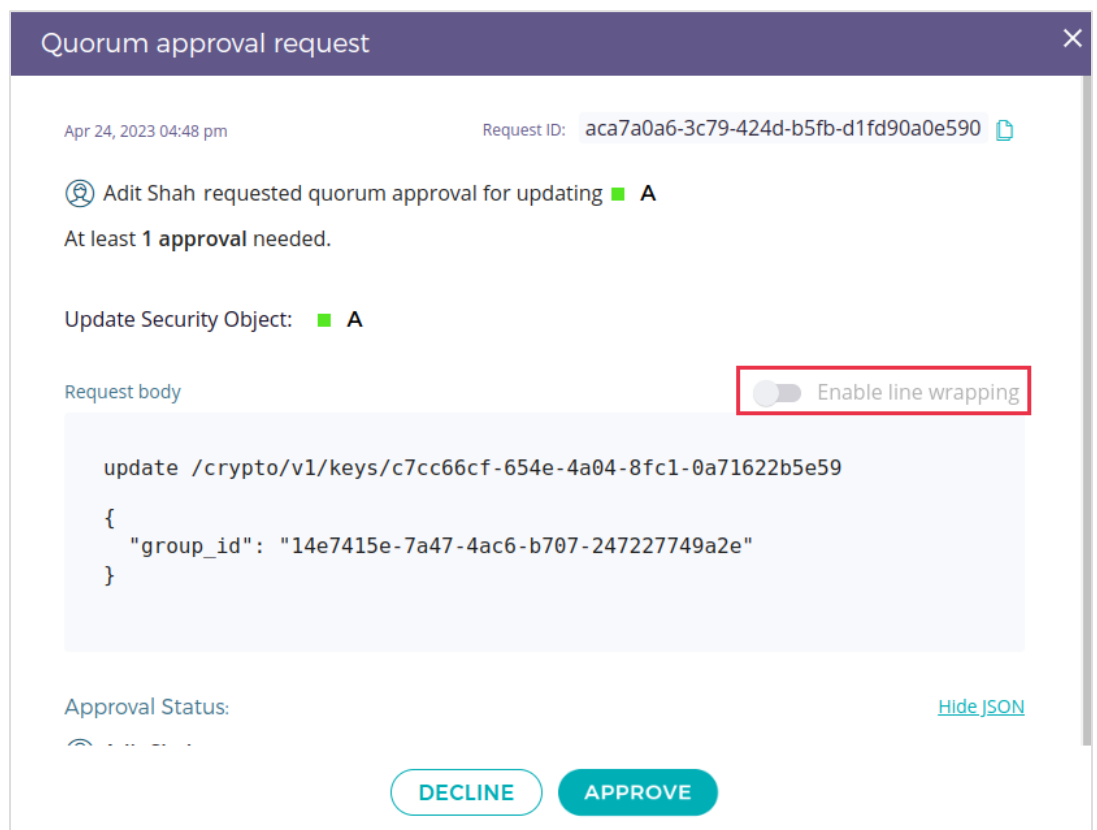
**Software:** Fortanix Data Security Manager SaaS

**Version:** 4.17

### 1. Improved the quorum approval request modal window for long request bodies (JIRA: ROFR-3953).

The following improvements are made:

- The dimension of the modal window for quorum approval requests is now bigger to view more content.
- The toggle **Enable line wrapping** is added for line wrapping in the JSON viewer.



Quorum approval request

Apr 24, 2023 04:48 pm Request ID: aca7a0a6-3c79-424d-b5fb-d1fd90a0e590

Adit Shah requested quorum approval for updating **A**  
At least **1 approval** needed.

Update Security Object: **A**

Request body  Enable line wrapping

```
update /crypto/v1/keys/c7cc66cf-654e-4a04-8fc1-0a71622b5e59
{
  "group_id": "14e7415e-7a47-4ac6-b707-247227749a2e"
}
```

Approval Status: [Hide JSON](#)

DECLINE APPROVE

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

### 2. Warn about deletion of pending invites when email is updated for an account (JIRA: ROFR-3976).

When updating the user's email using the **Profile** settings in DSM, a warning will be displayed to tell the user that all pending account invites of the user will be removed.

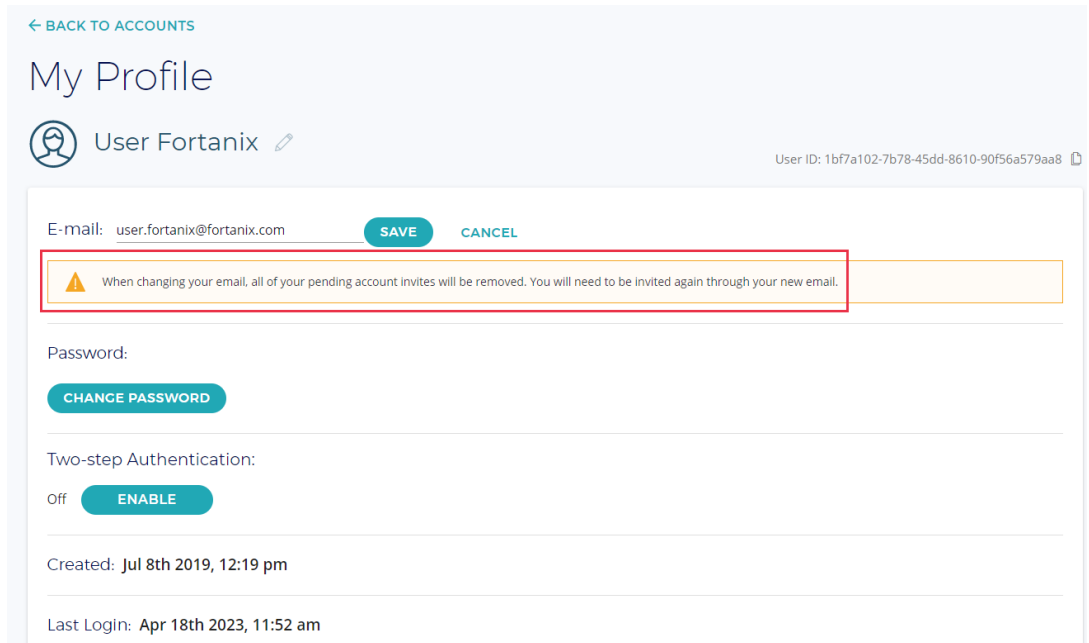
## RELEASE NOTE

**Date:** 16-May-23

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


**Software:** Fortanix Data Security Manager SaaS


**Version:** 4.17




← BACK TO ACCOUNTS

### My Profile

User Fortanix 

User ID: 1bf7a102-7b78-45dd-8610-90f56a579aa8 

E-mail:

 When changing your email, all of your pending account invites will be removed. You will need to be invited again through your new email.

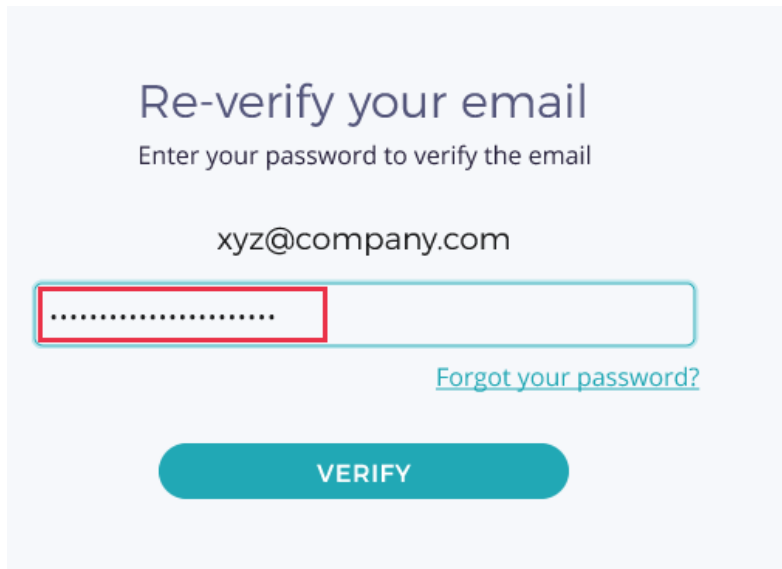
Password:

Two-step Authentication:  
Off

Created: Jul 8th 2019, 12:19 pm

Last Login: Apr 18th 2023, 11:52 am

3. Enforce users with a password who have logged in to DSM with OAuth while verifying an email to mandatorily log in with a password (JIRA: ROFR-3944).



## Re-verify your email

Enter your password to verify the email

xyz@company.com

[Forgot your password?](#)

## RELEASE NOTE

**Date:** 16-May-23

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

**Software:** Fortanix Data Security Manager SaaS

**Version:** 4.17

### 4. Added support to allow only verified users to Quorum approval policy using REST API (JIRA: PROD-6082):

This release does not allow unverified users to be added to the Quorum approval policy using REST API. The UI to disallow unverified users in the Quorum approval policy will be supported in the upcoming DSM releases. Users with pending invites will not be allowed to be added as an approver in the Quorum approval policy.

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

### 5. The `crypto/v1/derive` API now supports a new HKDF derive key mechanism variant (JIRA: PROD-4137).

For more details, refer to [Example Code: Deriving Security Object](#).

## OTHER IMPROVEMENTS

1. Added support for "first" in the BGP neighbor IP calculation method (JIRA: DEVOPS-3716).
2. The logo in the SAML validator is now optional (JIRA: ROFR-4003).
3. Only verified users can set up two-factor authentication and security code (JIRA: PROD-6080). For more details, refer to [User's Guide: Authentication and Authorization](#).

## INTEGRATIONS

1. Added support for Fortanix DSM with Cortex XSOAR integration (JIRA: PROD-4537). For more details, refer to [DSM with Cortex XSOAR integration Guide](#).

## CLIENT IMPROVEMENTS

1. Added support for `subjectAltName` extension of type `iPAddress` in PKCS#10 Certification Request Plugin (JIRA: PROD-6254).

## RELEASE NOTE

**Date:** 16-May-23

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

**Software:** Fortanix Data Security Manager SaaS

**Version:** 4.17

2. Updated the query enumeration tags in KMIP to avoid deserialization failure (JIRA: PROD-6566).
3. Updated the CNG client to support Citrix FAS integration (JIRA: PROD-6719).

## DSM-ACCELERATOR CLIENT IMPROVEMENTS

### 1. DSM-Accelerator Webservice:

- Added support to auto-delete keys from the cache based on TTL (JIRA: PROD-5640).
- Added support for policy awareness for security objects in the DSM-Accelerator Webservice (JIRA: PROD-5648).
- Added support for policy awareness for apps in DSM-Accelerator Webservice (JIRA: PROD-5649).
- Added app-based Effective Key Policy to Security Object Model (JIRA: PROD-6385).

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

### 2. DSM-Accelerator JCE Provider:

- Added support for expiration of Cache keys (JIRA: PROD-6533).
- Added support for policy awareness for security objects in the DSM-Accelerator JCE Provider (JIRA: PROD-6687).
- Support private CA signed-certificate in the DSM-Accelerator JCE Provider (JIRA: PROD-6430).

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

### 3. DSM-Accelerator PKCS#11 Client:

- Added Cache TTL support for DSM-Accelerator PKCS#11 library (JIRA: PROD-6534).

## RELEASE NOTE

**Date:** 16-May-23

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

**Software:** Fortanix Data Security Manager SaaS

**Version:** 4.17

For more details, refer to [Developer's Guide: Fortanix DSM-Accelerator PKCS#11 Client](#).

## TERRAFORM PROVIDER CLIENT IMPROVEMENTS

- Added support for creating and updating Key Access Justification policy when creating security objects for Google Cloud EKM (**JIRA: PROD-4928**).

## BUG FIXES

- Fixed the following issues in the GCP BYOK key rotation feature (**JIRA: ROFR-4056**).
  - The check box **Deactivate original key after rotation** is now removed.
  - The **Edit Parameters** button for Key Type is now removed since GCP only supports AES 256 key type/size.
  - Removed **Rotate to DSM key** check box at the bottom left corner of the GCP Rotate Key dialog box since the feature is not supported.
- Fixed an issue where the users were not able to add the reviewers in the Quorum policy and Key Custodian policy (**JIRA: ROFR-4048**).
- Fixed an issue where creating an RSA showed a "Restrict key operations" modal window (**JIRA: ROFR-4044**).
- Fixed an issue that resulted in a 404 error – page not found when accessing the security object table for a plugin (**JIRA: ROFR-4042**).
- Fixed an issue in the Quorum approval policy Configuration where in "Advanced options" OR should be the default option selected instead of AND (**JIRA: ROFR-4017**).
- Fixed an issue where after adding two-factor authentication, the user was unable to log in (**JIRA: PROD-6606**).
- Fixed an issue where the UI sometimes sends old captcha tokens to the backend, resulting in a 500 error (**JIRA: ROFR-4006**).

**RELEASE NOTE****Date:** 16-May-23**Subject:** Software changes, updates, bug fixes, etc.**Software:** Fortanix Data Security Manager SaaS**Version:** 4.17

- Fixed an issue in two-factor authentication where the modal window was not closing after approving a task (**JIRA: ROFR-4004**).
- Fixed an issue in the Salesforce easy wizard where the **Instance status** toggle was not getting disabled when clicked (**JIRA: ROFR-3996**).
- Fixed an issue where the user was able to see the custom roles without enabling the Custom Roles flag in the System Administration settings (**JIRA: ROFR-3992**).
- Fixed an issue where the Create group tutorial is shown even when you already have groups (**JIRA: ROFR-3981**).
- Fixed an issue where an empty label or value can be saved in **ATTRIBUTES/TAGS** tab for custom attributes (**JIRA: ROFR-3983**).
- Fixed an issue where the DSM UI does not support adding an existing plugin to a group when there is a quorum policy on the group (**JIRA: ROFR-3977**).
- Fixed an issue where the user was unable to create an ECKCDSA key with default values (**JIRA: ROFR-3974**).
- Fixed an issue where the user was getting a "Missing Cryptographic Policy in group" console error when clicking on the Apps page (**JIRA: ROFR-3964**).
- Fixed an issue where the "Copy API key" changed to "View API Key Details" after creating the Admin app (**JIRA: ROFR-3887**).
- Fixed an issue in DSM-Accelerator JCE where GCM, CCM, and OFB mode was not supported for AES encrypt or decrypt operation (**JIRA: PROD-6022**).
- Fixed an issue where the DataTable states selected in the filter were not retained during a screen refresh (**JIRA: ROFR-3233**).
- Fixed an issue where the **Pending Changes** message was not shown for a newly invited user (**JIRA: ROFR-4047**).

## RELEASE NOTE

**Date:** 16-May-23

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

**Software:** Fortanix Data Security Manager SaaS

**Version:** 4.17

- Fixed an issue that resulted in a "Token is invalid" message while validating the user's email in DSM (**JIRA: ROFR-4016**).
- Fixed an issue where the Quorum approval request was not being shown when viewing the DSM app API key if the group with quorum approval policy has approvers as users and an application (**JIRA: ROFR-3933**).

## KNOWN ISSUES

- 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**).
- Adding a key rotation policy to schedule key rotation for GCP BYOK keys is not supported (**JIRA: PROD: 6713**).

**Workaround:** You must manually rotate the key.

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

**Workaround:** You can manually copy the AES 256 key from a normal DSM group to a GCP-backed group.

- The "Rotate linked key" feature does not work where a Fortanix DSM source key is rotated along with its linked keys by choosing the "**Rotate linked keys**" check box, where the linked key might belong to a GCP group in which case rotating linked key results in rotating the key in GCP as well as generating the new key in GCP (**JIRA: ROFR: 4075**).

**Workaround:** You must first manually rotate the source key in the normal DSM group and then copy the rotated key to the GCP group.

- Saving Google Workspace CSE configuration using easy wizard results in an error in the UI, but the corresponding API call succeeds, and the



## RELEASE NOTE

**Date:** 16-May-23

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

**Software:** Fortanix Data Security Manager SaaS

**Version:** 4.17

configuration is saved successfully (**JIRA: ROFR: 4090**).

**Workaround:** Click **Cancel** to continue.

## 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

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 4.17