RELEASE NOTE

Date: 13-May-22

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

Software: Fortanix Data Security Manager SaaS

Version: 4.7

OVERVIEW

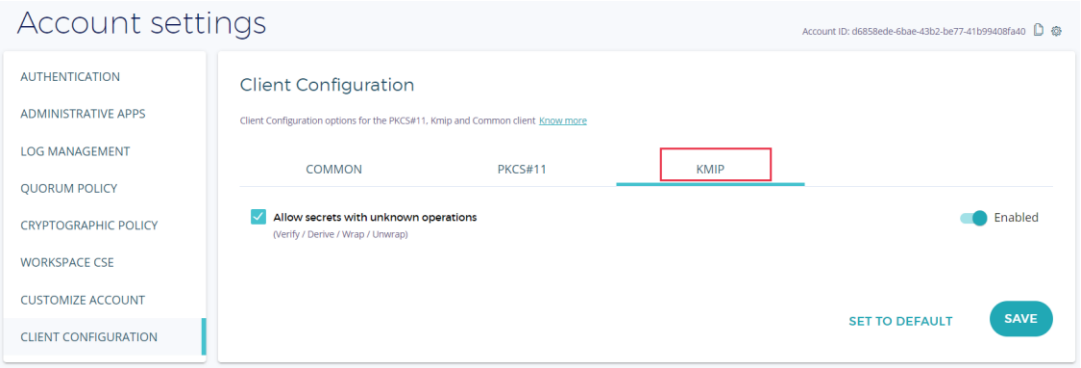
This document provides an overview of new features, general enhancements, improvements, and resolved issues in the Fortanix Data Security Manager (DSM) SaaS 4.7 release.

NOTE: This release is for **SaaS only** and not available for On-Prem installations.

NEW FUNCTIONALITY / FEATURES

1. **Client Configuration Support in Account Settings for KMIP (JIRA: ROFR-3197):**

   This release allows you to set the default configurations for KMIP clients in addition to PKCS#11 and Common clients on the Fortanix DSM Account Settings page.



   For more details, refer to User's Guide: Client Configurations.

2. **Key Access Justification at Key Level (JIRA: PROD-4246):**
   You can now configure the Google Key Access Justification policy for wrapping and unwrapping a key at the Key level in addition to the app level Key Access Justification policy in Fortanix DSM.

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

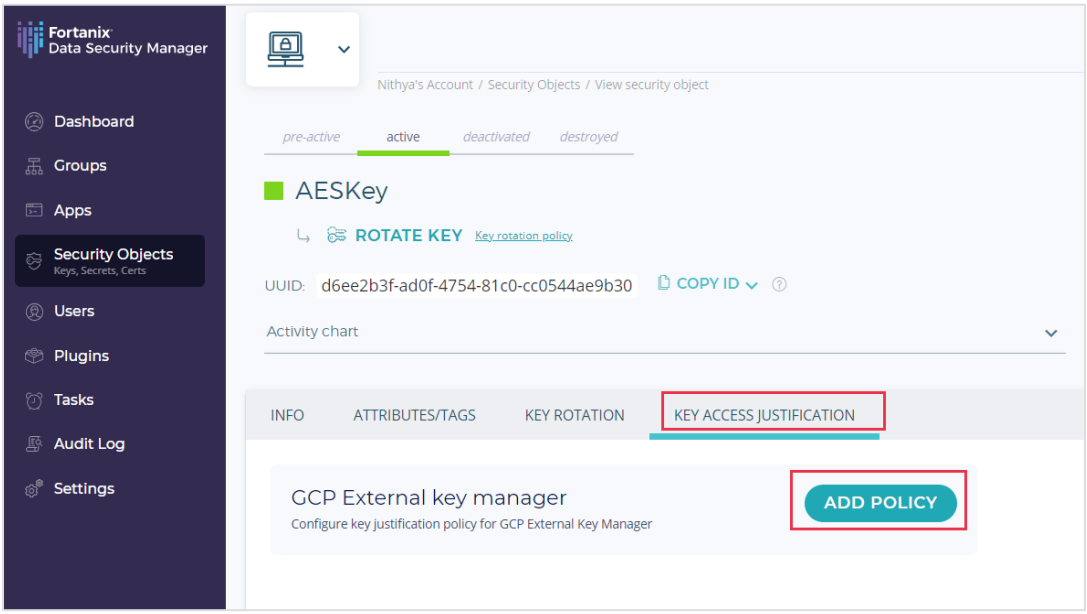
RELEASE NOTE

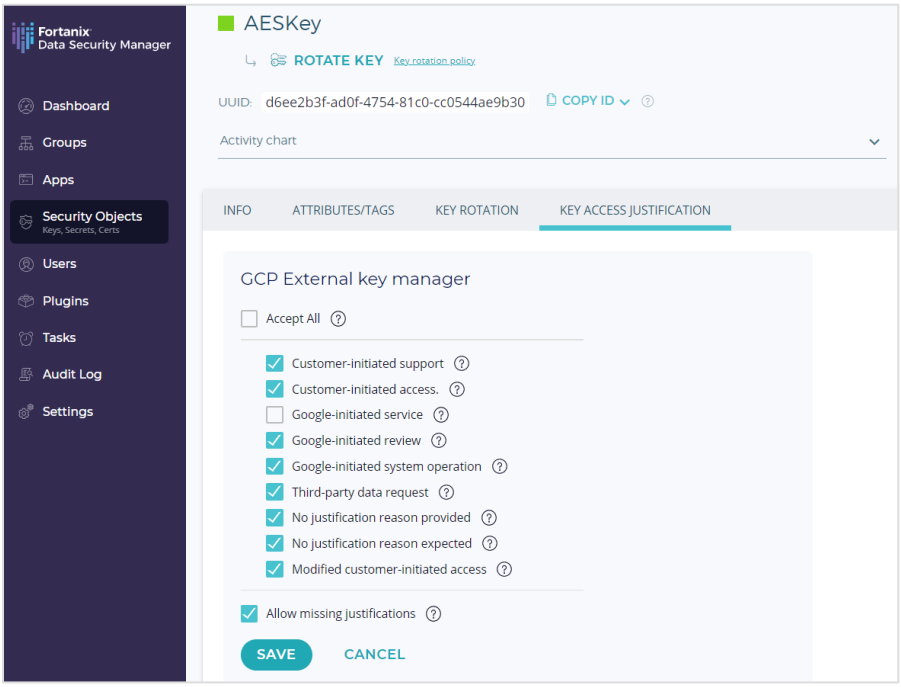
Date: 13-May-22

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

Software: Fortanix Data Security Manager SaaS

Version: 4.7





For more details refer to [User's Guide: Fortanix DSM with Google Cloud EKM Interface](#).

3. **Searchable Custom Attributes (API) (JIRA: PROD-2948):**

   This release adds API support to:

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

RELEASE NOTE

Date: 13-May-22

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

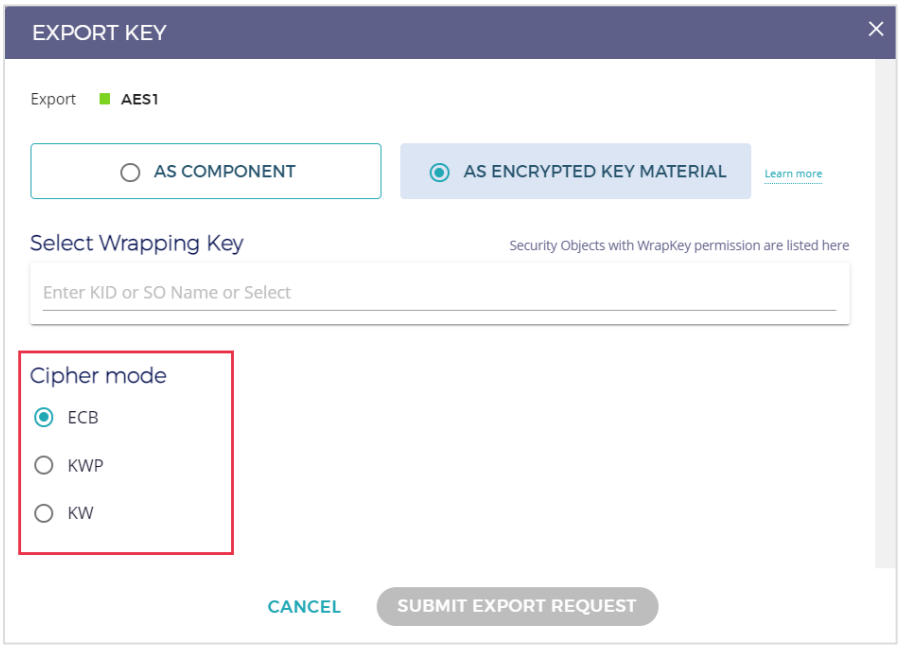
Software: Fortanix Data Security Manager SaaS

Version: 4.7

- Add commonly used custom metadata keys and store them in the Fortanix DSM account.
- Allow the custom metadata keys to be searchable in the Security Objects table.

ENHANCEMENTS TO EXISTING FEATURES

1. **Reuse TLS connections to AWS for AWS IAM authentication method (JIRA: ROQA-1211)**.
2. **Updates to key encryption modes (JIRA: ROFR-3179)**:
    a. Updated the label "Mode" to "Cipher mode" for key encryption modes when exporting an encrypted key.
    b. Updated the text for the three encryption modes to ECB, KWP, and KW.



3. **Disabled AWS KMS HSM in UI (JIRA: ROFR-3167)**.
4. **Renamed "Google Stackdriver" to "Google Cloud's operations suite" for External Log Management integration (JIRA: ROFR-3164)**.

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

RELEASE NOTE

Date: 13-May-22

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

Software: Fortanix Data Security Manager SaaS

Version: 4.7

5. **Updated the label "Seed" to "SEED" in the key create/import flow (JIRA: ROFR-3159)**.

OTHER IMPROVEMENTS

1. **Added consistency quorum to all the cqlsh insert/update commands (JIRA: PROD-4547):**
2. **Cassandra tunable values can now be configured by environment variables in the Kubernetes chart (JIRA: DEVOPS-2565)**.
3. **Enabled randomized layout of virtual address space (JIRA: DEVOPS-2504)**.
4. **Disabled network related Kernel runtime parameters for hosts and routers (JIRA: DEVOPS-2499)**.
5. Added support for **SecretData for KMIP client (JIRA: PROD-4365)**.
6. **Created Log Aggregator plugin for Cloudtrail and DSM logs (JIRA: PROD-4208)**.
7. **Improvements in the repair of the session table (JIRA: DEVOPS-1442)**.
8. **Set Interactive session timeout (JIRA: DEVOPS-2497)**.

BUG FIXES

1. Fixed an issue where the API key of an app cannot be viewed from the UI after quorum approval (**JIRA: ROFR-3176**).
2. Fixed an issue where IP whitelisting does not work for IPV4 (**JIRA: PROD-4565**).
3. Fixed an issue where the "Download CSV" button in the SysAdmin "Accounts" page does not generate any data (**JIRA: ROFR-3175**).
4. Fixed an issue where the "**Add Security Object**" button was enabled in the "**Security Objects**" tab in the detailed view of an app, user, and plugin (**JIRA: ROFR-3171**).

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

RELEASE NOTE

Date: 13-May-22

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

Software: Fortanix Data Security Manager SaaS

Version: 4.7

5. Fixed an issue where the log level of audit logs could not be set to show only the log of level - warnings, errors, and critical. (**JIRA: ROFR-3165**).
6. Fixed an issue where the user was unable to select a region for AWS KMS-HSM service (**JIRA: ROFR-3158**).
7. Fixed an issue where the audit log for administrative apps displayed the log of a previous administrative app when accessed (**JIRA: ROFR-3155**).
8. Fixed Google Workspace CSE invalid API path issue (**JIRA: PROD-4491**).
9. Fixed an issue that the error pages returned by Fortanix DSM had incorrect content type set making these pages potentially vulnerable to reflected cross site scripting attacks (**JIRA: PROD-4461**).
10. Fixed an issue where the PKCS#11 properties `C_GetMechanismList`, `C_GetMechanismInfo` does not report all the supported mechanisms (**JIRA: PROD-4458**).
11. Fixed an issue where some accounts are disabled for selection in the "**Accounts**" drop down when a user tries to access them (**JIRA: ROFR-3078**).
12. Fixed panic when downgrading from Fortanix DSM version 4.6 to 4.3 patch (**JIRA: PROD-4512**).
13. Fixed an issue where a user was unable to rotate an AWS key containing aliases (**JIRA: PROD-4492**).
14. Fixed an issue where the "Delete selected" and "Destroy selected" options for an AWS/Azure key were enabled in the Security Objects table view (**JIRA: ROFR-3146**).
15. Fixed the select account failure due to a backward compatibility issue caused by the HSM Gateway config (**JIRA: PROD-4482**).
16. Fixed an issue where a user with the "Auditor" role should not be able to see the "**Delete selected**" , "**Destroy selected**", **Enable logging**", and

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

RELEASE NOTE

Date: 13-May-22

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

Software: Fortanix Data Security Manager SaaS

Version: 4.7

"**Disable logging**" options when a security object is selected (**JIRA: ROFR-3144**).

17. Fixed an issue where the user should not be allowed to create a security object in the KMIP easy wizard integration flow in Fortanix DSM SaaS (**JIRA: ROFR-3143**).
18. Fixed an issue where the "**Add Security Object**" button was missing in the "**Security Objects**" tab in the detailed view of a group (**JIRA: ROFR-3142**).
19. Fixed an issue where the pod subnet IPs are not masked in the audit log (**JIRA: PROD-4474**).
20. Fixed an issue where some of the easy wizard integrations get disabled on "Tokenization and allow more plugins" checks in Fortanix DSM SaaS (**JIRA: ROFR-3139**).
21. Fixed an issue where users were able to create a Cohesity instance with a blank certificate (**JIRA: ROFR-3138**).
22. Fixed an issue where the users were unable to rotate an AES 256 key to a Fortanix DSM key in the Azure Managed HSM workflow (**JIRA: ROFR-3135**).
23. Fixed an issue where the account name with "underscore" is replaced with a "space" on the Accounts page (**JIRA: ROFR-3123**).
24. Fixed an issue where the "Delete key material" operation causes a 500 internal server error (**JIRA: PROD-4431**).
25. Fixed an issue where the "Know More" link in the "Client Configurations" settings page does not go to the correct documentation page (**JIRA: ROFR-3095**).
26. Fixed an issue where one of the `sdkms-ui` pod is in `ImagePullBackoff` state during an upgrade (**JIRA: DEVOPS-2207**).
27. Fixed an issue where the Fortanix DSM logo was of inappropriate size on the System Administration page (**JIRA: ROFR-2961**).

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

RELEASE NOTE

Date: 13-May-22

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

Software: Fortanix Data Security Manager SaaS

Version: 4.7

28. Fixed an issue where the deploy command returns an error on execution (**JIRA: DEVOPS-1012**).

QUALITY ENHANCEMENTS / UPDATES

- Patched Ubuntu OS packages. **(JIRA: DEVOPS-2607)**.

SECURITY FIXES

- Enforced the usage of `pam_wheel` for `su` authentication **(JIRA: DEVOPS-2496)**.
- Fixed a disabled Subresource Integrity (SRI) (**JIRA: PROD-4516**).
- Fixed a bug where essential validation checks were missing when allocating and processing `FifoDescriptor` **(JIRA: PLAT-896)**. In a scenario where an attacker has complete control of the address space, an attacker could leverage these missing checks to rewrite the stack pointer outside of the enclave into an attacker-crafted stack. By utilizing ROP the attacker could execute arbitrary code and leak anything accessible by the enclave.

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.

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

RELEASE NOTE

Date: 13-May-22

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

Software: Fortanix Data Security Manager SaaS

Version: 4.7

- 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**).

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

RELEASE NOTE

Date: 13-May-22

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

Software: Fortanix Data Security Manager SaaS

Version: 4.7

Fortanix Data Security Manager SaaS Release Notes

Release 4.7

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

✉ info@fortanix.com

🌐 www.fortanix.com