

## RELEASE NOTE

**Date:** 9-Sep-23

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

**Software:** Fortanix Data Security Manager

**Version:** 4.19.2244

## OVERVIEW

This document provides an overview of bug fixes and known issues in the Fortanix Data Security Manager (DSM) SaaS 4.19.2244 release.



### WARNING:

- You are **REQUIRED** to upgrade Fortanix DSM to version 4.13 or 4.16 before upgrading to version 4.19.2244. If you want to upgrade to 4.19.2244 from an earlier version, please reach out to the Fortanix Support team.
- Downgrading from Fortanix DSM version 4.19.2244 to any lower version is not possible.



### 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.
- 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

## IMPROVEMENTS

- Updated AIC BIOS to version ATLK0061 and Gigabyte BIOS to version F14 in the Fortanix DSM installer (**JIRA: DEVOPS-4217**).
- Fixed a node join issue when a new node is joined to an existing cluster (**JIRA: DEVOPS-4252**).

## RELEASE NOTE

**Date:** 9-Sep-23

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

**Software:** Fortanix Data Security Manager

**Version:** 4.19.2244

## KNOWN ISSUES

- The sync key API returns a “400 status code and response error” if its short-term access token expires during 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 normal DSM group and then copy the rotated key to the GCP group.

- An Azure Managed HSM external KMS group now also allows the following security object types to be generated or imported. But the Bring Your Own Key (BYOK) and rotate key functionality does not work for these security object types (**JIRA: ROFR-4192**).
  - EC
  - AES 128 and AES 192

**Workaround:** Do not generate or import security objects of type EC, AES 128, or AES 192 in an external KMS group of type Azure Managed HSM

## RELEASE NOTE

**Date:** 9-Sep-23

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

**Software:** Fortanix Data Security Manager

**Version:** 4.19.2244

since the only allowed security object types for an Azure key generated using the Generate or Import key workflows are:

- RSA key pairs ( RSA\_2048, RSA\_3072, and RSA\_4096).
  - AES 256
- The following security object types are not supported in Azure Managed HSM external KMS groups (**JIRA: ROFR-4187**).
  - DES
  - DES3
  - EC-KCDSA

**Workaround:** Do not generate or import security objects of type EC-KCDSA, DES, or DES3 in an external KMS group of type Azure Managed HSM since the only allowed security object types for an Azure key generated using the Generate or Import key workflows are:

- RSA key pairs ( RSA\_2048, RSA\_3072, and RSA\_4096).
  - AES 256
- 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.

- Unable to add Custom Attributes for a Fortanix DSM security object from its detailed view (**JIRA: ROFR-4252**).
  - Clicking the **ADD CUSTOM ATTRIBUTE** button does not load the **Label** and **Value** fields.

**Workaround:** Click the drop down for the “Custom attributes” section twice to load the Label and Value fields.

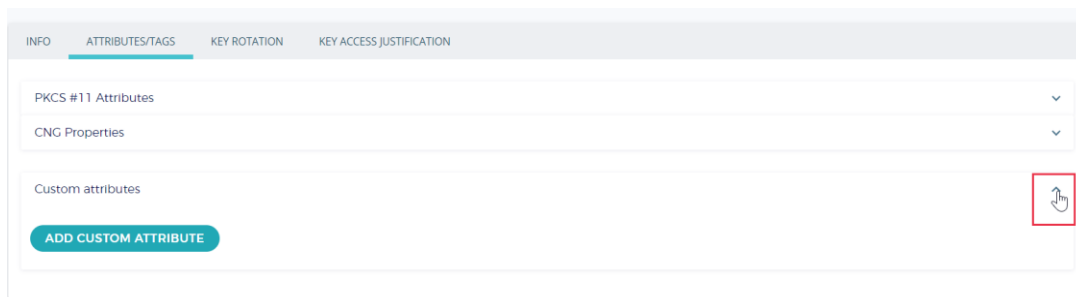
## RELEASE NOTE

**Date:** 9-Sep-23

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

**Software:** Fortanix Data Security Manager

**Version:** 4.19.2244



- When you type a label of the custom attribute, the text box loses focus.

**Workaround:** Enter the label of the custom attribute again for the second time to add the custom attribute successfully.

- 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**).
- Users will see the "Not a HSM group" error message while deleting the HSM/KMS group from the FIPS-backed group (**JIRA: ROFR-4245**).
- The `create` operation for security object creation does not work for the Azure Managed HSM plugin (**JIRA: PROD-7078**).
- The **AWS Key Policy** section alignment moved from the bottom of the security object detailed view to the right side of the page. This is a cosmetic issue only (**JIRA: ROFR-4241**).
- Users without two-factor authentication do not see the pop-up message “Unable to select this account. Reason: Two-factor authentication is required for this operation” when they select an account that has two-factor authentication configured (**JIRA: ROFR-4238**).
- The retry mechanism does not work as expected in the DSM-Accelerator Webservice (**JIRA: PROD-7068**).

## RELEASE NOTE

**Date:** 9-Sep-23

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

**Software:** Fortanix Data Security Manager

**Version:** 4.19.2244

- No error is displayed when the password length is specified as less than 8 digits in the **System Administration Settings** → **Minimum password length** section (**JIRA: ROFR-4234**).
- The **SUBMIT** button is not disabled when no Security Objects are selected or all security objects are in a disabled state and the user checks the **Rotate linked key** check box (**JIRA: ROFR-4233**).
- When hovering over a security object row in the **SECURITY OBJECTS** tab in the group detailed view, the blue row selection indicator appears too close to the check box for the row (**JIRA: ROFR-4232**).
- The UI labels in the **System Administrator Settings** → **Tasks** page are overlapping without the correct alignment (**JIRA: ROFR-4231**).
- The **SAVE CHANGES** button at the bottom of the **System Administration Settings** → **Email** page is disabled even when a value is provided for the field **Email for subscription update notifications** (**JIRA: ROFR-4229**).
- The Stats API GET operation does not get the "Total Operations" count correctly (**JIRA: PROD-7041**).
- Quoted special characters (for example, spaces) in e-mail addresses are not recognized in the search bar on the **System Administration Settings** → **Users** page (**JIRA: ROFR-4226**).
- After editing and saving the **System Administration Settings** → **Policies** page with the HSTS value disabled, the **HSTS** value still shows as enabled after the save (**JIRA: ROFR-4223**).
- When the Batch Sign operation is performed for **Curve Ed25519/X25519** in DSM-Accelerator Webservice, the status code is showing as 500 instead of 400 (**JIRA: PROD-7007**).
- The style of the **DELETE SELECTED**, **ENABLE LOGGING**, **DISABLE LOGGING**, **DESTROY SELECTED**, and **DOWNLOAD CSV** buttons is broken for the security object row in the Security Objects table (**JIRA: ROFR-4209**).

## RELEASE NOTE

**Date:** 9-Sep-23

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

**Software:** Fortanix Data Security Manager

**Version:** 4.19.2244

- If the email configuration is incorrect, clicking **RESEND VERIFICATION EMAIL** on the Fortanix DSM user interface (UI) will result in a 500 Internal Server Error from the `resend_confirm_email` API (**JIRA: PROD-9243**).



**TIP:** Before enforcing email confirmation, ensure the System Administrator's email has been confirmed. Otherwise, if the email configuration is incorrect, the administrator might get locked out of the system.

**Workaround:** Email verification is not enforced for the entire cluster; therefore, only a few users need to verify their emails. If the email configuration is incorrect, their accounts will remain accessible and not be blocked.

*For a complete list of new features, enhancements to existing features, other improvements, and bug fixes refer to the full description of the [DSM 4.19 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.
- Enable daily backups for the cluster.

## INSTALLATION

## RELEASE NOTE

**Date:** 9-Sep-23

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

**Software:** Fortanix Data Security Manager

**Version:** 4.19.2244

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.

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 Release Notes

Release 4.19.2244