RELEASE NOTES

Date: 13-Jun-23

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

Software: Fortanix Data Security Manager SaaS

Version: 4.18

OVERVIEW

This document provides an overview of new features, general improvements, and resolved issues in the Fortanix Data Security Manager (DSM) SaaS 4.18 release.

This release is superseded by June 20, 2023 release.

📌 **NOTE**:

- This release is for **SaaS only** and is not available for on-premises installations.

NEW FUNCTIONALITY / FEATURES

- **Added support for AWS GovCloud regions in the AWS BYOK group (JIRA: PM-39):**
  You can now select one of the following AWS GovCloud regions from the **Choose Region** drop down menu for AWS Key Management Service so that the AWS BYOK key upload operations are executed against the KMS in that region and the uploaded keys will appear usable by AWS GovCloud:
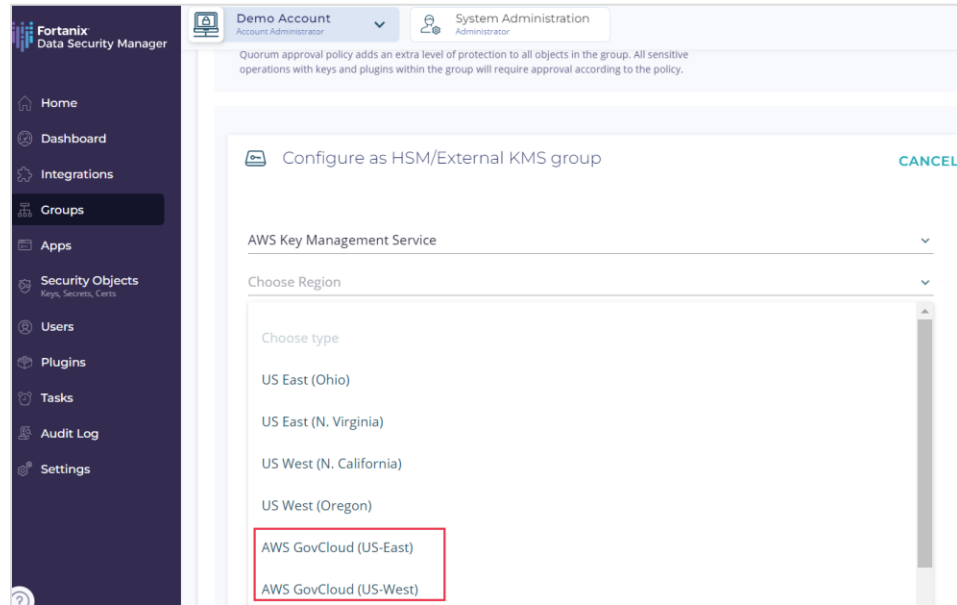   - **AWS GovCloud (US-East)**
    - **AWS GovCloud (US-West)**

RELEASE NOTES

Date: 13-Jun-23

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

Software: Fortanix Data Security Manager SaaS

Version: 4.18

For more details, refer to the *User's Guide: Fortanix DSM – AWS Key Management Service CDC Group Setup*.

- **Added Azure for US Government Service in the Azure BYOK group (JIRA: PM-39):**
  You can now select one of the following services when setting up an Azure Key Vault or Azure Managed HSM-backed group:
  - **global Azure**
  - **Azure for US Government**

  Where the "**global Azure**" option can be selected to authenticate and upload the key material to any non-GovCloud Azure service, and "**Azure for US Government**" is a new option added for the user to authenticate and upload key material to the specific Azure service set aside for the US government.
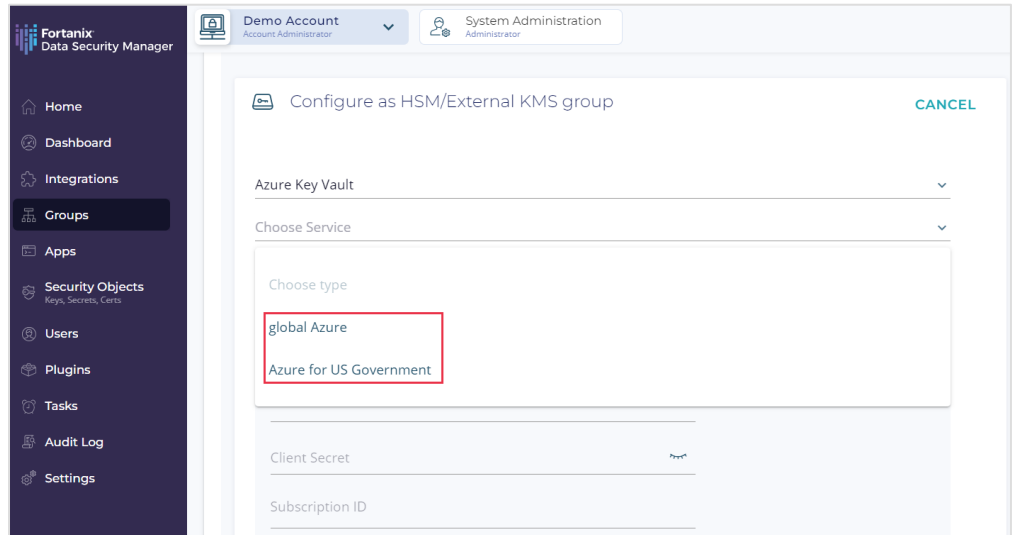
RELEASE NOTES

Date: 13-Jun-23

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

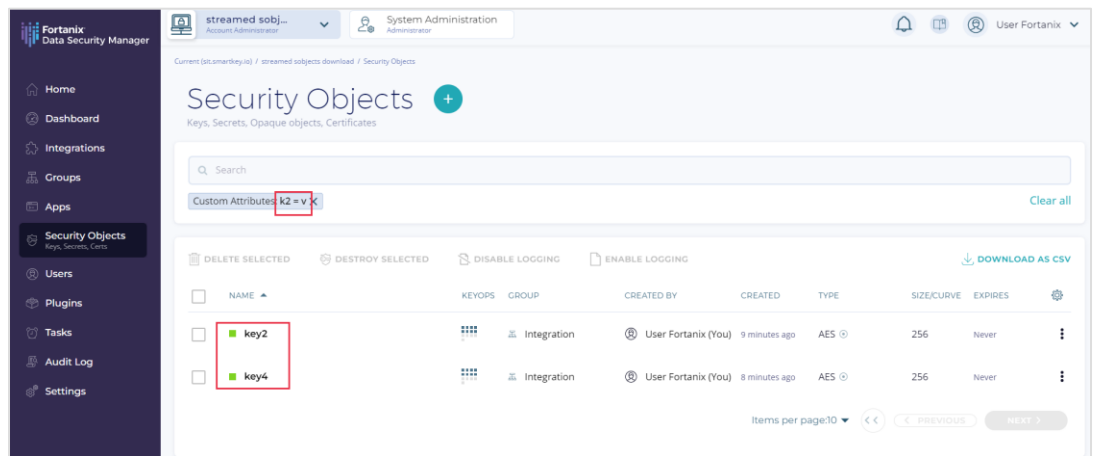**Software:** Fortanix Data Security Manager SaaS

Version: 4.18

For more details, refer to the [User's Guide: Fortanix DSM – Azure Key Vault CDC Group Setup](#) and [User's Guide: Azure Managed HSM](#).

ENHANCEMENTS TO EXISTING FEATURES

1. **Added support for partial text search for custom attributes (JIRA: ROFR-4065).**

   You can now use partial text search instead of exact text search using a custom attribute filter from the Security Objects table.

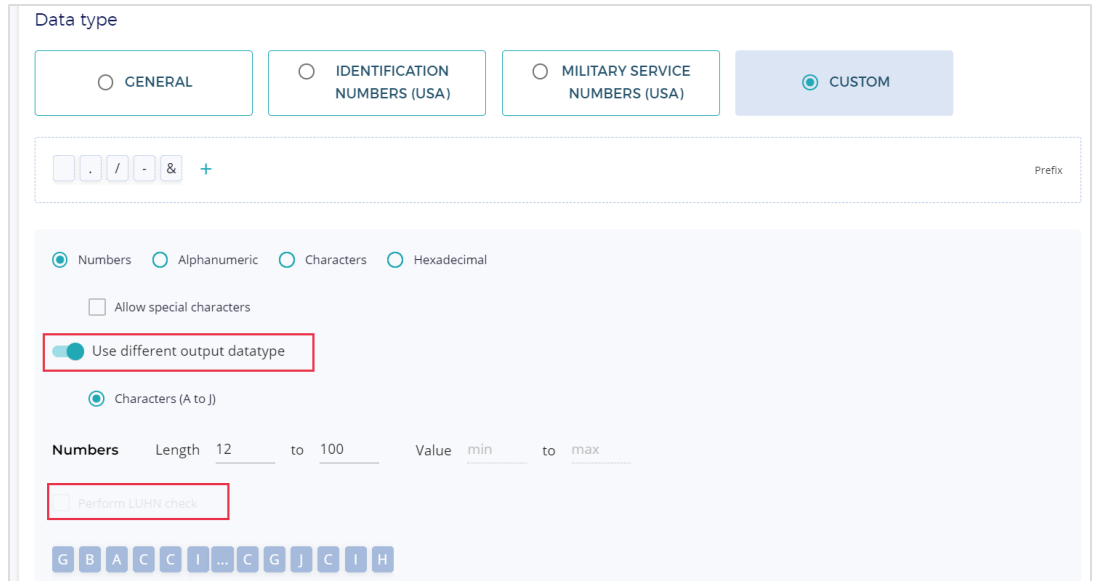2. **Reduced the DSM notification display time from 15 seconds to 5 seconds (JIRA: ROFR-4018).**

3. **Changed the Quorum approval policy to allow only verified users (JIRA: PROD-6082):** From this release onwards only users who have verified their email address can be added to the Quorum approval policy.

4. **Disabled the option "Perform LUHN check" for custom tokenization when the "Use different output datatype" toggle is enabled (JIRA: ROFR-3999):** When creating a tokenization security object of type **Custom**, if you enable the toggle **Use different output datatype**, then the **Perform LUHN check** option will be disabled since it is not applicable to the encrypted part with a non-numeric character set.

OTHER IMPROVEMENTS

1. **Updated the "Date" format in the security objects export report to ISO860 format (JIRA: PM-38).**

2. **A FIPS-backed group now additionally supports the following key types (JIRA: ROFR-4041):**

   - **EC** - NistP224, NistP256, NistP384, NistP521
   - **RSA**

3. Added email confirmation for self-provisioning in the System Administration settings if the email was not already verified (JIRA: PROD-4609).
4. Added account UUIDs in the DSM backend logs for all response codes (JIRA: PROD-6681).
5. Added support for logging bad authentication requests due to invalid captcha (JIRA: PROD-6653).
6. Documented APIs and models that are required for managing DSM plugins (JIRA: PROD-6309).
7. Added basic filtering protocol implementation at the API level (JIRA: PROD-6790).
8. Implemented a generic Batch API to call multiple APIs at the same time (JIRA: PROD-6589).
    - **Applied the Generic Batch API in the Quorum approval request API to support multiple actions that require a Quorum approval request (JIRA: PROD-3991).**

INTEGRATIONS

1. Added support for Google EKMS access through the Virtual Private Cloud (VPC) network (JIRA: PM-8). *For more details, refer to* [*Fortanix DSM with Google Cloud EKM Using VPC*](link) *guide.*

CLIENT IMPROVEMENTS

1. Added support for secret rotation in the Fortanix DSM CLI (JIRA: PROD-2904). *For more information, refer to* [*Developer's Guide: DSM CLI*](link).

DSM-ACCELERATOR IMPROVEMENTS

1. DSM-Accelerator Webservice:
    - **Added support to perform sign and verify operations for the DSM-Accelerator Webservice (JIRA: PROD-6704).**
    - **Implemented CLI for the DSM-Accelerator Webservice configuration parameters (JIRA: PROD-6772).**

- **Added key expiration timestamp to listener notifications in DSM-Accelerator Webservice (JIRA: PROD-6677).**
- **The DSM-Accelerator Webservice now uses the UnifiedProvider implementation (JIRA: PROD-6247).**

For more details, refer to the *Developer's Guide: Fortanix DSM-Accelerator Webservice*.

2. **DSM-Accelerator PKCS#11:**
   - **Added support to perform sign and verify operations for DSM-Accelerator PKCS#11 library (JIRA: PROD-6705).**
   - **Added cache TTL support for the DSM-Accelerator PKCS#11 library (JIRA: PROD-6534).**

For more details, refer to the *Developer's Guide: Fortanix DSM-Accelerator PKCS#11 Client*.

3. **DSM-Accelerator JCE Provider:**
   - **Added support to perform sign and verify operations for DSM-Accelerator JCE Provider (JIRA: PROD-6706).**
   - **The DSM-Accelerator JCE Provider now uses the UnifiedProvider implementation (JIRA: PROD-6247).**
   - **Moved all the environment variable settings to the appropriate configuration files for the DSM-Accelerator JCE Provider (JIRA: PROD-6776).**

For more details, refer to the *Developer's Guide: Fortanix DSM-Accelerator JCE Provider*.

TERRAFORM PROVIDER CLIENT FIXES

- Fixed an issue where the user was unable to create EC-KCDSA, DSA, and KCDSA keys using the Terraform Provider script **(JIRA: DEVOPS-3348)**.

- Fixed an issue where the user was unable to set the `group_id` variable after executing the `terraform apply` command in the `terraform.tfstate` file **(JIRA: DEVOPS-3899)**.

BUG FIXES

- Fixed an issue where saving a Google Workspace CSE configuration using the easy wizard resulted in an error in the DSM UI, but the corresponding API call succeeded and the configuration was saved successfully **(JIRA: ROFR: 4090)**.

- Fixed an issue where the DSM login screen was being shown briefly while navigating to the Fortanix Confidential AI login page **(JIRA: ROFR-4094)**.

- Fixed an issue where the DSM nodes were able to delete their own admin PKI entry **(JIRA: PROD-6820)**.

- Fixed a page crash when an app has an unknown `interface` field **(JIRA: ROFR-4131)**.

- Fixed an issue in the Azure HSM plugin that did not allow wrapping a key with a source group ID (Thales Luna HSM) **(JIRA: PROD-6816)**.

- Fixed an issue that results in DSM calling the `confirm_email` endpoint twice if an existing user has an existing password authentication session active in the browser and tries to reconfirm their email **(JIRA: ROFR-4118)**.

- Fixed an issue where the **CONFIRM EMAIL** link in the email fails with the message "Inappropriate authorization for the requested operation" for a user with SSO configured **(JIRA: PROD-6779)**.

- Fixed an issue where the DataTable filtering for users could not search certain users by name **(JIRA: ROFR-4101)**.

- Fixed an issue where searching a security object using the search text "elliptic curve" does not work **(JIRA: ROFR-4100)**.

RELEASE NOTES

Date: 13-Jun-23

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

Software: Fortanix Data Security Manager SaaS

Version: 4.18

- Fixed an issue where the "`DESIRED_KERNEL_MAJOR_VERSION`" was not defined in the `sdkms-setup.sh` script **(JIRA: DEVOPS-3885)**.

- Fixed an issue where destroying a key in a FIPS-backed group resulted in a message related to an AWS key in the detailed view of the key **(JIRA: ROFR-4084)**.

- Fixed an issue where after saving a FIPS-backed group, the **SAVE CHANGES** button does not grey out and remains active **(JIRA: ROFR-4081)**.

- Fixed an issue where the **Deactivate original key after rotation** checkbox was not removed from the Key Rotation Policy modal dialog for GCP BYOK keys after the policy was set **(JIRA: ROFR-4080)**.

- Fixed the logfile path in the 32-bit version of the Fortanix CNG provider **(JIRA: PROD-6715)**.

- Fixed an issue where the "Key rotation policy" was not supported for GCP BYOK keys **(JIRA: PROD-6713)**.

- Fixed an issue where the Derive key with DES and DES3 for HKDF mechanism resulted an error "Bad length 49 for DES key" **(JIRA: PROD-6709)**.

- Fixed an issue that now avoids database lookups for computing security object's enabled state **(JIRA: PROD-6699)**.

- Fixed an issue where the custom attributes were not shown in the DSM user interface even though the data was present in the response **(JIRA: ROFR-4061)**.

- Fixed an issue that resulted in a white background when performing a hover on the Quorum approval request on the DSM dashboard **(JIRA: ROFR-4057)**.

- Fixed an issue where the user had the option to edit a custom attribute even if it was already set in the "Key metadata policy" of the group **(JIRA: ROFR-4015)**.

- Fixed an issue where the users needed to do a hard refresh to remove quorum approval requests from previously visited accounts **(JIRA: ROFR-4008)**.

- Fixed an issue where the DSM Dashboard data was not updating on clicking the **Refresh** icon **(JIRA: ROFR-3986)**.

- Resolved an issue that caused panic when an RSA key was utilized in an encryption or decryption operation by the DSM-Accelerator Webservice **(JIRA: PROD-6552)**.

- Fixed an issue where self-provisioning into a new account for existing users marked the users as unverified **(JIRA: PROD-6535)**.

- Fixed an issue where Azure tags were removed when setting the "Key rotation policy" on the copied key in the Azure Cloud Data Control group **(JIRA: PROD-6361)**.

- Fixed an issue where the security object name was split into multiple lines in the detailed view of the security object **(JIRA: ROFR-4053)**.

- Fixed an issue where failing roles API calls were still captured in the Networks tab and logs were logged even though the Custom Roles feature was disabled at the cluster-level **(JIRA: ROFR-4070)**.

- Fixed various user lockout issues **(JIRA: PROD-6711)**:
  - Fixed an issue where user authentication failures from unknown users had the wrong actor type **(JIRA: PROD-6654)**.
  - Fixed an issue where user lockouts were repeatedly logged for locked-out users who were logging in with the correct credentials **(JIRA: PROD-6655)**.

- o Fixed an issue where the `ResetPassword` endpoint did not clear the user lockout **(JIRA: PROD-6657)**.
  - o Fixed an issue where user lockouts were audit logged under the severity-level `Info` **(JIRA: PROD-6618)**.
- Fixed an issue where linked key rotation did not work when the source group has a Quorum approval policy configured **(JIRA: PROD-5885)**.

QUALITY ENHANCEMENTS/UPDATES

- Upgraded Helm to version 3.11.3 (**JIRA: DEVOPS-3912**).
- Upgraded the 5.4 Kernel version to 5.4.0.147 (**JIRA: DEVOPS-3893**).
- Configured Cert Manager on Kubernetes 1.21.14 to provide certificates for peer encryption between Cassandra nodes (**JIRA: DEVOPS-3586**).

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` configuration 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**).
- Rotating a GCP BYOK virtual key to a Fortanix DSM-backed key (**Rotate to DSM key**) is not supported (**JIRA: PROD: 6722**).
  Workaround: You can manually copy the AES 256 key from a normal DSM group to a GCP-backed group.
- The "Rotate linked key" feature does not work when a Fortanix DSM source key is rotated along with its linked keys by selecting the "**Rotate linked keys**" check box, where the linked key might belong to a GCP group. In this

case rotating the linked key results in rotating the key in GCP as well as generating the new key in GCP (**JIRA: ROFR: 4075**).

Workaround: You must first manually rotate the source key in the normal DSM group and then copy the rotated key to the GCP group.

- An Azure Managed HSM external KMS group now also allows the following security object types to be generated or imported. But the Bring Your Own Key (BYOK) and rotate key functionality does not work for these security object types (**JIRA: ROFR: 4192**).

    o EC

    o AES 128 and AWS 192

Workaround: Do not generate or import security objects of type EC, AES 128, and AES 192 in an external KMS group of type Azure Managed HSM since the only allowed security object types for an Azure key generated using the Generate or Import key workflows are:

    o RSA key pairs (RSA_2048, RSA_3072, and RSA_4096).

    o AES 256

- For the Azure Managed HSM external KMS group, the following security object types are enabled (**JIRA: ROFR: 4187**).

    o DES

    o DES3

    o EC-KCDSA

Workaround: Do not generate or import security objects of type EC-KCDSA, DES, or DES3 in an external KMS group of type Azure Managed HSM since the only allowed security object types for an Azure key generated using the Generate or Import key workflows are:

    o RSA key pairs (RSA_2048, RSA_3072, and RSA_4096).

    o AES 256

RELEASE NOTES

Date: 13-Jun-23

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

Software: Fortanix Data Security Manager SaaS

Version: 4.18

- If an Azure key is rotated and then soft-deleted, only one version of the key is soft-deleted (**JIRA: PROD: 6947**).

  Workaround: Perform a key scan in DSM to synchronize the key state with Azure.

- Searching for an item without using the search filter in the Fortanix DSM Groups, Apps, and Security Objects table does not show any search results (**JIRA: ROFR: 4178**).

  Workaround: Perform a search using the search filter followed by the value. For example, search using the search filter "Name" followed by the value.
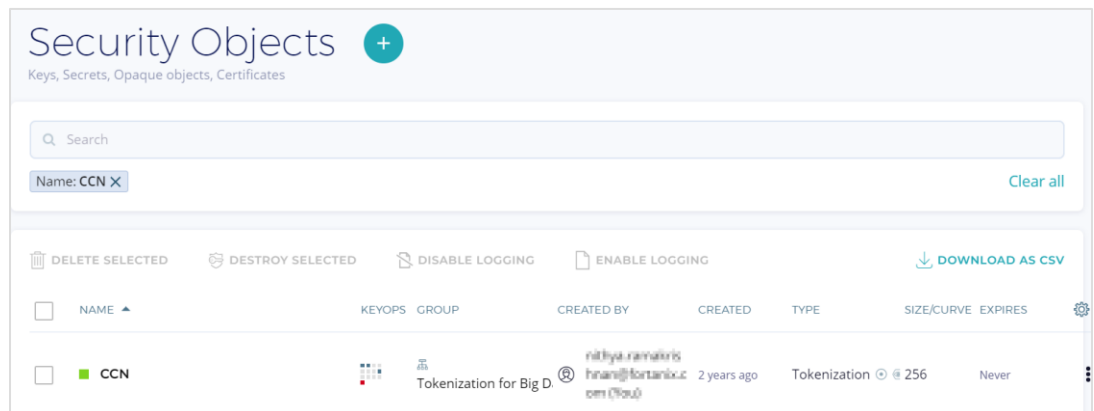
BEST PRACTICES

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.

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

✉ info@fortanix.com

⊕ www.fortanix.com

RELEASE NOTES

Date: 13-Jun-23

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

Software: Fortanix Data Security Manager SaaS

Version: 4.18

SUPPORT

For any questions regarding this release note, please contact support@fortanix.com

DISCLAIMERS

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

✉ info@fortanix.com

🌐 www.fortanix.com