What's New 'Cliff Notes'

SmartKey 2020.2.2

SmartKey 2020.2.2 contains changes for version 3.20.

New Features

Copy Key between Groups

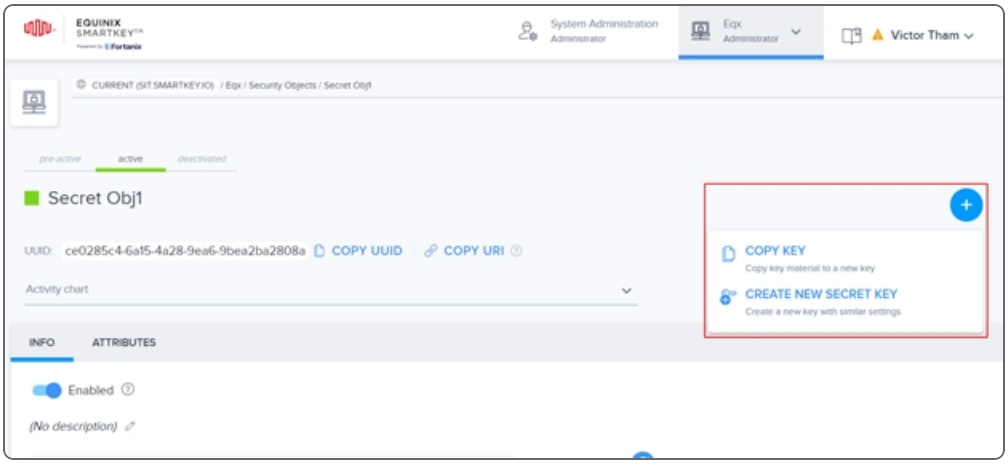
The copy key feature will copy a security object from a standard SmartKey group to another group. This feature has the following advantages:

- Maintains a single source of key material while using/importing that key across various SmartKey groups where applications in respective groups may need to use a single key to meet some business objectives.
- Maintains a link of various copies of same key material to the source key for audit and tracking purposes.
- Later, the user may want to re-key all the keys at various destinations centrally by re-keying/rotating the source key.

The following actions will take place as part of the copy key operation:

- A new key will be created into the target group. The new key will have the same key material as the original.
- The source key links to the copied keys. There will be a link maintained from all copied keys to the source key.

The Copy Key feature can be accessed through the detailed view of security object.



Enhancements to existing functions

Quorum Policy

Release 3.20 comes with major improvements in quorum policy.

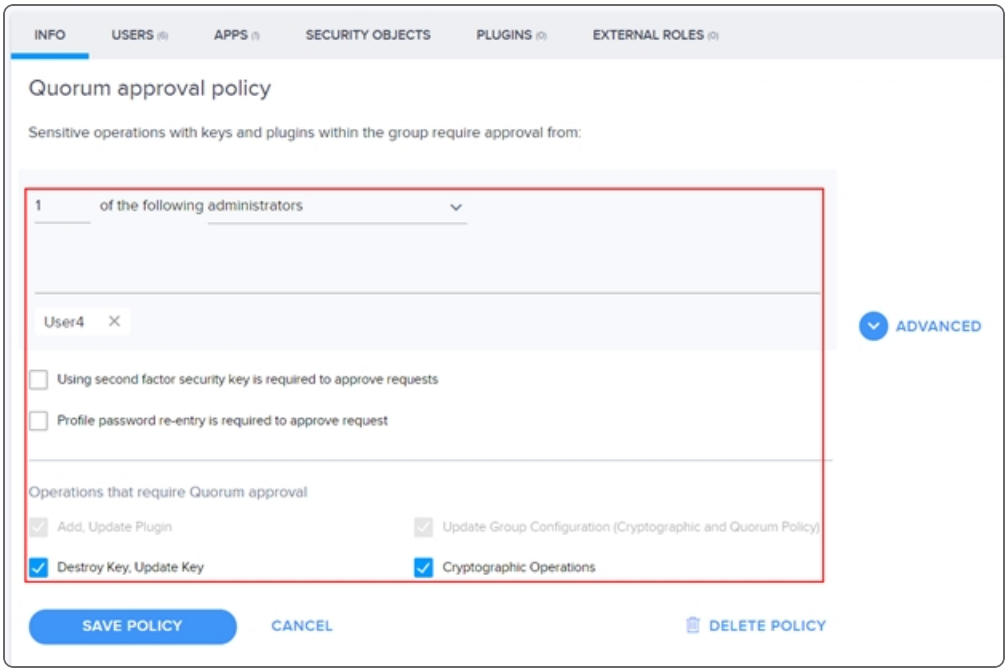
- A group administrator may enable a quorum approval policy on a group, which mandates that all security-sensitive operations in that group would require a quorum approval. Starting this release, the group admin can choose which operation to include for the quorum approval.

  The following operations are selected by default and cannot be altered.

  - Add, update plugin
  - Update Group Configuration (Cryptographic and Quorum Policy)

  On the group level, the following operations can be configured for quorum approval.

  - Destroy key, update key
  - Cryptographic operations



- On the account level, the account administrator now has the same ability to choose which operations to include for account quorum approval.

  The following operations are selected by default and cannot be altered.

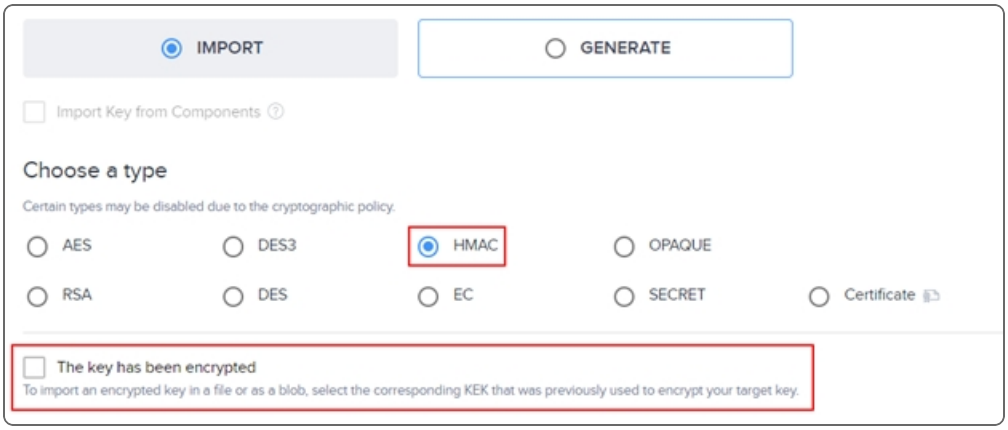
  - Quorum policy update

  On the account level, the following operations can be configured for quorum approval.

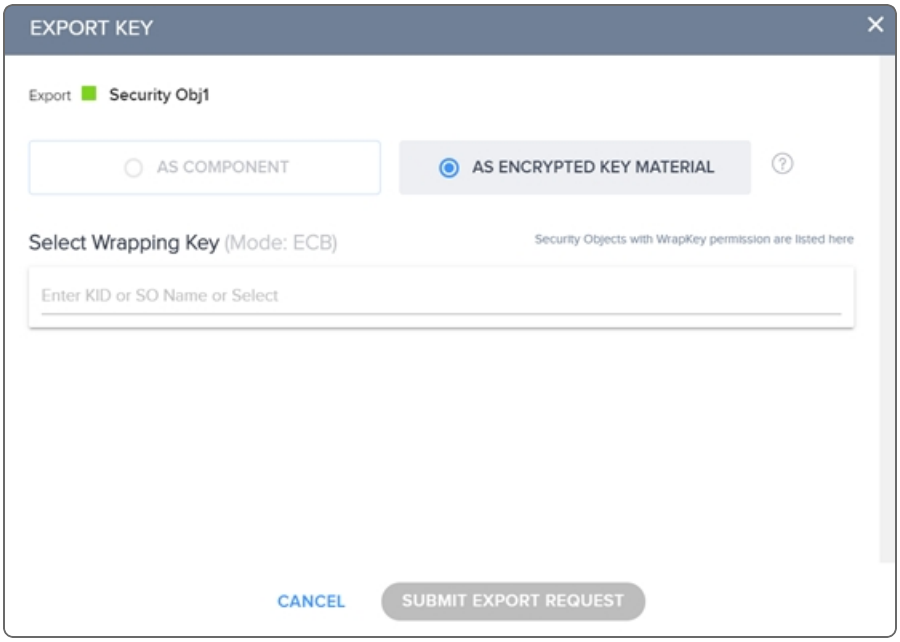
  - Update authentication methods
  - Cryptographic policy update
  - Log Management
- You can now add a reason to decline a quorum request. The denial reason will also be logged in the audit logs for future reference.

Improvements in Import/Export for HMAC keys

Full key import (HMAC): Allows a HMAC that was previously wrapped (encrypted) by a key from SmartKey to be imported using “The key has been encrypted” checkbox.



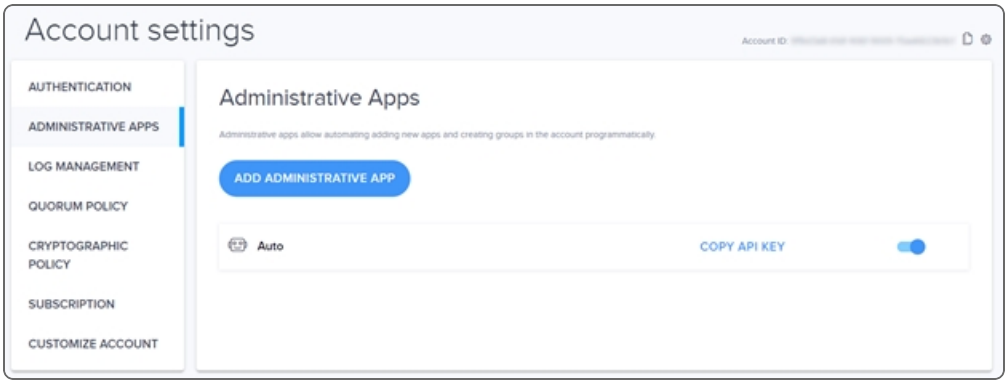
Full key Export: Allows a HMAC key to be exported where the Key should have the "Export" permission selected and a Quorum policy set. And the wrapping key must have a WRAP permission.



Service Accounts renamed to Administrative Apps

This function creates and manages special apps with access to account-level privileges, like adding new apps, or groups.

Note that account members and auditors are not allowed to add/update Administrative Apps, only administrators have this privilege.



Audit Logs

This release adds “response time” column to the audit logs.

Improvements in Splunk integration

Previously, when SmartKey sent requests to the Splunk server, any slowness in the transaction unintentionally caused a performance drop in the SmartKey APIs. In this release, we have introduced a way to send the Splunk logs in batches rather than creating a new client and connection for every single request. This should improve the performance of Splunk logging.

Improvements in Cryptographic Parameters in KMIP

This release adds support for the Create operation for the attribute Cryptographic Parameters.

Support for RSA sign, encrypt, and export permissions for Crypto Policy

This release adds support for the Signature, Encrypt, and Export permissions for RSA type of keys in the Group/Account level Crypto Policies.

Quality of life enhancements

- Fixed issues related to failed deployer pod during upgrade
- Cassandra Database has been updated to 3.11.7-1
- On the left menu bar, the Events tab has been split into two tabs - Audit Log and Tasks.

Bug Fixes

PKCS#11 client

- Fixed reauthentication issue when authenticating using app name and app secret

JCE client

- Fixed an issue which prevented “sdkms” keystore to load more than 1000 security objects.
- Modified Cipher behavior to use singlepart API if `Cipher.update()` is not used and directly `Cipher.doFinal(byte[])` is called. This makes the Cipher behavior in-line with JCA specification and improves latency if multipart is not intended for Cipher operation with smaller input. See https://docs.oracle.com/javase/8/docs/api/javax/crypto/Cipher.html#doFinal-byte:A-

Known Issues

- RSA keys with non-default `encryption_policy` or `signature_policy` will not work when used with default cryptographic policy created by UI. The Cryptographic Policy can be patched using API for appropriate policy in use for resolving this issue.

- Cannot delete Cryptographic Policy at account level when using Account quorum policy which enforces quorum requirement for cryptographic policy. Account quorum policy can be relaxed temporarily for allowing the removal of cryptographic policy.