

RELEASE NOTES

Date: 8-Aug-23

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

Software: Fortanix Data Security Manager SaaS

Version: 4.20

OVERVIEW

This document provides an overview of new features, general improvements, and resolved issues in the Fortanix Data Security Manager (DSM) SaaS 4.20 release.

This release is **superseded** by [August 28, 2023](#) release.



NOTE:

- This release is for **SaaS only** and is not available for on-premises installations. Updates in this release will be part of a future on-premises release.

NEW FUNCTIONALITY / FEATURES

- **Added a new app-based authentication for Google Workspace CSE (JIRA: PM-29):**

With this release, DSM account administrators can select between the existing user-based authentication and the new app-based authentication in the Google Workspace CSE easy wizard, allowing the Google Workspace users to only access the CSE related endpoints without having to accept a DSM user invitation or verify their e-mail address. Outside of the easy wizard, this can be done by selecting the new app authentication type **"Workspace CSE App Auth"** when adding new Google Workspace users as applications in the DSM **Apps** tab.

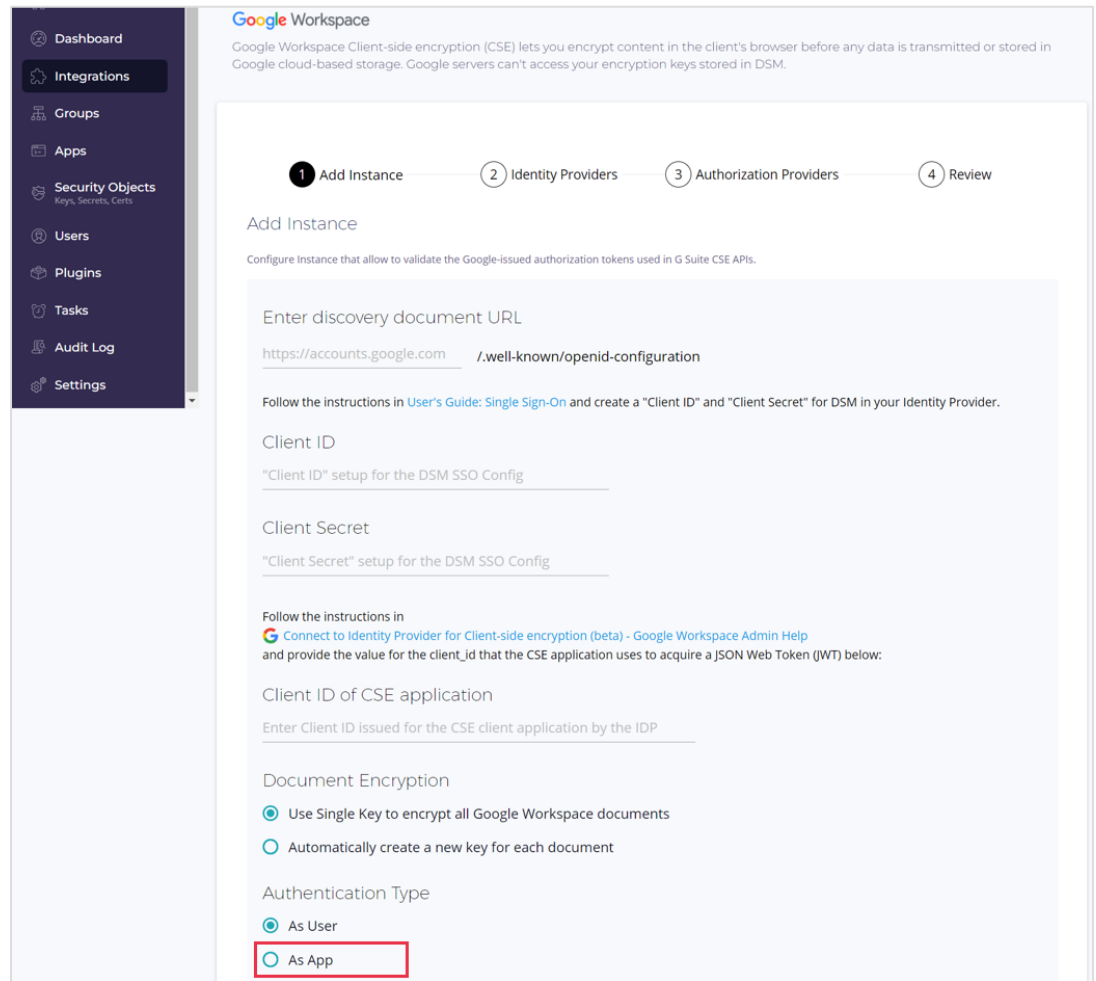
RELEASE NOTES

Date: 8-Aug-23

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

Software: Fortanix Data Security Manager SaaS

Version: 4.20



Google Workspace

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.

1 Add Instance — 2 Identity Providers — 3 Authorization Providers — 4 Review

Add Instance

Configure Instance that allow to validate the Google-issued authorization tokens used in G Suite CSE APIs.

Enter discovery document URL
<https://accounts.google.com/.well-known/openid-configuration>

Follow the instructions in [User's Guide: Single Sign-On](#) and create a "Client ID" and "Client Secret" for DSM in your Identity Provider.

Client ID
 "Client ID" setup for the DSM SSO Config

Client Secret
 "Client Secret" setup for the DSM SSO Config

Follow the instructions in [Connect to Identity Provider for Client-side encryption \(beta\) - Google Workspace Admin Help](#) and provide the value for the client_id that the CSE application uses to acquire a JSON Web Token (JWT) below:

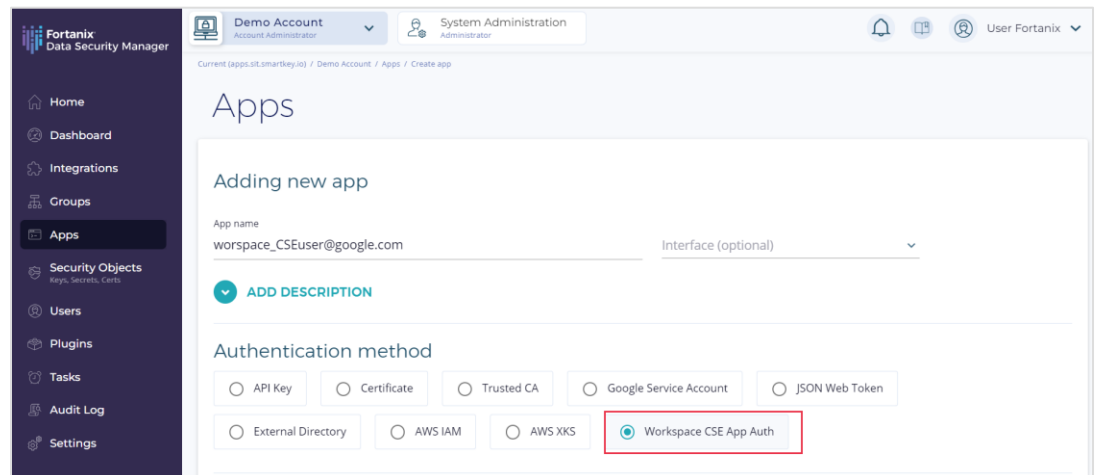
Client ID of CSE application
 Enter Client ID issued for the CSE client application by the IDP

Document Encryption

- ☒ Use Single Key to encrypt all Google Workspace documents
- ☐ Automatically create a new key for each document

Authentication Type

- ☒ As User
- ☐ As App



Fortanix Data Security Manager

Demo Account Account Administrator System Administration Administrator User Fortanix

Current (apps.sit.smarkey.io) / Demo Account / Apps / Create app

Apps

Adding new app

App name
 workspace_CSEuser@google.com Interface (optional)

[ADD DESCRIPTION](#)

Authentication method

- ☐ API Key
- ☐ Certificate
- ☐ Trusted CA
- ☐ Google Service Account
- ☐ JSON Web Token
- ☐ External Directory
- ☐ AWS IAM
- ☐ AWS XKS
- ☒ Workspace CSE App Auth

RELEASE NOTES

Date: 8-Aug-23

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

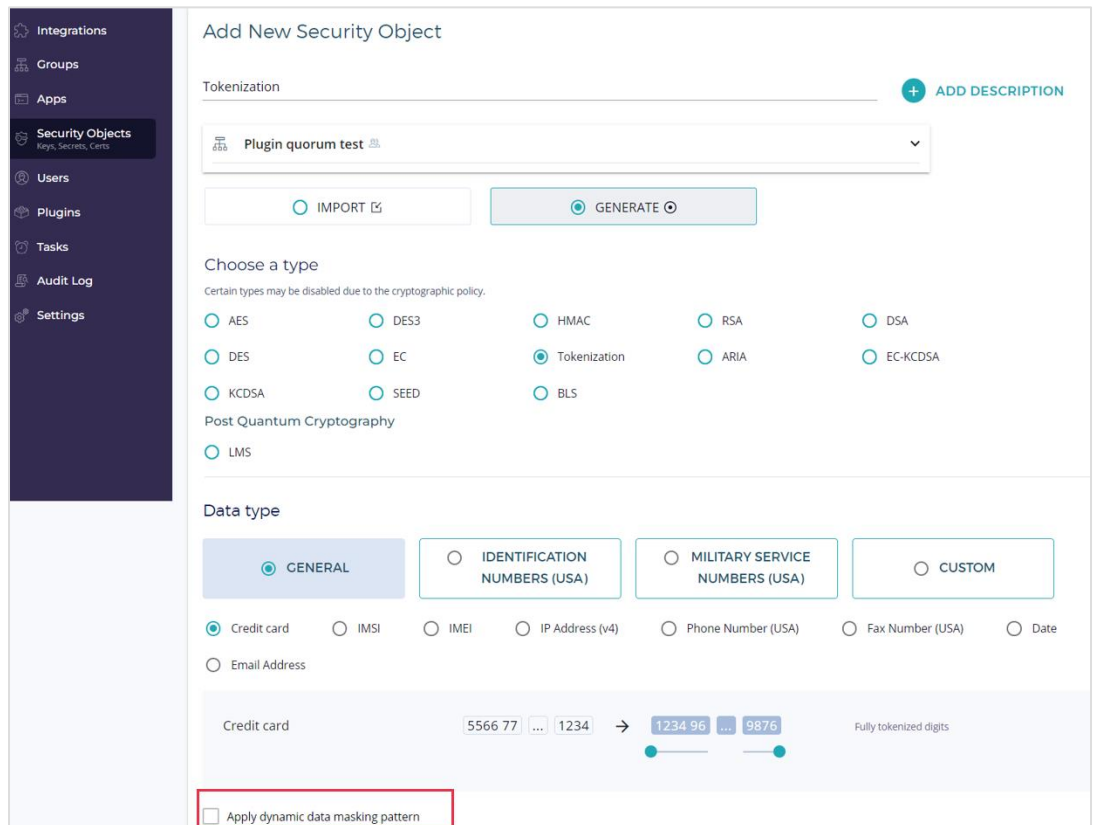
Software: Fortanix Data Security Manager SaaS

Version: 4.20

For more details, refer to the [Integration Guide: Fortanix DSM with Google Workspace CSE](#).

ENHANCEMENTS TO EXISTING FEATURES

1. Renamed “Add masking pattern” to “Apply dynamic data masking pattern” in the generate or import security object of type Tokenization workflow and in the Snowflake integration workflow (JIRA: PM-71).



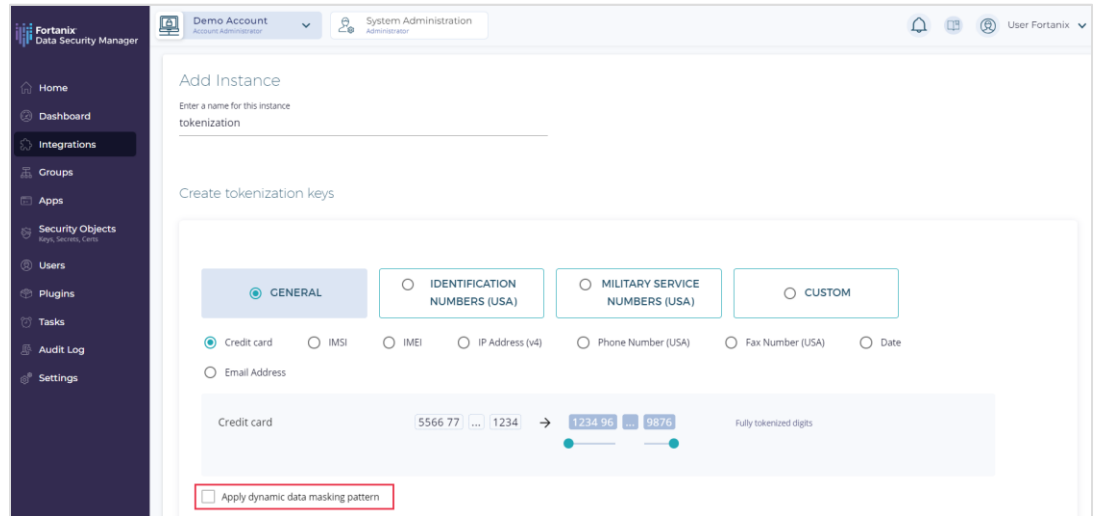
RELEASE NOTES

Date: 8-Aug-23

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

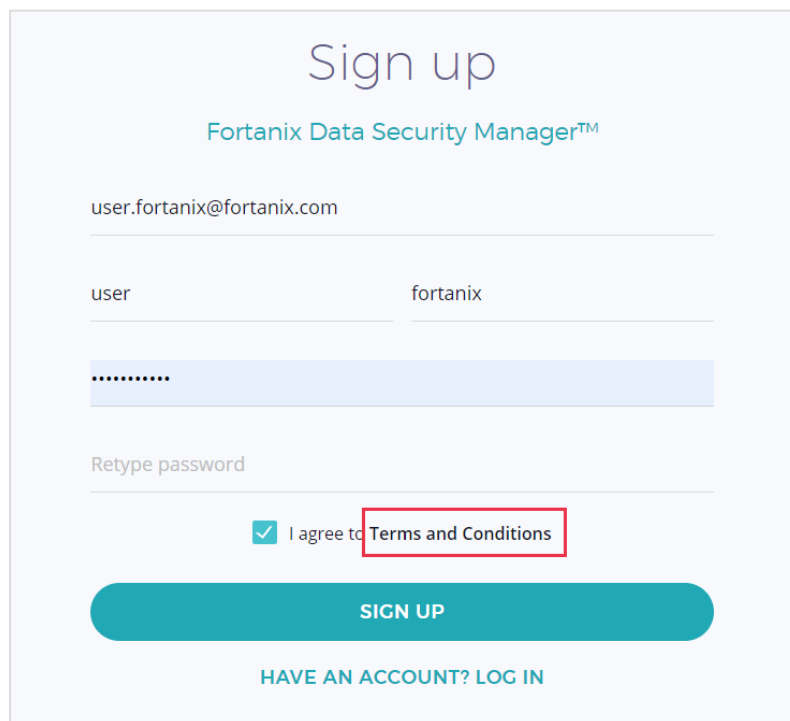
Software: Fortanix Data Security Manager SaaS

Version: 4.20



For more details, refer to [User's Guide: Tokenization](#).

- Updated the "Terms and Conditions" link on the SaaS Sign-up page to point to the "Fortanix DSM SaaS Terms of Use" on the Fortanix Website (JIRA: ROFR-4220).



RELEASE NOTES

Date: 8-Aug-23

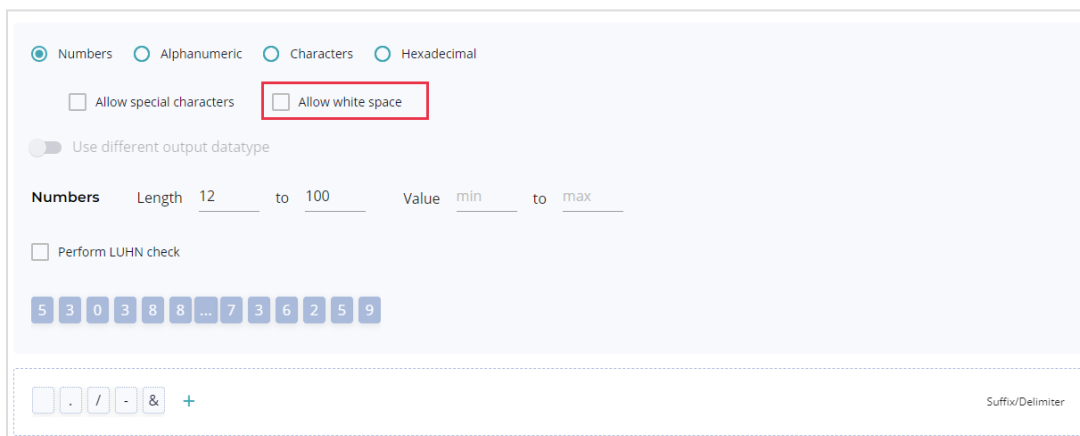
Subject: Software changes, updates, bug fixes, etc.

Software: Fortanix Data Security Manager SaaS

Version: 4.20

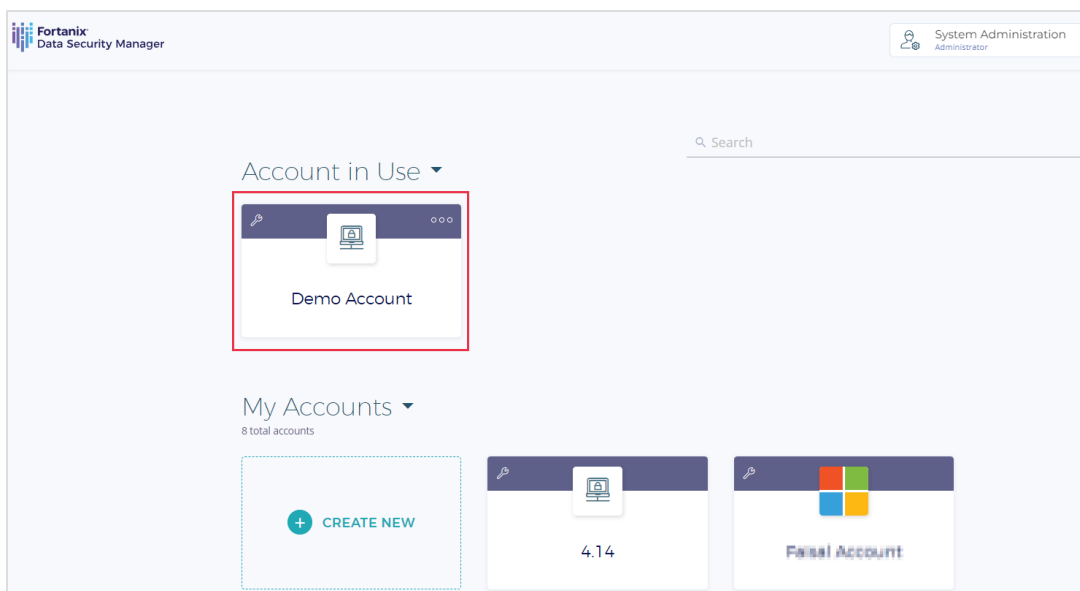
3. Added a new check box “Allow white space” for Custom tokens of type Numbers, Alphanumeric, or Characters (JIRA: ROFR-4210):

By selecting the “Allow white space” option, users can add whitespaces as characters anywhere in the token.



For more details, refer to [User's Guide: Tokenization](#).

4. Added support to store and automatically select the last selected DSM account ID when the user again logs in to Fortanix DSM (JIRA: ROFR-4203):



RELEASE NOTES

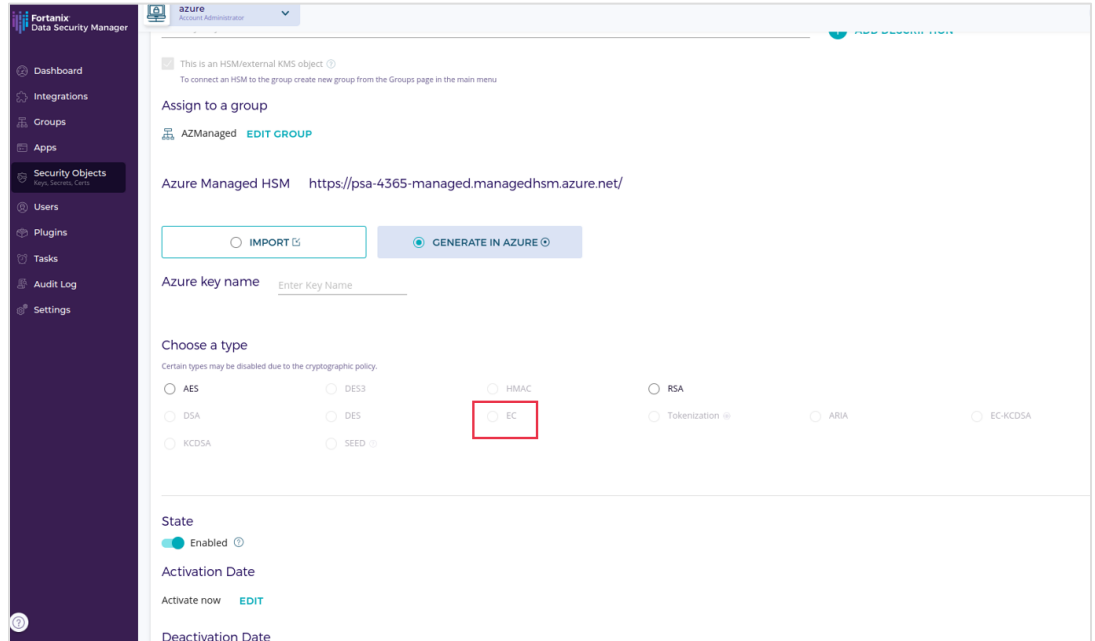
Date: 8-Aug-23

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

Software: Fortanix Data Security Manager SaaS

Version: 4.20

5. Disabled EC key for Azure Managed HSM group (JIRA: ROFR-4192):



This is an HSM/external KMS object. To connect an HSM to the group create new group from the Groups page in the main menu.

Assign to a group

AZManaged [EDIT GROUP](#)

Azure Managed HSM <https://psa-4365-managed.managedhsm.azure.net/>

☐ IMPORT ☒ GENERATE IN AZURE

Azure key name

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

State

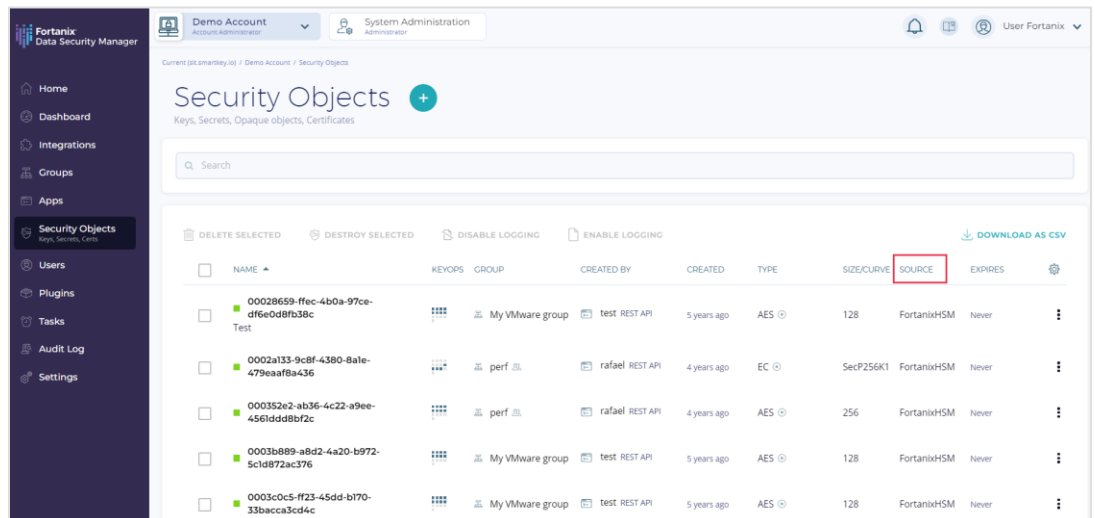
☒ Enabled

Activation Date

Activate now [EDIT](#)

Deactivation Date

6. Added the "Source" Column to the Security Object list view (JIRA: ROFR-4161).



Current (01:amrkey-01) / Demo Account / Security Objects

Security Objects [+](#)

Keys, Secrets, Opaque objects, Certificates

[DELETE SELECTED](#)
[DESTROY SELECTED](#)
[DISABLE LOGGING](#)
[ENABLE LOGGING](#)
[DOWNLOAD AS CSV](#)

<input type="checkbox"/>	NAME	KEYOPS	GROUP	CREATED BY	CREATED	TYPE	SIZE/CURVE	SOURCE	EXPIRES	⋮
<input type="checkbox"/>	00028659-ffe-4b0a-97ce-dfe0d8fb38c Test		My VMware group	test REST API	5 years ago	AES	128	FortanixHSM	Never	⋮
<input type="checkbox"/>	0002a133-9c8f-4380-8ale-479eaf8a436		perf	rafael REST API	4 years ago	EC	SecP256K1	FortanixHSM	Never	⋮
<input type="checkbox"/>	000352e2-ab36-4c22-a9ee-456idd8bf2c		perf	rafael REST API	4 years ago	AES	256	FortanixHSM	Never	⋮
<input type="checkbox"/>	0003b889-a8d2-4a20-b972-5cd872ac376		My VMware group	test REST API	5 years ago	AES	128	FortanixHSM	Never	⋮
<input type="checkbox"/>	0003c0c5-f123-45dd-b170-33baacca3cd4c		My VMware group	test REST API	5 years ago	AES	128	FortanixHSM	Never	⋮

RELEASE NOTES

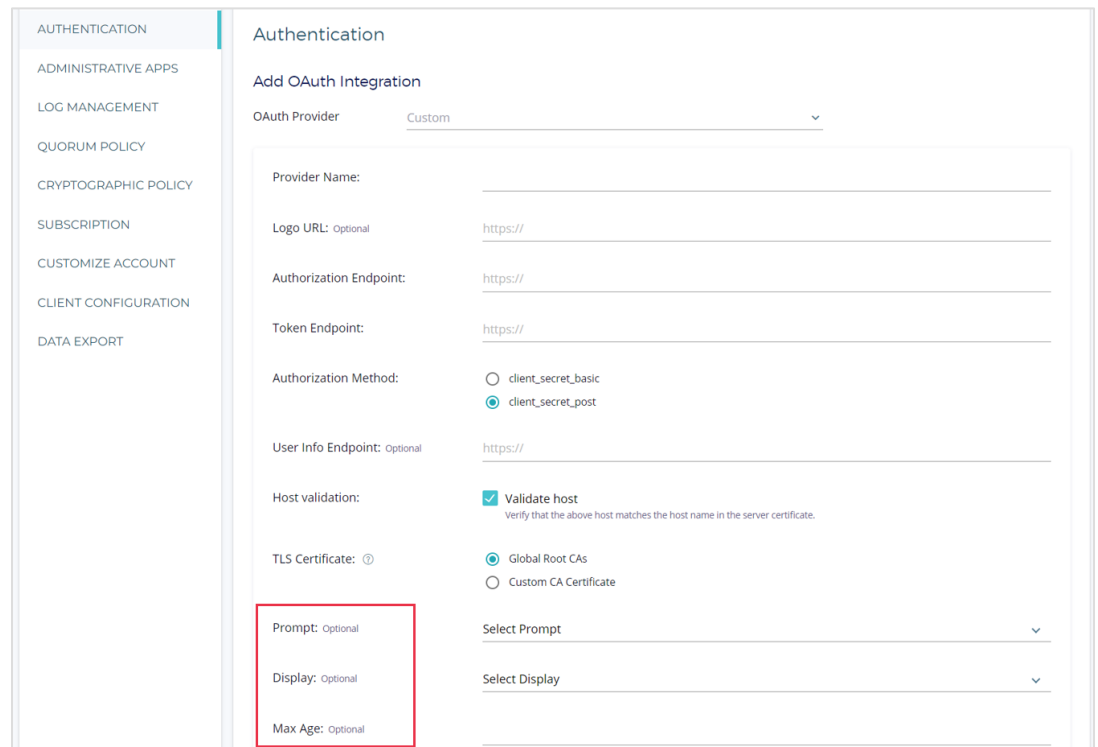
Date: 8-Aug-23

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

Software: Fortanix Data Security Manager SaaS

Version: 4.20

- Added the new optional fields: **Prompt**, **Display**, and **Max Age** to the **OAuth** Single Sign-On configuration form on the DSM account **Settings** → **Authentication** page. The default value for the **Prompt** field will be **Consent**. (JIRA: ROFR-3249).



For more details, refer to [User's Guide: Authentication](#).

- Added Tooltip to clarify the "Allow special characters" check box for the create tokenization security object of type "Custom" (JIRA: ROFR-4282).

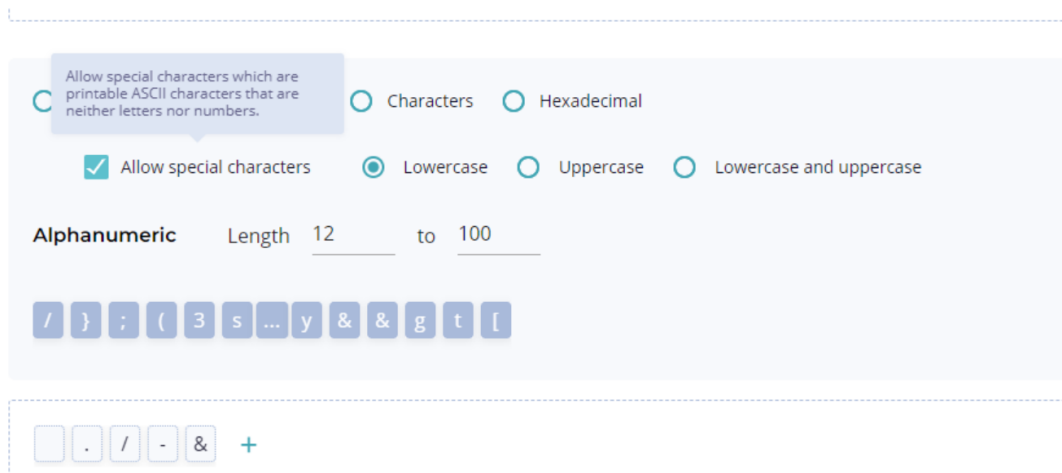
RELEASE NOTES

Date: 8-Aug-23

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

Software: Fortanix Data Security Manager SaaS

Version: 4.20



The screenshot shows the password policy configuration interface. It includes a tooltip that reads: "Allow special characters which are printable ASCII characters that are neither letters nor numbers." Below the tooltip, there are radio buttons for "Characters" and "Hexadecimal", both of which are unselected. There are also radio buttons for "Lowercase", "Uppercase", and "Lowercase and uppercase", all of which are unselected. A checkbox labeled "Allow special characters" is checked. Below these options, there is a section for "Alphanumeric" with a "Length" field set to "12" and a "to" field set to "100". At the bottom, there is a row of buttons for special characters: "/", "}", ";", "(", "3", "s", "...", "y", "&", "&", "g", "t", and "[". Below this row, there is another row of buttons: ".", "/", "-", "&", and a "+" button.

9. Updated the Data Custodian plugin title to "SAP Data Custodian" (JIRA: PROD-6742).
10. Added support to sort the security objects custom attributes in the CSV report (JIRA: ROFR-4186).

OTHER IMPROVEMENTS

- Added support for graceful fallback for tokenization types if the FPE pattern for the tokenization object returned from the API response does not match the predefined pattern saved in DSM UI (JIRA: ROFR-4211).
- Updated the readme file for the PGPSign script to add missing text (JIRA: PROD-6510).
- Added Open API documentation for cryptographic APIs (JIRA: PROD-6305).

INTEGRATIONS/USE CASES

- Fortanix DSM now supports integration with SAP for Tokenization (JIRA: IX-16). For more details, refer to [Fortanix DSM with SAP S/4 HANA](#)
- Fortanix DSM now supports integration with Cassandra TDE (JIRA: EXTREQ-871). For more details, refer to [Fortanix DSM with Cassandra TDE](#)

RELEASE NOTES

Date: 8-Aug-23

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

Software: Fortanix Data Security Manager SaaS

Version: 4.20

BUG FIXES

- Fixed an issue where the `auth_params` field was not accessible from the discover endpoint (**JIRA: PROD-7102**).
- Fixed an issue where the locate by custom attributes operation on security objects returns 1001 keys instead of 1000 keys (**JIRA: PROD-7087**).
- Fixed an issue where the DSM-Accelerator JCE Provider script had hardcoded values for the DSM version number (**JIRA: PROD-7067**).
- Fixed an issue where the style of the **DELETE SELECTED**, **ENABLE LOGGING**, **DISABLE LOGGING**, **DESTROY SELECTED**, and **DOWNLOAD CSV** buttons are broken for the security object row in the Security Objects table (**JIRA: ROFR-4209**).
- Fixed an issue where the security object count on the Security Objects page did not match the count in the **Security Object** tab in the detailed view of the Group (**JIRA: ROFR-4196**).
- Fixed an issue where the **Azure Tags** section was showing under the **Custom Attributes** section instead of showing as separate sections in an Azure Managed HSM backed group detailed view (**JIRA: ROFR-4193**).
- Fixed an issue where the Export permission was not disabled for AES, RSA, and EC keys in an Azure Managed HSM-backed group (**JIRA: ROFR-4191**).
- Fixed an issue where the user could not enter different values for the **Azure key name** and **GCP key name** fields when copying a key from a normal group to an Azure Managed HSM and GCP group simultaneously (**JIRA: ROFR-4189**).
- Fixed an issue where creating an Azure-backed group without a client secret can result in panics later (**JIRA: PROD-6939**).
- Fixed an issue where unsupported keys were not disabled during key creation in an Azure Managed HSM group (**JIRA: ROFR-4187**).

RELEASE NOTES

Date: 8-Aug-23

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

Software: Fortanix Data Security Manager SaaS

Version: 4.20

- Fixed an issue where the Key Encryption Key (KEK) feature was not disabled for an HSM/external KMS group (**JIRA: ROFR-4164**).
- Fixed an issue where a security object name with 60 characters overlaps on the **COPY KEY** and **CREATE NEW KEY** buttons on the right of the security object detailed view (**JIRA: ROFR-4156**).
- Fixed an issue where the user was unable to purge an Azure key in DSM (**JIRA: PROD-5659**).
- Fixed an issue where when a user hovers over a security object row in the **SECURITY OBJECTS** tab in the group detailed view, the blue row selection indicator appeared too close to the check box for the row (**JIRA: ROFR-4232**).
- Fixed an issue where a user was unable to edit another user's role using the "**EDIT USER ROLE**" option in the **USERS** tab in the detailed view of a group (**JIRA: ROFR-4325**).
- Fixed the certificate import bug in the Fortanix DSM JCE Provider KeyStore (**JIRA: PROD-7051**).

KNOWN ISSUES

- The DSM login page is shown briefly after performing an SSO login (**JIRA: ROFR-4148**).
- The `stats` APIs does not work as expected in DSM 4.13 and above (**JIRA: PROD-6769**).
- The sync key API returns a "400 status code and response error" if its short-term access token expires during synchronization of a group linked to AWS KMS (**JIRA: PROD-3903**). **Workaround:** increase the timeout of the temporary session token beyond the expected duration of the sync key operation.

RELEASE NOTES

Date: 8-Aug-23

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

Software: Fortanix Data Security Manager SaaS

Version: 4.20

- `exclude` does not work in the `proxy` configuration for operations such as attestation (**JIRA: PROD-3311**).
- Rotating a GCP BYOK key to a pre-existing Fortanix DSM-hosted key (**Rotate to DSM key**) is not supported (**JIRA: PROD-6722**).
Workaround: You can manually copy an existing AES 256 key from a normal DSM group to a GCP-backed group. This key automatically becomes the currently active crypto key version in the GCP key ring.
- The “Rotate linked key” feature fails with an error for keys in an externally backed group where the external entity is a Google Cloud Platform key ring (**JIRA: PROD-6828**).
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**).
 - EC
 - AES 128 and AES 192**Workaround:** Do not generate or import security objects of type EC, AES 128, or 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:
 - RSA key pairs (RSA_2048, RSA_3072, and RSA_4096).
 - AES 256
- 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**).

RELEASE NOTES

Date: 8-Aug-23

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

Software: Fortanix Data Security Manager SaaS

Version: 4.20

- EC
- AES 128 and AES 192

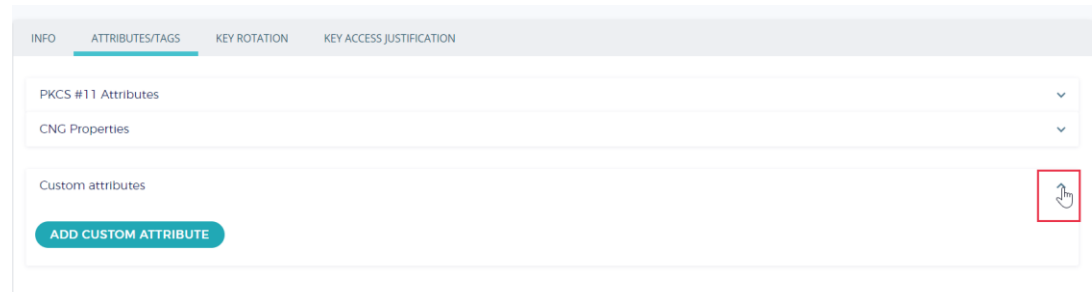
Workaround: Do not generate or import security objects of type EC, AES 128, or AES 192 in an external KMS group of type Azure Managed HSM since the only allowed security object types for an Azure key generated using the Generate or Import key workflows are:

- RSA key pairs (RSA_2048, RSA_3072, and RSA_4096).
- AES 256
- 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.

- Unable to add Custom Attributes for a Fortanix DSM security object from its detailed view (**JIRA: ROFR-4252**).
 - Clicking the **ADD CUSTOM ATTRIBUTE** button does not load the **Label** and **Value** fields.

Workaround: Click the drop down for the “Custom attributes” section twice to load the Label and Value fields.



The screenshot shows the 'ATTRIBUTES/TAGS' tab in the Fortanix Data Security Manager interface. It displays a list of attributes: 'PKCS #11 Attributes', 'CNG Properties', and 'Custom attributes'. Below the 'Custom attributes' section, there is a red box highlighting the 'ADD CUSTOM ATTRIBUTE' button and a hand icon pointing to the 'Custom attributes' dropdown menu, indicating the area where the issue occurs.

- When you type a label of the custom attribute, the text box loses focus.

Workaround: Enter the label of the custom attribute again for the second time to add the custom attribute successfully.

RELEASE NOTES

Date: 8-Aug-23

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

Software: Fortanix Data Security Manager SaaS

Version: 4.20

- Increasing the “**Retention period for Audit Logs**” setting at the account level duplicates the “purge audit log” message in the audit logs (**JIRA: PROD-7031**).
- Users will see the "Not a HSM group" error message while deleting the HSM/KMS group from the FIPS-backed group (**JIRA: ROFR-4245**).
- The `create` operation for security object creation does not work for the Azure Managed HSM plugin (**JIRA: PROD-7078**).
- The **AWS Key Policy** section alignment moved from the bottom of the security object detailed view to the right side of the page. This is a cosmetic issue only (**JIRA: ROFR-4241**).
- Users without two-factor authentication do not see the pop-up message “Unable to select this account. Reason: Two-factor authentication is required for this operation” when they select an account that has two-factor authentication configured (**JIRA: ROFR-4238**).
- The retry mechanism does not work as expected in the DSM-Accelerator Webservice (**JIRA: PROD-7068**).
- The **SUBMIT** button is not disabled when no Security Objects are selected or all security objects are in a disabled state and the user checks the **Rotate linked key** check box (**JIRA: ROFR-4233**).
- The **SUBMIT** button is not disabled when no Security Objects are selected or all security objects are in a disabled state and the user checks the **Rotate linked key** check box (**JIRA: ROFR-4233**).
- When the Batch Sign operation is performed for **Curve Ed25519/X25519** in DSM-Accelerator Webservice, the status code is showing as 500 instead of 400 (**JIRA: PROD-7007**).
- When a user logs in to a DSM account with Azure OAuth login details where the account was configured with OAuth Single Sign-On authentication method with “**No Roles can login with password**” option, it redirects the

RELEASE NOTES

Date: 8-Aug-23

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

Software: Fortanix Data Security Manager SaaS

Version: 4.20

user again to the Azure OAuth log in page again instead of redirecting to the selected account (**JIRA: ROFR-4298**).

- When a key is soft-deleted from the DSM Azure Key Vault Cloud Data Control (CDC) group, the “Purge deleted key” button is not visible in the UI (**JIRA: PROD-7202**).
- Rotating a linked AWS KMS key when the source key in a regular DSM group is rotated, does not display the modal window to confirm the linked key rotation (**JIRA: ROFR-4324**).
- The “Copy Key” feature for LMS key results in an error (**JIRA: PROD-7336**).

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.

SUPPORT

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

DISCLAIMERS

RELEASE NOTES

Date: 8-Aug-23

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

Software: Fortanix Data Security Manager SaaS

Version: 4.20

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 4.20