

RELEASE NOTES

Date: 28-May-24

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

Software: Fortanix Data Security Manager SaaS

Version: 4.28

OVERVIEW

This document provides an overview of new features, general improvements, and resolved issues in the Fortanix Data Security Manager (DSM) SaaS 4.28 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

- Removed the **Transparent Encryption Proxy (TEP)** wizard from the **Integrations** tab on Fortanix DSM. (**JIRA: ROFR-4795**).

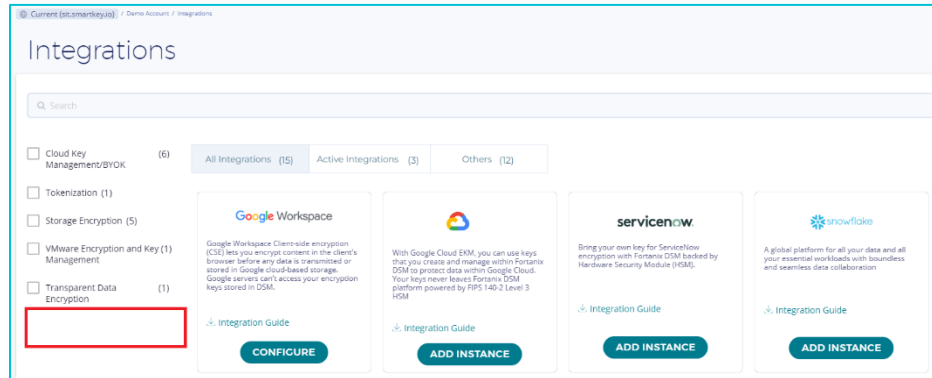


Figure 1: Removed TEP Wizard

DSM ACCELERATOR IMPROVEMENTS AND BUG FIXES

- **DSM Accelerator JCE Provider:**
 - Added support for Thin Jar bundled distribution in DSM Accelerator JCE Provider (**JIRA: PM-236**). For more details, refer to the [DSM JCE Client Downloads](#).

RELEASE NOTES

Date: 28-May-24

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

Software: Fortanix Data Security Manager SaaS

Version: 4.28

- Added local cache export support in DSM Accelerator JCE Provider (**JIRA: PROD-8473**). For more details, refer to the [Developer's Guide: DSM Accelerator JCE Provider](#).

- **DSM Accelerator Webservice:**

- Added local cache export support in DSM Accelerator Webservice (**JIRA: PROD-8473**). For more details, refer to the [Developer's Guide: DSM Accelerator Web Service](#).

KNOWN ISSUES

- When you edit the **starting time** of a Key rotation policy for a security object with the value as single digit time, for example: 01:00 am, it shows an error "**Invalid date/time selected. Please make sure you filled in a valid 12-hour time**" (**JIRA: ROFR-4786**).

Workaround: Re-enter the rotate start time by removing the "0" before the single digit time and enter a new time (e.g. 01:00 am to 2:00 am).

- After downgrading Fortanix DSM to version 4.25, it still shows the **Node size** field with a null value for LMS keys that were added in DSM version 4.26, even though the Node size is not a supported parameter in the older version (**JIRA: PROD-8278**).
- Unable to create an LMS key with the following height combinations of 20.
 - 5, 20, and vice versa
- The hyperlink color for the field "**Follow the instructions in**" in the "**Add Instance**" form for Google Workspace Client-Side Encryption (CSE) still reflects the old link color value (**JIRA: ROFR-4789**).

RELEASE NOTES

Date: 28-May-24

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

Software: Fortanix Data Security Manager SaaS

Version: 4.28



Figure 2: Client ID of CSE Application

- 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.

- 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.

RELEASE NOTES

Date: 28-May-24

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

Software: Fortanix Data Security Manager SaaS

Version: 4.28

- The `create` operation for security object creation does not work for the Azure Managed HSM plugin (**JIRA: PROD-7078**).
- 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.

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.

RELEASE NOTES

Date: 28-May-24

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

Software: Fortanix Data Security Manager SaaS

Version: 4.28

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 © 2024 Fortanix, Inc. All rights reserved.

Fortanix Data Security Manager SaaS Release Notes

Release 4.28