RELEASE NOTES

Date: 5-Mar-24

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

Software: Fortanix Data Security Manager SaaS

Version: 4.26

OVERVIEW

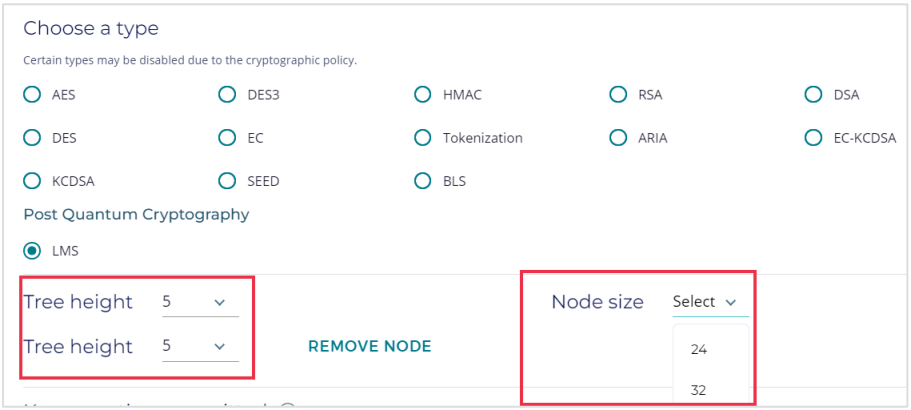
This document provides an overview of new features, general improvements, and resolved issues in the Fortanix Data Security Manager (DSM) SaaS 4.26 release.

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

- **Updated the LMS security object information in the generate security object flow** (**JIRA: PM-122**).
    - L1 and L2 height are now replaced by list of Heights **[h1, h2].**
    - The **Node size** field can have the value **24** or **32**.
    - The detailed view of an LMS key now shows the digest algorithm.
    - The KCV value in the LMS key detailed view is now removed.
    - The LMS variants now additionally supports:
        - Vanilla LMS (1-level HSS)
        - N24 and M24



Fortanix, Inc. | 3910 Freedom Circle | Suite 104 | Santa Clara, CA 95052 | +1 650.943.2484
info@fortanix.com
www.fortanix.com

RELEASE NOTES

Date: 5-Mar-24

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

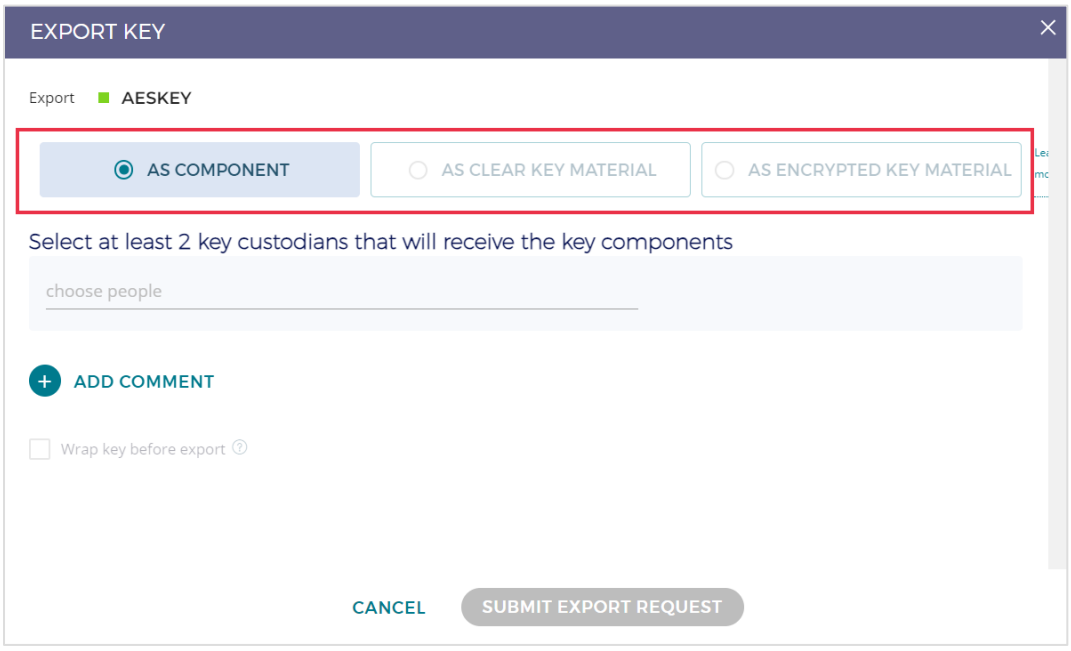
Software: Fortanix Data Security Manager SaaS

Version: 4.26

For more details, refer to LMS FAQ.

See Known Issues for a known issue related to this feature.

- **Combined the modal window for "direct key export" and "Export As Components/As Encrypted Key Material" into a single UI (JIRA: ROFR-4695).**



Fortanix, Inc. | 3910 Freedom Circle | Suite 104 | Santa Clara, CA 95052 | ☎ +1 650.943.2484
✉ info@fortanix.com
🌐 www.fortanix.com

RELEASE NOTES

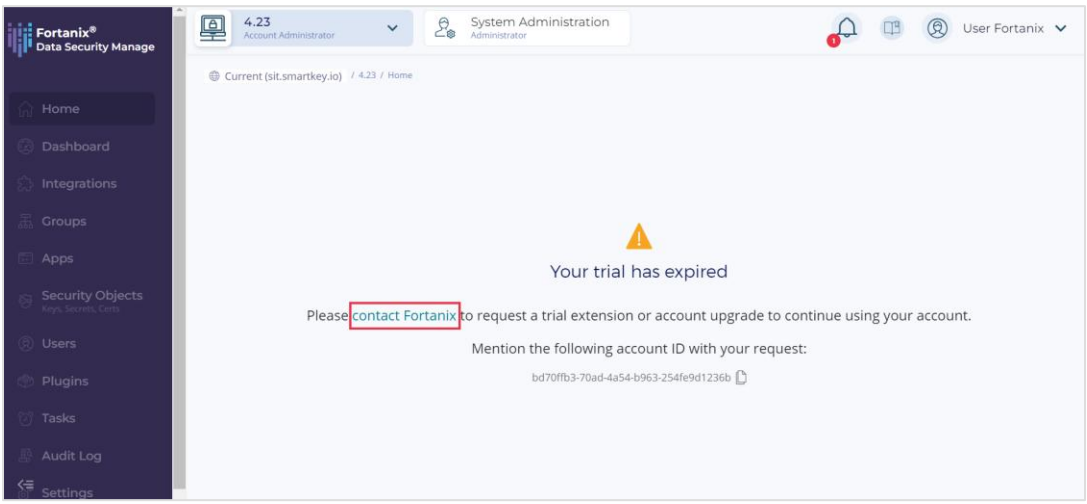
Date: 5-Mar-24

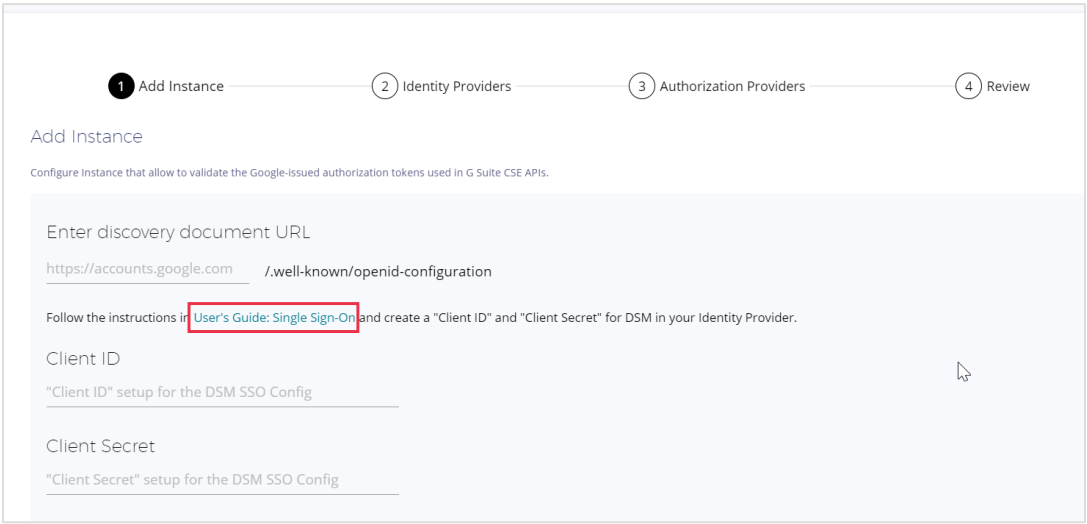
Subject: Software changes, updates, bug fixes, etc.

Software: Fortanix Data Security Manager SaaS

Version: 4.26

- **The copy operation for LMS key is removed since copying an LMS key might lead to repeated signing states and break security**. (**JIRA: PROD-6313**).
- **Replaced the hyperlinks in the DSM contact Fortanix UI and Google CSE UI with the new call to action (CTA) color #007A8D to make all the UI hyperlink color consistent (JIRA: ROFR-4697).**





See "Section: Known Issues" for links that are not updated to the new color.

OTHER IMPROVEMENTS

Fortanix, Inc. | 3910 Freedom Circle | Suite 104 | Santa Clara, CA 95052 | ☎ +1 650.943.2484
✉ info@fortanix.com
🌐 www.fortanix.com

RELEASE NOTES

Date: 5-Mar-24

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

Software: Fortanix Data Security Manager SaaS

Version: 4.26

- Disabled TLS resumption in TLS 1.2 and 1.3 **(JIRA: PROD-8242).**
- Improved the logic that checks whether DSM is in read-only mode and displays the banner **(JIRA: ROFR-4714)**.
- Fortanix DSM now allows HMAC Verify operation with AES key **(JIRA: PM-224)**.

DSM INTEGRATIONS

- Added support for Pure Storage integration with DSM **(JIRA: EXTREQ-1010**). *For more details, refer to DSM with Pure Storage Integration Guide*.

DSM ACCELERATOR IMPROVEMENTS AND BUG FIXES

- **DSM Accelerator JCE Provider:**
  - Added more detailed logging to DSM Accelerator JCE Provider client **(JIRA: PROD-8197)**. *For more details, refer to the Developer's Guide DSM Accelerator JCE Provider*.
  - Added support for configuring retry interval (`retry_for`) value in DSM Accelerator JCE Provider **(JIRA: PROD-7778)**. *For more details, refer to the Developer's Guide DSM Accelerator JCE Provider*.
  - Fixed retry logic in DSM Accelerator JCE Provider in case of intermittent connection breakages on the client end such as broken pipe or connection timeouts. A default retry duration of 30 seconds will be applied if not configured specifically **(JIRA: PROD-8046)**.
- **DSM Accelerator PKCS#11:**
  - Added support for configuring retry interval (`retry_for`) value in DSM Accelerator PKCS#11 **(JIRA: PROD-7777**). *For more details, refer to the Developer's Guide DSM Accelerator PKCS#11*.

BUG FIXES

Fortanix, Inc. | 3910 Freedom Circle | Suite 104 | Santa Clara, CA 95052 | ☎ +1 650.943.2484
✉ info@fortanix.com
🌐 www.fortanix.com

RELEASE NOTES

Date: 5-Mar-24

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

Software: Fortanix Data Security Manager SaaS

Version: 4.26

- Resolved an issue with importing single-height LMS keys **(JIRA: PROD-8247)**.
- Fixed an issue where a user was unable to restore an Azure-backed key after purging **(JIRA: PROD-7488)**.
- Fixed an issue where the user continued to receive "Trial has Expired" pop-up notifications for expired trial accounts **(JIRA: ROFR-4633)**.
- Fixed an issue where the user was unable to delete the key description from the key detailed view **(JIRA: ROFR-4672)**.
- Fixed an issue where wrapping an AES key with an RSA key during export was not sending the wrapping mode in the payload **(JIRA: ROFR-4698)**.
- Fixed an issue where the checkbox to confirm deleting key material of a reimported AWS key is not selected by default **(JIRA: ROFR-4701)**.
- Fixed an issue where the virtual keys in DSM did not have the cloud-side creation date (**JIRA: PROD-8061, PROD-8177**).
- Fixed an issue during key rotation where updating the key **Curve** while editing the key parameters did not automatically update the **Hashing Algorithm** and vice-versa (**JIRA: ROFR-4711**).
- Fixed an issue where when the user moves from one browser tab to another, the DSM account switcher always displays the account name from the previously selected tab in the new tab's account switcher (**JIRA: ROFR-4715**).
- Fixed an issue where the DSM UI results in an error when rotating linked AWS multi-region keys. The issue was fixed by disabling the AWS multi-region key rotation operation (**JIRA: ROFR-4721**).
- Fixed an issue where the **Origin IP Address** field was missing from the log entries that were sent to the Syslog Server (**JIRA: PROD-8116**).
- Fixed an issue where when a **Google Service Account** app is assigned to multiple groups, the credential object of the app is always overwritten by

Fortanix, Inc. | 3910 Freedom Circle | Suite 104 | Santa Clara, CA 95052 | ☎ +1 650.943.2484
✉ info@fortanix.com
🌐 www.fortanix.com

the recently updated or newly added groups `get_public_key` and `get_cryptospace_info` permissions instead of combining all the group permissions (**JIRA: ROFR-4750**).

- Fixed an issue on the LMS key generation screen where the node size did not show a default value of 24 (**JIRA: ROFR-4774**).
- Fixed an issue where the DSM user interface was unable to rotate an LMS key having only a single LMS tree height (**JIRA: ROFR-4775**).

KNOWN ISSUES

NEW 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).
- When a user creates an LMS key using the DSM API with `null` as the value of the node size, the detailed view of the key in the DSM UI shows the **Node size** value as empty, even though the system defaults to 32 if no value was provided (**JIRA: PROD-8246**).
- 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

Fortanix, Inc. | 3910 Freedom Circle | Suite 104 | Santa Clara, CA 95052 | ☎ +1 650.943.2484
✉ info@fortanix.com
🌐 www.fortanix.com

RELEASE NOTES

Date: 5-Mar-24

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

Software: Fortanix Data Security Manager SaaS

Version: 4.26

- 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**).

OLD ISSUES

- 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.

Fortanix, Inc. | 3910 Freedom Circle | Suite 104 | Santa Clara, CA 95052 | ☎ +1 650.943.2484
✉ info@fortanix.com
🌐 www.fortanix.com

RELEASE NOTES

Date: 5-Mar-24

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

Software: Fortanix Data Security Manager SaaS

Version: 4.26

- 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.
- 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, Inc. | 3910 Freedom Circle | Suite 104 | Santa Clara, CA 95052 | ☎ +1 650.943.2484
✉ info@fortanix.com
🌐 www.fortanix.com

RELEASE NOTES

Date: 5-Mar-24

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

Software: Fortanix Data Security Manager SaaS

Version: 4.26

Fortanix Data Security Manager SaaS Release Notes

Release 4.26

Fortanix, Inc. | 3910 Freedom Circle | Suite 104 | Santa Clara, CA 95052 | ☎ +1 650.943.2484

✉ info@fortanix.com

🌐 www.fortanix.com