

## RELEASE NOTE

**Date:** 29-Apr-22

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

**Software:** Fortanix Data Security Manager

**Version:** 4.6.2049

## OVERVIEW

This document provides an overview of the resolved issues and known issues in the Fortanix Data Security Manager (DSM) 4.6.2049 release.

This release is superseded by [May 16, 2022, release](#).



### WARNING:

- It is "REQUIRED" to upgrade Fortanix DSM to version 4.3 or 4.4 before upgrading to version 4.6.2049. If you want to upgrade to 4.6.2049 from an older version, please reach out to the Fortanix Customer Success team.
- Before downgrading Fortanix DSM from version 4.6. 2049 to older releases, remove all the IPv6 rules under the cluster IP-Policy setting.



### NOTE:

- After the software package is uploaded, the expected time to upgrade a 3-node cluster is about 1.5 to 2 hours from version 4.3 or 4.4 to 4.6.2049.

## BUG FIXES

1. Fixed an invalid API path while setting up Fortanix DSM for Google Workspace CSE (**JIRA: PROD-4491**).
2. Fixed IP whitelisting for IPV4 with App IP policy (**JIRA: PROD-4565**).
3. Fixed an issue where the App credentials (API key) cannot be viewed from the Fortanix DSM UI after quorum approval (**JIRA: ROFR-3176**).

## KNOWN ISSUES

- An account could be lost if account tables are inconsistent between nodes. Make sure a backup is successful before proceeding with ANY upgrade (**JIRA: PROD-4234**).
- When a node is removed from a 3-node cluster with build 4.2.2087, and the 2-node cluster is upgraded with build 4.3.xxxx, it is possible that the deploy

## RELEASE NOTE

**Date:** 29-Apr-22

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

**Software:** Fortanix Data Security Manager

**Version:** 4.6.2049

job is exited and marked completed before cluster upgrade (**JIRA:**

**DEVOPS-2068**).

Workaround: If all the pods are healthy, you can deploy the version again.

- 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**).

## 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.

## INSTALLATION

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)

**RELEASE NOTE****Date:** 29-Apr-22**Subject:** Software changes, updates, bug fixes, etc.**Software:** Fortanix Data Security Manager**Version:** 4.6.2049**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 © 2022 Fortanix, Inc. All rights reserved.

Fortanix Data Security Manager Release Notes

Release 4.6.2049