RELEASE NOTE

Date: 27-Feb-24

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

Software: Fortanix Data Security Manager

Version: 4.16.2367

OVERVIEW

This document provides an overview of bug fixes and known issues in the Fortanix Data Security Manager (DSM) 4.16.2367 release.

⚠ **WARNING**:

- You are **REQUIRED** to upgrade Fortanix DSM to version 4.11 or 4.13 before upgrading to version 4.16.2367. If you want to upgrade to 4.16.2367 from an older version, please reach out to the Fortanix Support team.
- After upgrading to version 4.16.2367, Fortanix DSM can **NO LONGER** be downgraded to any prior version. This is due to limitations of common infrastructure components such as Docker and Kubernetes.

📌 **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.

BUG FIXES

- Fixed an issue where, due to incorrect computation of leap year future dates, it will cause Fortanix Plugins to crash on February 29th, 2024 **(JIRA: PROD-8274).**

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

RELEASE NOTE

Date: 27-Feb-24

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

Software: Fortanix Data Security Manager

Version: 4.16.2367

For a complete list of new features, enhancements to existing features, other improvements, and bug fixes refer to the full description of the DSM 4.16 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.

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

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 NOTE

Date: 27-Feb-24

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

Software: Fortanix Data Security Manager

Version: 4.16.2367

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

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.

Fortanix Data Security Manager Release Notes

Release 4.16.2367