# Fortanix Data Security Manager Release Note

## RELEASE NOTE

**Date:** 13-Apr-22

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

**Software:** Fortanix Data Security Manager

**Version**: 4.6

## OVERVIEW

This document provides an overview of new features, general enhancements, improvements, and resolved issues in the Fortanix Data Security Manager (DSM) 4.6 release.

This release is superseded by April 29, 2022, release.

**WARNING**:

- It is "REQUIRED" to upgrade Fortanix DSM to version 4.3 or 4.4 before upgrading to version 4.6. If you want to upgrade to 4.6 from an older version, please reach out to the Fortanix Customer Support team.
- Before downgrading Fortanix DSM from version 4.6 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.

## NEW FUNCTIONALITY / FEATURES

1. **Support for Key generation/Bring Your Own Key (BYOK) in Azure HSM for Premier Tier Key Vaults. (JIRA: ROFR-2950):**

   This release adds support for Azure Premium key vaults which include HSM-protected keys that can be created to be Software-protected or Hardware-protected keys.

Fortanix, Inc. | 44 Castro St #305| Mountain View, CA 94041| +1 628.400.2043
info@fortanix.com
www.fortanix.com

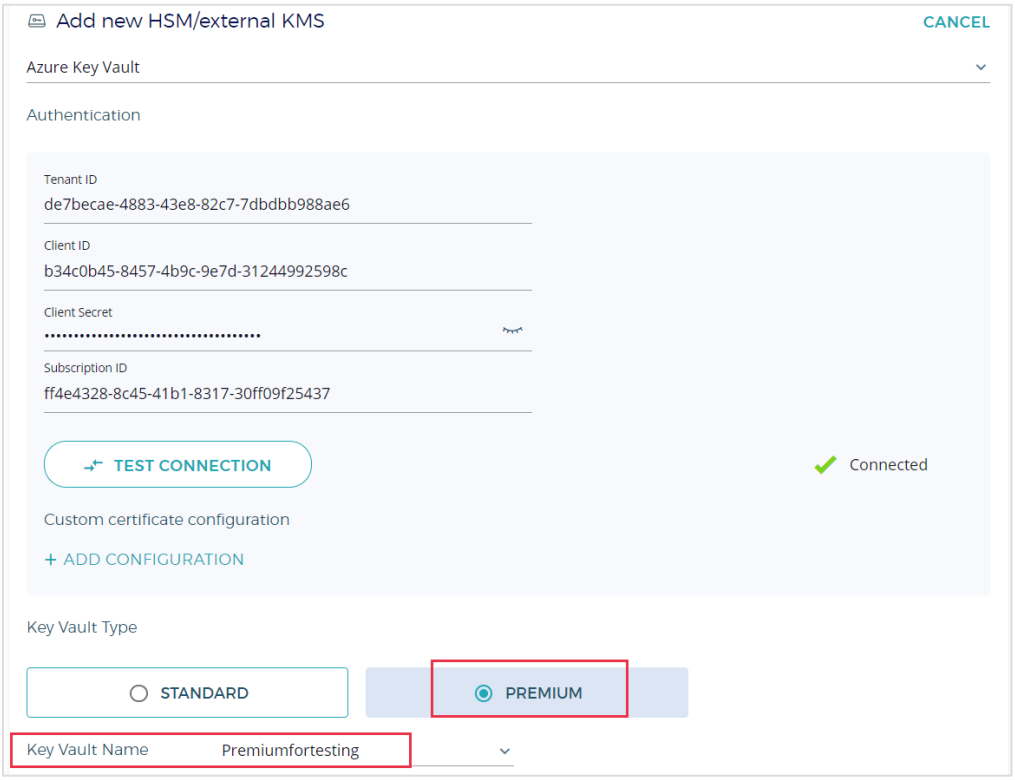
**RELEASE NOTE**

**Date:** 13-Apr-22

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

**Software:** Fortanix Data Security Manager

**Version**: 4.6




*For more details, refer to User's Guide: Azure Key Vault.*

2. **Group based on Azure Managed HSM and Bring Your Own Key (BYOK) for Azure Managed HSM. (JIRA: ROFR-3026):**

   With the Fortanix DSM 4.6 release, Azure Managed HSM is added to the list of supported Key Management Systems in HSM/external KMS groups. This release supports the management of keys in Azure-managed HSMs that supports HSM-protected keys. Fortanix DSM now allows to:

   - Configure an Azure Managed HSM group in Fortanix DSM.
   - Generate, Import, and Copy key (BYOK) into Azure Managed HSM.
   - Rotate keys in the Azure Managed HSM group. This allows users to rotate keys natively in Azure Managed HSM.
   - Soft delete key deletion in Azure Managed HSM.

Fortanix, Inc. | 44 Castro St #305| Mountain View, CA 94041| ☎ +1 628.400.2043
✉ info@fortanix.com
🌐 www.fortanix.com

**RELEASE NOTE**

**Date:** 13-Apr-22

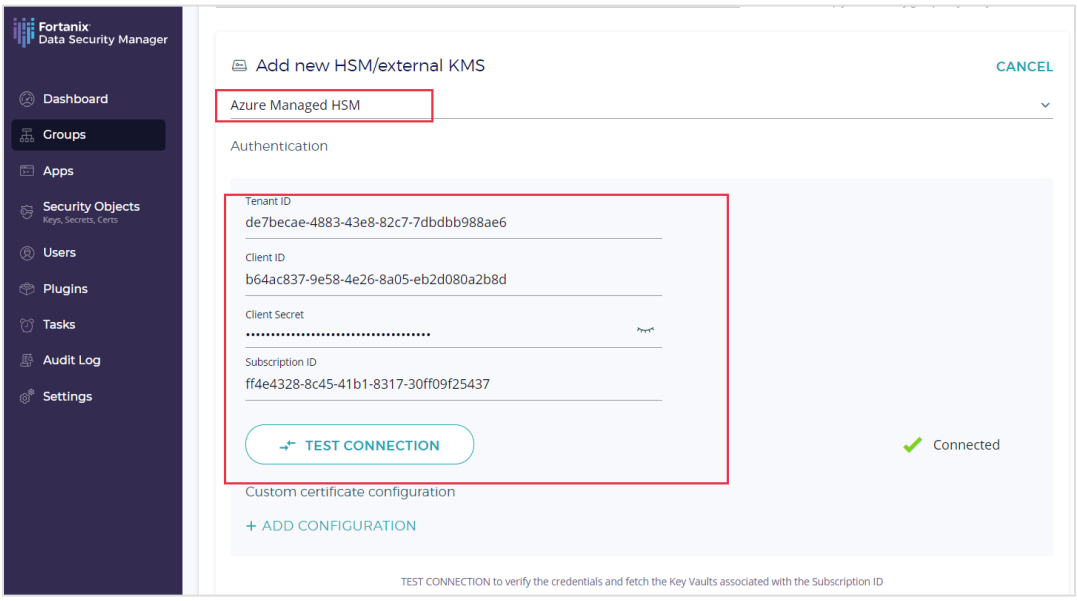
**Subject:** Software changes, updates, bug fixes, etc.

**Software:** Fortanix Data Security Manager

**Version**: 4.6

Fortanix, Inc. | 44 Castro St #305| Mountain View, CA 94041| ☎ +1 628.400.2043
✉ info@fortanix.com
🌐 www.fortanix.com

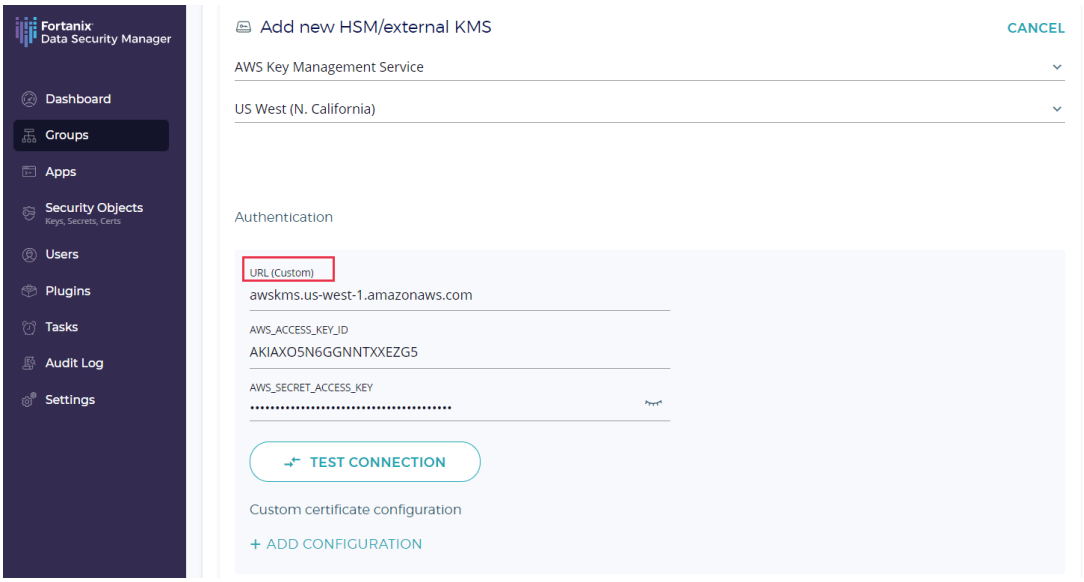
- Enable/Disable keys in Azure Managed HSM directly.




*For more details refer to the User's Guide: Azure Managed HSM.*

3. **Support Custom AWS KMS URL (JIRA: ROFR-3071):**

   This release adds Custom URL support for the AWS region. In the case of a custom URL, the **URL** label will change to **URL (Custom)**.




*For more details, refer to User's Guide: AWS Key Management Service.*

4. **Client Configuration Support in Account Settings (JIRA: ROFR-2776)**: You can now set the default configurations for clients such as PKCS#11 and

**RELEASE NOTE**

**Date:** 13-Apr-22

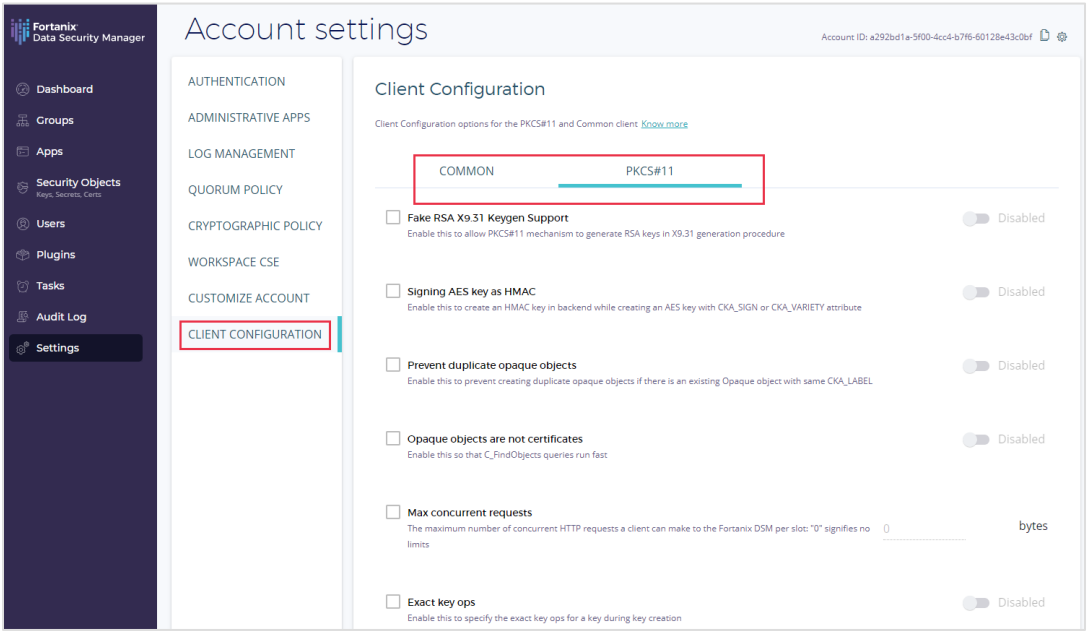
**Subject:** Software changes, updates, bug fixes, etc.

**Software:** Fortanix Data Security Manager

**Version**: 4.6

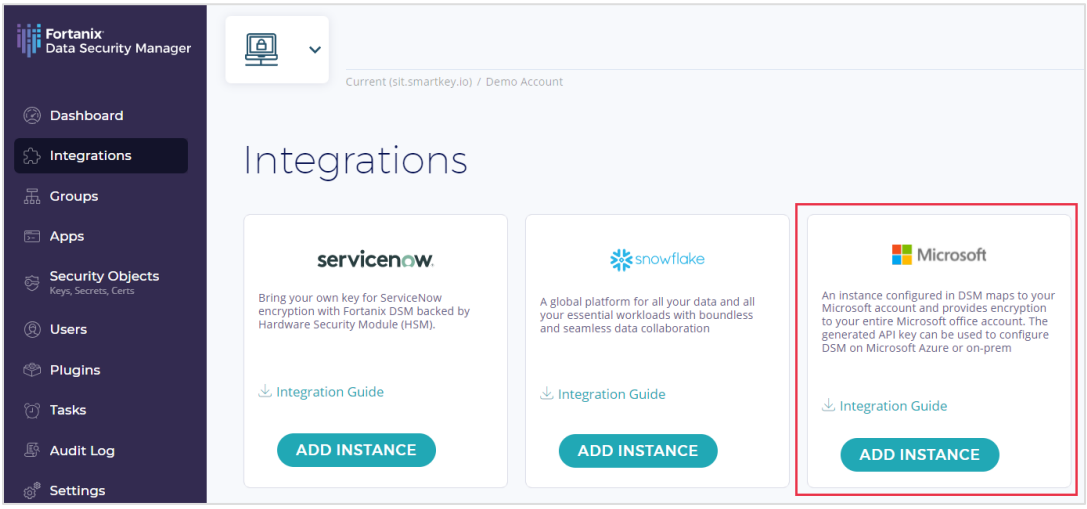
Fortanix, Inc. | 44 Castro St #305| Mountain View, CA 94041| ☎ +1 628.400.2043
✉ info@fortanix.com
🌐 www.fortanix.com

Common clients on the Fortanix DSM Account Settings page. This makes it simpler to configure many clients.




*For more details, refer to the User's Guide: Client Configuration.*

5. **Easy button wizard for Microsoft DKE integration (JIRA: ROFR-3041)**: You can now configure and integrate Fortanix DSM SaaS solution with Microsoft DKE service for customer managed encryption keys.




*For more details, refer to the Use Case Guide: Microsoft DKE integration.*

**RELEASE NOTE**

**Date:** 13-Apr-22

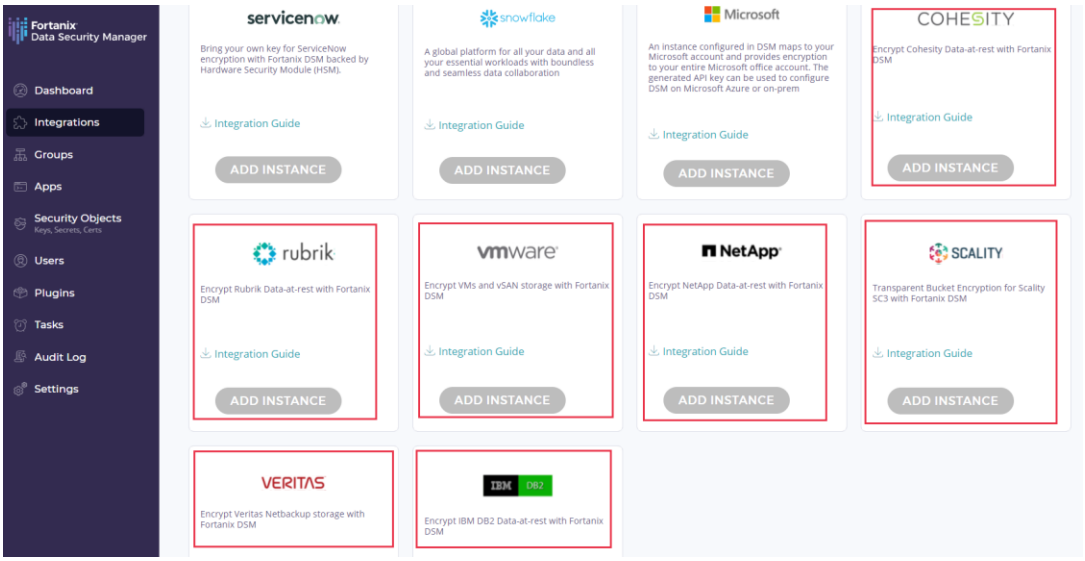
**Subject:** Software changes, updates, bug fixes, etc.

**Software:** Fortanix Data Security Manager

**Version**: 4.6

6. **Easy button wizard for KMIP integration (JIRA: ROFR-3083)**:

   You can now configure and integrate Fortanix DSM SaaS solution with KMIP for Cohesity, VMware, Rubrik, IBM DB2, VMware, NetApp, and Veritas.




   For more details, refer to the following KMIP use case guides:

   - Using Fortanix DSM for Cohesity Encryption Keys
   - Fortanix DSM with DKE for Microsoft 365
   - Using Fortanix DSM as External KMIP in Rubrik
   - Using Fortanix DSM with IBM DB2
   - Using Fortanix DSM with NetApp ONTAP
   - Using Fortanix DSM with Scality S3C
   - Using Fortanix DSM to Secure VMWare Virtual Environments

7. **Support for Oracle TDE heartbeat ciphertext caching (JIRA: PROD-3660):** You can now optionally cache Oracle heartbeat checks by updating the PKCS#11 config file so that there is no connectivity loss between Fortanix DSM and the Oracle Database Server. *For more details on how to enable this option, refer to the Fortanix DSM with Oracle TDE integration guide.*
8. **Support for LDAP authentication when using SSH to connect with Fortanix DSM (JIRA: DEVOPS-1363):** Users of the LDAP directory can now

Fortanix, Inc. | 44 Castro St #305| Mountain View, CA 94041| ☎ +1 628.400.2043
✉ info@fortanix.com
🌐 www.fortanix.com

**RELEASE NOTE**

**Date:** 13-Apr-22

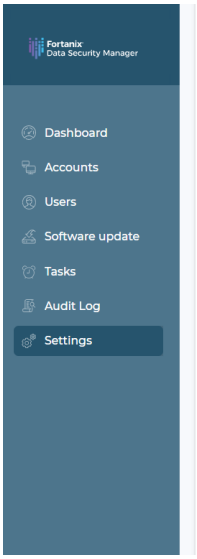
**Subject:** Software changes, updates, bug fixes, etc.

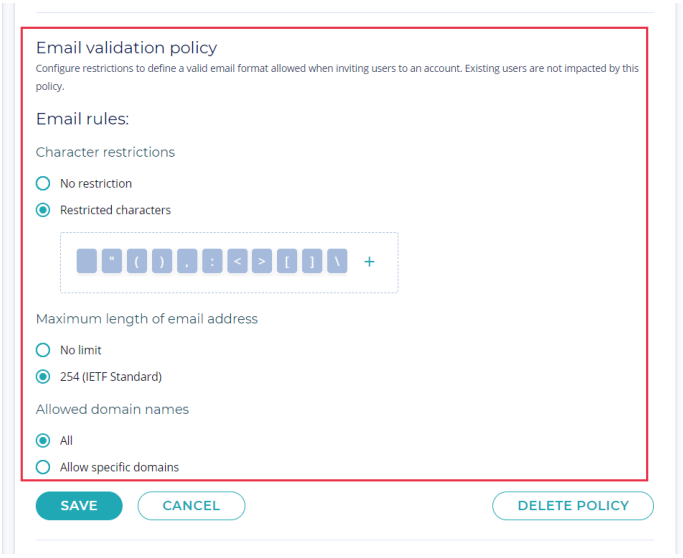
**Software:** Fortanix Data Security Manager

**Version**: 4.6

configure LDAP authentication using SSH to connect with Fortanix DSM. *For more information on how to configure LDAP authentication using SSH, refer to User's Guide: Authentication*.

9. **Email Validation Policy (JIRA: PROD-3991)**: When new users are invited or added to an account, you can configure rules to define a valid email format which will be enforced while inviting them. *For more details on how to configure this policy, refer to Administration Guide: Sysadmin Settings-Policies*.




10. **HMG external load balancer support for health check (JIRA: PROD-4185)**: You can now configure an external load balancer optionally, to evenly distribute traffic across multiple HSM Gateways to ensure high availability. *For more details, refer to the User's Guide: HSM Gateway*.
11. **Custom datatype support for attributes in KMIP specification (JIRA: PROD-4051)**: *For more details, refer to the FAQ: KMIP coverage*.
12. **Added support in the Fortanix DSM SysAdmin UI for `oauth_client` and `cai-base-url` cluster configuration (JIRA: ROFR-2920)**.

Fortanix, Inc. | 44 Castro St #305| Mountain View, CA 94041| ☎ +1 628.400.2043
✉ info@fortanix.com
🌐 www.fortanix.com

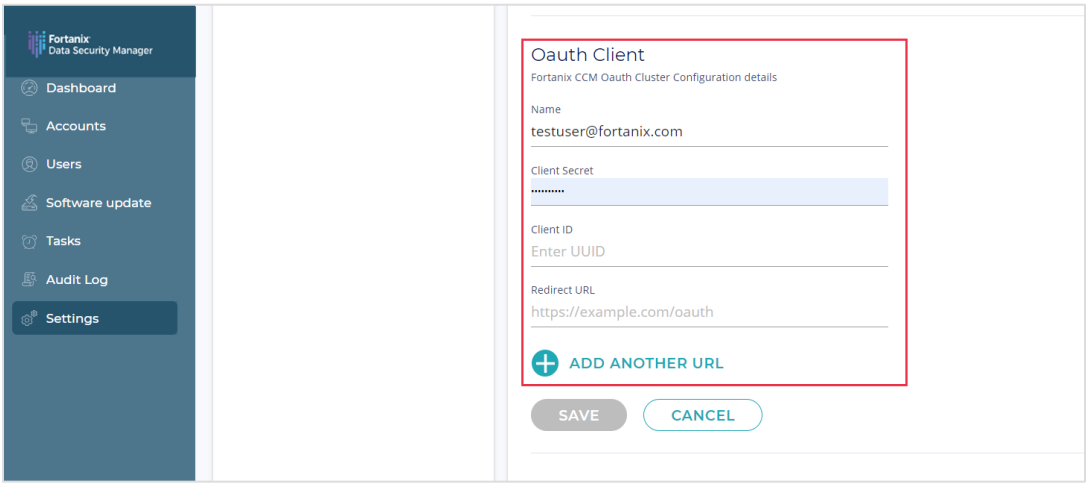
**RELEASE NOTE**

**Date:** 13-Apr-22

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

**Software:** Fortanix Data Security Manager

**Version**: 4.6




## ENHANCEMENTS TO EXISTING FEATURES

1. **A key can now be created in a FIPS Level 3 backed Fortanix DSM group for BYOK to AWS KMS/Azure Key Vault (JIRA: PROD-4040)**.
2. **This release now supports key restore using Azure backup blob when LUNA is used as the backend HSM for Azure Key Vault Plugin (JIRA: PROD-4248)**.
3. **Added randomness to the key-encryption key (KEK) in Azure Key Vault (JIRA: PROD-4292)**: By adding randomness in the naming scheme for KEK, it provides uniqueness and avoids collisions and subsequent failures when rotation use cases are involved.
4. **Improved error messages in logs when a client is connecting with KMIP (JIRA: PROD-4307)**: The error messages in logs now show what key operations for the key the client is trying to add, and what are the allowed operations.
5. **Implemented server-side table processing (JIRA: ROFR-1817)**: Server-side table processing improves the runtime performance of Fortanix DSM with full filtering, sorting, and pagination support.

Fortanix, Inc. | 44 Castro St #305| Mountain View, CA 94041| ☎ +1 628.400.2043
✉ info@fortanix.com
🌐 www.fortanix.com

**RELEASE NOTE**

**Date:** 13-Apr-22

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

**Software:** Fortanix Data Security Manager

**Version**: 4.6

6. **Implemented server-side processed DataTable for the Security Objects page (JIRA: ROFR-3131)**.
7. **Implemented server-side processed DataTable for the security objects list view in the group/app/user/plugin detailed views (JIRA: ROFR-3129)**.
8. **Removed the Fortanix DSM App Name size restriction of 100 to support lengthy app names (JIRA: ROFR-3082)**.
9. **Support different object types for different Azure Key Vault types (JIRA: ROFR-3110)**. *For more information, refer to the User's Guide: Azure Key Vault and User's Guide: Azure Managed HSM.*

**OTHER IMPROVEMENTS**

1. **Improved handling of Deploy Job failures (JIRA: DEVOPS-1802):**
2. **Removed rsync package (JIRA: DEVOPS-1891):** The rsync package is removed since the service causes a security risk by its usage of unencrypted protocols for communication.
3. **Adjusted the warmup-proxy-cache cronjob to run every hour (JIRA: DEVOPS-1951).** This change keeps the job from interrupting a Fortanix DSM cluster upgrade, which requires every job to be completed before the cluster can be upgraded.
4. **Added Linux packages/commands to the Fortanix DSM installer for troubleshooting production issues (JIRA: DEVOPS-2101)**.
5. **The upgrade is now aborted when the main tables and primary tables have a mismatch (JIRA: DEVOPS-2274)**.
6. **HSTS is now offered over port 4445 so that Fortanix DSM appliances are PCI compliant (JIRA: DEVOPS-2405)**.
7. **The two-factor authentication (2FA) for Quorum Policy at the account and group level can only be enabled if all approvers have 2FA enabled (JIRA: PROD-2455)**.
8. **Improved the JCE provider client for AWS SDK compatibility (JIRA: PROD-3969)**.

Fortanix, Inc. | 44 Castro St #305| Mountain View, CA 94041| ☎ +1 628.400.2043
✉ info@fortanix.com
🌐 www.fortanix.com

**RELEASE NOTE**

**Date:** 13-Apr-22

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

**Software:** Fortanix Data Security Manager

**Version**: 4.6

9. **The JCE provider is updated to now include X-Request-ID (JIRA: PROD-4123)**.
10. **The KAT self-tests are now automatically invoked when the system starts for FIPS level 1 certification (JIRA: PROD-4153)**.
11. **Created cron job to check subscription of all accounts and trigger emails for top 10 account admins and system admins (JIRA: PROD-4157)**.
12. **Added optional header fields to KMIP in the correct order (JIRA: PROD-4249)**.
13. **Added Wrap/Unwrap operations to the list of ignored operations when creating a Secret object (JIRA: PROD-4420)**.
14. **Added `key-type` to the `validate_key_ops` function that logs invalid key operations (JIRA: PROD-4432)**.

**BUG FIXES**

1. Fixed an issue where the `10-kubeadm.conf` file is older when upgraded to Kubernetes 1.12 version **(JIRA: DEVOPS-2239).**
2. Fixed a cluster downgrade issue when an older version of a node is joined to a newer version causing the cluster to downgrade (**JIRA: DEVOPS-2131**).
3. Fixed etcd configuration issues during Fortanix DSM upgrade (**JIRA: DEVOPS-2296**).
4. Fixed Kubernetes 1.10 to 1.11 upgrade failure (**JIRA: DEVOPS-2297**).
5. Fixed an issue where the cleanup script `dsm_cleanup_es.sh` exits when migration is not complete (**JIRA: DEVOPS-2324**).
6. Fixed an issue where Cassandra cannot find SEED when all the Fortanix DSM nodes restart and requires manual recovery (**JIRA: DEVOPS-2411**).
7. Fixed an issue where all Fortanix DSM account administrators without a security key were locked out of an account when the "Mandatory two-factor authentication to log in with password" was enabled in the Account Settings (**JIRA: PROD-2436**).

Fortanix, Inc. | 44 Castro St #305| Mountain View, CA 94041| ☎ +1 628.400.2043
✉ info@fortanix.com
🌐 www.fortanix.com

**RELEASE NOTE**

**Date:** 13-Apr-22

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

**Software:** Fortanix Data Security Manager

**Version**: 4.6

8. Fixed an issue where external groups were able to create Secret and Opaque objects (**JIRA: PROD-3876**).
9. Fixed an issue where deleting/disabling of parent account does not delete/disable all child accounts (**JIRA: PROD-3880**).
10. Fixed an error while wrapping the external RSA key in PKCS8 format (**JIRA: PROD-4043**).
11. Fixed a double logging issue by moving logging from `handle_operation` into the KMIP path (**JIRA: PROD-4181**).
12. Fixed HSM Gateway initialization error which now initializes PKCS#11 with `CFK_OS_LOCKING_OK` to perform locking before calling PKCS#11 functions (**JIRA: PROD-4195**).
13. Fixed an HMG undefined behavior in Rust `pkcs11` crate that causes the `C_Initialize` to fail (**JIRA: PROD-4222**).
14. Fixed an issue where the Content-Length header was not added to HTTP requests with the body for outbound calls (**JIRA: PROD-4232**).
15. Fixed panic in production that had `unimplemented!()` method in `key_mgmt.rs` (**JIRA: PROD-4294**).
16. Fixed an issue where a user was not able to copy an EC key from the standard DSM group to Azure (**JIRA: PROD-4374**).
17. Fixed an issue when deleting key material using the "Delete Key Material" option in an AWS KMS backed group threw 500 internal server error (**JIRA: PROD-4431**).
18. Fixed an issue where the `secrets_operation` count for reporting does not increase beyond 100, but `num_operations` count continues to increase (**JIRA: PROD-4433**).
19. Fixed an issue that does not allow scanning keys in an Azure Standard Key Vault-backed group (**JIRA: PROD-4436**).

Fortanix, Inc. | 44 Castro St #305| Mountain View, CA 94041| ☎ +1 628.400.2043
✉ info@fortanix.com
🌐 www.fortanix.com

**RELEASE NOTE**

**Date:** 13-Apr-22

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

**Software:** Fortanix Data Security Manager

**Version**: 4.6

20. Fixed an issue where you cannot rotate a key containing aliases (**JIRA: PROD-4492**).
21. Fixed an issue where an incorrect month was shown on the Fortanix DSM dashboard due to UTC → local time logic error (**JIRA: ROFR-3074**).
22. Fixed an issue during the audit log export operation that omits the "Actor" field when it is repeated multiple times (**JIRA: ROFR-3077**).
23. Fixed an issue in Azure BYOK where incorrect values were selected in the drop down for key vault selection in the Standard or Premium Key Vault type (**JIRA: ROFR-3087**).
24. Fixed an issue where users were unable to select the HSM/External KMS type in the drop-down list on the first click (**JIRA: ROFR-3096**).
25. Fixed an issue where the Frontend does not always show fetched key vaults for managed HSM (**JIRA: ROFR-3104**).
26. Fixed an issue in the GCP BYOK configuration steps where uploading a private key clears the uploaded file when you click on the screen (**JIRA: ROFR-3106**).
27. Fixed an issue where **DOWNLOAD CSV** option on the dashboard downloads more data than for the requested period (**JIRA: ROFR-3108**).
28. Fixed an error in server-side table processing, that does not allow navigating to a group from the Security Object table view (**JIRA: ROFR-3121**).
29. Fixed an issue where notifications were not displayed when updating a key (**JIRA: ROFR-3122**).
30. Fixed an issue on the Security Objects page, where the **Select All** check box does not list the number of security objects selected (**JIRA: ROFR-3125**).
31. Fixed an issue where users were unable to delete a security object from a group with a quorum policy configured (**JIRA: ROFR-3126**).

Fortanix, Inc. | 44 Castro St #305| Mountain View, CA 94041| ☎ +1 628.400.2043
✉ info@fortanix.com
🌐 www.fortanix.com

**RELEASE NOTE**

**Date:** 13-Apr-22

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

**Software:** Fortanix Data Security Manager

**Version**: 4.6

32. Fixed an issue where users were not able to rotate an AES 256 key in Azure Managed HSM to a Fortanix DSM Key (**JIRA: ROFR-3135**).
33. Fixed an issue where the **ADD SECURITY OBJECT** button was missing in the **SECURITY OBJECTS** tab in a detailed view of a group (**JIRA: ROFR-3142**).
34. Fixed an issue where a user with an "Auditor" role was able to select all the security objects from the Security Objects page and see the options to delete selected, destroy selected, disable logging, enable logging (**JIRA: ROFR-3144**).
35. Fixed an issue in the AWS KMS and Azure Key Vault key creation workflow, where after the keys were created and selected from the AWS KMS/Azure Key Vault group detailed view, options to delete and destroy the keys were visible and enabled (**JIRA: ROFR-3146**).

## QUALITY ENHANCEMENTS / UPDATES

- Upgraded Cassandra to 3.11.12 version **(JIRA: DEVOPS-2312)**.

## SECURITY FIXES

- sudo commands now uses pseudo-terminal **(JIRA: DEVOPS-2001)**.

## 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 job is exited and marked completed before cluster upgrade (**JIRA: DEVOPS-2068**).

Fortanix, Inc. | 44 Castro St #305| Mountain View, CA 94041| ☎ +1 628.400.2043
✉ info@fortanix.com
🌐 www.fortanix.com

**RELEASE NOTE**

**Date:** 13-Apr-22

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

**Software:** Fortanix Data Security Manager

**Version**: 4.6

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**).

## 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** | 4344/4279 |
| **AES 256: GCM Encryption/Decryption** | 4373/4160 |
| **AES 256: FPE Encryption/Decryption** | 2439/2428 |
| **AES 256 Key Generation** | 1118 |
| | |
| **RSA 2048 Encryption/Decryption** | 3962/1136 |
| **RSA 2048 Key Generation** | 47 |
| **RSA 2048 Sign/Verify** | 1142/3984 |
| **EC NISTP256 Sign/Verify** | 638/339 |
| | |
| **Data Security Manager Plugin (Hello world plugin)** | 1857 (invocations/second) |

- **Azure Standard_DC8_v2**

Fortanix, Inc. | 44 Castro St #305| Mountain View, CA 94041| ☎ +1 628.400.2043
✉ info@fortanix.com
🌐 www.fortanix.com

**RELEASE NOTE**

**Date:** 13-Apr-22

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

**Software:** Fortanix Data Security Manager

**Version**: 4.6

| KEY TYPES AND OPERATIONS | THROUGHPUT (Operations/second on a 3-node [Standard_DC8_v2] cluster) |
|---|---|
| **AES 256: CBC Encryption/Decryption** | 3261/3373 |
| **AES 256: GCM Encryption/Decryption** | 3337/3174 |
| **AES 256: FPE Encryption/Decryption** | 1981/1961 |
| **AES 256 Key Generation** | 1070 |
| | |
| **RSA 2048 Encryption/Decryption** | 2992/1003 |
| **RSA 2048 Key Generation** | 63 |
| **RSA 2048 Sign/Verify** | 994/3132 |
| **EC NISTP256 Sign/Verify** | 531/294 |
| | |
| **Data Security Manager Plugin (Hello world plugin)** | 1768 (invocations/second) |

## 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.

Fortanix, Inc. | 44 Castro St #305| Mountain View, CA 94041| ☎ +1 628.400.2043
✉ info@fortanix.com
🌐 www.fortanix.com

## RELEASE NOTE

**Date:** 13-Apr-22

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

**Software:** Fortanix Data Security Manager

**Version**: 4.6

## 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.

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

Fortanix, Inc. | 44 Castro St #305| Mountain View, CA 94041| ☎ +1 628.400.2043

✉ info@fortanix.com

🌐 www.fortanix.com