

RELEASE NOTE

Date: 2-Mar-23

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

Software: Fortanix Data Security Manager SaaS

Version: 4.15

OVERVIEW

This document provides an overview of new features, general enhancements, improvements, and resolved issues in the Fortanix Data Security Manager (DSM) SaaS 4.15 release.

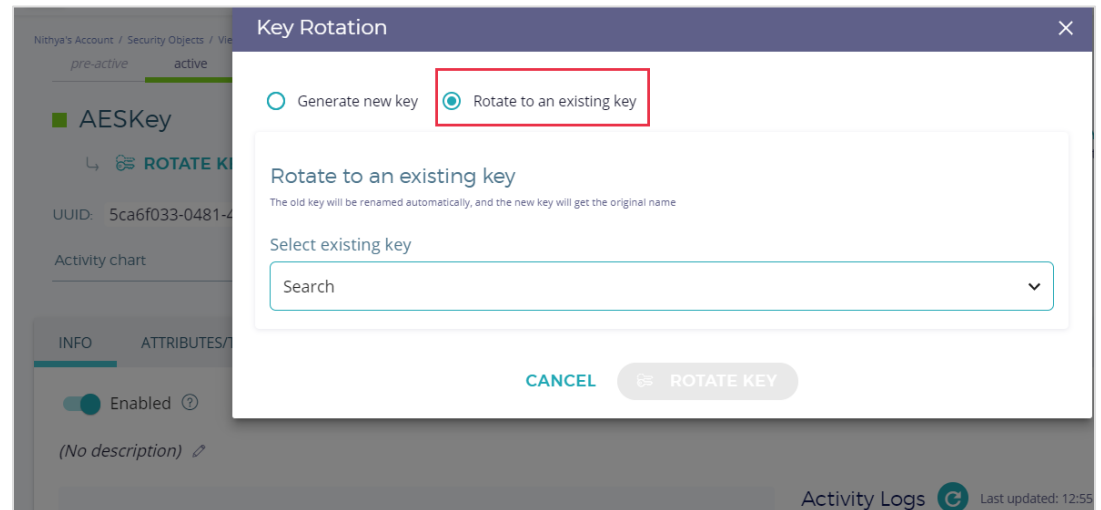


NOTE: This release is for **SaaS only** and not available for On-Prem installations.

NEW FUNCTIONALITY / FEATURES

1. Rotate a Fortanix DSM security object to an existing security object (JIRA: PROD-5855):

This release adds support for the ability to rotate a Fortanix DSM key to the value of an existing key so that the key lifecycle history and rotation history are maintained.



For more details refer to the [User's Guide: Key Lifecycle Management](#).

RELEASE NOTE

Date: 2-Mar-23

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

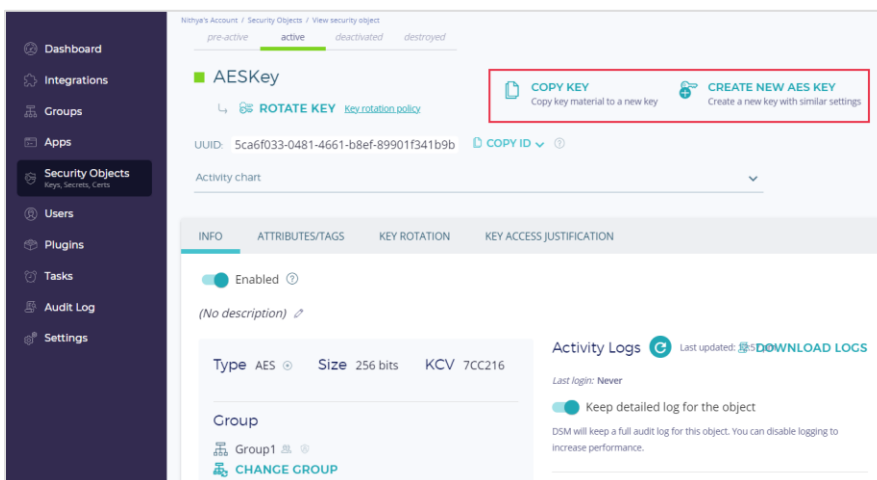
Software: Fortanix Data Security Manager SaaS

Version: 4.15

ENHANCEMENTS TO EXISTING FEATURES

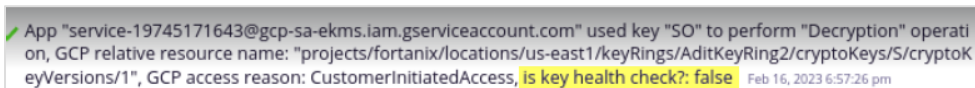
1. Improved the design for the Fortanix DSM copy key workflow (JIRA: ROFR-3844).

The **NEW OBJECT** option on the security object detailed view now has an improved design to copy a key and create a new key with the same parameters as an existing security object.



For more details refer to the [User's Guide: Copy Key](#).

2. Removed “is key health check?: true/false” from the GCP EKM audit logs (JIRA: PROD-6387).



The screenshot shows a GCP EKM audit log entry. The log text is: 'App "service-19745171643@gcp-sa-ekms.iam.gserviceaccount.com" used key "SO" to perform "Decryption" operation, GCP relative resource name: "projects/fortanix/locations/us-east1/keyRings/AditKeyRing2/cryptoKeys/S/cryptoKeyVersions/1", GCP access reason: CustomerInitiatedAccess, is key health check?: false Feb 16, 2023 6:57:26 pm'. The field 'is key health check?: false' is highlighted in yellow.

3. Added new “Custom Attributes” column in the Fortanix DSM Security Objects “Download as CSV” report (JIRA: ROFR-3893).

This release adds a new column that will contain all the custom attributes as a JSON-encoded string. You can apply a substring filter on the CSV column as per your needs in Excel.

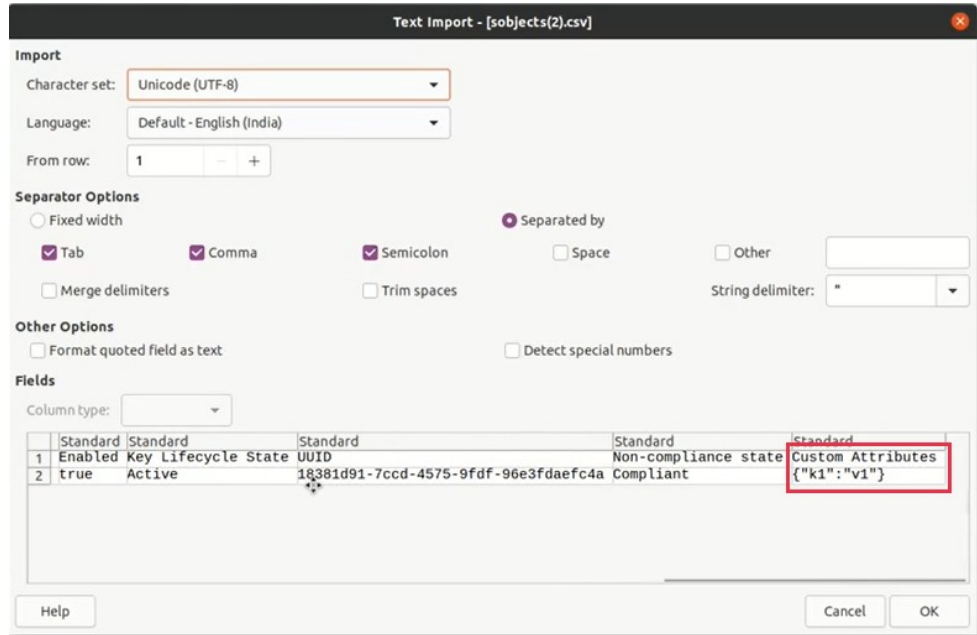
RELEASE NOTE

Date: 2-Mar-23

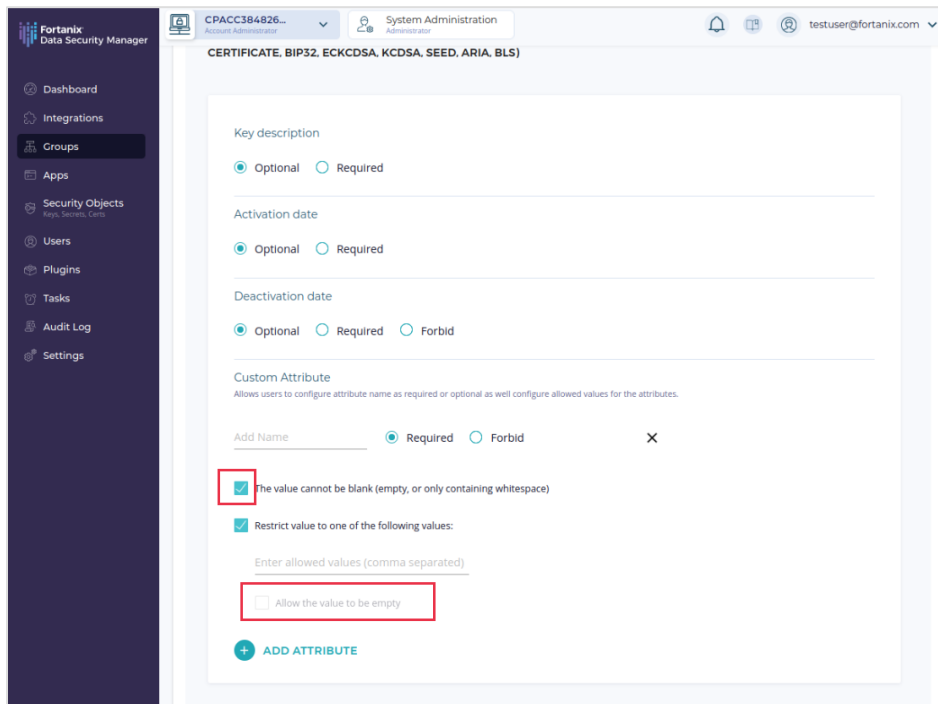
Subject: Software changes, updates, bug fixes, etc.

Software: Fortanix Data Security Manager SaaS

Version: 4.15



4. Disabled the “Allow the value to be empty” option when “The value cannot be blank (empty, or only containing whitespace)” option is selected when configuring the Key Metadata policy for a group (JIRA: ROFR-3873).



RELEASE NOTE

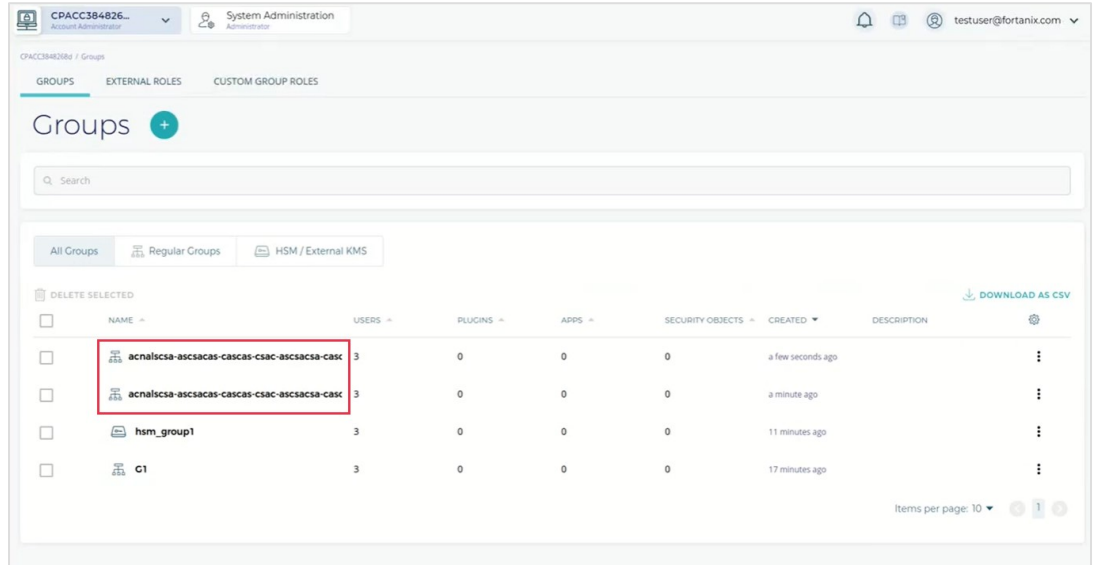
Date: 2-Mar-23

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

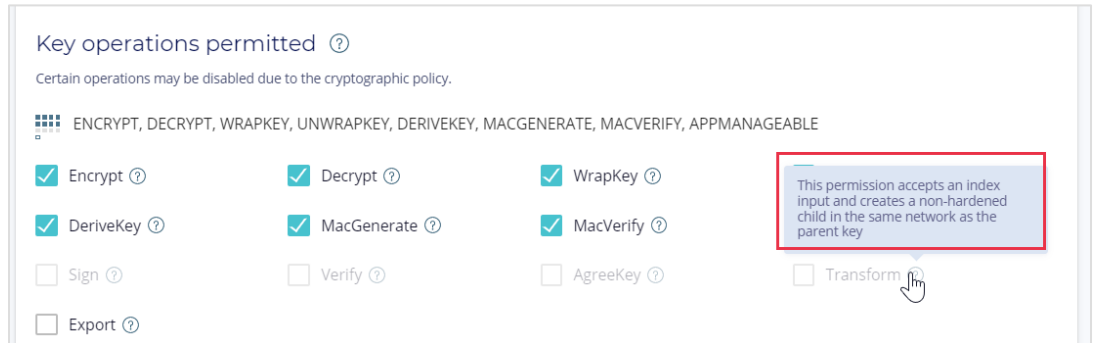
Software: Fortanix Data Security Manager SaaS

Version: 4.15

5. The Fortanix DSM Groups table will not collapse the group names on small screen widths (JIRA: ROFR-3866).



6. Improved the tooltip for the security object “Transform” permission (JIRA: ROFR-3858).



7. Improved the activity logs for Plugin (JIRA: ROFR-3839).

The plugin activity logs on the Plugin detail page now also show the plugin audit logs where the plugin is the actor.

8. Improved the Fortanix DSM App detailed view so that it does not fetch LDAP credentials on page load. (JIRA: ROFR-3827).

The LDAP credentials in the app detailed view can now only be accessed by clicking the “Show credentials” button.

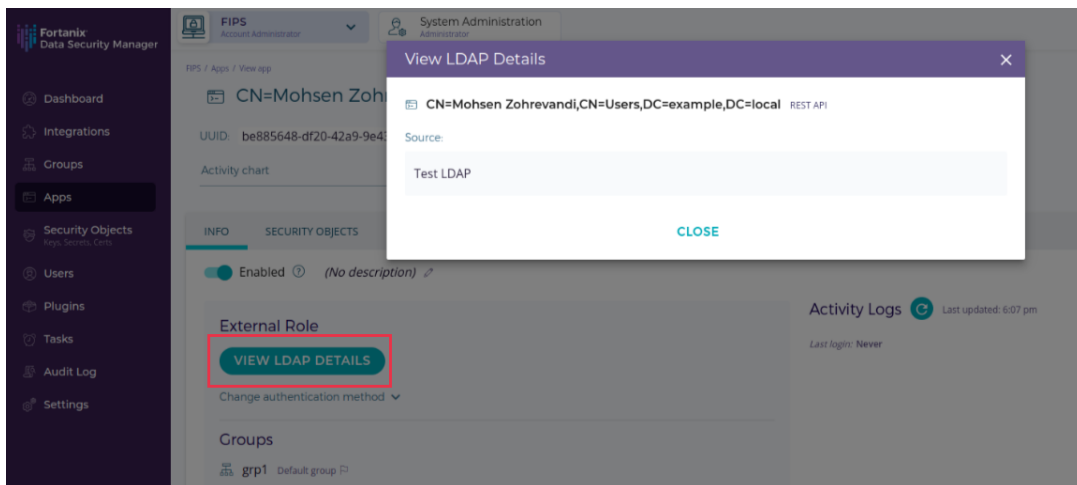
RELEASE NOTE

Date: 2-Mar-23

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

Software: Fortanix Data Security Manager SaaS

Version: 4.15



9. Deduplicated the text “(Formerly known as Equinix SmartKey)” in various email templates (JIRA: PROD-6072).

You have been invited to join an account on Fortanix Data Security Manager (Formerly known as Equinix SmartKey)

Hello, example@fortanix.com

You have been invited by User A (example211@gmail.com) to join an account on Fortanix Data Security Manager (Formerly known as Equinix SmartKey)! Join Fortanix Data Security Manager (Formerly known as Equinix SmartKey) Account: BYOE. Please accept the invitation by clicking on the button below.

ACCEPT INVITATION

If you don't like clicking buttons, you may copy/paste this link to your browser:
<https://www.sit.smartkey.io>

You can safely ignore and discard this email if you don't want to take this action.

Thanks,
 Data Security Manager Team

RELEASE NOTE

Date: 2-Mar-23

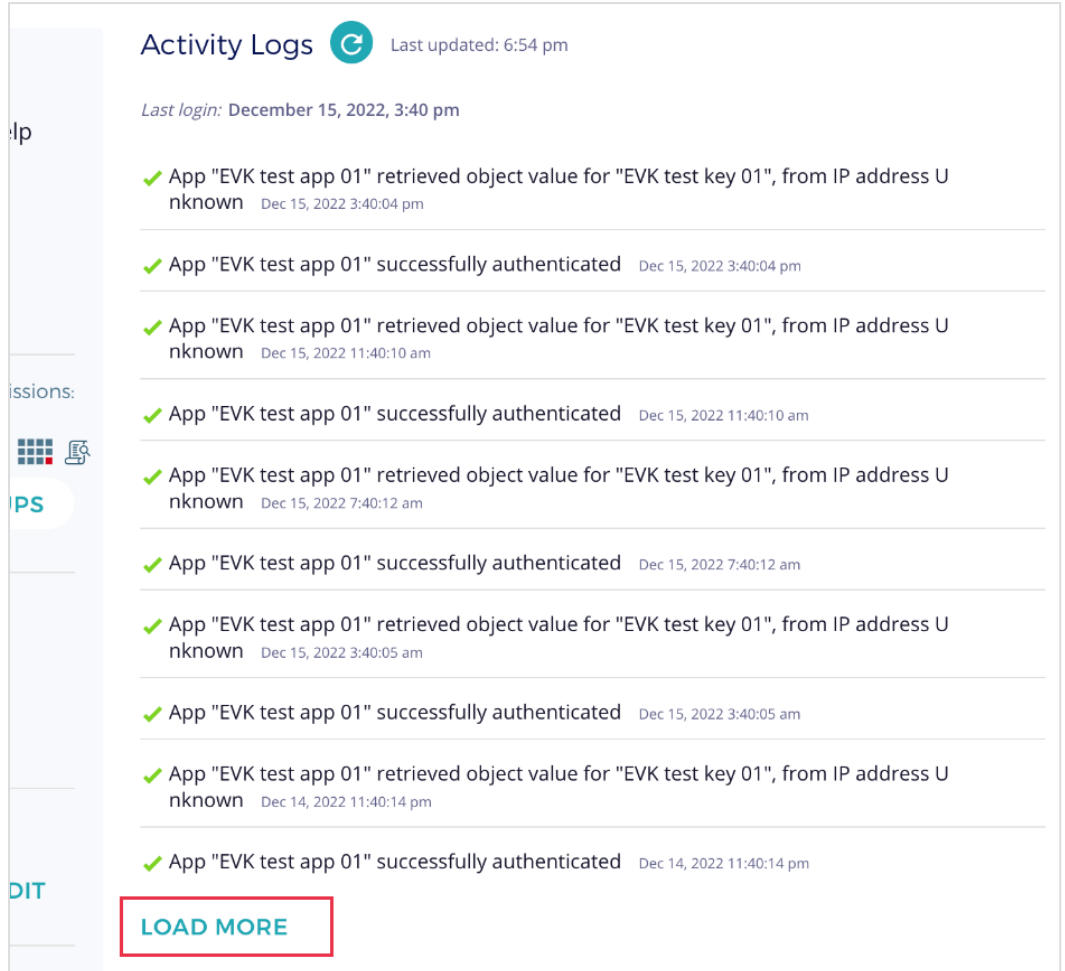
Subject: Software changes, updates, bug fixes, etc.

Software: Fortanix Data Security Manager SaaS

Version: 4.15

10. Added “Load more” button in the Activity Logs in the Fortanix DSM app detailed view (JIRA: ROFR-3816).

This release adds a “Load more” button in the Activity Logs for the Fortanix DSM apps when there are more than 10 items.



The screenshot displays the 'Activity Logs' section of the Fortanix DSM app. It features a header with a refresh icon and the text 'Last updated: 6:54 pm'. Below the header, there is a list of activity logs. Each log entry starts with a green checkmark icon, followed by a description of the activity and a timestamp. The activities include retrieving object values and successful authentications. At the bottom of the list, there is a red-bordered button labeled 'LOAD MORE'.

11. Removed Ed25519 and X25519 curves when generating a security object of type EC-KCDSA (JIRA: ROFR-3720).

RELEASE NOTE

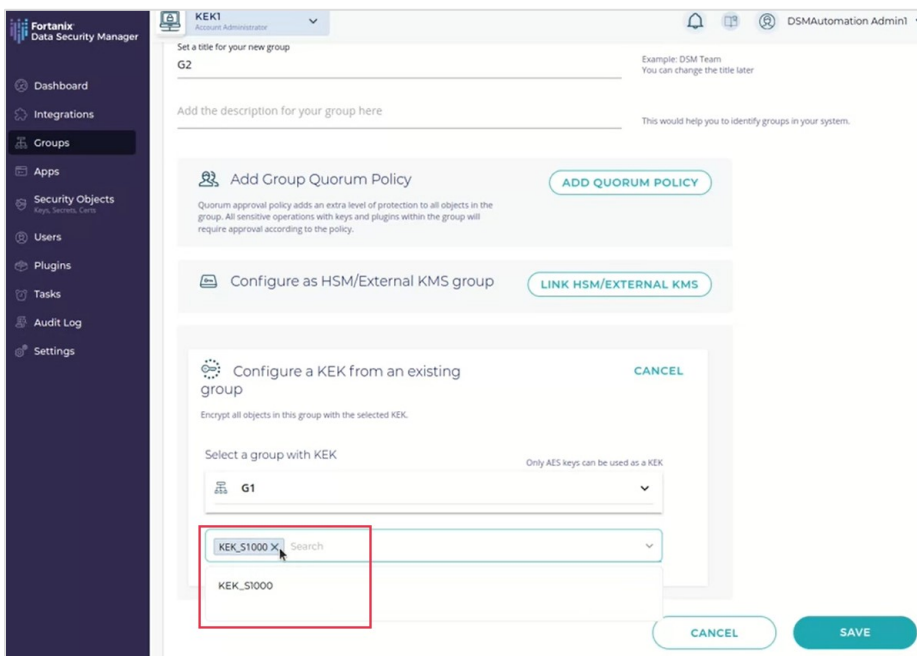
Date: 2-Mar-23

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

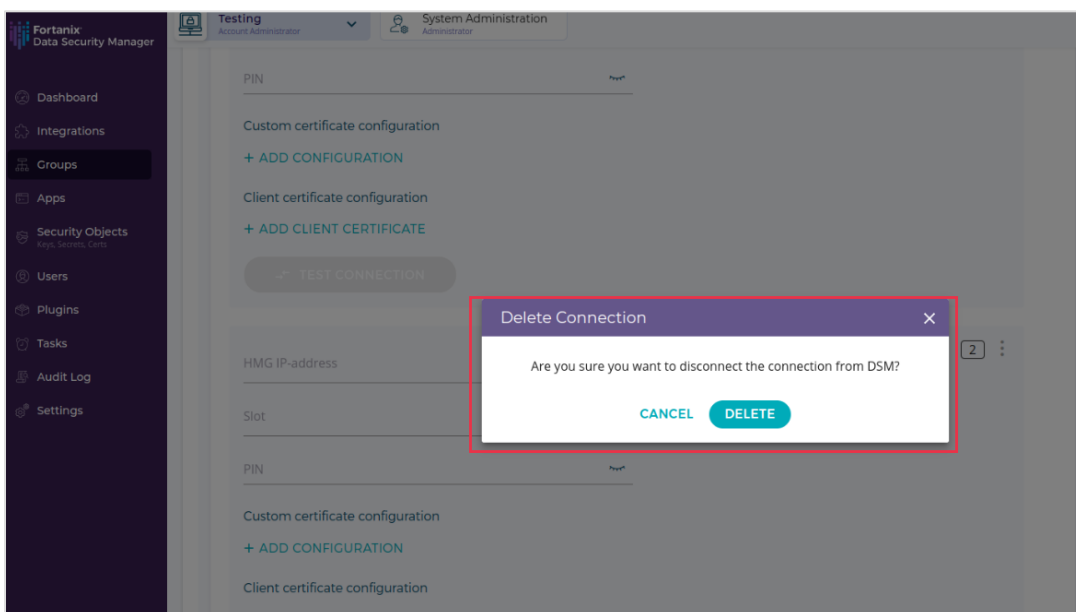
Software: Fortanix Data Security Manager SaaS

Version: 4.15

12. Support for LazySelect component to load KEKs in the drop down for the “Configure KEK from an existing group” workflows in the New Groups page and Group’s detail page (JIRA: ROFR-3648).



13. Added a confirmation box when deleting an HSM/KMS connection (JIRA: ROFR-2473).



RELEASE NOTE

Date: 2-Mar-23

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

Software: Fortanix Data Security Manager SaaS

Version: 4.15

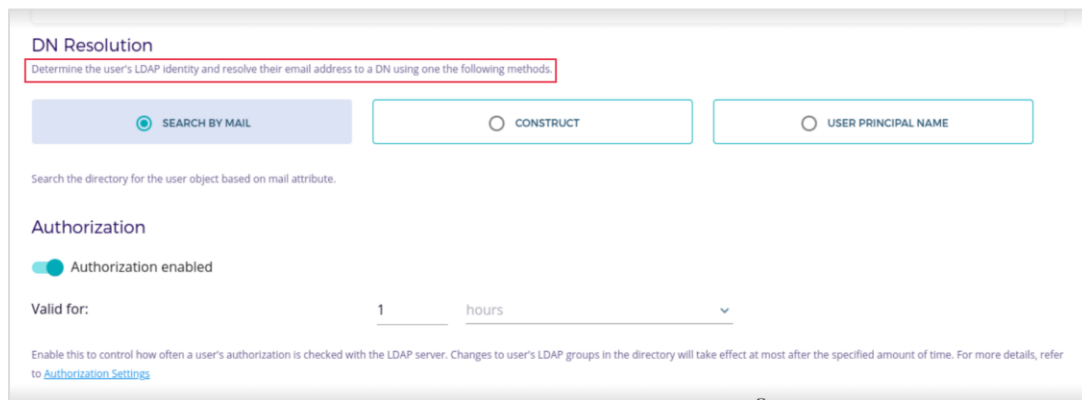
14. Added missing tooltips and better descriptions for various options in the UI (JIRA: ROFR-2298).

- Added better tooltip description for the **Allow missing justification** option for the **Google Service Account** authentication method.
- Added better tooltip description for **MacGenerate** security object permission.
- Added missing tooltip description for **Operations permitted** heading in the "Set app permissions for objects in the group" modal window.

15. Disallow a user from uploading more than three DSM software versions at any time (JIRA: ROFR-2298).

The Software upload workflow now prevents you from uploading more than three DSM software files and prompts you to delete one of the staged versions of the DSM software when you exceed more than three packages.

16. Added description for the LDAP DN resolution methods in the DSM LDAP settings configuration page (JIRA: ROFR-2111).



OTHER IMPROVEMENTS

- Added a new node label to the Kubernetes node during cluster upgrade (JIRA: DEVOPS-3665).
- The BIOS package is now installed on the Fortanix DSM servers (JIRA: DEVOPS-3579).

RELEASE NOTE

Date: 2-Mar-23

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

Software: Fortanix Data Security Manager SaaS

Version: 4.15

3. The `crypto/v1/keys` API now support filter by 'enabled' (JIRA: PROD-6162).
4. Refactored the "Activity Logs" code to a single reusable component (JIRA: ROFR-3852).
5. Refactored the code for the Add application modal window from the Groups detailed view to use the same component as the regular Add application flow (JIRA: ROFR-3835).
6. Added support for signing of SAML authentication requests for SSO integration using SAML (JIRA: PROD-3273).
7. Enhanced the database data encoding (JIRA: PROD-816).
8. Created a script to automate FIPS cluster (JIRA: PROD-5829).
9. Updated unmaintained packages common in DSM SaaS OS versions (JIRA: DEVOPS-3487).
10. The `client/pgpsign/ci-test.sh` script now uses the PGP version from the official Python repository (JIRA: PROD-4101).

INTEGRATIONS

1. Added support for IIS integration with Fortanix CNG provider (JIRA: PROD-4537). For more information, refer to [DSM with Microsoft IIS Guide](#).

CLIENT IMPROVEMENTS

1. Published the following Fortanix DSM clients to the public repository (JIRA: DEVOPS-3326):

The following Fortanix DSM clients are now available for download in Linux repositories.

- [PKCS#11](#)
- [HSM Gateway](#)
- [Sequoia-PGP](#)

2. **PKCS#11:** The Fortanix DSM PKCS#11 client now uses `keytool -alias` input for the security object name (JIRA: PROD-5720).

RELEASE NOTE

Date: 2-Mar-23

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

Software: Fortanix Data Security Manager SaaS

Version: 4.15

3. Sequoia-PGP:

- a. Implemented sq-dsm CLI to the get list of keys per app ID (JIRA: PROD-6220).
- b. Added support for the generation of signature subkey as a separate entity within DSM (JIRA: PROD-5998).

DSM-ACCELERATOR CLIENT IMPROVEMENTS

1. **DSM-Accelerator JCE Provider:** The `libdsmaccelerator.so` path is now configurable (JIRA: PROD-6186).
2. **DSM-Accelerator Webservice:**
 - a. Added support for certificate chain in TLS certificate (JIRA: PROD-5651).
 - b. Added support for granular key cache management (JIRA: PROD-5494).

For more details, refer to [Developer's Guide: Fortanix DSM-Accelerator Webservice](#).

TERRAFORM PROVIDER CLIENT IMPROVEMENTS

1. **Added LDAP support for Terraform Provider** (JIRA: DEVOPS-3550).

For a complete list of features supported by the Fortanix DSM Terraform provider, refer to the [Developer's Guide: Terraform Provider](#).

QUALITY ENHANCEMENTS/UPDATES

- Added support for Kubernetes upgrade from 1.19 to 1.21 (JIRA: DEVOPS-3204). For more details, refer to the [Administration Guide: Kubernetes Upgrade from 1.19 to 1.21](#).

BUG FIXES

- Aligned the radio button for USER PRINCIPAL NAME in the LDAP settings configuration page (JIRA: ROFR-2800).

RELEASE NOTE

Date: 2-Mar-23

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

Software: Fortanix Data Security Manager SaaS

Version: 4.15

- The logo image size when logging in using Single Sign-On (SSO) is resized to fit (**JIRA: ROFR-2603**).
- Fixed an issue where the on-prem-managed-kubernetes deployment still makes requests to the `admin/v1/cluster/software` API (**JIRA: ROFR-3889**).
- Fixed an issue where the `config.toml.containerd` was still pointing to `k8s.gcr.io` (**JIRA: DEVOPS-3686**).
- Fixed an issue where the CA rotation was failing on Kubernetes version 1.21.14 (**JIRA: DEVOPS-3677**).
- Fixed an Oracle database crash on the production cluster backed by FIPS and an MS-SQL database backup failure. (**JIRA: PROD-6358**).
- Fixed an issue where clicking **VIEW CERTIFICATE** in the app's detailed view causes a page crash (**JIRA: ROFR-3890**).
- Fixed an issue where app creation using "Trusted CA" authentication was not working as expected (**JIRA: ROFR-3888**).
- Fixed an issue where upgrading from 4.14 RC build (2401) to latest the master (6588) was stuck with deploy pods in error state (**JIRA: DEVOPS-3595**).
- Fixed an issue where `[CEP Encryption]Keyspec=1` did not work with the windows CSP provider (**JIRA: PROD-6258**).
- Fixed an issue where the user was unable to see the contents of the BMC package after upgrading to DSM 4.13. (**JIRA: DEVOPS-3580**).
- Fixed an issue where the custom metadata was not getting updated for keys in a FIPS-backed group from the DSM UI (**JIRA: ROFR-3863**).
- Fixed an issue where a key type was not disabled in the create security object flow even though all the key sizes for that key were disallowed in the account-level cryptographic policy. (**JIRA: ROFR-3861**).

RELEASE NOTE

Date: 2-Mar-23

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

Software: Fortanix Data Security Manager SaaS

Version: 4.15

- Fixed an issue where an app count was not updated when adding an app to a group using the Groups table view (**JIRA: ROFR-3860**).
- Addressed the plugin and marketplace API security issues (**JIRA: PROD-6148**).
- Fixed an incorrect font for the Settings tab in the side navigation bar (**JIRA: ROFR-3841**).
- Fixed an issue that did not show a popup or notification after deleting the group, app, user, and plugin from their respective detailed views (**JIRA: ROFR-3838**).
- Fixed an issue where editing a custom attribute in the create security object form did not allow empty values (**JIRA: ROFR-3825**).
- Fixed an issue when adding a Key Metadata policy for a group where configuring the Custom Attribute section with restrictive values starting with a comma did not allow saving the policy (**JIRA: ROFR-3824**).
- Fixed an error when using Cloud HSM keys on encrypt calls using DSM/HSMG (**JIRA: PROD-5981**).
- Fixed an issue in the DSM SaaS subscription where deselecting the **Tokenization** option for **Add-Ons** does not remove the tokenization option from security object types (**JIRA: ROFR-3778**).
- Fixed an issue where the key wrap using RSA Key did not show the supported padding schemes (**JIRA: ROFR-3750**).
- Fixed an issue where the **Approve** button was not clickable while editing or deleting the Account quorum policy (**JIRA: ROFR-3687**).
- Fixed an issue where upgrading from DSM 4.11patch 2 to 4.12 was stuck on AWS 9nodes (Similar Hostname issue) (**JIRA: DEVOPS-3291**).
- Fixed an issue in custom tokenization where preserving the right block in partial expansion does not show proper index post security object creation (**JIRA: ROFR-3303**).

RELEASE NOTE

Date: 2-Mar-23

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

Software: Fortanix Data Security Manager SaaS

Version: 4.15

- Fixed an issue that did not validate the app name for an IAM AWS app in the DSM app creation flow (**JIRA: ROFR-2981**).
- Fixed a truncation issue for a new section in the DSM SaaS quorum approval request window on Firefox (**JIRA: ROFR-2979**).
- Fixed an issue in the System Administration dashboard where the pods summary was not truncated when there were many pods (**JIRA: ROFR-2974**).
- Fixed an issue in the create security object flow that loses form state after an error occurs (**JIRA: ROFR-3128**).
- Fixed an issue where large logo images of type SVG were not rendered correctly in the account selection dropdown (**JIRA: ROFR-2921**).
- Fixed an issue where syncing key in one HSM/KMS group resulted in all HSM/KMS groups showing "Scanning for keys" (**JIRA: ROFR-2897**).
- Fixed an issue on the System Administration Policies page where recaptcha was sometimes shown as disabled even when enabled (**JIRA: ROFR-2885**).
- Fixed a page crash when typing the plugin name in create plugin flow (if typed quickly) (**JIRA: ROFR-2880**).
- Fixed an issue where exporting a secret key in Hex format into a file and importing it in DSM from the same file results in the error message: "Not a valid Hex value" (**JIRA: ROFR-2840**).
- Fixed an issue where if the `kid` of a key is not part of the first 1000 keys in the GET keys API, it results in incorrect data being displayed (**JIRA: ROFR-2839**).
- Fixed an issue in the App create flow where **Save** button gets disabled when switching away from the page (**JIRA: ROFR-3455**).
- Fixed an issue in the DSM app creation flow where the UI showed the wrong color code for a destroyed key (**JIRA: ROFR-2824**).

RELEASE NOTE

Date: 2-Mar-23

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

Software: Fortanix Data Security Manager SaaS

Version: 4.15

- Fixed an issue where a newly created regular group is set as an HSM/KMS group on security object creation (**JIRA: ROFR-2722**).
- Fixed an issue where a group table shows a Tokenization security object type as an AES security object type (**JIRA: ROFR-2698**).
- Fixed an issue where the DSA key sizes should be listed in a drop down menu instead of a text box in the key rotation model window (**JIRA: ROFR-243**).
- Fixed an issue where Quorum approval requests results in a 500 internal error on specific group page when quorum policy expires (**JIRA: PROD-6038**).
- Fixed an issue where unverified users are now prevented from being added to a DSM account (**JIRA: PROD-6004**).

KNOWN ISSUES

- 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**).
- Unable to create an app when a Custom Group Role has the **Create Apps** permission enabled (**JIRA: PROD: 5764**).

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.

RELEASE NOTE

Date: 2-Mar-23

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

Software: Fortanix Data Security Manager SaaS

Version: 4.15

- Only issue accounts to trusted administrators.
- Utilize strong passwords.
- Monitor logs.

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 © 2023 Fortanix, Inc. All rights reserved.
Fortanix Data Security Manager SaaS Release Notes
Release 4.15