RELEASE NOTE

Date: 15-Feb-22

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

Software: Fortanix Data Security Manager

Version: 4.4

OVERVIEW

This document provides an overview of new features, general enhancements, improvements, and resolved issues in the Fortanix Data Security Manager (DSM) 4.4 release.

This release is superseded by March 04, 2022, release.

WARNING:

- It is "REQUIRED" to upgrade Fortanix DSM to version 4.2 or 4.3 before upgrading to version 4.4.

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 4.2 or 4.3 to 4.4.

NEW FUNCTIONALITY / FEATURES

1. **Key metadata policy for Fortanix DSM groups. (JIRA: ROFR-2686):**

   Key metadata policies can be set on Fortanix DSM groups which allow users to configure certain restrictions on the "metadata" associated with security objects. Here, "metadata" refers to certain features of security objects that are not covered by Cryptographic policies. For example, custom metadata, description, expiry, and so on. This policy allows users to specify that certain metadata "must be present", "must not be present", or "must be present and have certain value".

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

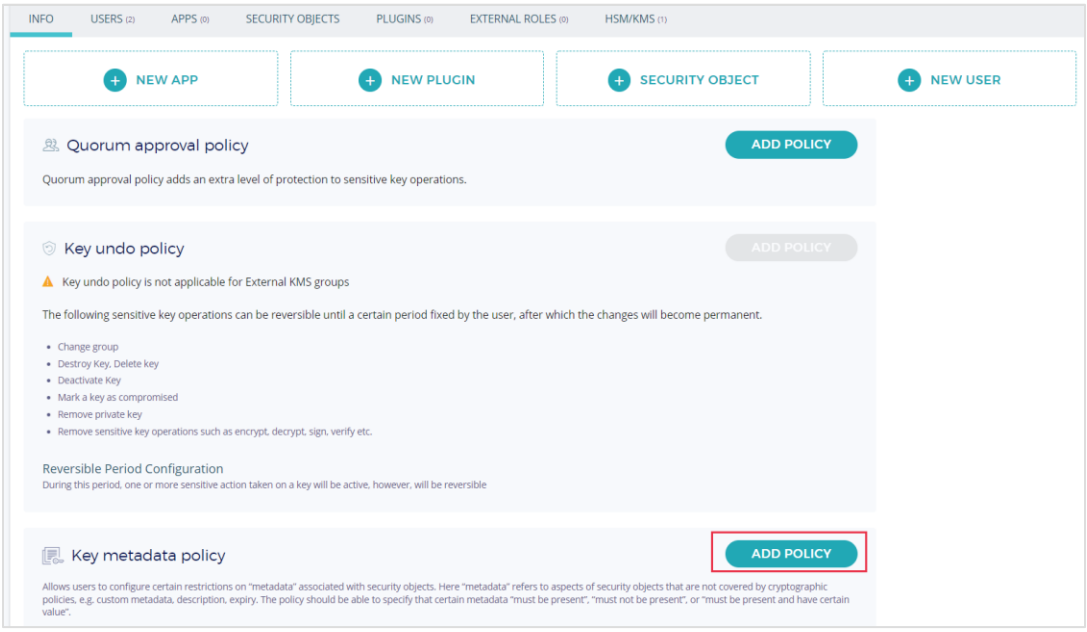
RELEASE NOTE

Date: 15-Feb-22

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

Software: Fortanix Data Security Manager

Version: 4.4



For more details refer to the User's Guide: Key metadata policy.

2. **Group based on external Google Cloud Platform (GCP) KMS and Bring Your Own Key (BYOK) for GCP (JIRA: ROFR-2643):**

   GCP Key Management Service is added to the list of supported Key Management Systems in HSM/External KMS groups. Fortanix DSM can now manage keys in GCP and allows to:

   - Configure the GCP KMS group in Fortanix DSM.
   - Import and copy key (Bring Your Own Key - BYOK) into GCP KMS.
   - Enable/Disable keys in GCP KMS directly.

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

RELEASE NOTE

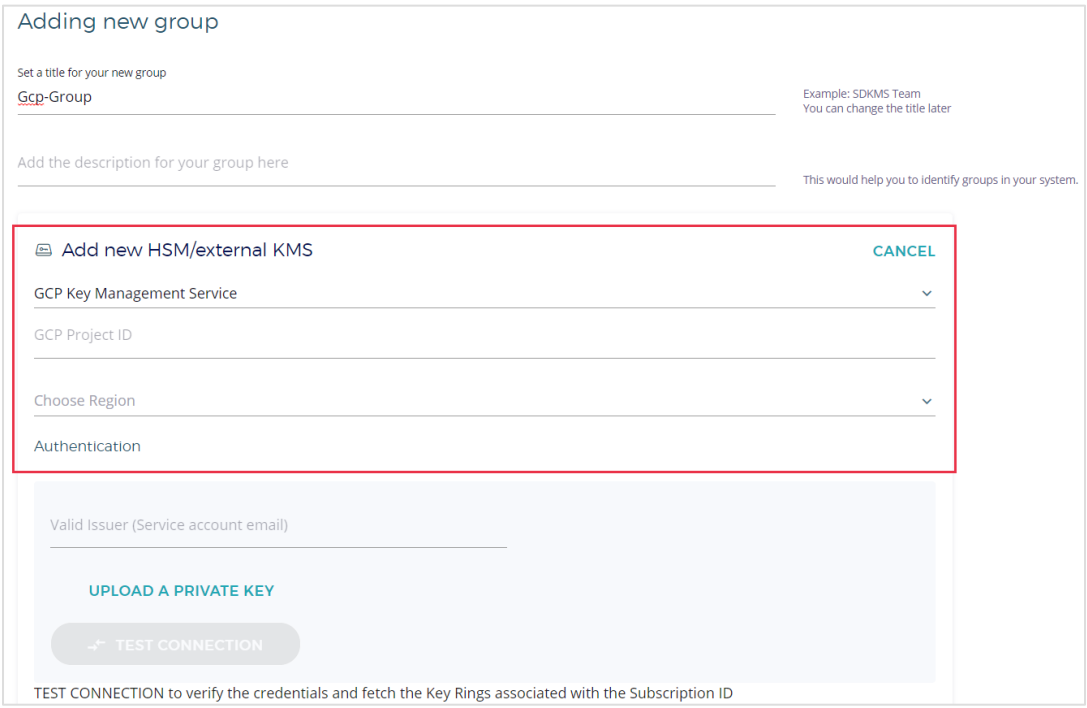
Date: 15-Feb-22

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

Software: Fortanix Data Security Manager

Version: 4.4

Edit AWS Customer Master Key attributes such as tag and alias for keys.



For more details refer to the User's Guide: GCP Cloud Key Management.

3. **Billable metrics support in Fortanix DSM Account and Sys Admin dashboard (JIRA: ROFR-2842):**

   Fortanix DSM now shows the usage of resources associated with an account. Real-time and historical data of these metrics can now be viewed in the Fortanix DSM account and Sys Admin dashboard.

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

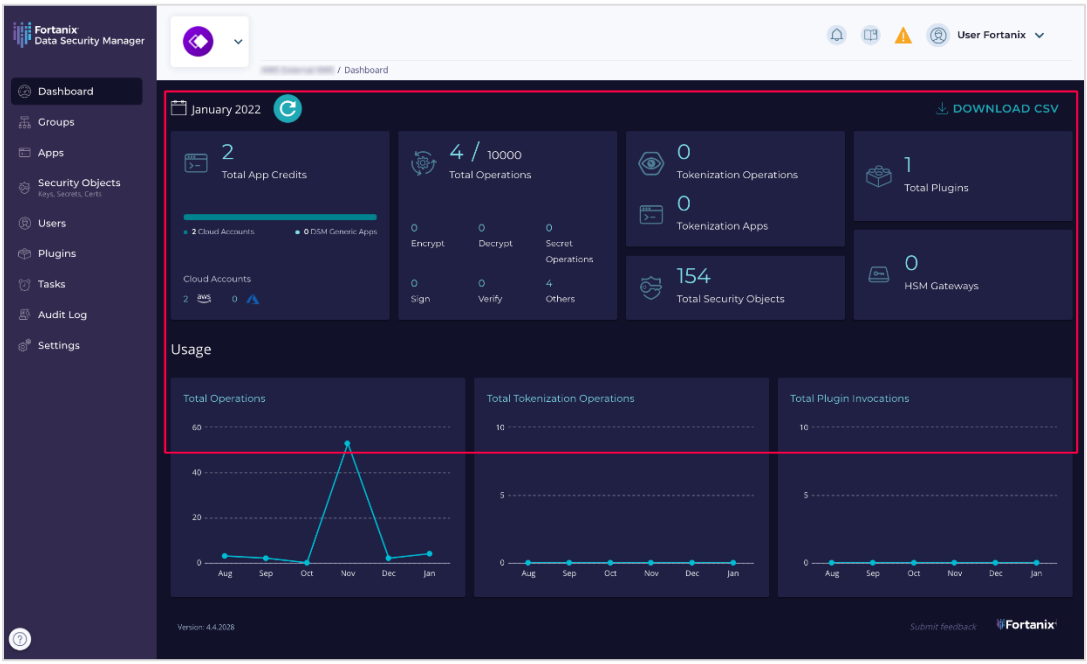
RELEASE NOTE

Date: 15-Feb-22

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

Software: Fortanix Data Security Manager

Version: 4.4



For more details, refer to [User's Guide: Fortanix DSM Usage Metrics](#).

4. **Support Fortanix DSM on Azure non-SGX VMs (JIRA: DEVOPS-2123)**: This release supports the standard deployment of Fortanix DSM on non-SGX Azure VMs. *For more details, refer to the [Fortanix DSM Installation from Azure Marketplace guide](#).*

ENHANCEMENTS TO EXISTING FEATURES

1. **Simplified UI for authorization provider in Google Workspace CSE (JIRA: ROFR-2973):**
   You can now select Google Drive and Docs to configure this option as an authorization provider so that the authorization settings will be automatically included for Google Drive and Docs.

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

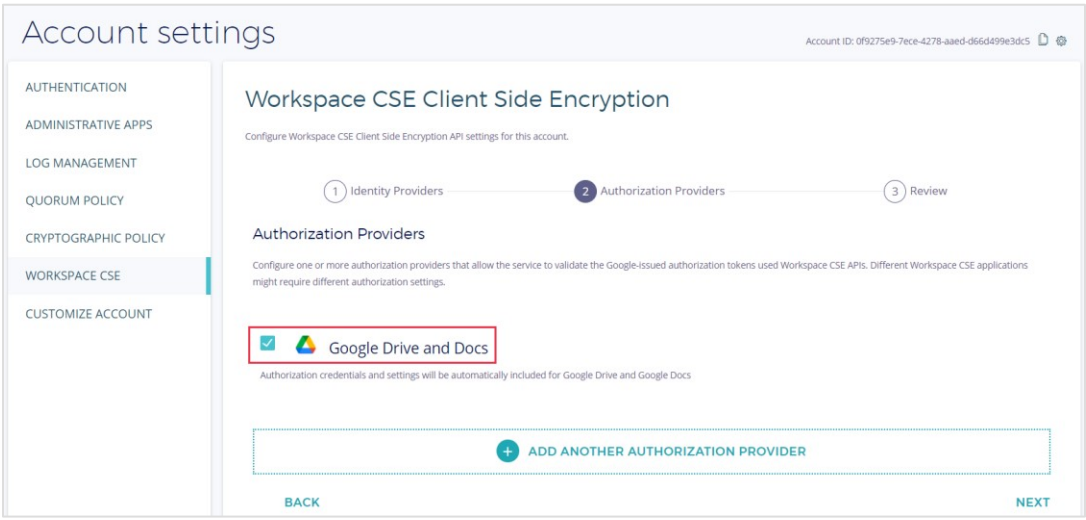
RELEASE NOTE

Date: 15-Feb-22

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

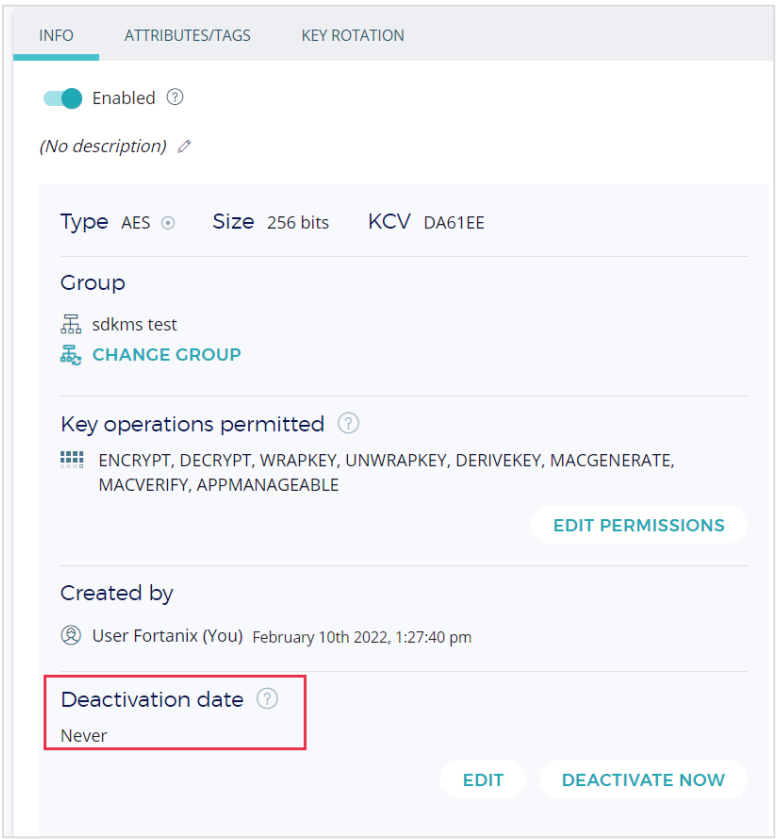
Software: Fortanix Data Security Manager

Version: 4.4



For more details, refer to User's Guide: Using Google Workspace CSE with Fortanix DSM.

2. **The "Expires" field in the detailed view of a security object is now renamed to "Deactivation date" in the UI (JIRA: ROFR-2973):**



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

RELEASE NOTE

Date: 15-Feb-22

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

Software: Fortanix Data Security Manager

Version: 4.4

3. **Fortanix DSM account name change now initiates quorum approval (JIRA: ROFR-2870):**
   Renaming an account now generates a quorum approval request. *For more details, refer to the User's Guide: Quorum Policy*.
4. **Cluster Master Key protection for Software version of DSM (JIRA: PROD-3404)**:
   When Fortanix DSM is deployed on platforms that do not support Intel SGX, such as AWS, the Cluster Master Key is now protected using another key. This key can be stored on an external instance of Fortanix DSM, for example, an on-prem cluster. *For more details, refer to the Administration Guide: Cluster Deployment Key Protection – non-SGX*.
5. **Public key authentication for SCP backup (JIRA: DEVOPS-1320)**:
   You can now set passwordless authentication for SCP backup. *For more details refer to Administration Guide: Backup and Restore in Fortanix DSM*.
6. **Fortanix DSM SaaS usage metrics are now reported on the dashboard (JIRA: PROD-3940)**: *For more details, refer to the User's Guide: Usage Metrics*.

OTHER IMPROVEMENTS

1. **All world-writable folders have their sticky bit set (JIRA: DEVOPS-1880):**
   This improvement prevents the ability to delete or rename files in the world-writable directories (such as `/tmp`) that are owned by another user.
2. **Set external HSM credentials in k8s secret using sdkms-cluster (JIRA: PROD-2162):**
   This allows the Cluster Master Key (CMK) to be protected by an external HSM when outside SGX.
3. **Audit logs will not be deleted during the account delete operation (JIRA: PROD-3843)**.

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

RELEASE NOTE

Date: 15-Feb-22

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

Software: Fortanix Data Security Manager

Version: 4.4

4. **Security object filter operation now supports filtering by state (JIRA: PROD-3981)**.
5. **Azure BYOK plugin now supports extractable keys in Luna HSM (JIRA: PROD-3965)**.

BUG FIXES

1. Fixed an issue where the sdkms-cluster update fails if `cluster-config.sdkms` secret is missing **(JIRA: DEVOPS-2072).**
2. Fixed HMG issue with Sync Keys for SanSec HSM (**JIRA: PROD-3330**).
3. Fixed Azure BYOK plugin "out of memory" error when the key vault has more than a certain number of keys (**JIRA: PROD-3568**).
4. Fixed an issue that now allows pagination support for Azure BYOK key versions in the UI (**JIRA: PROD-3623**).
5. Allow Admin apps to change user roles (**JIRA: PROD-3671**).
6. Fixed an issue where Fortanix DSM returns 403 error due to a bug related to group existence check when an administrative app tries to create a new security object or crypto app (**JIRA: PROD-3678**).
7. Fixed an issue where AWS Scan fails with 500 ERROR (**JIRA: PROD-3787**).
8. Fixed an issue where Azure Managed HSM and Premium plugins were throwing stack trace instead of actual error message in case of misconfiguration (**JIRA: PROD-4014**).
9. Fixed an issue where `/sys/v1/accounts` creates panic (**JIRA: PROD-4109**).
10. Fixed an issue where the normal plugin details page in the Fortanix DSM UI hangs if GitHub access is not available (**JIRA: ROFR-2899**).

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

RELEASE NOTE

Date: 15-Feb-22

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

Software: Fortanix Data Security Manager

Version: 4.4

QUALITY ENHANCEMENTS / UPDATES

- Upgraded the exabgp base container to Ubuntu 20.04 version **(JIRA: DEVOPS-1413)**.

SECURITY

1. Disabled all USB drives on the FX-2200 appliance by default **(JIRA: DEVOPS-1882)**. *For more details, refer to the Fortanix DSM FX2200 Hardware Guide*.

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**).

  Workaround: If all the pods are healthy, you can deploy the version again.
- The sync key API returns “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**).
- Fortanix DSM cluster upgrade is interrupted when the warmup-proxy-cache job is running, and the next iteration starts as soon as the current one completes (**JIRA: DEVOPS-1951**).

  Workaround: Delete the cronjob warmup-proxy-cache before starting the upgrade:

```
kubectl delete cronjob warmup-proxy-cache
```

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

RELEASE NOTE

Date: 15-Feb-22

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

Software: Fortanix Data Security Manager

Version: 4.4

The upgrade process will recreate this cronjob for the cluster

- `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	4753/4634
AES 256: GCM Encryption/Decryption	4896/4705
AES 256: FPE Encryption/Decryption	2564/2555
AES 256 Key Generation	1165
RSA 2048 Encryption/Decryption	4383/1173
RSA 2048 Key Generation	48
RSA 2048 Sign/Verify	1168/4330
EC NISTP256 Sign/Verify	642/336
Data Security Manager Plugin (Hello world plugin)	1978 (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	3535/3620
AES 256: GCM Encryption/Decryption	3404/3770

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

RELEASE NOTE

Date: 15-Feb-22

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

Software: Fortanix Data Security Manager

Version: 4.4

KEY TYPES AND OPERATIONS	THROUGHPUT (Operations/second on a 3-node [Standard_DC8_v2] cluster)
AES 256: FPE Encryption/Decryption	2270/2281
AES 256 Key Generation	1055
RSA 2048 Encryption/Decryption	3547/1161
RSA 2048 Key Generation	67
RSA 2048 Sign/Verify	1147/3273
EC NISTP256 Sign/Verify	635/345
Data Security Manager Plugin (Hello world plugin)	1816 (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: 15-Feb-22

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

Software: Fortanix Data Security Manager

Version: 4.4

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 Data Security Manager Release Notes

Release 4.4

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

✉ info@fortanix.com

🌐 www.fortanix.com