GUIDE

SDS ENCRYPTION SERVICE FOR GOOGLE WORKSPACE

LOG GUIDE

Document last updated: September 4, 2024

Reference: sds-en-sds_for_gw-log_guide

Table of contents

1. Getting started

The SDS encryption service for Google Workspace generates logs for every operation, making it possible to trace all operations performed and potential issues. The logs are in JSON format and are hosted by Stormshield.

A unique identifier in UUIDV4 format is automatically generated for each request. This is the correlation ID linking all logs related to the same request or event.

To view your logs, send an export request to Stormshield at *data-security-business-unit@stormshield.eu*.

This document describes all the logs likely to be generated by the SDS encryption service for Google Workspace in a Saas environment.

2. Generic log fields

The following fields are displayed for all logs generated by SDS encryption service for Google Workspace in SaaS mode, in the order shown in the table.

- **Mandatory** fields are systematically present in logs for successful requests, but may be absent for unsuccessful requests.
- **Optional** fields can be present or absent in both cases.

Field	Description	Type	Mandatory/Optional
timestamp	Date and time at which the log was created. In UTC format. Example: "2023-12-05T09:27:58.936Z"	String in ISO 8601 format	Mandatory
severity	Level of severity of the log. Prescribed values: • *emerg*: The system is unusable, • *alert*: The problem must be fixed immediately, • *crit*: Critical error, • *err*: Non-critical error, • *warning*: The operation was successful but generated a warning, • *notice*: Unusual event not requiring corrective action, • *info*: Normal operation information message, • *debug*: Information useful to developers for troubleshooting the application.	String	Mandatory
application_version	Application version. Example: "4.3.0.2354"		Mandatory
kind	Log family to which the log belongs. Prescribed value: • *domain*: SDS encryption service for Google Workspace business operation logs.	String	Mandatory
category	Log category. Prescribed values: • *cse*: Logs of business requests issued by the SDS encryption service for Google Workspace. • *authentication*: Logs of authentication token verification actions.	String	Mandatory

Field	Description	Type	Mandatory/Optional
action	Event that occurred. Prescribed values: • unwrap, • privilegedwrap, • takeout, • privilegedunwrap, • rewrap, • digest, • certs, • wrapprivatekey, • privatekeysign, • privatekeydecrypt, • privilegedprivatekeydecrypt	String	Mandatory
log_version	Current version of log format. Prescribed value: *2*	Integer	Mandatory
process_id	Process ID. Example: *4031*	Integer	Mandatory
correlation_id	Unique identifier linking all logs relating to the same request or event. Example: "*146f73b6-c15d-4488-984c-97726cf86587*"	String	Mandatory

The fields in the *error* block described below are displayed for all logs generated by the SDS encryption service for Google Workspace in the event of an error when executing the action:

Field	Description	Type	Mandatory/Optional
code	Error number. Example: *2006003*	Integer	Mandatory
message	Error message. Example: *Unauthorized request*	String	Mandatory

3. Domain- Business operation logs

The log fields described below relate to business operations performed by the SDS encryption service for Google Workspace. They belong to the *Domain* log family (Kind:domain).

3.1 *cse* category

This category of logs contains all the business requests made by the SDS encryption service for Google Workspace.

3.1.1 wrap, unwrap, privilegedwrap and digest actions

- *wrap*: a *wrap* request has been made. This is the case whenever a key is encrypted.
- *unwrap*: an *unwrap* request has been made. This is the case whenever a key is decrypted.
- *privilegedwrap*: a *privilegedwrap* request has been made. This is the case whenever a bulk file import is in progress.
- *digest*: a *digest* request has been made. This is the case whenever a migration or encryption operation to a backup KACLS is in progress.

All these actions generate an "info" severity log in the event of success, or a "crit" severity log in the event of an error.

The log fields for these actions are as follows:

Field	Description	Type	Required/Optional
tenant_id	Tenant identifier. Example: *025f02fe-bee2-444b-bf76-b5ead30327c0*	String in uuid v4 format	Mandatory
reason	Additional context about the operation. Example: *Reason of the request*	String	Mandatory
email	User's email address. Example: *alice.dupont@gmail.com*	String	Mandatory
google_email	User's Google account email address. This field is always absent in the case of a *digest* action. Example: *alice.google@gmail.com*	String	Optional
google_application	Google Workspace application concerned by the operation. Prescribed values: • *meet*, • *drive*, • *calendar*	String	Mandatory
resource_name	Resource identifier. Example: *//googleapis.com/drive/files/10JsaKJM5JES1yi79QCKx-13w0R1i8JPU"*	String	Mandatory

Field	Description	Type	Required/Optional
perimeter_id	Identifier for additional verification of authentication and authorization requests. Example: *Perimeter_id of the request*	String	Mandatory
kek_id	Identifier of the KEK used. Example: *ed7e4c13-6199-30a3-7bce-1c82a9e31e21*	String	Mandatory

3.1.2 rewrap action

The *rewrap* action means that a *rewrap* request has been made. This is the case whenever a migration or encryption operation to a backup KACLS is in progress.

This action generates an "info" severity log in the event of success, or a "crit" severity log in the event of an error.

The log fields for this action are as follows:

Field	Description	Type	Required/Optional
tenant_id	Tenant identifier. Example: *025f02fe-bee2-444b-bf76-b5ead30327c0*	String in uuid v4 format	Mandatory
reason	Additional context about the operation. Example: *Reason of the request*	String	Mandatory
email	User's email address. Example: *alice.dupont@gmail.com*	String	Mandatory
google_application	Google Workspace application concerned by the operation. Prescribed values: • *meet*, • *drive*, • *calendar*	String	Mandatory
resource_name	Resource identifier. Example: *//googleapis.com/drive/files/10JsaKJM5JES1yi79QCKx-13w0R1i8JPU"*	String	Mandatory
perimeter_id	Identifier for additional verification of authentication and authorization requests. Example: *Perimeter_id of the request*	String	Mandatory
kek_id	Identifier of the KEK used. Example: *ed7e4c13-6199-30a3-7bce-1c82a9e31e21*	String	Mandatory
original_kacls_url	URL of the KACLS to be migrated. Example: *https://cse.mysds.io/api/v1/f438ae27-f33d-1fa3-b1e2-efc4d7635684*	String (URL)	Mandatory

3.1.3 certs action

The *certs* action means that a *certs* request has been made. This is the case whenever a migration or encryption operation to a backup KACLS is in progress and a certificate request is issued by another KACLS.

This action generates an "info" severity log in the event of success, or a "crit" severity log in the event of an error.

The log fields for this action are as follows:

Field	Description	Type	Required/Optional
tenant_id	Tenant identifier. Example: *025f02fe-bee2-444b-bf76-b5ead30327c0*	String in uuid v4 format	Mandatory
keys	KACLS public certificate in JSON Web Key Set format as defined in RFC 7517. Example provided by Google.	JSON Web Key Set object	Mandatory

Other public certificate example:

```
"keys":   [
          {
                "kty": "RSA",
                "n": "o_mYVlR9dFTVilwx-aFhLNX-kdO-ClsYf8qP5fMVG-9-
wycen6oBmAmoQOumZP8zS3Sj6fxIC3PYB9wwW-2qAQuB7kEDT6V03-
8SIUz9S1lw",
                "e": "AQAB",
                "kid": "kacls-to-kacls-migration-key",
                "use": "sig",
                "alg": "RS256"
          }
    ]
```

3.1.4 Privilegedunwrap action

The *privilegedunwrap* action means that a *privilegedunwrap* request has been made. This is the case whenever a migration or encryption operation to a backup KACLS is in progress.

This action generates an "info" severity log in the event of success, or a "crit" severity log in the event of an error.

The log fields for this action are as follows:

Field	Description	Type	Required/Optional
tenant_id	Tenant identifier. Example: *025f02fe-bee2-444b-bf76-b5ead30327c0*	String in uuid v4 format	Mandatory
reason	Additional context about the operation. Example: *Reason of the request*	String	Mandatory
resource_name	Resource identifier. Example: *//googleapis.com/drive/files/10JsaKJM5JES1yi79QCKx-13w0R1i8JPU"*	String	Mandatory

Field	Description	Type	Required/Optional
perimeter_id	Identifier for additional verification of authentication and authorization requests. Example: *Perimeter_id of the request*	String	Mandatory
kek_id	Identifier of the KEK used. Example: *ed7e4c13-6199-30a3-7bce-1c82a9e31e21*	String	Mandatory

3.1.5 takeout action

The *takeout* action means that an encrypted document is exported from Google.

This action generates an "info" severity log in the event of success, or a "crit" severity log in the event of an error.

Drive application

The *takeout* action linked to the Google Drive application means that a *privilegedunwrap* request has been made. This is the case each time an encrypted document is exported from Google.

The log fields for this action are as follows:

Field	Description	Type	Mandatory/ Optional
tenant_id	Tenant identifier. Example: *025f02fe-bee2-444b-bf76-b5ead30327c0*	String in uuid v4 format	Mandatory
reason	Additional context about the operation. Example: *Reason of the request*	String	Mandatory
email	User's email address. Example: *alice.dupont@gmail.com*	String	Mandatory
google_email	User's Google account email address. This field is always absent in the case of a *digest* action. Example: *alice.google@gmail.com*	String	Optional
google_ application	Google Workspace application concerned by the operation. Prescribed values: • *meet* • *drive* • *calendar*	String	Mandatory
resource_name	Resource identifier. Example: *//googleapis.com/drive/files/10JsaKJM5JES1yi790CKx-13w0R1i8JPU"*	String	Mandatory
perimeter_id	Identifier for additional verification of authentication and authorization requests. Example: *Perimeter_id of the request*	String	Mandatory
kek_id	Identifier of the KEK used. Example: *ed7e4c13-6199-30a3-7bce-1c82a9e31e21*	String	Mandatory

Gmail application

The *takeout* action linked to the Gmail application means that a *privilegedprivatekydecrypt* request has been made. This is the case each time an encrypted email is exported from Google.

The log fields for this action are as follows:

Field	Description	Type	Required/ Optional
tenant_id	Tenant identifier. Example: *025f02fe-bee2-444b-bf76-b5ead30327c0*	String in uuid v4 format	Mandatory
reason	Additional context about the operation. Example: *Reason of the request*	String	Mandatory
email	User's email address. Example: *alice.dupont@gmail.com*	String	Mandatory
google_email	User's Google account email address. This field is always absent in the case of a *digest* action. Example: *alice.google@gmail.com*	String	Optional
google_application	Google Workspace application concerned by the operation. Prescribed values: • *gmail*	String	Mandatory
kek_id	Identifier of the KEK used. Example: *ed7e4c13-6199-30a3-7bce-1c82a9e31e21*	String	Mandatory
spki_hash_base64	Base64 digest of the private key. Example: *EUV0iaJF1j3cfQnp6laGjmFr5bSdarcic0AoSG9RJWI=*	String	Mandatory
spki_hash_algorithm	Encryption algorithm used. Prescribed value: • *SHA-256*	String	Mandatory
private_key_used_algorithm	Encryption algorithms used in this operation. Example: *RSA/ECB/PKCS1Padding*	String	Mandatory
private_key_supported_algorithms	Encryption and signature algorithms supported by this key. Example: *"["RSA/ECB/PKCS1Padding","SHA1withRSA", "SHA256withRSA"]*	String	Mandatory
private_key_mode	Type of private key used during the operation. Prescribed values: • *private-key-pem*: Users' private keys are stored encrypted at Google, • *private-key-name*: Users' private keys are stored in a KMS and never removed. Only the names of the private keys are stored at Google.	String	Mandatory

3.1.6 privatekeysign and privatekeydecrypt actions

- *privatekeysign*: a privatekeysign request has been made. This is the case each time an email is signed for encryption.
- *privatekeydecrypt*: a *privatekydecrypt* request has been made. This is the case every time an encrypted email is decrypted.

These actions generate an "info" severity log in the event of success, or a "crit" severity log in the event of an error.

The log fields for these actions are as follows:

Field	Description	Type	Required/ Optional
tenant_id	Tenant identifier. Example: *025f02fe-bee2-444b-bf76-b5ead30327c0*	String in uuid v4 format	Mandatory
reason	Additional context about the operation. Example: *Reason of the request*	String	Mandatory
email	User's email address. Example: *alice.dupont@gmail.com*	String	Mandatory
google_email	User's Google account email address. This field is always absent in the case of a *digest* action. Example: *alice.google@gmail.com*	String	Optional
google_application	Google Workspace application concerned by the operation. Prescribed values: • *gmail*	String	Mandatory
kek_id	Identifier of the KEK used. Example: *ed7e4c13-6199-30a3-7bce-1c82a9e31e21*	String	Mandatory
perimeter_id	Identifier for additional verification of authentication and authorization requests. Example: *Perimeter_id of the request*	String	Mandatory
message_id	Identifier of the message on which the signature or decryption operation has been performed. Example: *<CADBpGcUzg2iGuYyRoGkQg4F8sHXNoQtxbSxS70iyJgvpDb0g @mail.gmail.com>*	String	Mandatory
spki_hash_base64	Base64 digest of the private key. Example: *EUV0iaJF1j3cfQnp6laGjmFr5bSdarcic0AoSG9RJWI=*	String	Mandatory
spki_hash_algorithm	Encryption algorithm used. Prescribed value: • *SHA-256*	String	Mandatory
private_key_used_algorithm	Encryption algorithms used in this operation. Example: *RSA/ECB/PKCS1Padding*	String	Mandatory
private_key_supported_algorithms	Encryption and signature algorithms supported by this key. Example: *"["RSA/ECB/PKCS1Padding","SHA1withRSA", "SHA256withRSA"]*	String	Mandatory

Field	Description	Type	Required/ Optional
private_key_mode	Type of private key used during the operation. Prescribed values: • *private-key-pem*: Users' private keys are stored encrypted at Google, • *private-key-name*: Users' private keys are stored in a KMS and never removed. Only the names of the private keys are stored at Google.	String	Mandatory

3.1.7 wrapprivatekey action

The *wrapprivatekey* action means that a *wrapprivatekey* request has been made. This is the case whenever a user's private key is encrypted for Gmail.

This action generates an "info" severity log in the event of success, or a "crit" severity log in the event of an error.

The log fields for these actions are as follows:

Field	Description	Type	Required/ Optional
tenant_id	Tenant identifier. Example: *025f02fe-bee2-444b-bf76-b5ead30327c0*	String in uuid v4 format	Mandatory
kek_id	Identifier of the KEK used. Example: *ed7e4c13-6199-30a3-7bce-1c82a9e31e21*	String	Mandatory
perimeter_id	Identifier for additional verification of authentication and authorization requests. Example: *Perimeter_id of the request*	String	Mandatory
private_key_supported_algorithms	Encryption and signature algorithms supported by this key. Example: "*["RSA/ECB/PKCS1Padding","SHA1withRSA", "SHA256withRSA"]*	String	Mandatory
private_key_mode	Type of private key used during the operation. Prescribed values: • *private-key-pem*: Users' private keys are stored encrypted at Google, • *private-key-name*: Users' private keys are stored in a KMS and never removed. Only the names of the private keys are stored at Google.	String	Mandatory

STORMSHIELD