Fortanix Data Security Manager Release Note

RELEASE NOTE

Date: 27-Jan-23

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

Software: Fortanix Data Security Manager SaaS

Version: 4.14

OVERVIEW

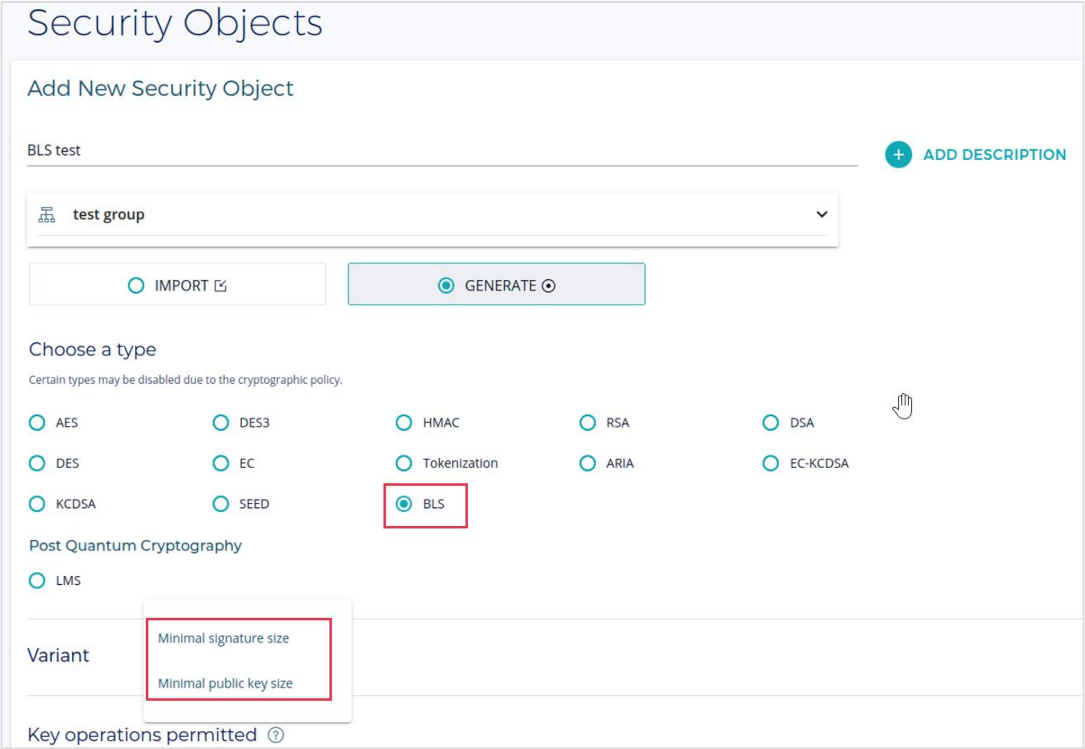
This document provides an overview of new features, general enhancements, improvements, and resolved issues in the Fortanix Data Security Manager (DSM) SaaS 4.14 release.

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

NEW FUNCTIONALITY / FEATURES

1. **Support for BLS key type (JIRA: PROD-4660):**

   This release adds support for generating a new key type called BLS key which is a digital signature scheme that can be used on blockchains for signature aggregation.



Security Objects

Add New Security Object

BLS test

test group

○ IMPORT ● GENERATE

Choose a type

Certain types may be disabled due to the cryptographic policy.

○ AES ○ DES3 ○ HMAC ○ RSA ○ DSA
○ DES ○ EC ○ Tokenization ○ ARIA ○ EC-KCDSA
○ KCDSA ○ SEED ● BLS

Post Quantum Cryptography

○ LMS

Variant: Minimal signature size / Minimal public key size

Key operations permitted

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

RELEASE NOTE

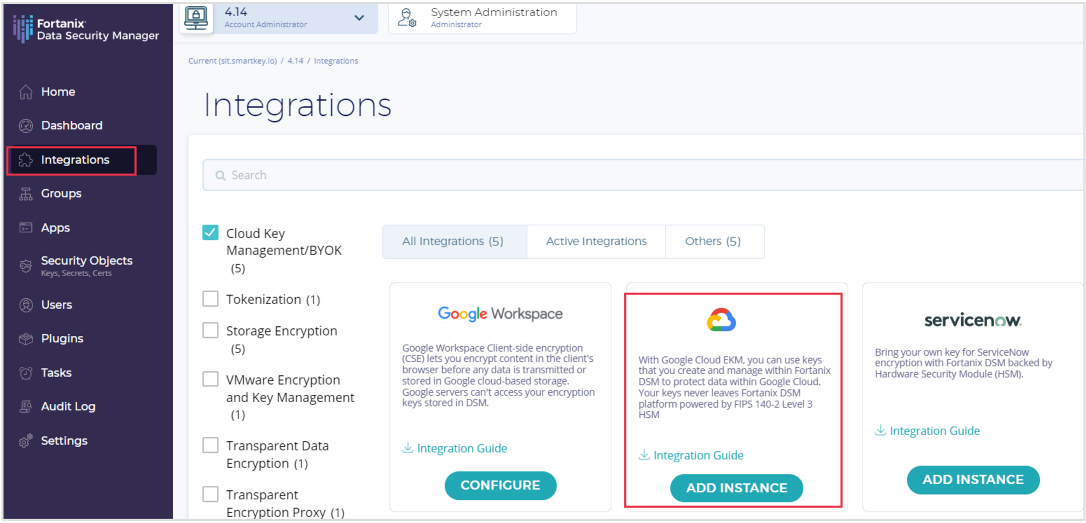
Date: 27-Jan-23

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

Software: Fortanix Data Security Manager SaaS

Version: 4.14

2. Added support for easy wizard integration for Google Cloud EKM interface **(JIRA: ROFR-3152):**



Integrations

☑ Cloud Key Management/BYOK (5)
□ Tokenization (1)
□ Storage Encryption (5)
□ VMware Encryption and Key Management (1)
□ Transparent Data Encryption (1)
□ Transparent Encryption Proxy (1)

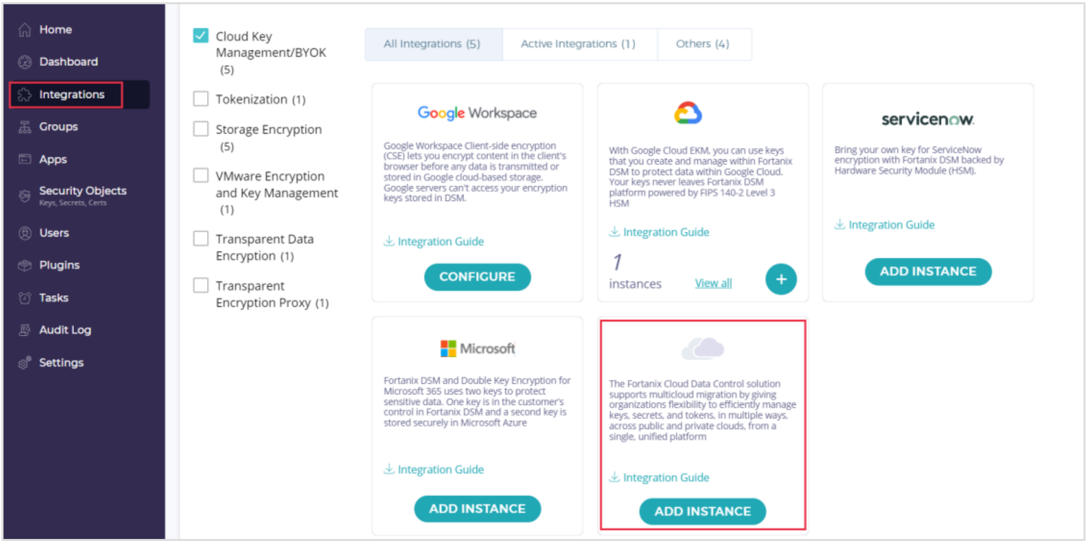
Google Workspace Client-side encryption (CSE) lets you encrypt content in the client's browser before any data is transmitted or stored in Google cloud-based storage. Google servers can't access your encryption keys stored in DSM.

With Google Cloud EKM, you can use keys that you create and manage within Fortanix DSM to protect data within Google Cloud. Your keys never leaves Fortanix DSM platform powered by FIPS 140-2 Level 3 HSM

Bring your own key for ServiceNow encryption with Fortanix DSM backed by Hardware Security Module (HSM).

For more details refer to the [Integration Guide: Fortanix DSM with Google EKM Interface].

3. Added support for easy wizard integration for Cloud Data Control AWS BYOK **(JIRA: ROFR-3152):**



☑ Cloud Key Management/BYOK (5)
□ Tokenization (1)
□ Storage Encryption (5)
□ VMware Encryption and Key Management (1)
□ Transparent Data Encryption (1)
□ Transparent Encryption Proxy (1)

Google Workspace Client-side encryption (CSE) lets you encrypt content in the client's browser before any data is transmitted or stored in Google cloud-based storage. Google servers can't access your encryption keys stored in DSM.

With Google Cloud EKM, you can use keys that you create and manage within Fortanix DSM to protect data within Google Cloud. Your keys never leaves Fortanix DSM platform powered by FIPS 140-2 Level 3 HSM

Bring your own key for ServiceNow encryption with Fortanix DSM backed by Hardware Security Module (HSM).

Fortanix DSM and Double Key Encryption for Microsoft 365 uses two keys to protect sensitive data. One key is in the customer's control in Fortanix DSM and a second key is stored securely in Microsoft Azure

The Fortanix Cloud Data Control solution supports multicloud migration by giving organizations flexibility to efficiently manage keys, secrets, and tokens, in multiple ways, across public and private clouds, from a single, unified platform

For more details refer to the [User's: AWS KMS Group Setup- Using Easy Wizard].

Fortanix, Inc. | 3910 Freedom Circle | Suite 104 | Santa Clara, CA 95052 | ☎ +1 650.943.2484

✉ info@fortanix.com

www.fortanix.com

ENHANCEMENTS TO EXISTING FEATURES

RELEASE NOTE

Date: 27-Jan-23

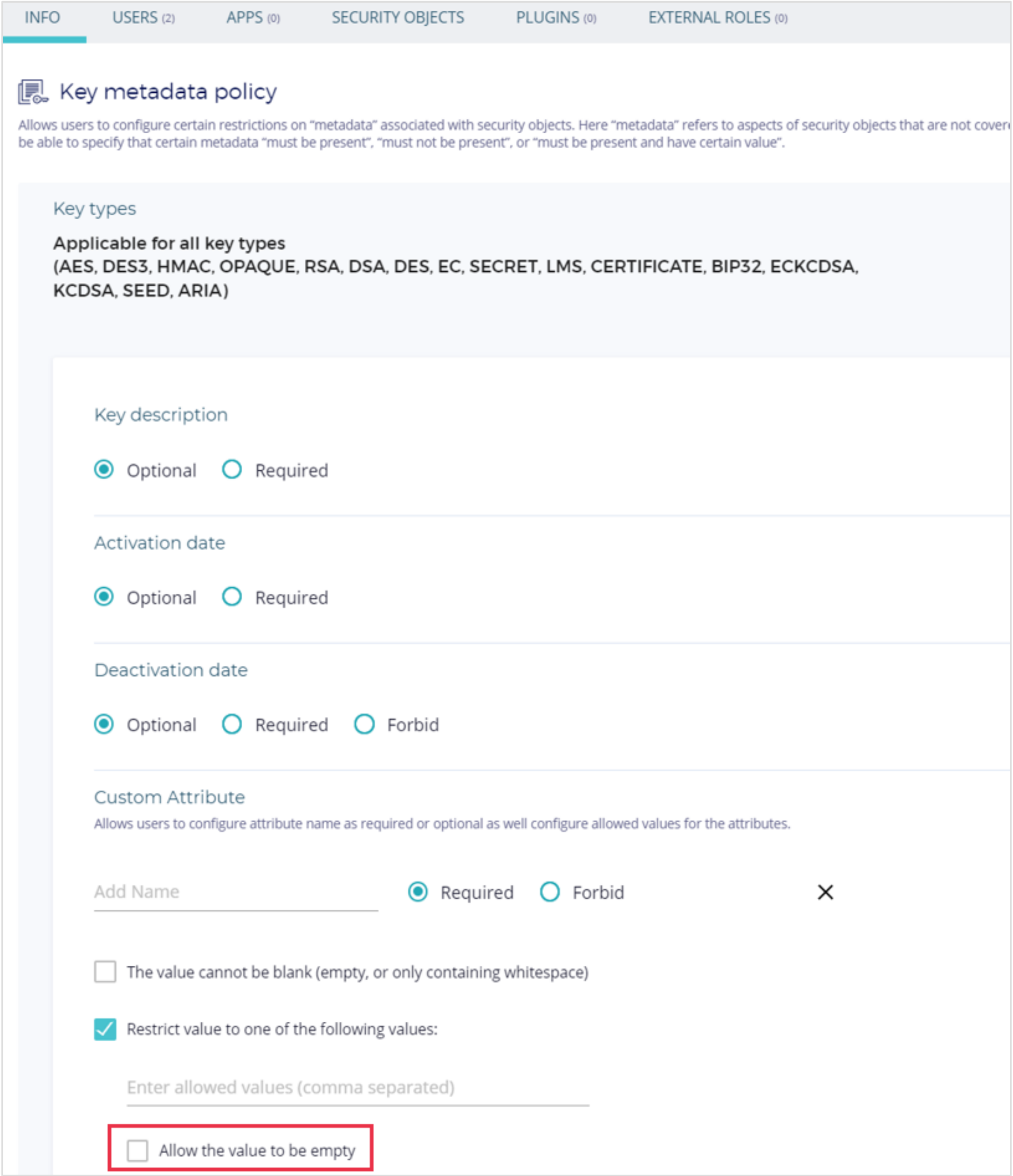
Subject: Software changes, updates, bug fixes, etc.

Software: Fortanix Data Security Manager SaaS

Version: 4.14

1. **Custom attributes can now be set as empty in the group's Key metadata policy (JIRA: PROD-5985)**.

   This release allows you to create a security object with empty custom attributes that can be set at the group-level in the Key metadata policy.



INFO | USERS (2) | APPS (0) | SECURITY OBJECTS | PLUGINS (0) | EXTERNAL ROLES (0)

Key metadata policy

Allows users to configure certain restrictions on "metadata" associated with security objects. Here "metadata" refers to aspects of security objects that are not cover
be able to specify that certain metadata "must be present", "must not be present", or "must be present and have certain value".

Key types

Applicable for all key types
(AES, DES3, HMAC, OPAQUE, RSA, DSA, DES, EC, SECRET, LMS, CERTIFICATE, BIP32, ECKCDSA, KCDSA, SEED, ARIA)

Key description

● Optional ○ Required

Activation date

● Optional ○ Required

Deactivation date

● Optional ○ Required ○ Forbid

Custom Attribute

Allows users to configure attribute name as required or optional as well configure allowed values for the attributes.

Add Name ● Required ○ Forbid ✕

□ The value cannot be blank (empty, or only containing whitespace)

☑ Restrict value to one of the following values:

Enter allowed values (comma separated)

□ Allow the value to be empty

For more details refer to the User's Guide: Key Metadata Policy.

RELEASE NOTE

Date: 27-Jan-23

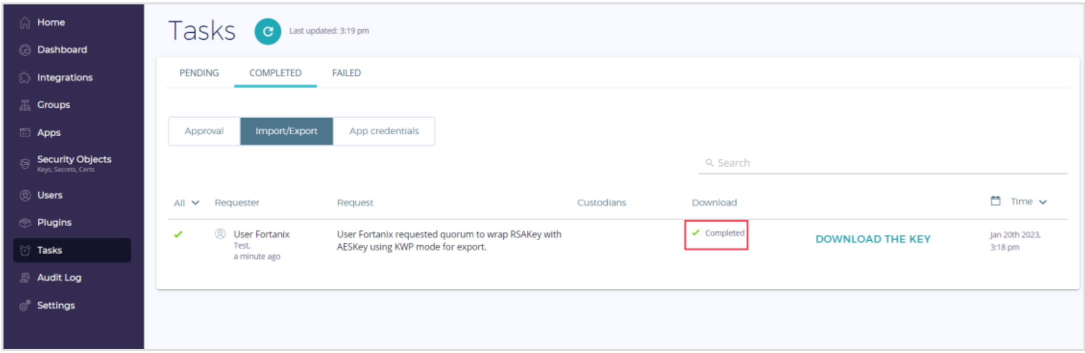
Subject: Software changes, updates, bug fixes, etc.

Software: Fortanix Data Security Manager SaaS

Version: 4.14

2. Added “Download” column to Quorum approval request Completed->Import/Export status page (JIRA: ROFR-3834).

After a user downloads an asymmetric key from the Tasks -> Completed -> Import/Export page, the status of the download completion is shown in the new “Download” column.



Tasks Last updated: 3:19 pm

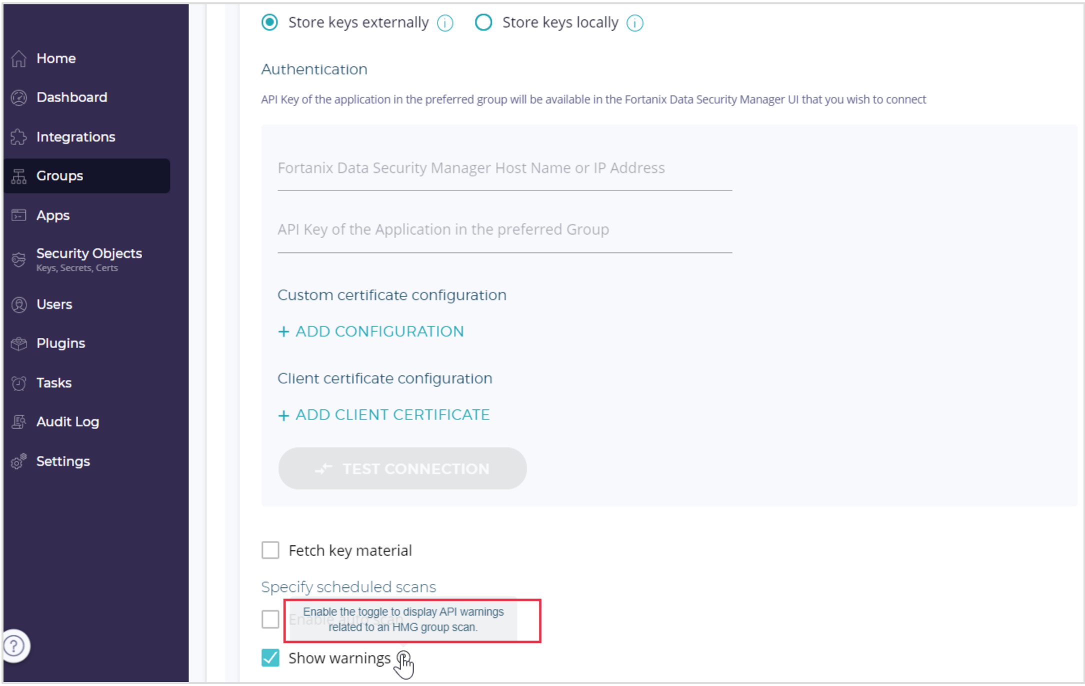
PENDING COMPLETED FAILED

Approval Import/Export App credentials

Search

All	Requester	Request	Custodians	Download		Time
✓	User Fortanix Test. a minute ago	User Fortanix requested quorum to wrap RSAKey with AESKey using KWP mode for export.		✓ Completed	DOWNLOAD THE KEY	Jan 20th 2023, 3:18 pm

3. Added a tooltip for the “Show warnings” field in the Extended Virtual keys form (JIRA: ROFR-3820).



● Store keys externally ○ Store keys locally

Authentication

API Key of the application in the preferred group will be available in the Fortanix Data Security Manager UI that you wish to connect

Fortanix Data Security Manager Host Name or IP Address

API Key of the Application in the preferred Group

Custom certificate configuration

+ ADD CONFIGURATION

Client certificate configuration

+ ADD CLIENT CERTIFICATE

□ Fetch key material

Specify scheduled scans

□ Enable the toggle to display API warnings related to an HMG group scan.

☑ Show warnings

RELEASE NOTE

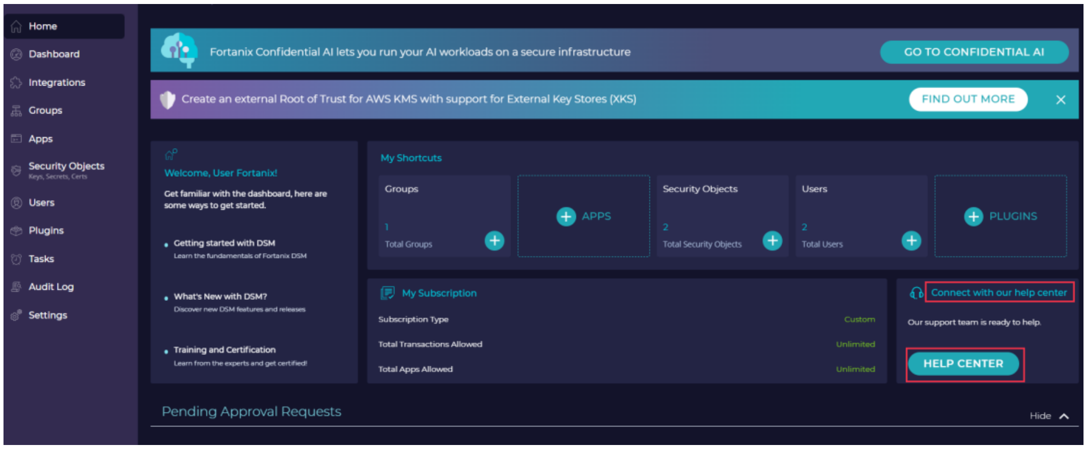
Date: 27-Jan-23

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

Software: Fortanix Data Security Manager SaaS

Version: 4.14

4. **Updated text on the DSM Home page (JIRA: PROD-5279)**.
    - Updated the section "**Need some assistance**" to "**Connect with our help center**".
    - Updated the button "**CONTACT**" to "**HELP CENTER**".



Fortanix Confidential AI lets you run your AI workloads on a secure infrastructure

Create an external Root of Trust for AWS KMS with support for External Key Stores (XKS)

Welcome, User Fortanix!

Get familiar with the dashboard, here are some ways to get started.

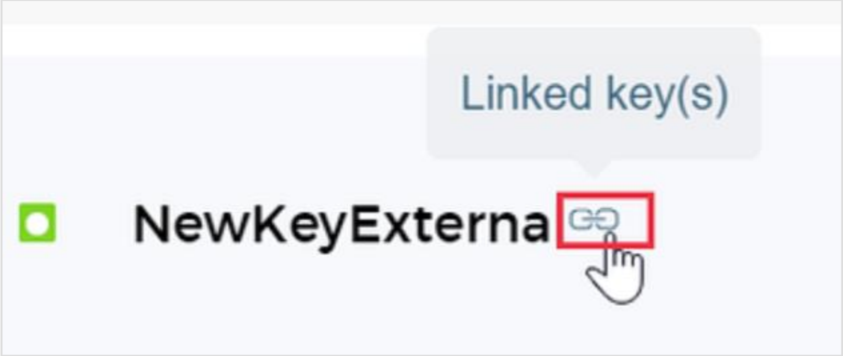
- Getting started with DSM
  Learn the fundamentals of Fortanix DSM
- What's New with DSM?
  Discover new DSM features and releases
- Training and Certification
  Learn from the experts and get certified!

Subscription Type	Custom
Total Transactions Allowed	Unlimited
Total Apps Allowed	Unlimited

Connect with our help center

Our support team is ready to help.

5. **Show the icon for "linked key" for a key in the Security Objects table only when the key is copied from a local Fortanix DSM group (JIRA: ROFR-3782)**.



6. **Redesigned the "Integrations" page in Fortanix DSM (JIRA: ROFR-3764)**.

   The integration page now allows users to:

    - Search an integration using the Search bar.
    - Filter an integration using the check box for an integration category.

Fortanix, Inc. | 3910 Freedom Circle | Suite 104 | Santa Clara, CA 95052 | ☎ +1 650.943.2484
info@fortanix.com
www.fortanix.com

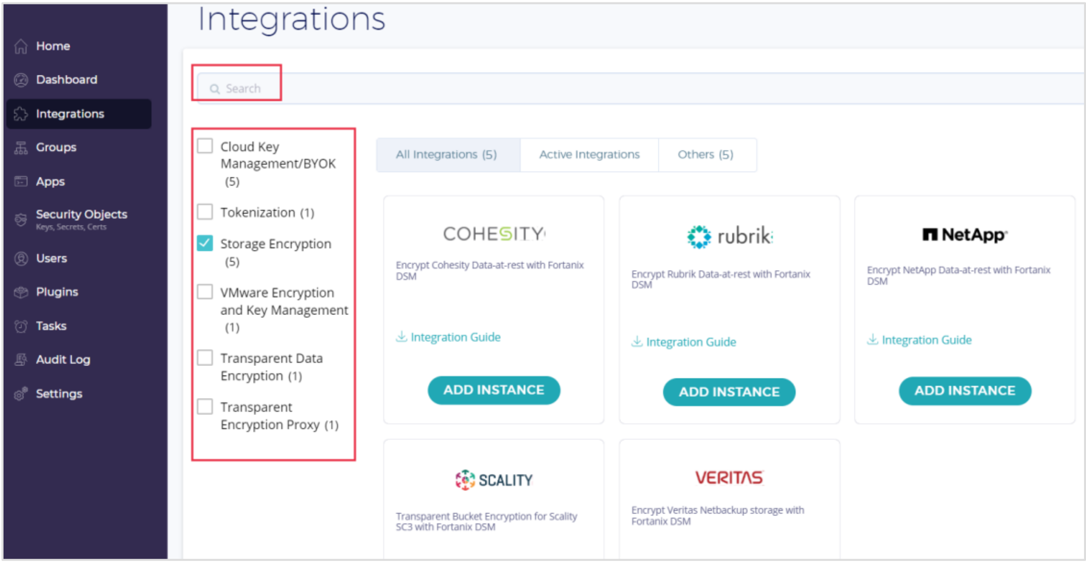
RELEASE NOTE

Date: 27-Jan-23

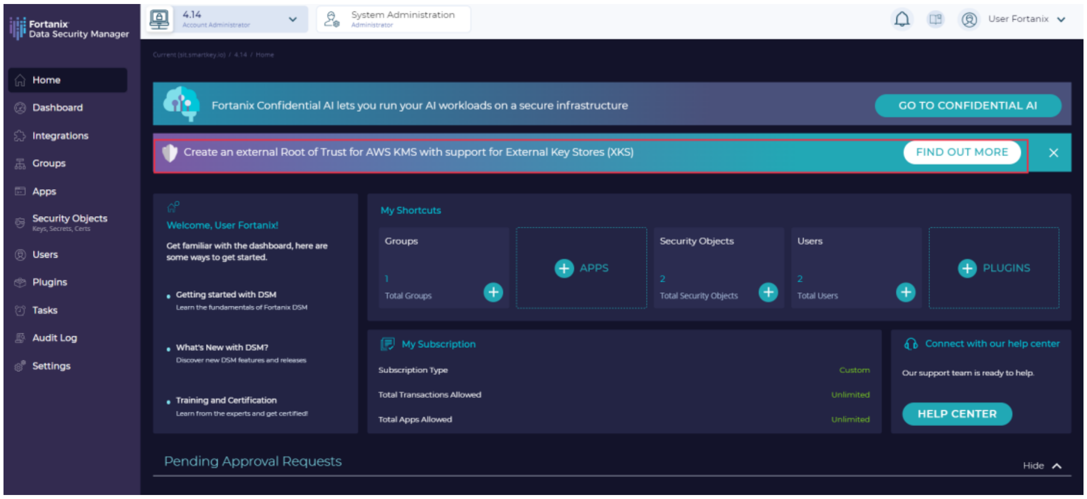
Subject: Software changes, updates, bug fixes, etc.

Software: Fortanix Data Security Manager SaaS

Version: 4.14


Integrations
Home
Dashboard
Integrations
Groups
Apps
Security Objects
Keys, Secrets, Certs
Users
Plugins
Tasks
Audit Log
Settings
Search
□ Cloud Key Management/BYOK (5)
□ Tokenization (1)
☑ Storage Encryption (5)
□ VMware Encryption and Key Management (1)
□ Transparent Data Encryption (1)
□ Transparent Encryption Proxy (1)
All Integrations (5)
Active Integrations
Others (5)
COHESITY
Encrypt Cohesity Data-at-rest with Fortanix DSM
Integration Guide
ADD INSTANCE
rubrik
Encrypt Rubrik Data-at-rest with Fortanix DSM
Integration Guide
ADD INSTANCE
NetApp
Encrypt NetApp Data-at-rest with Fortanix DSM
Integration Guide
ADD INSTANCE
SCALITY
Transparent Bucket Encryption for Scality SC3 with Fortanix DSM
VERITAS
Encrypt Veritas Netbackup storage with Fortanix DSM

7. **Added AWS XKS banner on the Home page (JIRA: ROFR-3752).**


Fortanix Data Security Manager
4.14
Account Administrator
System Administration
Administrator
User Fortanix
Home
Dashboard
Integrations
Groups
Apps
Security Objects
Keys, Secrets, Certs
Users
Plugins
Tasks
Audit Log
Settings
Fortanix Confidential AI lets you run your AI workloads on a secure infrastructure
GO TO CONFIDENTIAL AI
Create an external Root of Trust for AWS KMS with support for External Key Stores (XKS)
FIND OUT MORE
Welcome, User Fortanix!
Get familiar with the dashboard, here are some ways to get started.
Getting started with DSM
Learn the fundamentals of Fortanix DSM
What's New with DSM?
Discover new DSM features and releases
Training and Certification
Learn from the experts and get certified
My Shortcuts
Groups
1
Total Groups
APPS
Security Objects
2
Total Security Objects
Users
2
Total Users
PLUGINS
My Subscription
Subscription Type
Custom
Total Transactions Allowed
Unlimited
Total Apps Allowed
Unlimited
Connect with our help center
Our support team is ready to help.
HELP CENTER
Pending Approval Requests
Hide

8. **Improved the depiction of the total plugins limit and plugins in use on the DSM subscription page (JIRA: ROFR-3687).**

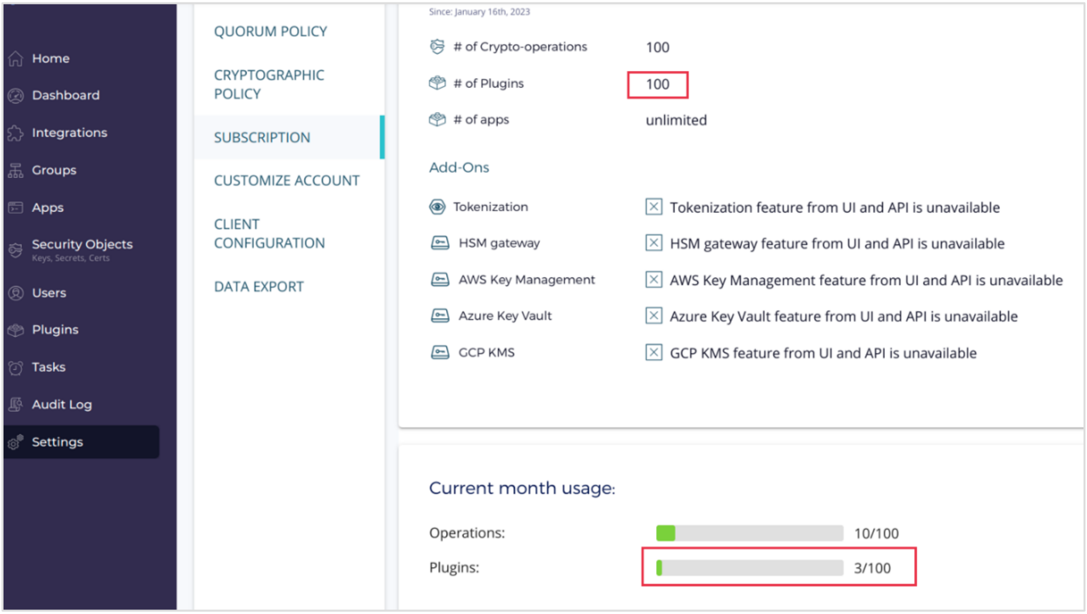
RELEASE NOTE

Date: 27-Jan-23

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

Software: Fortanix Data Security Manager SaaS

Version: 4.14



Since: January 16th, 2023

# of Crypto-operations	100
# of Plugins	100
# of apps	unlimited

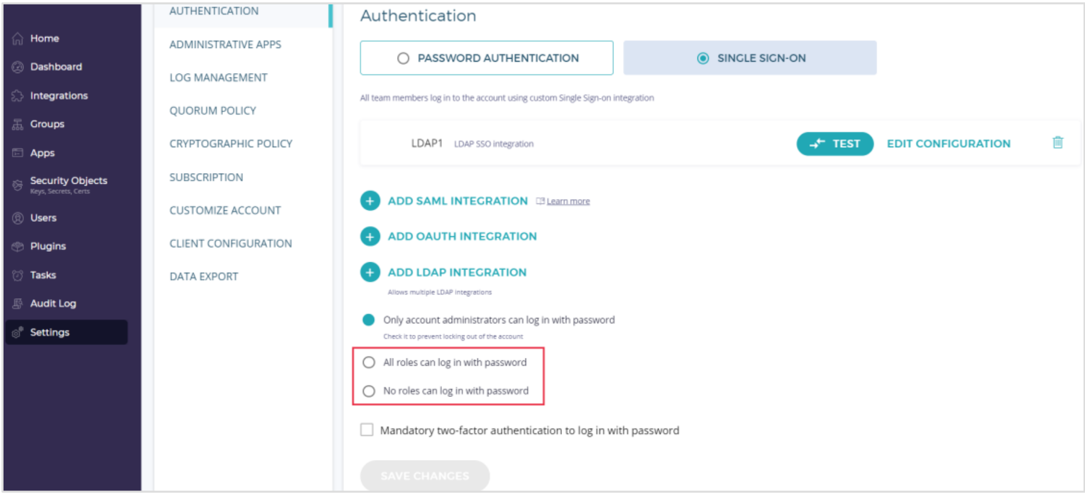
Add-Ons

Tokenization	☒ Tokenization feature from UI and API is unavailable
HSM gateway	☒ HSM gateway feature from UI and API is unavailable
AWS Key Management	☒ AWS Key Management feature from UI and API is unavailable
Azure Key Vault	☒ Azure Key Vault feature from UI and API is unavailable
GCP KMS	☒ GCP KMS feature from UI and API is unavailable

Current month usage:

Operations:	10/100
Plugins:	3/100

9. **The Authentication page in the DSM Account Settings page now covers all combinations of use of local password (JIRA: ROFR-3324).**



Authentication

○ PASSWORD AUTHENTICATION ● SINGLE SIGN-ON

All team members log in to the account using custom Single Sign-on integration

LDAP1 LDAP SSO integration

Allows multiple LDAP integrations

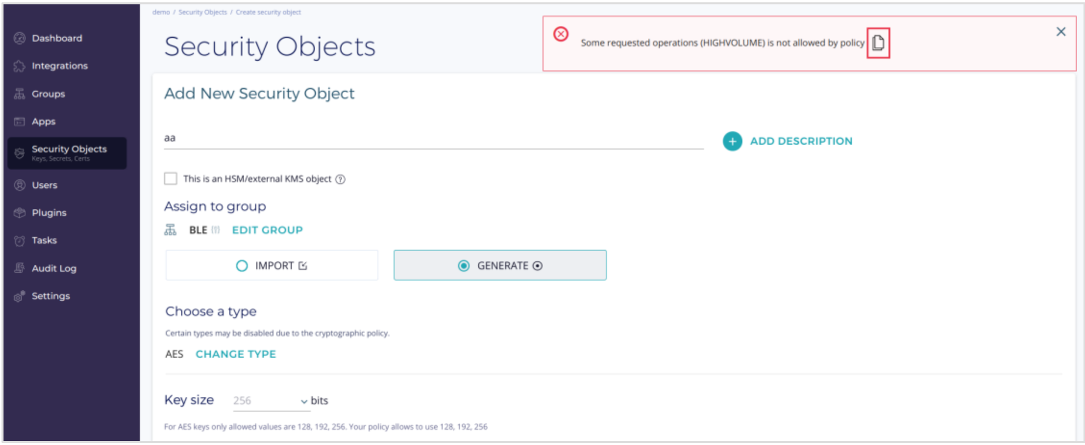
● Only account administrators can log in with password
Check it to prevent locking out of the account

○ All roles can log in with password

○ No roles can log in with password

□ Mandatory two-factor authentication to log in with password

10. **Added support to copy error message text in toast notifications (JIRA: PROD-3292).**



Some requested operations (HIGHVOLUME) is not allowed by policy

Add New Security Object

aa

□ This is an HSM/external KMS object

Assign to group

BLE

Choose a type

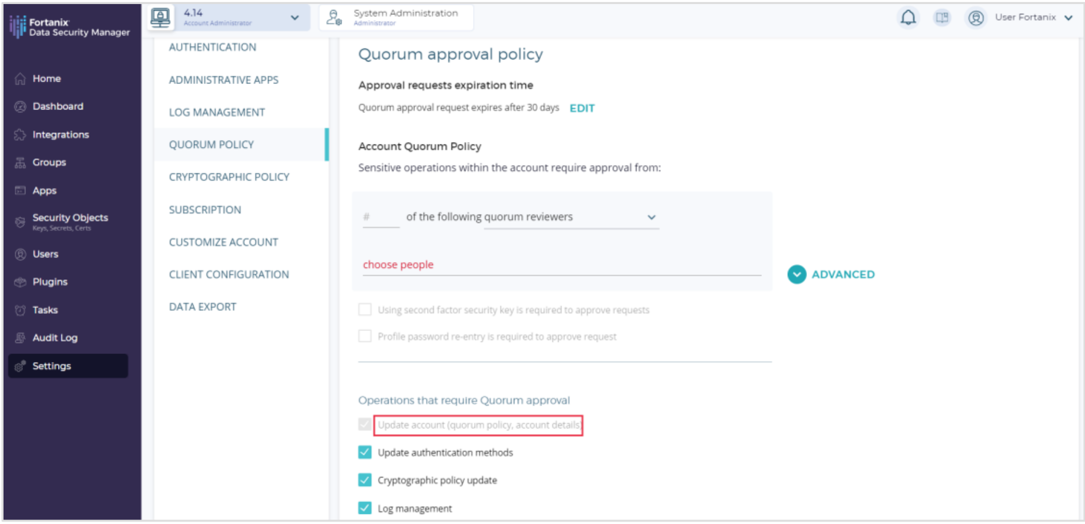
Certain types may be disabled due to the cryptographic policy.

AES

Key size 256 bits

For AES keys only allowed values are 128, 192, 256. Your policy allows to use 128, 192, 256

11. Updated Account Quorum Policy option text (JIRA: ROFR-3044).



Quorum approval policy

Approval requests expiration time

Quorum approval request expires after 30 days

Account Quorum Policy

Sensitive operations within the account require approval from:

# of the following quorum reviewers

choose people

□ Using second factor security key is required to approve requests

□ Profile password re-entry is required to approve request

Operations that require Quorum approval

☑ Update account (quorum policy, account details)

☑ Update authentication methods

☑ Cryptographic policy update

☑ Log management

12. Updated the description for Secrets – Show value (JIRA: ROFR-3001)

The description text after importing a secret is updated to inform user where they can download the key material after quorum approval when they click **SHOW VALUE**.

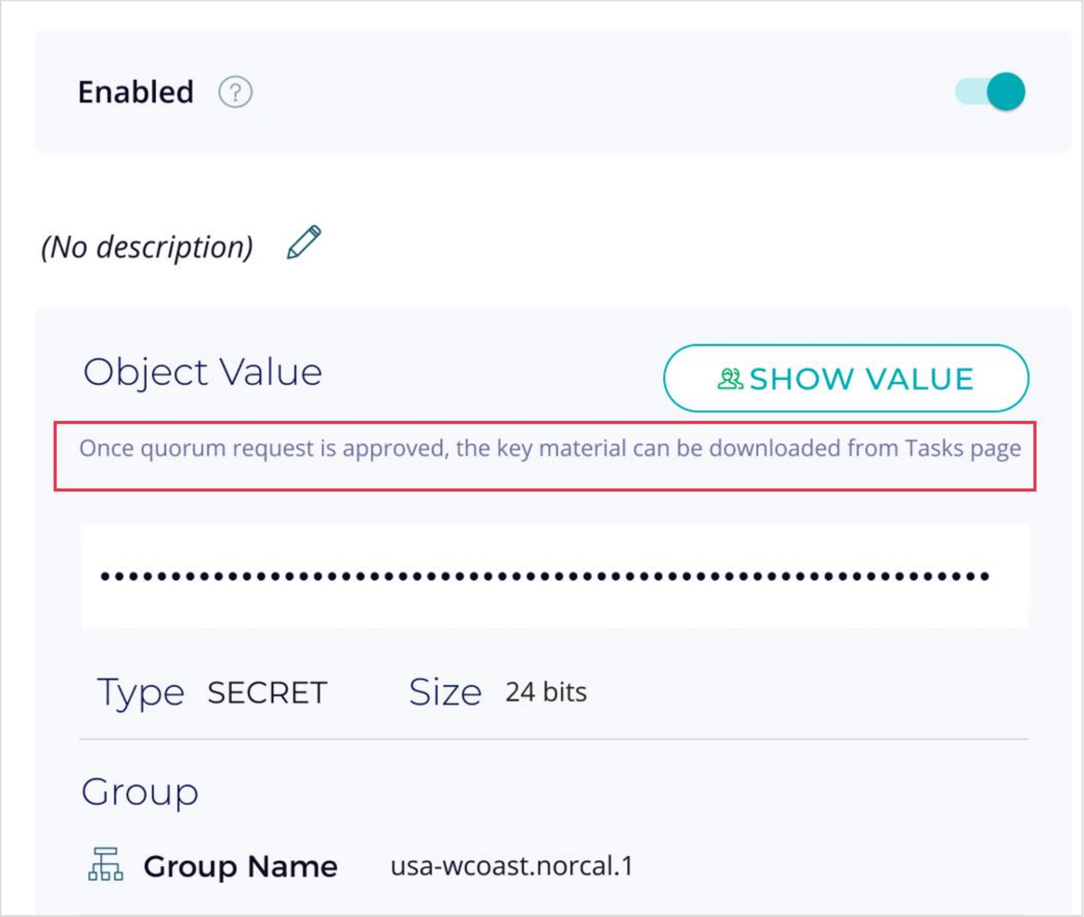
RELEASE NOTE

Date: 27-Jan-23

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

Software: Fortanix Data Security Manager SaaS

Version: 4.14



Once quorum request is approved, the key material can be downloaded from Tasks page

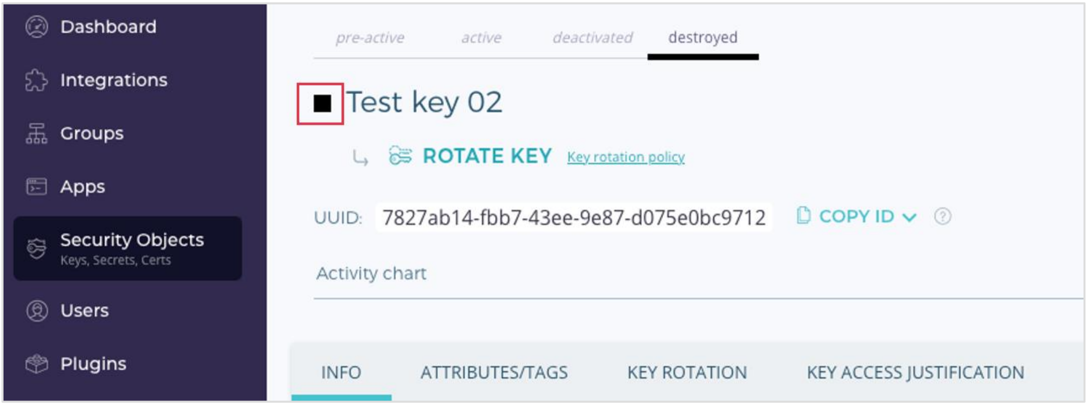
••

Type SECRET   Size 24 bits

Group

Group Name usa-wcoast.norcal.1

13. **The key state icon is updated to black color for a destroyed key from a previous red color (JIRA: ROFR-2749)**.



■ Test key 02

UUID: 7827ab14-fbb7-43ee-9e87-d075e0bc9712

RELEASE NOTE

Date: 27-Jan-23

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

Software: Fortanix Data Security Manager SaaS

Version: 4.14

OTHER IMPROVEMENTS

1. **Added support for setting the “Activation Date” attribute in the “Create key pair” operation for private keys (JIRA: PROD-6095).**
2. **Added support for setting the 'Deactivation Date' attribute for operations such as ‘Create Key Pair’ and ‘rekey keypair’ (JIRA: PROD-6110).**
3. **Added backend logs to track the progress of audit log purge task (JIRA: PROD-6031).**
4. **Added support for `deleteAttribute` operation to delete attributes of the managed object (JIRA: PROD-5884).**
5. **Added support for 'Activation Date' and 'Deactivation Date' attributes in 'Locate' operation (JIRA: PROD-5873).**
6. **Added support for using managed Cassandra from SGX (JIRA: PROD-5826).**
7. **Added support for online attestation for DCAP (JIRA: PROD-5827).**
8. **Added support for explicitly enabling scalable processors for new clusters (JIRA: PROD-5786).**
9. **Implemented a method to get the value '`IvCounterNonce`' from the '`EncryptResponse`' object (JIRA: PROD-5973).**
10. **Added support for deployment automation of SQL TDE and rotation via PowerShell (JIRA: PROD-2088).**

CLIENT IMPROVEMENTS

1. **JCE: Added a new constructor with key operations (JIRA: PROD-5681).**
2. **KMIP: Added new features for KMIP server Java client (JIRA: PROD-5872).**

QUALITY ENHANCEMENTS/UPDATES

- Added the ability to rotate Kubernetes root certificate (**JIRA: DEVOPS-1501**). *For more details, refer to the Administration Guide: Kubernetes Root CA Rotation*.
- Added the ability for cluster TLS certificate key rotation (**JIRA: PROD-578**).

BUG FIXES

- Fixed an issue where the **DONE** button was disabled in the Security Objects page for a search filter of type “is one of” and “is none of” **(JIRA: ROFR-3870)**.
- Fixed a crash when adding Google Workspace Easy Wizard integration and then deleting Google SSO **(JIRA: ROFR-3868)**.
- Fixed an issue where the user was unable to delete SSO authentication **(JIRA: ROFR-3867)**.
- Fixed an issue where the user was able to click the **INSTALL** button for any upgrade from Fortanix DSM UI **(JIRA: ROFR-3856)**.
- Fixed an issue where `get_csrs` was failing due to incorrect parameters in config-values configmap **(JIRA: DEVOPS-3529)**.
- Fixed an issue where updating the pagination results in an error **(JIRA: ROFR-3836)**.
- Fixed an issue where updating the “azure-key-name” custom metadata field causes future updates to fail **(JIRA: PROD-6131)**.
- Fixed arithmetic errors in plugins **(JIRA: PROD-6124)**.
- Fixed an issue where if the user sets "Log retention days" to an older date for which the logs lie in an old database table, then audit log purging is not happening. **(JIRA: PROD-6119)**.
- Fixed confusing text on the Quorum approval request dialog **(JIRA: ROFR-3828)**.

RELEASE NOTE

Date: 27-Jan-23

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

Software: Fortanix Data Security Manager SaaS

Version: 4.14

- Fixed an issue where the actor name was not shown for audit log entry when the actor is a plugin **(JIRA: ROFR-3819)**.
- Fixed an issue where the DSM-Accelerator webservice was unable to perform local DES3-CBC and CBCNOPAD key:112 encrypt or decrypt operations **(JIRA: PROD-6056)**.
- Fixed an issue where the user was unable to import other keys after trying to import the KCDSA key **(JIRA: ROFR-3812)**.
- Fixed an issue where an LMS key did not allow APPMANAGEABLE or VERIFY permissions **(JIRA: ROFR-3509)**.
- Fixed an issue in Google Workspace CSE where the Key service URL was hard coded to the AMER cluster **(JIRA: ROFR-3810)**.
- Fixed an issue where the Quorum policy change requests do not display well in Firefox on a Linux machine **(JIRA: ROFR-3807)**.
- Fixed an issue where certain keys that are allowed in the group-level cryptographic policy but removed from the account-level cryptographic policy are not allowed to be created at the group level until the page is refreshed **(JIRA: ROFR-3803)**.
- Fixed an issue that now allows validating searching for UUIDs in data tables such as security objects list, app list, audit log list, and so on **(JIRA: ROFR-3798)**.
- Fixed an issue that did now allow reducing the `log_retention_period` from 2 to 1 day **(JIRA: ROFR-3786)**.
- Fixed an issue that now does not allow X25519 and ED25519 keys to be wrapped using AES key with KWP mode **(JIRA: ROFR-3785)**.
- Fixed an issue where group policy indicators were not displayed on apps and plugins pages **(JIRA: ROFR-3776)**.

- Fixed an issue in Azure BYOK flow where n-1 azure tags were getting pushed to Azure KMS key when Azure tags are added after key creation **(JIRA: PROD-5949)**.
- Fixed missing tooltip for AWS Multi region keys **(JIRA: ROFR-3774)**.
- Fixed an issue where the import operation creates two key versions instead of one for GCP-backed groups **(JIRA: PROD-5944)**.
- Fixed an issue where the user was unable to create an EC key after the ECKCDSA type is selected and then the EC type is selected **(JIRA: ROFR-3765)**.
- Fixed an issue where the DSM SCP backup config requires manually editing secrets **(JIRA: DEVOPS-3398)**.
- Fixed an issue in the Customize Account workflow where uploading an SVG file format logo from the accounts page results in an error **(JIRA: ROFR-3736)**.
- Fixed an issue where the **New Features** and **Customization** in the **Settings** tab in the System Administration view has the same parent class name: "tab-customizations" **(JIRA: ROFR-3731)**.
- Fixed an issue where switching from the sysadmin to the regular account results in a 403 error in `GET (admin/v1/cluster)` **(JIRA: ROFR-3749)**.
- Fixed an issue where the IP address is not captured in the sysadmin log for a User login **(JIRA: PROD-5774)**.
- Fixed an issue in custom tokenization where conflicting suffix type in between the 'Hexadecimal' data type, does not show an error message **(JIRA: ROFR-3676)**.
- Fixed an issue that now shows an error message when LDAP login API exceeds the maximum time limit **(JIRA: ROFR-3593)**.

RELEASE NOTE

Date: 27-Jan-23

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

Software: Fortanix Data Security Manager SaaS

Version: 4.14

- Fixed an issue in custom tokenization where entering `min_length` as `length_limit` (4294967295) does not allow `max_length_limit` to exceed 9 digits **(JIRA: ROFR-3458)**.
- Fixed an issue in custom tokenization where entering `max_value` of more than 17 digits, takes the value as 0 for the remaining digits. **(JIRA: ROFR-3457)**.
- Fixed an issue in custom tokenization where the user was unable to create a custom token security object with a max value containing 1.0e+21 **(JIRA: ROFR-3455)**.
- Fixed an issue where the UI was showing the wrong color code for a destroyed key **(JIRA: ROFR-3002)**.
- Fixed an issue where the scroll bar was missing for a modal window **(JIRA: ROFR-2798)**.

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**).

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 at least two System Administrator accounts.

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 4.14