STORMSHIELD

SDS ENCRYPTION SERVICE FOR GOOGLE WORKSPACE

RELEASE NOTES

Version 4.4.0

Document last updated: December 30, 2024

Reference: sds-en-sds-for-gw-release_notes-v4.4

Table of contents

Version number

The business name of the SDS encryption service for Google Workspace 4.4.0 corresponds to version number 4.4.0.212.

SDS encryption service for Google Workspace 4.4.0 new features and enhancements

For information about the Google services supported by the SDS encryption service for Google Workspace (client-side encryption), refer to the section *Which services CSE supports* of Google documentation About client-side encryption.

Environment

Deployment via a Docker image

In addition to the traditional RPM-based installation it is now possible to install using a Docker image.

New requirements for installation in RPM mode

The SDS encryption service for Google Workspace now requires RedHat Enterprise 8.10 or 9 to be installed.

Gmail message encryption

The SDS encryption service for Google Workspace now supports the *SHA512withRSA* algorithm for key encryption for Gmail.

Support for Google features

Google Drive and external users

The SDS encryption service for Google Workspace is now compatible with the Google Guest access feature. This enables users outside your company to access your encrypted content on Google Drive. To do this, you must configure a dedicated identity provider for Google Drive Guest users and add them to the list of authorized providers in the *config.json* file, section **tenants > user_authentication > idps**.

For more information, refer to the Google documentation.

Mass import of files to Google Drive

The SDS encryption service for Google Workspace now supports the mass importing of sensitive data into Google Drive. Data imported from third-party storage are encrypted by the SDS encryption service for Google Workspace in Google Drive. See an example on Github googleworkspace.

This Beta feature is currently under development at Google.

For more information, refer to the Google documentation and contact Google Support.

SDS CryptoAPI

The new SDS CryptoAPI feature provides two API routes, *crypto/encrypt* and *crypto/decrypt*, which enable data to be encrypted and decrypted, completely independently of Google.

You can write OPA rules for the CryptoAPI in dedicated files.

SDS CryptoAPI is currently in its alpha version. Stormshield does not guarantee that it will be possible to decrypt data encrypted with this version with a later version of the feature.

Support for Google Meet hardware

The new delegation feature enables a user to delegate their authentication to join an encrypted Google Meet conference from a room with Meet hardware. This feature is in *alpha* version.

Logs

Business operations logs (kind:domain)

- Generation of authentication tokens for delegation (*cse* category - *delegate* action)
- Key management as a service *(kmaas* category)
- Queries concerning KEK keys (kek *category*)
- Validation of authorization tokens (*authorization* category)
- Validation of authentication tokens (*authentication* category)

Logs of operations related to the environment (kind:system)

- Web server related operations(*server* category)
- Key Management System operations *(kms* category)

SDS encryption service for Google Workspace 4.4.0 fixes

The SDS encryption service for Google Workspace now displays an error at startup if the private key format entered in the *migration* section of the configuration file is not in base 64 format. This check prevents migration operations from failing afterwards.

The reception log for an HTTP request is now displayed, even if the body format of the request is incorrect. This correction only concerns the log in the new V2 format.

The SDS encryption service for Google Workspace now displays an error at startup when the *authorization* section of the configuration file is empty.

The following deprecated cryptographic suites are no longer supported to connect to the KMS via KMIP.

- TLS_RSA_WITH_AES_256_CBC_SHA256(0x003d)
- TLS_RSA_WITH_AES_256_CBC_SHA(0x0035)
- TLS_RSA_WITH_AES_256_GCM_SHA384(0x009d)
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384(0xc02c)
- TLS_RSA_WITH_AES_128_CBC_SHA256(0x003c)

Known issues

The up-to-date list of the known issues related to this version of the SDS encryption service for Google Workspace is available on the **Knowledge Base** Stormshield. To connect to the Knowledge base, use the same identifiers as for **MyStormshield**.

Previous versions of SDS encryption service for Google Workspace

In this section, you will find the new features from previous versions of SDS encryption service for Google Workspace.

4.3.2		Resolved vulnerabilities	
4.3.1			Bug fixes
4.3	Features	Resolved vulnerabilities	Bug fixes
4.2.4			Bug fixes
4.2.3			Bug fixes
4.2.2			Bug fixes
4.2.1	Features		Bug fixes
4.2	Features		
4.1.1	Features		
4.1	Features		Bug fixes
4.0	Features		
3.0	Features		
1.2.1	Features		

Resolved vulnerability in SDS encryption service for Google Workspace 4.3.2

A medium severity vulnerability was fixed.

Details on this vulnerability can be found on our website:

- https://advisories.stormshield.eu/2024-033/

SDS encryption service for Google Workspace 4.3.1 fix

An issue when validating authentication on privileged routes caused the SDS encryption service for Google Workspace to stop unexpectedly if a KACLS was configured as a backup KACLS. This issue has been fixed.

SDS encryption service for Google Workspace 4.3 new features and enhancements

For information about the Google services supported by the SDS encryption service for Google Workspace (client-side encryption), refer to the section *Which services CSE supports* of Google documentation About client-side encryption.

New version numbering

Version numbers for the SDS encryption service for Google Workspace Saas and On Premises have been harmonized. They now use the following numbering pattern:

<major>.<minor>.<corrective>.<build>

The table below indicates the version number which corresponds to a business name:

Version name	Version number
4.3	4.3.0.158
4.3 beta 1	4.3.0.145

Environment

New installation requirements

SDS encryption service for Google Workspace now requires NodeJS 20, OpenSSL 3.0 and RedHat Enterprise 8.8 or 9 to benefit from the latest security updates.

Start-up time of the SDS encryption service for Google Workspace

The start-up time of the SDS encryption service for Google Workspace has been optimized.

TLS algorithms

The number of TLS algorithms used by default have been restricted to improve the security of incoming and outgoing communications.

Connections to the Key management System (KMS)

Connections to the KMS are no longer closed after each operation, but now remain open. When a connection problem occurs, the SDS encryption service for Google Workspace tries to reconnect, and logs are issued to inform the administrator.

Support for Google features

Support for Gmail on mobile

With the SDS encryption service for Google Workspace, users can now encrypt their emails in Gmail on iOS and Android mobile devices.

Edit encrypted Excel files with Google Sheets

Users can now view and edit encrypted Excel files directly with Google Sheets.

For more information, refer to the Google documentation.

Encrypted import of Excel files into Google Sheets

Users can now import and encrypt Microsoft Excel files into Google Sheets.

For more information, refer to the Google documentation.

Manage comments and action items on Google Docs

The SDS encryption service for Google Workspace is now compatible with comment and action item management on Google Docs.

For more information, refer to the Google documentation.

Co-host management in Google Meet

The SDS encryption service for Google Workspace is now compatible with the Google Meet co-host feature.

For more information, refer to the Google documentation.

External Google Meet invitations

The SDS encryption service for Google Workspace now supports Google's Beta feature for inviting external participants to Google Meet conferences. To do this, you must configure two dedicated identity providers and add them to the list of authorized providers in the *config.json* file, section **tenants > user_authentication > idps**.

This Beta feature is currently under development at Google. Contact Google Support for more information on implementation and limitations.

Encryption and signature keys

It is now possible to use different keys to decrypt and sign Gmail messages.

Gmail messages signing

PKCS1.5 signing using the KMIP protocol is now supported when the SDS encryption service for Google Workspace is configured to store the keys in the KMS to secure Gmail.

Administration route authentication

Authentication of privileged administration routes and authentication of the route used to initialize Google users for Gmail message encryption are now different to enhance security.

Algorithms for checking JWT tokens

It is now possible to configure the list of algorithms used to check the validity of authorization and authentication tokens (JWT).

Bulk file import

The SDS encryption service for Google Workspace now supports bulk import of encrypted files into Google Drive using a compatible third-party software. A new API route, `/privilegedwrap`, has been added for this purpose. It can only be used with administration rights.

For more information, refer to the Google documentation.

Resolved vulnerability in SDS encryption service for Google Workspace 4.3

Two medium severity vulnerabilities were fixed.

Details on these vulnerabilities can be found on our website:

- https://advisories.stormshield.eu/2024-009/
- https://advisories.stormshield.eu/2024-010/
- https://advisories.stormshield.eu/2024-012/
- https://advisories.stormshield.eu/2024-013/

SDS encryption service for Google Workspace 4.3 fixes

The type returned in the logs related to the identity provider configuration retrieval is now correct.

431 errors are now handled correctly when the requests received have too long headers.

Error messages issued when a proxy is unreachable have been improved.

The reading of environment variables when starting the SDS encryption service for Google Workspace has been optimized.

The management and display of network errors in logs have been improved.

A log is now issued for each outgoing connection made by the SDS encryption service for Google Workspace.

SDS encryption service for Google Workspace 4.2.4 fix

An issue when validating authentication on privileged routes caused the SDS encryption service for Google Workspace to stop unexpectedly if a KACLS was configured as a backup KACLS. This issue has been fixed.

SDS encryption service for Google Workspace 4.2.3 fix

An issue occurring when calculating the *key_hash* resource during migration between a third-party external key service (KACLS) and the SDS encryption service for Google Workspace has been fixed.

SDS encryption service for Google Workspace 4.2.2 fix

Some issues relating to the migration system between a third-party external key service (KACLS) and the SDS encryption service for Google Workspace have been fixed.

SDS encryption service for Google Workspace 4.2.1 new features and enhancements

For information about the Google services supported by the SDS encryption service for Google Workspace (client-side encryption), refer to the section *Which services CSE supports* of Google documentation **About client-side encryption**.

Support for Google Meet on mobile devices

With the SDS encryption service for Google Workspace, users can now encrypt confidential video conferences and calls in Google Meet. In addition to the Google Workspace Web Client, this feature is now available on iOS and Android mobile devices.

SDS encryption service for Google Workspace 4.2.1 fixes

When performing a migration between two KACLSs or using a backup KACLS, a migration token is generated by the SDS encryption service for Google Workspace. It was generated with the wrong time unit for the iat (issued at) and exp (expiration date) fields, which could make it impossible to migrate.

The SDS encryption service for Google Workspace no longer stops unexpectedly if a request parameter has the wrong type when calling the REST API. This error could have been exploited to execute a Denial of Service (DDOS) attack.

SDS encryption service for Google Workspace 4.2 new features and enhancements

For information about the Google services supported by the SDS encryption service for Google Workspace (client-side encryption), refer to the section *Which services CSE supports* of Google documentation About client-side encryption.

Google Meet in-meeting chat

The content of Google Meet chat messages can now be secured with the SDS encryption service for Google Workspace.

Periodic refresh of KEKs

If you are using a Key Management System (KMS), you can now set the refresh frequency for KEKs.

One-off refresh of KEKs

KEK retrieval has been optimized. A one-off KEK refresh is now performed if the KEK ID cannot be found in the host local cache. This may occur if you have several instances of the SDS encryption service for Google Workspace.

Thales Ciphertrust Manager Key management system

It is now possible to use the private keys for Gmail S/MIME in the Thales Ciphertrust Manager via REST API. The list of algorithms supported in this mode is limited. For more information, refer to the *Administration guide* of the SDS encryption service for Google Workspace.

Customized access rules (OPA)

Custom claims provided by the identity provider can now be used to create OPA rules.

HTTPS proxy

You can now exclude certain endpoints from the HTTPS proxy.

SDS encryption service for Google Workspace 4.1.1 new features and enhancements

For information about the Google services supported by the SDS encryption service for Google Workspace (client-side encryption), refer to the section *Which services CSE supports* of Google documentation **About client-side encryption**.

Compatibility with RedHat 9.0.

Support for chat messages in Google Meet

The content of Google Meet chat messages can now be secured with the SDS encryption service for Google Workspace.

SDS encryption service for Google Workspace 4.1 new features and enhancements

For information about the Google services supported by the SDS encryption service for Google Workspace (client-side encryption), refer to the section *Supported services and data types* of Google documentation About client-side encryption.

Support for Google Drive

With the SDS encryption service for Google Workspace, users can now encrypt confidential files in Google Drive and read them. This feature is available on Windows and macOS workstations, and on mobile iOS and Android devices.

Support for Gmail

Gmail messages and attachments can now be secured with the SDS encryption service for Google Workspace.

Support for Google Calendar

Google Calendar data can now be secured with the SDS encryption service for Google Workspace.

Support of customized access rules

The SDS encryption service for Google Workspace now supports the Open Policy Agent (OPA) technology, allowing administrators to create their own customized access rules to the SDS encryption service for Google Workspace.

Migration of the KACLS

The SDS encryption service for Google Workspace is compatible with Google's new specifications regarding the migration of an encryption service (KACLS) to another, allowing in particular a massive migration in a single operation.

Identity provider

The local *config.json* configuration file now makes it possible to add several clientIDs for the user connection. Google applications configured locally will therefore be supported.

It is now possible to use OpenID JWKS (JSON Webkey Set) configurations to configure user identity providers.

Remote configuration file

Access to the remote configuration file *.well-known/cse-configuration* can now be disabled so that the local file can be used to validate user authentication.

Mass extraction and decryption of encrypted data

To ensure that data can be reversed, you can now extract all encrypted data and decrypt all of it in a single action using the Google tool (currently in beta version) and the SDS encryption service for Google Workspace. Stormshield must first provide you with a specific configuration. Please note that in the Beta version of the Google tool, only Gmail and Drive files can be used after decryption. Files from other Google Workspace applications are decrypted but not usable.

Compliance with RFC 7519

The SDS encryption service for Google Workspace is now compliant with RFC 7519 and supports multiple values for the "aud" field of the authentication token.

HTTPS proxy

If there is an HTTPS proxy in your network environment, it can now be used to manage the external requests of the SDS encryption service for Google Workspace.

Cache

The SDS encryption service for Google Workspace now includes a cache for external requests (e.g., openid connect, jwks), which optimizes response time.

Logs

Some logs are now issued for the */health* API route.

SDS encryption service for Google Workspace 4.1 fixes

The SDS encryption service for Google Workspace now lists the right options for the */status* API route.

The SDS encryption service for Google Workspace now checks the UUID-V4 format for the *tenant_id* provided by the Key management system (KMS).

Requests no longer fail if the value of the *kacls_url* parameter in the *config.json* file ends with the / character. Both URL formats - with or without / - are supported.

The configuration file cleanup and validation processes have been improved. These operations are no longer simultaneous, but executed consecutively.

Access privileges to configuration files have been restricted. The SDS encryption service for Google Workspace now requires configuration files to hold read and write access privileges for the current user and read-only privileges for the current group. Otherwise a warning will be raised.

SDS encryption service for Google Workspace 4.0 new features and enhancements

Support for Google Meet

Google Meet data can now be secured with the SDS encryption service for Google Workspace.

Using two KACLS

The SDS encryption service for Google Workspace is compatible with the new Google feature that allows two KACLS to coexist for the purpose of migrating from one service provider to another. For example, new files can be encrypted with the SDS encryption service for Google Workspace, while older files protected by another KACLS provider can be decrypted.

Operating system

The SDS encryption service for Google Workspace can now be installed on a server hardened with Security-Enhanced Linux (SElinux).

The SDS encryption service for Google Workspace is now compatible with RedHat Enterprise Linux 8.6 and only this version.

User authentication

User authentication can now be strengthened on privileged API routes by using a configured IdP.

Key management system (KMS)

In KMS mode, KEKs are no longer stored in the configuration file but in the KMS from now on.

KEKs are now automatically and transparently refreshed in KMS mode.

SDS encryption service for Google Workspace 3.0 new features and enhancements

Collaboration with external users

The users are now able to securely share Google Drive files (Docs, Sheets and Slides) with other users who work in different companies equipped with Google Client-Side Encryption.

There are two ways to configure this feature:

- Through the local configuration file, *config.json*, by specifying several identity providers in the *local_cse_configurations* section,
- Through a remote configuration file, */.well-known/cse-configuration*, located at the root of your domain.

Key management system (KMS)

It is now possible to add a key management system (KMS) to your SDS encryption service for Google Workspace infrastructure to secure key storage. In such a configuration, the key encryption keys (KEKs) are protected with a master key managed by the KMS. The KEKs in the keks.json file are thus encrypted.

New NodeJS 16 requirement

SDS encryption service for Google Workspace now requires NodeJS 16 to benefit from the latest security updates. It is available with RedHat Enterprise 8.

Summary of features in SDS encryption service for Google Workspace 1.2.1

With SDS encryption service for Google Workspace, you can guarantee the absolute confidentiality of your corporate data and benefit from Google Workspace collaboration tools at the same time, while complying with the regulatory restrictions of your sector.

Users can therefore protect their data before sending it to Google Workspace applications. Uncrypted data and encryption keys are never sent to Google.

The following are the features in SDS encryption service for Google Workspace 1.2.1:

Protection of files before sharing them	Users protect their files on their workstations via their browsers.
Sharing of files in shared spaces	Users share their protected files on Google Workspace.
Management of privileges on files	The operations that each user can perform depend on the privileges that the Google Workspace administrator has granted in the configuration. For example, the privilege of sharing files with external users who belong to specific domains.
Verification of authorized persons	During each operation in which a file is protected or modified, the solution will ensure that persons allowed to look up the file are trustworthy.

Contact

To contact our Stormshield Technical Assistance Center (TAC):

- https://mystormshield.eu/
All requests to technical support must be submitted through the incident manager in the private-access area https://mystormshield.eu, under Technical support > Manage cases.
- +33 (0) 9 69 329 129
In order for us to provide high-quality service, you are advised to use this communication method only to follow up on incidents that have been created earlier on https://mystormshield.eu.

All images in this document are for representational purposes only, actual products may differ.