Fortanix Data Security Manager Release Note

RELEASE NOTE

Date: 12-Sep-23

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

Software: Fortanix Data Security Manager

Version: 4.21.2284

OVERVIEW

This document provides an overview of new improvements and known issues in the Fortanix Data Security Manager (DSM) SaaS 4.21.2284 release.

NOTE:

- This release is for SaaS only and is not available for on-premises installations.

IMPROVEMENTS

- Updated AIC BIOS to version ATLK0061 and Gigabyte BIOS to version F14 in the Fortanix DSM installer **(JIRA: DEVOPS-4217).**
- Added checks to see if the Key Attestation Authority Certificates are signed by the correct Root CAs **(JIRA: PROD-7243).**
- Added support to re-issue attestation statement if the Key Attestation Authority Certificate is renewed **(JIRA: PROD-7475).**

KNOWN ISSUES

- The DSM login page is shown briefly after performing an SSO login **(JIRA: ROFR-4148)**.
- 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**).
- Unable to create an app when a Custom Group Role has the **Create Apps** permission enabled. This affects users who need to create App or Plugin entries (**JIRA: PROD-5764**).

Fortanix, Inc. | 44 Castro St #305| Mountain View, CA 94041| ☎ +1 628.400.2043
✉ info@fortanix.com
🌐 www.fortanix.com

RELEASE NOTE

Date: 12-Sep-23

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

Software: Fortanix Data Security Manager

Version: 4.21.2284

Workaround: use the predefined Administrative User definition under Settings.

- 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.
- 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**).
- Error during DSM login in a new or existing cluster (**JIRA: ROFR-4370**).

Fortanix, Inc. | 44 Castro St #305| Mountain View, CA 94041| ☎ +1 628.400.2043
✉ info@fortanix.com
🌐 www.fortanix.com

RELEASE NOTE

Date: 12-Sep-23

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

Software: Fortanix Data Security Manager

Version: 4.21.2284

Workaround: In the browser developer tools, clear the **auth.accountId** field from Local storage.

- After logging in to Fortanix DSM, you will see an additional region mentioned in the DSM UI breadcrumbs navigation **(JIRA: ROFR-4390)**.

For a complete list of new features, enhancements to existing features, other improvements, bug fixes, and known issues refer to the full description of the DSM 4.21 release note.

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 System Administrator accounts.
- Enable daily backups for the cluster.

SUPPORT

For any questions regarding this release note, please contact support@fortanix.com

DISCLAIMERS

Fortanix, Inc. | 44 Castro St #305| Mountain View, CA 94041| ☎ +1 628.400.2043
✉ info@fortanix.com
🌐 www.fortanix.com

RELEASE NOTE

Date: 12-Sep-23

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

Software: Fortanix Data Security Manager

Version: 4.21.2284

Fortanix Data Security Manager Release Notes

Release 4.21.2284

Fortanix, Inc. | 44 Castro St #305| Mountain View, CA 94041| ☎ +1 628.400.2043

✉ info@fortanix.com

🌐 www.fortanix.com