Fortanix Data Security Manager Release Note

RELEASE NOTE

Date: 27-Mar-23

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

Software: Fortanix Data Security Manager

Version: 4.19

OVERVIEW

This document provides an overview of new features, improvements, and resolved issues in the Fortanix Data Security Manager (DSM) 4.19 release.

This release is superseded by September 09, 2023 release.

WARNING:

- You are **REQUIRED** to upgrade Fortanix DSM to version 4.13 or 4.16 before upgrading to version 4.19. If you want to upgrade to 4.19 from an earlier version, please reach out to the Fortanix Support team.
- Downgrading from Fortanix DSM version 4.19 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.

NEW FEATURES

1. Added Single Sign-On support for System Administration accounts (**JIRA: ROFR-3094**).

   This release adds support for configuring the following SSO integrations in DSM:

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

RELEASE NOTE

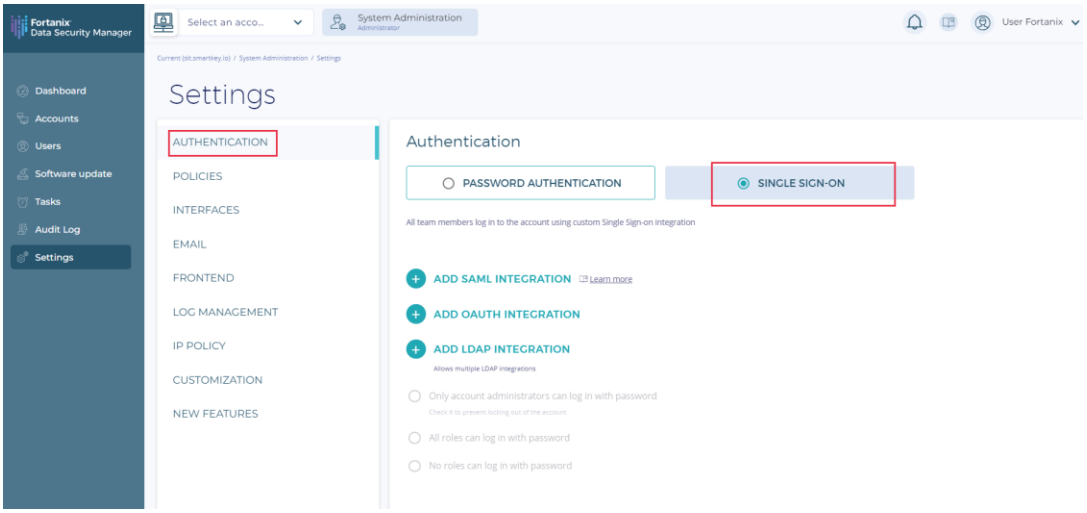
Date: 27-Mar-23

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

Software: Fortanix Data Security Manager

Version: 4.19

- SAML
- OAUTH
- LDAP



For more details, refer to System Administration Settings: Authentication.

ENHANCEMENTS TO EXISTING FEATURES

1. **Added UUID validation for Client ID in the "OAuth Client" Configuration section under the System Administration Policies settings page (JIRA: ROFR-4082).**
2. **Disabled linked and copied security objects that belong to external HSM or external KMS groups other than AWS and Azure from the list for the "Rotate linked keys" feature (JIRA: ROFR-4141).**
3. **Added support to display the "Total number of DSM applications created" on the System Administration Accounts detailed view (JIRA: ROFR-4120).**

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

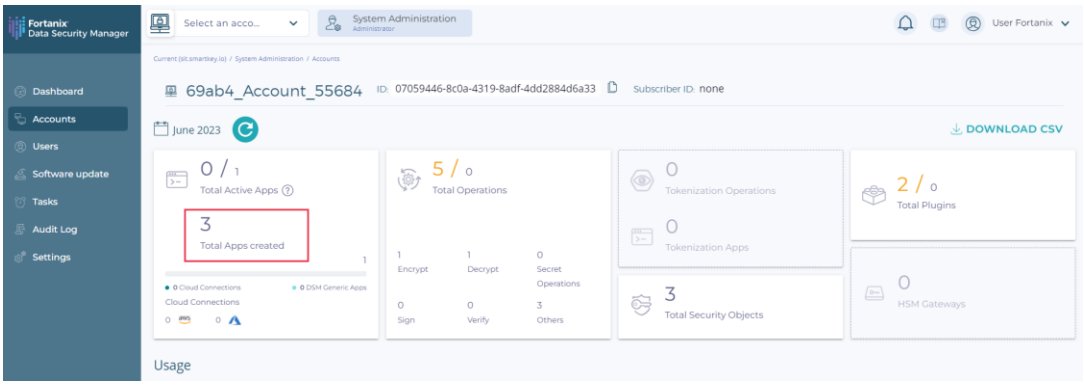
RELEASE NOTE

Date: 27-Mar-23

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

Software: Fortanix Data Security Manager

Version: 4.19



OTHER IMPROVEMENTS

- **Implemented a generic Batch API to call multiple APIs in sequence (JIRA: PROD-6589).**
    - Added audit logs for all the APIs under the Generic Batch API (**JIRA: PROD-3991**).
- **Added support to package and install `nvmupdate64e` in the Fortanix DSM installer (JIRA: DEVOPS-3969).**
- **Improved precheck procedure to be performed before the DSM software upgrade (JIRA: DEVOPS-4052).** *For more details, refer to Fortanix DSM Software Upgrade Manual Prechecks guide.*
- **Disallowed accidentally sending sensitive user data through the `EmailReverfication` form (JIRA: ROFR-4170).**
- **The Sensu monitoring server artifacts are now updated with containerd (JIRA: DEVOPS-3834).**
- **Improved audit log purging by making it more robust (JIRA: PROD-5921).**
- **Added support to configure the `prompt` value for OAuth using the DSM REST API (JIRA: PROD-5726).**
- **Added email confirmation for self-provisioning in the System Administration settings if the email was not already verified (JIRA: PROD-4609).**
- **Added support for "first" in the BGP neighbor IP calculation method (JIRA: DEVOPS-3716).**

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-Mar-23

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

Software: Fortanix Data Security Manager

Version: 4.19

- **With the 4.19 release, for new customers setting up Google CSE integration, all users who are invited to use the CSE feature must accept the Fortanix DSM account invitation and verify their email address. This restriction is temporary and will be removed in a future release (JIRA: PROD-6752).**

  NOTE: For existing customers using the Google CSE Workspace feature, users need not verify their email address to use this feature.

INTEGRATIONS/USE CASES

- **Implemented procedural verification of key-pair origin and provenance (JIRA: PROD-6758).** *For more details, refer to Fortanix DSM for Verification of Key Pair Origin and Provenance.*
- **Added support for DSM with Venafi – Keyless TLS integration (JIRA: EXTREQ-697**). *For more details, refer to Fortanix DSM with Venafi -Keyless TLS guide.*
- **Added support for DSM with Keyfactor IIS Orchestrator integration (JIRA: EXTREQ-421**). *For more details, refer to Fortanix DSM with Keyfactor IIS Orchestrator guide.*
- **Added support for DSM with Microsoft SQL Server TDE Always Encrypted Database (JIRA: PROD-6350).** *For more details, refer to Fortanix DSM with Microsoft SQL Server – Always Encrypted.*

CLIENT IMPROVEMENTS

- **Added support for the FF1 format-preserving encryption mode for tokenization in the DSM JCE Provider (JIRA: PROD-6869).** *For more details, refer to Developer's Guide: Client - JCE Provider.*
- **Added support for adding IP addresses in PKCS#11 configuration for `api_endpoint` (JIRA: PROD-6684).**

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-Mar-23

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

Software: Fortanix Data Security Manager

Version: 4.19

- **Published the Microsoft CNG/EKM Provider client (Windows 32-bit Installer) (JIRA: PROD-6714).** *For more details, click here.*
- **Added support for verifying signatures in Windows CNG client (JIRA: PROD-6921).**

DSM-ACCELERATOR IMPROVEMENTS

- **DSM-Accelerator JCE Provider:**
    - **Added support for the FF1 format preserving encryption mode for tokenization in the DSM-Accelerator JCE Provider (JIRA: PROD-6869).** *For more details, refer to the Developer's Guide: Fortanix DSM-Accelerator JCE Provider.*
    - **Improved log messages for detailed logging of encryption and decryption operations in the DSM-Accelerator JCE Provider (JIRA: PM-12).**
- **DSM-Accelerator Webservice:**
    - **Added Guidelines to persist logs for DSM-Accelerator Webservice (JIRA: PROD-5641).**

      For more details, refer to the Administration Guide: Fortanix DSM-Accelerator Webservice External logging Setup Guide.
    - **Improved log messages for detailed logging of encryption and decryption operations in the DSM-Accelerator Webservice (JIRA: PM-12).**
    - **Added support for Batch Sign and Batch Verify operations in DSM-Accelerator Webservice (JIRA: PROD-6849).**

      For more details, refer to the Developer's Guide: Fortanix DSM-Accelerator Webservice.
- **DSM-Accelerator PKCS#11:**

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-Mar-23

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

Software: Fortanix Data Security Manager

Version: 4.19

- **Improved log messages for detailed logging of encryption and decryption operations in the DSM-Accelerator PKCS#11 (JIRA: PM-12).**

QUALITY ENHANCEMENTS/UPDATES

- **Moved to cert manager and deployed on Kubernetes 1.21.14 (JIRA: DEVOPS-3586).** *For post-upgrade checks after migrating to cert manager, refer to Fortanix DSM post upgrade checks guide.*

BUG FIXES

- Fixed an issue in the **System Administration Settings → Policies** page where empty text field validation was performed for each key press (**JIRA: ROFR-4127**).
- Fixed an issue where the **System Administration Settings → Accounts** page did not list any accounts (**JIRA: ROFR-4125)**.
- Fixed an issue in the **System Administration Settings → Policies → Minimum password length** section where setting the values for **Max sequence** and **Max repetition** was not shown after saving (**JIRA: ROFR-4076**).
- Fixed an issue where rotating the Kubernetes certificates within the cluster failed (**JIRA: DEVOPS-3995**).
- Fixed the user lockout issue that occurs when there are many parallel requests (**JIRA: PROD-6712**).
- Fixed an issue where the `sdkms-cluster remove` command took a long time to execute (**JIRA: DEVOPS-3787**).
- Fixed an issue where the GET operation for KMIP fails for HMAC keys (**JIRA: PROD-5518**).
- Fixed a page crash when users or groups are filtered by their Description field (**JIRA: ROFR-4218**).

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-Mar-23

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

Software: Fortanix Data Security Manager

Version: 4.19

- Updated the auto-generated Cassandra Cert-Manager CA validity period from 90 days to 10 years (**JIRA: DEVOPS-4046**).
- Fixed an issue where `AuditLogTime` API had an incorrect example in the Open API output (**JIRA: PROD-6998**).
- Fixed a page crash in the "Add application" flow when selecting the option "**Set app secret key size**" (**JIRA: ROFR-4194**).
- Fixed an issue where self-provisioned users did not need to be verified to join a DSM account when user verification was required (**JIRA: PROD-6943**).
- Fixed an issue where the style of the pagination component was broken in the Security Objects table (**JIRA: ROFR-4180**).
- Fixed an issue where new DSM account creation failed after selecting an expired DSM SaaS Trial account (**JIRA: PROD-6891**).
- Fixed an issue where creating a security object of type EC in an existing FIPS-backed group showed the curve type as "(Unknown)" (**JIRA: ROFR-4166**).
- Fixed an issue on the Security Object list page where the text "Please enter a valid value" was not going away after removing the invalid value for search parameters such as Elliptic Curve, UUID, State, and so on. (**JIRA: ROFR-4162**).
- Fixed an issue where, after creating a security object with an Azure Tag, there was no edit button to modify the Azure Tag (**JIRA: ROFR-4159**).
- Fixed an issue in the user's profile page where the message "When changing your email, all of your pending account invites will be removed." was shown even when email confirmation was not enforced (**JIRA: ROFR-4157**).

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-Mar-23

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

Software: Fortanix Data Security Manager

Version: 4.19

- Fixed an issue where after creating a Snowflake integration using the easy wizard, the "View API Key Details" button label did not change to "Copy API Key" (**JIRA: ROFR-4145**).
- Fixed an issue where the **System Administration Settings → Policies → Security parameters**: **HTTP Strict Transport Security (HSTS)** field was shown as selected even when it was disabled (**JIRA: ROFR-4132**).
- Fixed an issue where the disabled toggle in the Email Configuration shows as "Email enabled" (**JIRA: ROFR-4128**).
- Fixed an issue where **System Administration Settings → Policies → Email Validation Policies** was not shown after saving (**JIRA: ROFR-4123**).
- Improved the description that appears when the user hovers their mouse pointer over an HSM/KMS group icon in the Copy Key modal window when copying a key from the HSM group to an HSM/External KMS group (**JIRA: ROFR-4122**).
- Improved the tooltip that appears when the user hovers their mouse pointer over an HSM/KMS group icon in the Groups table (**JIRA: ROFR-4121**).
- Fixed an issue when deactivating the key where the CPU utilization was showing 100% for the Cassandra process (**JIRA: PROD-6788**).
- Fixed an issue where the DSM backend incorrectly normalizes audit log range queries (**JIRA: PROD-6759**).
- Fixed a "Failed to load items" error that was briefly displayed when moving from the Security Objects page to the System Administration Settings page (**JIRA: ROFR-4079**).
- Fixed an issue where the user was able to add unverified users to the account Quorum approval policy (**JIRA: PROD-6708**).

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-Mar-23

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

Software: Fortanix Data Security Manager

Version: 4.19

- Fixed an issue where the editing or adding an alias in AWS for a DSM-managed AWS key did not replicate that addition or update to DSM (**JIRA: ROFR-4063**).
- Fixed an issue where multiple users could be created with e-mail addresses that should normalize to the same value (for example: differed only in uppercase/lowercase letters) (**JIRA: PROD-6594**).
- Fixed an issue where reusing the same CAPTCHA for signup resulted in a 500 error instead of a 400-range error. Reusing prior CAPTCHA response information is not supported (**JIRA: PROD-6536**).
- Fixed an issue where during an upgrade to DSM version 4.18, the first deploy pod goes to error state (**JIRA: DEVOPS-4008**).
- Fixed an issue where users were unable to confirm their email during the email verification workflow (**JIRA: ROFR-4243**).
- Fixed a multi-factor authentication (MFA) issue for devices registered before July 2022 **(JIRA: SOPS-255)**.

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**).
- 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**). Workaround: use the predefined Administrative User definition under Settings.

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-Mar-23

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

Software: Fortanix Data Security Manager

Version: 4.19

- 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 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

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-Mar-23

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

Software: Fortanix Data Security Manager

Version: 4.19

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:

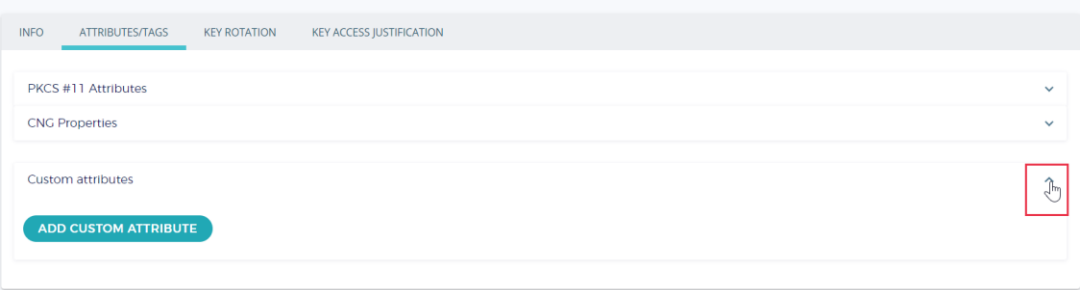
- RSA key pairs (RSA_2048, RSA_3072, and RSA_4096).
- AES 256

- 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.



  - 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.

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-Mar-23

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

Software: Fortanix Data Security Manager

Version: 4.19

- 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**).
- 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**).

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-Mar-23

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

Software: Fortanix Data Security Manager

Version: 4.19

- 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**).

FORTANIX DATA SECURITY MANAGER PERFORMANCE STATISTICS

- **Series 2**

KEY TYPES AND OPERATIONS	THROUGHPUT (Operations/second on a 3-node cluster)
AES 256: CBC Encryption/Decryption	4,402/4,441
AES 256: GCM Encryption/Decryption	4,380/4,326
AES 256: FPE Encryption/Decryption	2,150/2,139
AES 256 Key Generation	1,139

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-Mar-23

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

Software: Fortanix Data Security Manager

Version: 4.19

KEY TYPES AND OPERATIONS	THROUGHPUT (Operations/second on a 3-node cluster)
RSA 2048 Encryption/Decryption	3814/1,027
RSA 2048 Key Generation	30
RSA 2048 Sign/Verify	1,045/3,777
EC NISTP256 Sign/Verify	976/573
Data Security Manager Plugin (Hello world plugin)	1753 (invocations/second)

- **Azure Standard_DC8_v2**

KEY TYPES AND OPERATIONS	THROUGHPUT (Operations/second on a 3-node [Standard_DC8_v2] cluster)
AES 256: CBC Encryption/Decryption	3,768/3,755
AES 256: GCM Encryption/Decryption	3,728/3,726
AES 256: FPE Encryption/Decryption	2.067/2,037
AES 256 Key Generation	923
RSA 2048 Encryption/Decryption	3,420/1,169
RSA 2048 Key Generation	42
RSA 2048 Sign/Verify	1,162/3,507
EC NISTP256 Sign/Verify	917/533
Data Security Manager Plugin (Hello world plugin)	1735 (invocations/second)

- **Series 2 JCE**

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-Mar-23

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

Software: Fortanix Data Security Manager

Version: 4.19

KEY TYPES AND OPERATIONS	THROUGHPUT (Operations/second on a 3-node cluster)
AES 256: CBC Encryption/Decryption	3,546/3,557
AES 256 Key Generation	1,087
RSA 2048 Key Generation	30
RSA 2048 Sign/Verify	851/1,856
EC NISTP256 Sign/Verify	811/504
Data Security Manager Plugin (Hello world plugin)	1644 (invocations/second)

- **Azure Standard_DC8 JCE**

KEY TYPES AND OPERATIONS	THROUGHPUT (Operations/second on a 3-node [Standard_DC8 JCE] cluster)
AES 256: CBC Encryption/Decryption	3,556/3,603
AES 256 Key Generation	945
RSA 2048 Key Generation	42
RSA 2048 Sign/Verify	911/1,843
EC NISTP256 Sign/Verify	763/486
Data Security Manager Plugin (Hello world plugin)	1,693 (invocations/second)

FORTANIX DATA SECURITY MANAGER – ACCELERATOR PERFORMANCE STATISTICS

- **Runtime Environment**

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-Mar-23

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

Software: Fortanix Data Security Manager

Version: 4.19

NOTE:

- The following table lists the standard recommended runtime environment. You can choose a higher configuration for better performance.
- DSM-Accelerator was run in the runtime environment listed below for performance testing.

ITEM	SPECIFICATION
Number of Cores	4
CPU	Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz
RAM	32 GiB

- **DSM-Accelerator Webservice**

NOTE: The performance numbers below are captured with a single node; if you need higher performance or throughput, then we recommend adding multiple nodes.

KEY TYPES AND OPERATIONS	THROUGHPUT (Operations/second on a 1-node cluster)
AES 256: CBC Encryption/Decryption	12,848/12,834
AES 256: GCM Encryption/Decryption	13,228/13,235
AES 256: FPE Encryption/Decryption	4,850/4,806

- **Additional Modes**

KEY TYPES AND OPERATIONS	THROUGHPUT (Operations/second on a 1-node cluster)
AES 256: CBCNOPAD Encryption/Decryption	11,528/11,421
AES 256: CFB Encryption/Decryption	13/491/13,458
AES 256: CTR Encryption/Decryption	13,444/13,550

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-Mar-23

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

Software: Fortanix Data Security Manager

Version: 4.19

KEY TYPES AND OPERATIONS	THROUGHPUT (Operations/second on a 1-node cluster)
AES 256: OFB Encryption/Decryption	13,490/12,631

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

RELEASE NOTE

Date: 27-Mar-23

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

Software: Fortanix Data Security Manager

Version: 4.19

Fortanix Data Security Manager SaaS Release Notes

Release 4.19

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

✉ info@fortanix.com

🌐 www.fortanix.com