RELEASE NOTE

Date: 26-Aug-22

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

Software: Fortanix Data Security Manager SaaS

Version: 4.10

OVERVIEW

This document provides an overview of new features, general enhancements, improvements, and resolved issues in the Fortanix Data Security Manager (DSM) SaaS 4.10 release.

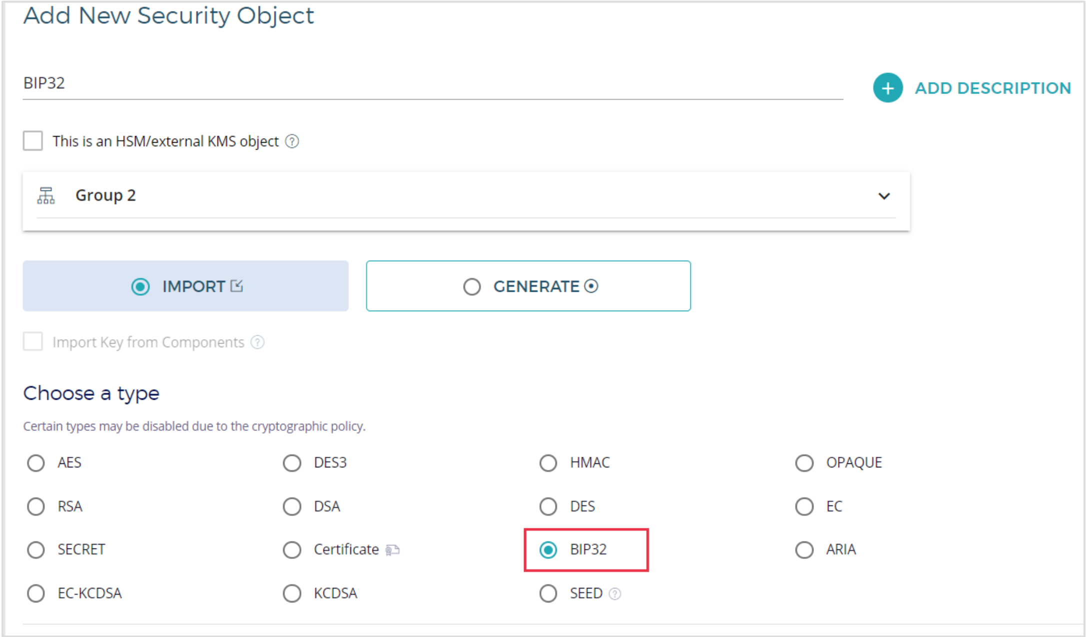
This release is superseded by the August 30, 2022, release.

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

NEW FUNCTIONALITY / FEATURES

1. Native BIP32 Key API Support (JIRA: PROD-4261):

This release allows you to import a new type of security object called BIP32. BIP32 is a parent key inside a Bitcoin hierarchical deterministic wallet (HD Wallet). This key can be used to recover all keys beneath it in the tree, for example: it can be used to sign transaction hashes and derive hardened and non-hardened children.



Add New Security Object

BIP32

☐ This is an HSM/external KMS object

Group 2

● IMPORT ○ GENERATE

☐ Import Key from Components

Choose a type

Certain types may be disabled due to the cryptographic policy.

○ AES	○ DES3	○ HMAC	○ OPAQUE
○ RSA	○ DSA	○ DES	○ EC
○ SECRET	○ Certificate	● BIP32	○ ARIA
○ EC-KCDSA	○ KCDSA	○ SEED	

RELEASE NOTE

Date: 26-Aug-22

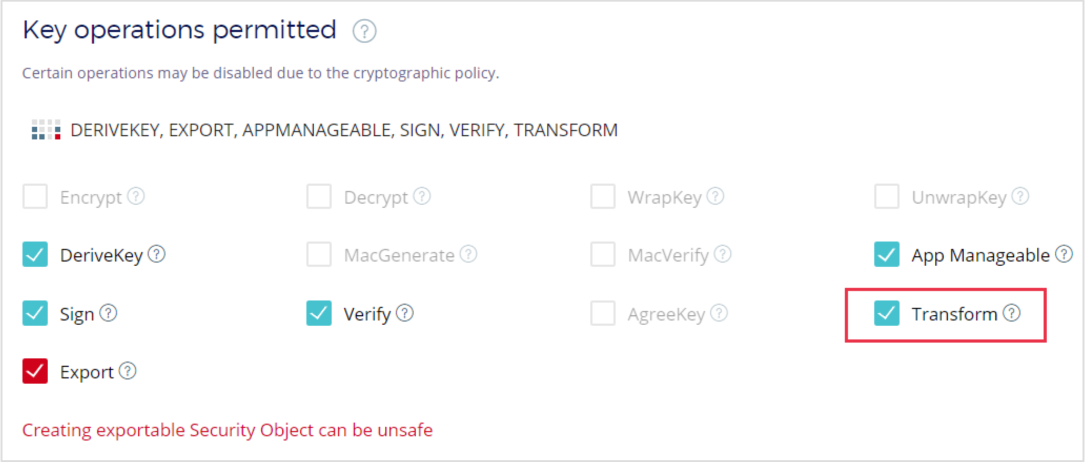
Subject: Software changes, updates, bug fixes, etc.

Software: Fortanix Data Security Manager SaaS

Version: 4.10

For more details, refer to User's Guide: Key Lifecycle Management.

2. **Added a new operation for BIP32 keys (JIRA: ROFR-3459):**
   - "Transform" operation for non-hardened child key.



Key operations permitted ?

Certain operations may be disabled due to the cryptographic policy.

DERIVEKEY, EXPORT, APPMANAGEABLE, SIGN, VERIFY, TRANSFORM

□ Encrypt ?	□ Decrypt ?	□ WrapKey ?	□ UnwrapKey ?
☑ DeriveKey ?	□ MacGenerate ?	□ MacVerify ?	☑ App Manageable ?
☑ Sign ?	☑ Verify ?	□ AgreeKey ?	☑ Transform ?
☑ Export ?			

Creating exportable Security Object can be unsafe

For more details, refer to User's Guide: Key Lifecycle Management.

3. **Added "Transform" operation to the app and group permitted operations for the BIP32 keys (JIRA: ROFR-3467):**

   When you create a group or app from the Fortanix DSM UI, it will additionally have the new "TRANSFORM operation active by default.

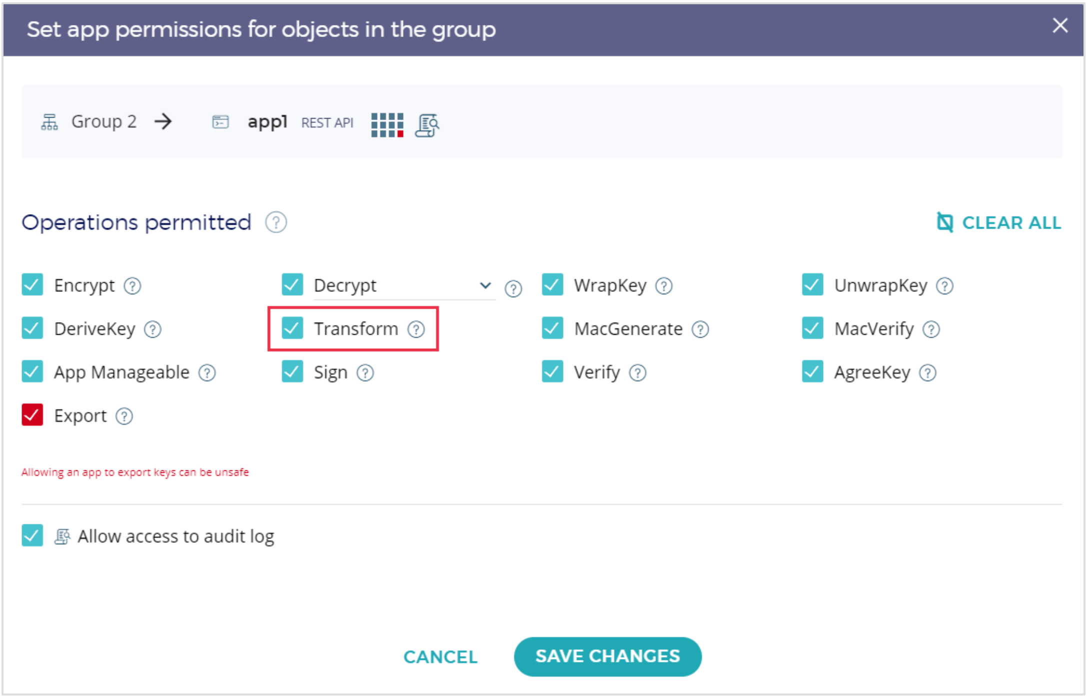
RELEASE NOTE

Date: 26-Aug-22

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

Software: Fortanix Data Security Manager SaaS

Version: 4.10



Set app permissions for objects in the group

Group 2 → app1 REST API

Operations permitted

CLEAR ALL

☑ Encrypt
☑ Decrypt
☑ WrapKey
☑ UnwrapKey
☑ DeriveKey
☑ Transform
☑ MacGenerate
☑ MacVerify
☑ App Manageable
☑ Sign
☑ Verify
☑ AgreeKey
☑ Export

Allowing an app to export keys can be unsafe

☑ Allow access to audit log

For more details, refer to [User's Guide: Security Controls for Fortanix Data Security Manager Applications](#).

4. **Allow downloading all security objects as a CSV file (JIRA: ROFR-3451):** In addition to downloading the currently visible security objects on the Security Objects page using the **DOWNLOAD AS CSV** option, you can also download all the security objects in the account using the **DOWNLOAD ALL** button.

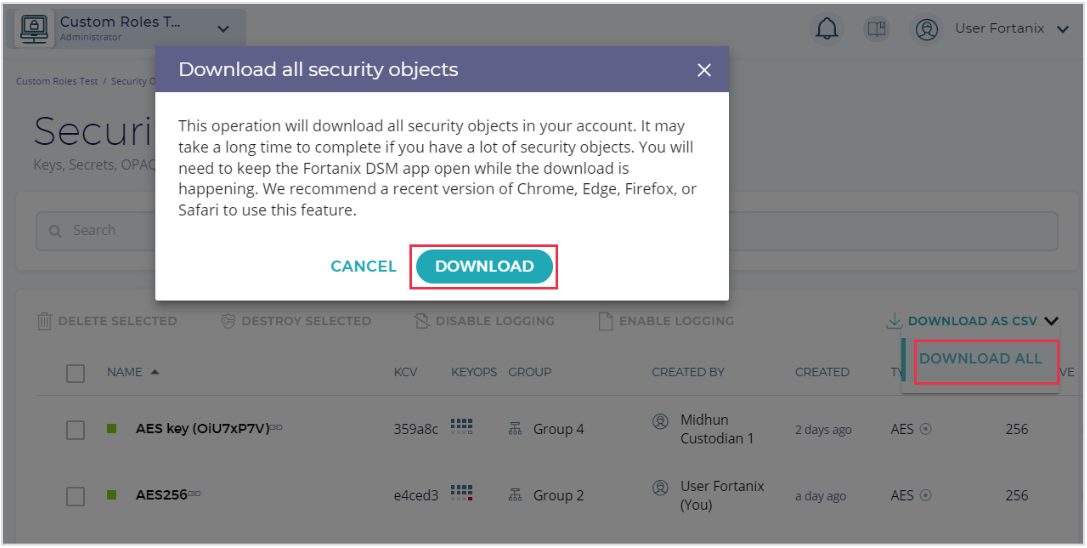
RELEASE NOTE

Date: 26-Aug-22

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

Software: Fortanix Data Security Manager SaaS

Version: 4.10



Download all security objects

This operation will download all security objects in your account. It may take a long time to complete if you have a lot of security objects. You will need to keep the Fortanix DSM app open while the download is happening. We recommend a recent version of Chrome, Edge, Firefox, or Safari to use this feature.

CANCEL DOWNLOAD

□	NAME ▲	KCV	KEYOPS	GROUP	CREATED BY	CREATED	TY	VE
□	AES key (OiU7xP7V)	359a8c		Group 4	Midhun Custodian 1	2 days ago	AES	256
□	AES256	e4ced3		Group 2	User Fortanix (You)	a day ago	AES	256

5. **Support for BYOK Plugin for Oracle Cloud Infrastructure (OCI) Vault (JIRA: PROD-4050):** This release adds support for generating a symmetric and asymmetric encryption key in Fortanix DSM and then BYOK it into the OCI vault.

   For more details, refer to User's Guide: Plugin Library.

ENHANCEMENTS TO EXISTING FEATURES

1. **Automatic Linked key rotation for Azure Keys (JIRA: PROD-5163)**.

   You can now schedule a key rotation policy for the Fortanix DSM source key that has linked Azure keys that are copies of the source key so that the linked Azure keys are also periodically rotated automatically. This can be enabled by selecting the **Rotate all copied keys** option.

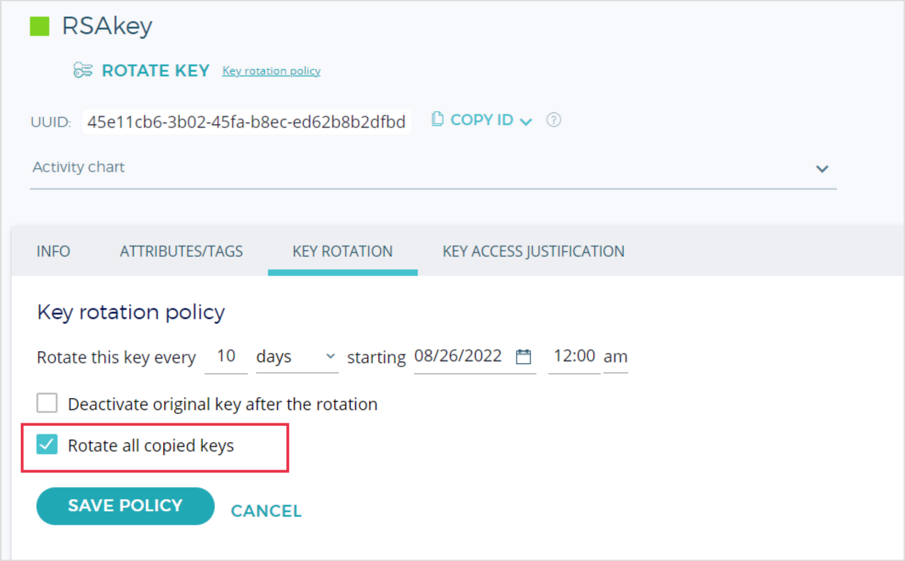
RELEASE NOTE

Date: 26-Aug-22

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

Software: Fortanix Data Security Manager SaaS

Version: 4.10



UUID: 45e11cb6-3b02-45fa-b8ec-ed62b8b2dfbd

Key rotation policy

Rotate this key every 10 days starting 08/26/2022 12:00 am

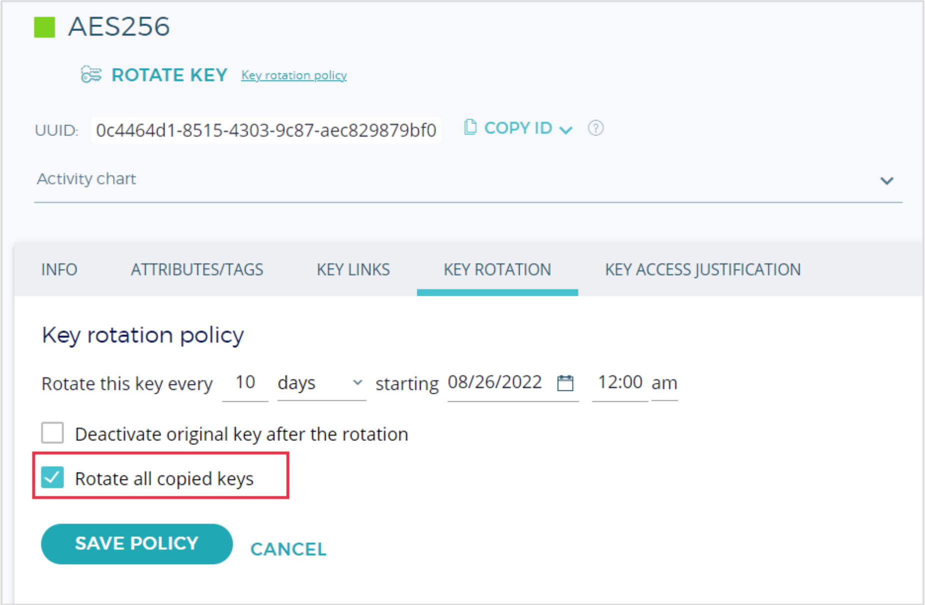
□ Deactivate original key after the rotation

☑ Rotate all copied keys

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

2. **Automatic Linked key rotation for AWS External KMS Keys (JIRA: PROD-5050)**.

   You can now schedule a key rotation policy for the Fortanix DSM source key that has linked AWS KMS keys that are copies of the source key so that the linked AWS KMS keys are also periodically rotated automatically. This can be enabled by selecting the **Rotate all copied keys** option.



🟩 AES256

ROTATE KEY Key rotation policy

UUID: 0c4464d1-8515-4303-9c87-aec829879bf0 COPY ID

Activity chart

Key rotation policy

Rotate this key every 10 days starting 08/26/2022 12:00 am

☐ Deactivate original key after the rotation

☑ Rotate all copied keys

For more details, refer to User's Guide: AWS External KMS.

3. **Automatic Linked key rotation for Azure Managed HSM Keys (JIRA: PROD-3037)**.

   You can now schedule a key rotation policy for the Fortanix DSM source key that has linked AWS Managed HSM keys that are copies of the source key so that the linked Azure Managed HSM keys are also periodically rotated automatically. This can be enabled by selecting the **Rotate all copied keys** option.

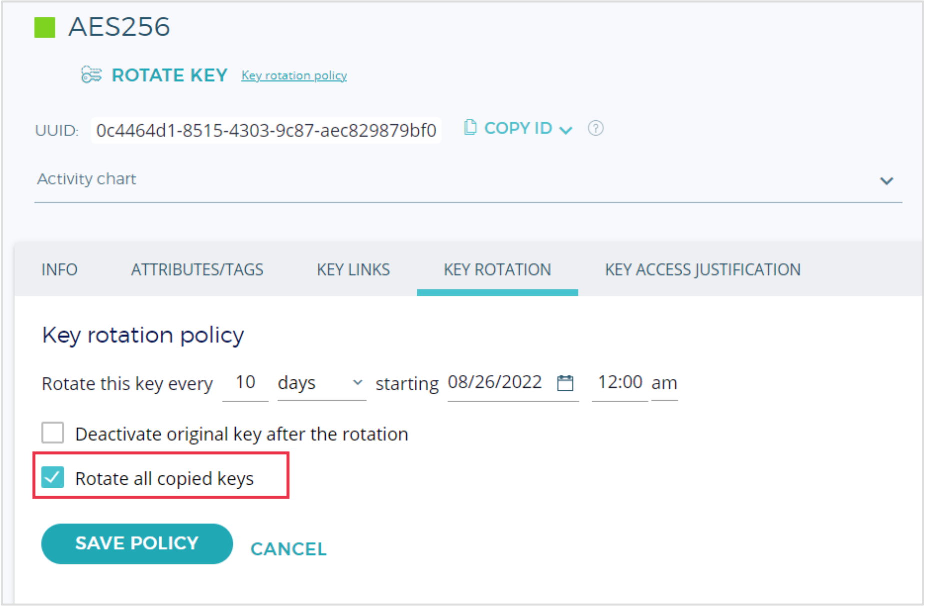
RELEASE NOTE

Date: 26-Aug-22

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

Software: Fortanix Data Security Manager SaaS

Version: 4.10



AES256

UUID: 0c4464d1-8515-4303-9c87-aec829879bf0

Key rotation policy

Rotate this key every 10 days starting 08/26/2022 12:00 am

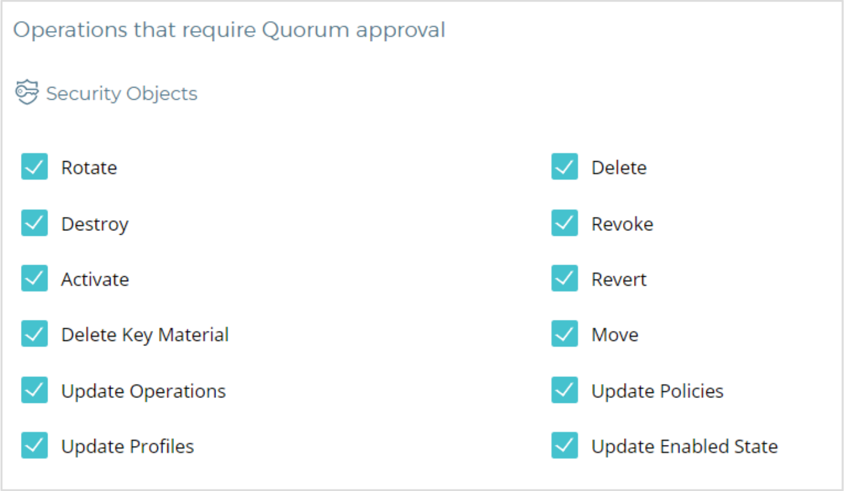
□ Deactivate original key after the rotation

☑ Rotate all copied keys

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

4. **The "Create" permission is now hidden for Quorum approval policy for a Fortanix DSM group (JIRA: ROFR-3159)**.

   As there is no Quorum policy check for the "Create" operation and the action of creating a security object does not initiate a Quorum approval request, hence the "Create" security object operation is hidden from the list of operations that require quorum approval.



Operations that require Quorum approval

Security Objects

☑ Rotate

☑ Destroy

☑ Activate

☑ Delete Key Material

☑ Update Operations

☑ Update Profiles

☑ Delete

☑ Revoke

☑ Revert

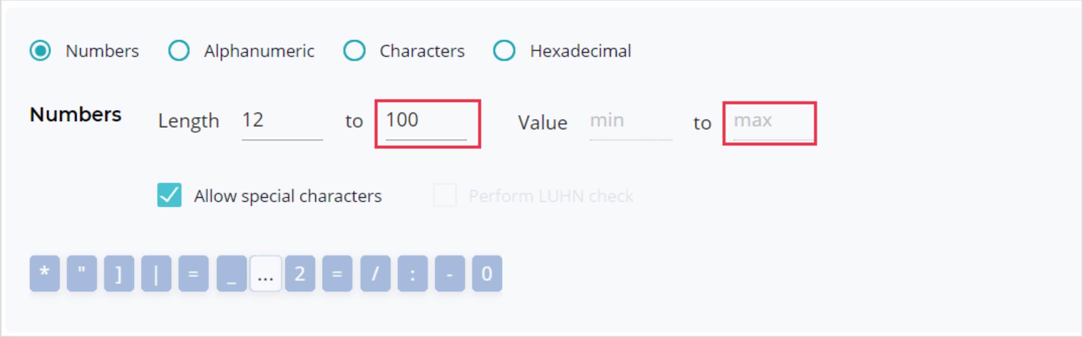
☑ Move

☑ Update Policies

☑ Update Enabled State

5. **Custom Tokenization – restored max Length limit and removed max Value limit (JIRA: ROFR-3295).**

   Added max **Length** limit for custom tokenization and removed the wrongly added limit for the max **Value** field.



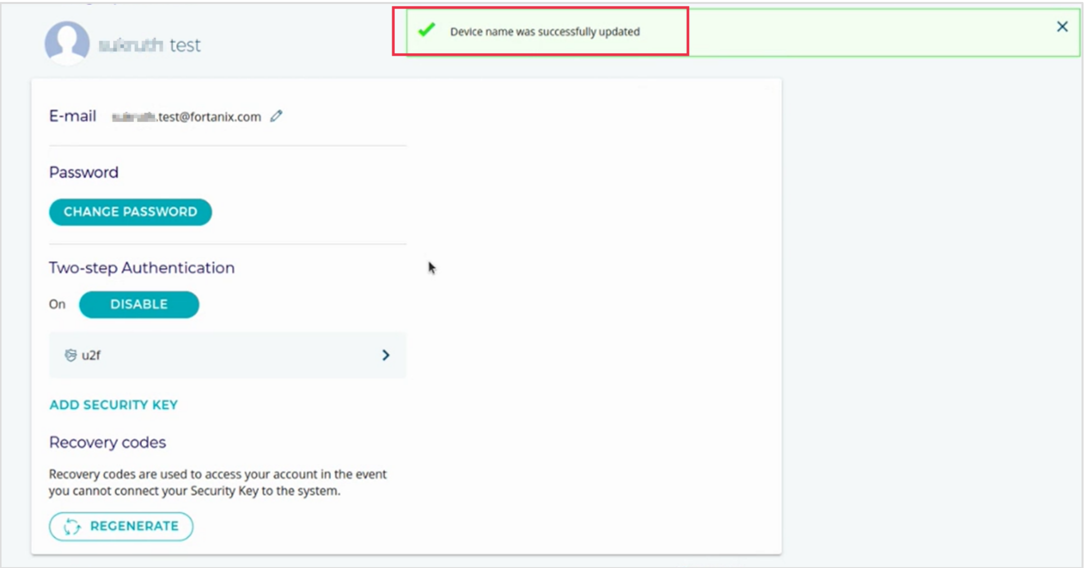
● Numbers ○ Alphanumeric ○ Characters ○ Hexadecimal

Numbers Length 12 to 100 Value min to max

☑ Allow special characters □ Perform LUHN check

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

6. **Added toast message when renaming and deleting the u2f security key (JIRA: ROFR-3295).**



[redacted] test

✓ Device name was successfully updated ✕

E-mail [redacted].test@fortanix.com

Password

CHANGE PASSWORD

Two-step Authentication

On DISABLE

u2f

ADD SECURITY KEY

Recovery codes

Recovery codes are used to access your account in the event you cannot connect your Security Key to the system.

REGENERATE

OTHER IMPROVEMENTS

1. **Flattened the cache structure for Signed JWT to avoid the small cap on the number of keys per source (JIRA: PROD-5195).**
2. **Enhanced the API for Fortanix DSM Groups (JIRA: PROD-4603).**

RELEASE NOTE

Date: 26-Aug-22

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

Software: Fortanix Data Security Manager SaaS

Version: 4.10

3. **Obtained the relations/mapping report for Fortanix DSM security objects, groups, users, and so on (JIRA: PROD-4571).**
4. **Enhanced the `GET All accounts` API to take query parameters for `start` and `end` to be able to return all accounts (JIRA: PROD-4093).**

BUG FIXES

1. Fixed an issue where the backend ignores `connect-src` whitelist in the `manifest.json` file (**JIRA: ROFR-3176**).
2. Fixed an issue where after upgrading to DSM 4.9, `GET_SOBJECTS` was returned by error in the UI during quorum approval (**JIRA: PROD-5196**).
3. Fixed an issue where the Fortanix AWX plugin was not working as expected (**JIRA: DEVOPS-2982**).
4. Fixed an issue where `ActionType::Administrative` is used instead of `ActionType::RunPlugin` during plugin invocation. (**JIRA: PROD-5185**).
5. Fixed an issue where the sdkms-cli shows a byte array instead of a base64 encoding strong (**JIRA: PROD-5170**).
6. Fixed an issue where a user was unable to add a Quorum policy to an existing KEK group after removing the Quorum policy (**JIRA: PROD-5159**).
7. Fixed a JSON error message on the deletion of Splunk log integration (**JIRA: ROFR-3424**).
8. Fixed a user PATCH panic in mfa/u2f path (**JIRA: PROD-5132**).
9. Fixed an issue where a user should not be allowed to update the group of KEK to another secondary group (**JIRA: ROFR-3415**).
10. Fixed an issue where a user was unable to delete a security object after deleting the group (**JIRA: PROD-5005**).
11. Fixed backend parsing issues for minimum/maximum length custom token schemas (**JIRA: ROFR-3293**).

12. Fixed an issue where a password continued to be stored while disabling the U2F (**JIRA: ROFR-3284**).
13. Fixed alignment issues and error message updates on the U2F recovery page (**JIRA: ROFR-3272**).
14. Fixed an issue where the input Secret object values were not saved after importing resulting in a mismatch with the output Secret object value for the value format text(UTF-8) (**JIRA: ROFR-3225**).

QUALITY ENHANCEMENTS / UPDATES

- Set `dclocal_read_repair` to `0` on all tables in Cassandra keyspace. **(JIRA: DEVOPS-2898)**.
- Implemented Cassandra Heap and Memory Tuning **(JIRA: DEVOPS-2898)**.
- Implemented audit log partitioning by time in Cassandra database **(JIRA: PROD-5150)**.
- Enabled `trickle_fsync` by setting it to `true` in Cassandra when using with solid-state drives (SSDs) for better performance **(JIRA: DEVOPS-2896)**.
- Configured Cassandra to use G1GC in JVM for performing more efficient JVM Garbage Collections (GCs) **(JIRA: DEVOPS-2566)**.

SECURITY FIXES

1. Blocked the ICMP and TCP timestamp requests that can be used to determine system time **(JIRA: DEVOPS-2915)**.
2. Set etcd ciphersuite to `TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256` to ensure that all communication has guarantees **(JIRA: DEVOPS-2914)**.

RELEASE NOTE

Date: 26-Aug-22

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

Software: Fortanix Data Security Manager SaaS

Version: 4.10

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 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.
-

RELEASE NOTE

Date: 26-Aug-22

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

Software: Fortanix Data Security Manager SaaS

Version: 4.10

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.

Fortanix Data Security Manager SaaS Release Notes

Release 4.10