RELEASE NOTES

Date: 29-Jul-25

Subject: Software changes, updates, bug fixes, and so on.

Software: Fortanix Data Security Manager

Version: 5.0.2833.3149

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

OVERVIEW

This document provides an overview of improvements in the Fortanix Data Security Manager (DSM) 5.0.2833.3149 release.

WARNING:

- You are **REQUIRED** to upgrade Fortanix DSM to version 4.36 Patch 1 before upgrading to version 5.0.2833.3149.
    - However, due to the BIOS update, if you want to upgrade Fortanix DSM to version 5.0.2833.3149 from version 4.34 Patch 3, then you must follow the upgrade path 4.34 Patch 3 → 4.36 Patch 4 → 5.0.2833.3149.
    - If you want to upgrade Fortanix DSM to version 5.0.2833.3149 from a version earlier than 4.34, please contact the Fortanix Support team at your earliest to validate the upgrade path.
- Downgrade from 5.0.2833.3149 to any prior version is not supported due to an upgrade of the appliance operating system.

NOTE:

- If you are using a custom sudo user, ensure that the default **administrator** user is enabled with root privileges **before upgrading to Fortanix DSM version 5.0.2833.3149**. The **administrator** user must be able to log in with a password and be part of the sudo group. During the upgrade, the `/etc/sudoers` file is overwritten, which can result in the loss of sudo access for the custom sudo user.
- 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 before the Fortanix DSM software upgrade. If required, the BIOS version

RELEASE NOTES

Date: 29-Jul-25

Subject: Software changes, updates, bug fixes, and so on.

Software: Fortanix Data Security Manager

Version: 5.0.2833.3149

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

should be upgraded to the latest version and verified by Fortanix Support for a smooth upgrade.

- If your Fortanix DSM version is 4.31 or later, then the HSM Gateway version must also be 4.31 or later. Similarly, if the HSM Gateway version is 4.31 or later, then your Fortanix DSM version must be 4.31 or later.
- Do not remove a Fortanix DSM node during the upgrade to version 5.0.2833.3149. Please contact Fortanix Support in case of an error or issue.

IMPROVEMENTS

- Fortanix DSM now allows extending the default six-week grace period for trusting the last signed and published Trusted Computing Base (TCB) version for Azure DCv2 virtual machines (VMs) through a cluster-wide configurable setting. This setting only applies to customers who run clusters with hardware attestation enabled **(JIRA: PROD-10366)**.
- Updated the Fortanix DSM node `join-policy` to allow scalable platform support, enabling Azure DCv3 virtual machines (VMs) to join clusters previously restricted to DCv2 VMs. This only applies to customers who run Azure clusters with hardware attestation enabled. **(JIRA: PROD-10364)**.
- Updated AST 2500 firmware for Series 2 Gigabyte Baseboard Management Controllers (BMCs) to version 12.72.04 to address the vulnerability outlined in the American Megatrends International (AMI) Security Advisory (AMI-SA-2025003) **(JIRA: PROD-10104)**.

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 5.0 release notes.

RELEASE NOTES

Date: 29-Jul-25

Subject: Software changes, updates, bug fixes, and so on.

Software: Fortanix Data Security Manager

Version: 5.0.2833.3149

INSTALLATION

To install the DSM Runtime Encryption® SGX (on-prem/Azure) and Software (AWS/Azure/VMWare) packages, Download Here..

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 Data Security Manager Release Notes

Release 5.0.2833.3149

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

✉ info@fortanix.com

🌐 www.fortanix.com