



**STORMSHIELD**



GUIDE

# SDS ENCRYPTION SERVICE FOR GOOGLE WORKSPACE

## LOG GUIDE

Document last updated: December 30, 2024

Reference: `sds-en-sds_for_gw-log_guide`



# Table of contents

1. Getting started .....	3
2. Generic log fields .....	4
3. Domain- Business operation logs .....	6
3.1 cse category .....	6
3.1.1 wrap, unwrap, privilegedwrap and digest actions .....	6
3.1.2 rewrap action .....	7
3.1.3 certs action .....	8
3.1.4 privilegedunwrap action .....	9
3.1.5 takeout action .....	10
3.1.6 privatekeysign and privatekeydecrypt actions .....	14
3.1.7 wrapprivatekey action .....	16
3.1.8 delegate action .....	16
3.2 kmaas category .....	17
3.2.1 Encrypt and decrypt actions .....	17
3.3 kek category .....	18
3.3.1 Load action .....	18
3.4 authentication category .....	18
3.4.1 Verify action .....	18
3.5 authorization category .....	20
3.5.1 Verify action .....	20
4. System - Environment logs .....	23
4.1 server category .....	23
4.1.1 Starting action .....	23
4.1.2 Started action .....	23
4.2 kms category .....	23
4.2.1 connect action .....	24
4.2.2 Disconnect action .....	24
4.2.3 Operation action .....	24
4.3 resource category .....	25
4.3.1 get action .....	25
5. HTTP- HTTP request logs .....	26
5.1 request category .....	26
5.1.1 receive action .....	26



# 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.

If you are using SDS encryption service for Google Workspace in SaaS mode, to view your logs, submit an export request to Stormshield at [data-security-business-unit@stormshield.eu](mailto:data-security-business-unit@stormshield.eu).

In On Premise mode, refer to the SDS encryption service for Google Workspace Administration Guide for more information on log locations.

This document describes all the logs likely to be generated by the SDS encryption service for Google Workspace. The vast majority of logs are common to both SaaS and On Premises modes of SDS encryption service for Google Workspace. Some logs are generated only in On Premises mode. These are accompanied by the **On Prem Only** label.



## 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: <ul style="list-style-type: none"><li>• <i>emerg</i>: The system is unusable,</li><li>• <i>alert</i>: The problem must be fixed immediately,</li><li>• <i>crit</i>: Critical error,</li><li>• <i>err</i>: Non-critical error,</li><li>• <i>warning</i>: The operation was successful but generated a warning,</li><li>• <i>notice</i>: Unusual event not requiring corrective action,</li><li>• <i>info</i>: Normal operation information message,</li><li>• <i>debug</i>: Information useful to developers for troubleshooting the application.</li></ul>	String	Mandatory
application_version	Application version. Example: "4.3.0.2354"		Mandatory
kind	Log family to which the log belongs. Prescribed values: <ul style="list-style-type: none"><li>• <i>domain</i>: SDS encryption service for Google Workspace business operation logs.</li><li>• <i>system</i>: Logs relating to the operations concerning the environment.</li><li>• <i>http</i>: Logs relating to the HTTP operations of the SDS encryption service for Google Workspace.</li></ul>	String	Mandatory
category	Log category. Examples of possible values: <ul style="list-style-type: none"><li>• <i>cse</i>: Logs of business requests issued by the SDS encryption service for Google Workspace.</li><li>• <i>authentication</i>: Logs of authentication token verification actions.</li></ul>	String	Mandatory



Field	Description	Type	Mandatory/Optional
action	Event that occurred. Examples of possible values: <ul style="list-style-type: none"><li>• unwrap,</li><li>• privilegedwrap,</li><li>• takeout,</li><li>• privilegedunwrap,</li><li>• rewrap,</li><li>• digest,</li><li>• certs,</li><li>• wrapprivatekey,</li><li>• privatekeysign,</li><li>• privatekeydecrypt,</li><li>• privilegedprivatekeydecrypt</li></ul>	String	Mandatory
log_version	Current version of log format. Prescribed value: 2	Integer	Mandatory
hostname <small>On Prem Only</small>	Host name. Example: <i>MyCSEServer</i>	String	Mandatory
process_id	Process ID. Example: <i>4031</i>	Integer	Mandatory
correlation_id	Unique identifier linking all logs relating to the same request or event. Example: <i>"146f73b6-c15d-4488-984c-97726cf86587"</i>	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 <small>On Prem Only</small>	Error number. Example: <i>2006003</i>	Integer	Mandatory
message <small>On Prem Only</small>	Error message. Example: <i>Unauthorized request</i>	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	Mandatory/Optional
tenant_id	Tenant identifier. Example: <i>025f02fe-bee2-444b-bf76-b5ead30327c0</i>	String in uuid v4 format	Mandatory
reason	Additional context about the operation. Example: <i>Reason of the request</i>	String	Mandatory
email	User's email address. Example: <i>alice.dupont@gmail.com</i>	String	Mandatory
google_email	User's Google account email address. This field is always absent in the case of a <i>digest</i> action. Example: <i>alice.google@gmail.com</i>	String	Optional
google_application	Google Workspace application concerned by the operation. Prescribed values: <ul style="list-style-type: none"><li>• <i>meet</i>,</li><li>• <i>drive</i>,</li><li>• <i>calendar</i></li></ul>	String	Mandatory
resource_name	Resource identifier. Example: <i>//googleapis.com/drive/files/10JsaKJM5JES1yi79QCKx-13wOR1i8JPU"</i>	String	Mandatory



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

Example of logs for the successful *wrap* action:

```
{
  "tenant_id": "025f02fe-bee2-444b-bf76-b5ead30327c0",
  "reason": "reason of the request",
  "email": "alice@gmail.com",
  "google_email": "alice.google@gmail.com",
  "application": "meet",
  "resource_name": "resource name for this request",
  "perimeter_id": "perimeter id for the request",
  "kek_id": "ed7e4c13-6199-30a3-7bce-encrypted_kek_b64"
}
```

Example of logs for the successful *privilegedwrap* action:

```
{
  "tenant_id": "025f02fe-bee2-444b-bf76-b5ead30327c0",
  "reason": "reason of the request",
  "email": "alice@gmail.com",
  "google_email": "alice.google@gmail.com",
  "google_application": "meet|drive...",
  "resource_name": "resource name for this request",
  "perimeter_id": "perimeter id for the request",
  "kek_id": "ed7e4c13-6199-30a3-7bce-1c82a9e31e21"
}
```

Example of logs for the successful *digest* action:

```
{
  "tenant_id": "025f02fe-bee2-444b-bf76-b5ead30327c0",
  "reason": "reason of the request",
  "email": "alice@gmail.com",
  "google_application": "meet|drive...",
  "resource_name": "resource name for this request",
  "perimeter_id": "perimeter id for the request",
  "kek_id": "ed7e4c13-6199-30a3-7bce-1c82a9e31e21"
}
```

### 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	Mandatory/Optional
tenant_id	Tenant identifier. Example: <i>025f02fe-bee2-444b-bf76-b5ead30327c0</i>	String in uuid v4 format	Mandatory



Field	Description	Type	Mandatory/Optional
reason	Additional context about the operation. Example: <i>Reason of the request</i>	String	Mandatory
email	User's email address. Example: <i>alice.dupont@gmail.com</i>	String	Mandatory
google_application	Google Workspace application concerned by the operation. Prescribed values: <ul style="list-style-type: none"><li>• <i>meet</i>,</li><li>• <i>drive</i>,</li><li>• <i>calendar</i></li></ul>	String	Mandatory
resource_name	Resource identifier. Example: <i>//googleapis.com/drive/files/10JsaKJM5JES1yi79QCKx-13wOR1i8JPU"</i>	String	Mandatory
perimeter_id	Identifier for additional verification of authentication and authorization requests. Example: <i>Perimeter_id of the request</i>	String	Mandatory
kek_id	Identifier of the KEK used. Example: <i>ed7e4c13-6199-30a3-7bce-1c82a9e31e21</i>	String	Mandatory
original_kacls_url	URL of the KACLS to be migrated. Example: <i>https://cse.mysds.io/api/v1/f438ae27-f33d-1fa3-b1e2-efc4d7635684</i>	String (URL)	Mandatory

Example of logs for the successful *rewrap* action:

```
{
  "tenant_id": "025f02fe-bee2-444b-bf76-b5ead30327c0",
  "reason": "reason of the request",
  "email": "alice@gmail.com",
  "google_application": "meet|drive...",
  "resource_name": "resource name for this request",
  "perimeter_id": "perimeter id for the request",
  "kek_id": "ed7e4c13-6199-30a3-7bce-1c82a9e31e21",
  "original_kacls_url": "https://cse.mysds.io/api/v1/f468ae37-f33d-4fb3-b3e2-fec2d7635684"
}
```

### 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. It returns the KACLS public certificate.

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	Mandatory/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 <a href="#">RFC 7517</a> . <a href="#">Example provided by Google</a> .	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"
  }
]
```

Example of logs for the successful *certs* action:

```
{
  "tenant_id": "025f02fe-bee2-444b-bf76-b5ead30327c0",
  "keys": [
    {
      "kty": "RSA",
      "n": "o_mYVlR9dFTVilwx-aFhLNx-kdO-ClSYf8qP5fMVG-9-
zAx0oYMSCjZuvE78ZF_
FwSmxu2AeDkCVXpLwbRXkbOKc83MHC8czp80RuGjy3I6vhNocdZBhnJ5H7fAFN
OmtD_C3xVFtd006H7sd2AQQ_zoEwV0qISSLS_
uZbr6gwsixRUUARSvEmGUUqt0lOnXnie1cKMu1mdbcCmhfZH3g5n2Z1bcq8u8
6KlIcZ8T0Wnu1PGMhXML4mhe6z3KH3PWqvoeYj4ILzz5KEI6zrMun-
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	Mandatory/Optional
tenant_id	Tenant identifier. Example: <i>025f02fe-bee2-444b-bf76-b5ead30327c0</i>	String in uuid v4 format	Mandatory
reason	Additional context about the operation. Example: <i>Reason of the request</i>	String	Mandatory
resource_name	Resource identifier. Example: <i>//googleapis.com/drive/files/10JsaKJM5JES1yi79QCKx-13w0R1i8JPU"</i>	String	Mandatory
perimeter_id	Identifier for additional verification of authentication and authorization requests. Example: <i>Perimeter_id of the request</i>	String	Mandatory
kek_id	Identifier of the KEK used. Example: <i>ed7e4c13-6199-30a3-7bce-1c82a9e31e21</i>	String	Mandatory

Example of logs for the successful *privilegedunwrap* action:

```
{
  "tenant_id": "025f02fe-bee2-444b-bf76-b5ead30327c0",
  "reason": "reason of the request",
  "resource_name": "resource name for this request",
  "perimeter_id": "perimeter id for the request",
  "kek_id": "ed7e4c13-6199-30a3-7bce-1c82a9e31e21"
}
```

### 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: <i>025f02fe-bee2-444b-bf76-b5ead30327c0</i>	String in uuid v4 format	Mandatory
reason	Additional context about the operation. Example: <i>Reason of the request</i>	String	Mandatory
email	User's email address. Example: <i>alice.dupont@gmail.com</i>	String	Mandatory



Field	Description	Type	Mandatory/ Optional
google_email	User's Google account email address. This field is always absent in the case of a <i>digest</i> action. Example: <i>alice.google@gmail.com</i>	String	Optional
google_application	Google Workspace application concerned by the operation. Prescribed values: <ul style="list-style-type: none"><li>• <i>meet</i></li><li>• <i>drive</i></li><li>• <i>calendar</i></li></ul>	String	Mandatory
resource_name	Resource identifier. Example: <i>//googleapis.com/drive/files/10JsaKJM5JES1yi79QCKx-13w0R1i8JPU"</i>	String	Mandatory
perimeter_id	Identifier for additional verification of authentication and authorization requests. Example: <i>Perimeter_id of the request</i>	String	Mandatory
kek_id	Identifier of the KEK used. Example: <i>ed7e4c13-6199-30a3-7bce-1c82a9e31e21</i>	String	Mandatory

Example of logs for the successful *takeout* action:

```
{
  "tenant_id": "125f02fe-bee2-444b-bf76-b5ead30327d3",
  "reason": "reason of the request",
  "google_application": "drive|meet|calendar",
  "kek_id": "cd7e4c13-6299-30a3-2ace-1a82a9c31e65",
  "email": "xUV0gaJF1j6dfQnp6IaGmmFr5bSdarcicOAoSG9RkzI=",
  "google_email": "SHA-256",
  "resource_name": "RSA/ECB/PKCS1Padding",
  "perimeter_id": ["RSA/ECB/PKCS1Padding", "SHA1withRSA", "SHA256withRSA"]
}
```

```
{
  "tenant_id": "125f02fe-bee2-444b-bf76-b5ead30327d3",
  "reason": "reason of the request",
  "google_application": "drive|meet|calendar",
  "kek_id": "cd7e4c13-6299-30a3-2ace-1a82a9c31e65",
  "email": "xUV0gaJF1j6dfQnp6IaGmmFr5bSdarcicOAoSG9RkzI=",
  "google_email": "SHA-256",
  "resource_name": "RSA/ECB/PKCS1Padding",
  "perimeter_id": ["RSA/ECB/PKCS1Padding", "SHA1withRSA", "SHA256withRSA"]
}
```

### Gmail application

The *takeout* action linked to the Gmail application means that a *privilegedprivatekeydecrypt* 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	Mandatory/ Optional
tenant_id	Tenant identifier. Example: <i>025f02fe-bee2-444b-bf76-b5ead30327c0</i>	String in uuid v4 format	Mandatory
reason	Additional context about the operation. Example: <i>Reason of the request</i>	String	Mandatory
email	User's email address. Example: <i>alice.dupont@gmail.com</i>	String	Mandatory
google_email	User's Google account email address. This field is always absent in the case of a <i>digest</i> action. Example: <i>alice.google@gmail.com</i>	String	Optional
google_application	Google Workspace application concerned by the operation. Prescribed values: <ul style="list-style-type: none"><li>• <i>gmail</i></li></ul>	String	Mandatory
kek_id	Identifier of the KEK used. Example: <i>ed7e4c13-6199-30a3-7bce-1c82a9e31e21</i>	String	Mandatory
spki_hash_base64	Base64 digest of the private key. Example: <i>EUVDiaJF1j3cf0np6laGjmFr5bSdarcic0AoSG9RJWI=</i>	String	Mandatory
spki_hash_algorithm	Encryption algorithm used. Prescribed value: <ul style="list-style-type: none"><li>• <i>SHA-256</i></li></ul>	String	Mandatory
private_key_used_algorithm	Encryption algorithms used in this operation. Example: <i>RSA/ECB/PKCS1Padding</i>	String	Mandatory
private_key_supported_algorithms	Encryption and signature algorithms supported by this key. Example: <i>["RSA/ECB/PKCS1Padding", "SHA1withRSA", "SHA256withRSA"]</i>	String	Mandatory
private_key_mode	Type of private key used during the operation. Prescribed values: <ul style="list-style-type: none"><li>• <i>private-key-pem</i>: Users' private keys are stored encrypted at Google,</li><li>• <i>private-key-name</i>: Users' private keys are stored in a KMS and never removed. Only the names of the private keys are stored at Google.</li></ul>	String	Mandatory

Field	Description	Type	Mandatory/ Optional
tenant_id	Tenant identifier. Example: <i>025f02fe-bee2-444b-bf76-b5ead30327c0</i>	String in uuid v4 format	Mandatory



Field	Description	Type	Mandatory/ Optional
reason	Additional context about the operation. Example: <i>Reason of the request</i>	String	Mandatory
email	User's email address. Example: <i>alice.dupont@gmail.com</i>	String	Mandatory
google_email	User's Google account email address. This field is always absent in the case of a <i>digest</i> action. Example: <i>alice.google@gmail.com</i>	String	Optional
google_application	Google Workspace application concerned by the operation. Prescribed values: <ul style="list-style-type: none"> <li><i>gmail</i></li> </ul>	String	Mandatory
kek_id	Identifier of the KEK used. Example: <i>ed7e4c13-6199-30a3-7bce-1c82a9e31e21</i>	String	Mandatory
spki_hash_base64	Base64 digest of the private key. Example: <i>EUVOiaJF1j3cfQnp6IaGjmFr5bSdarcicOAoSG9RJWI=</i>	String	Mandatory
spki_hash_algorithm	Encryption algorithm used. Prescribed value: <ul style="list-style-type: none"> <li><i>SHA-256</i></li> </ul>	String	Mandatory
private_key_used_algorithm	Encryption algorithms used in this operation. Example: <i>RSA/ECB/PKCS1Padding</i>	String	Mandatory
private_key_supported_algorithms	Encryption and signature algorithms supported by this key. Example: <i>["RSA/ECB/PKCS1Padding", "SHA1withRSA", "SHA256withRSA"]</i>	String	Mandatory
private_key_mode	Type of private key used during the operation. Prescribed values: <ul style="list-style-type: none"> <li><i>private-key-pem</i>: Users' private keys are stored encrypted at Google,</li> <li><i>private-key-name</i>: Users' private keys are stored in a KMS and never removed. Only the names of the private keys are stored at Google.</li> </ul>	String	Mandatory

Example of logs for the successful *takeout* action:

```
{
  "tenant_id": "025f02fe-bee2-444b-bf76-b5ead30327c0",
  "reason": "reason of the request",
  "google_application": "gmail",
  "email": "alice@gmail.com",
  "google_email": "alice.google@gmail.com",
  "kek_id": "ed7e4c13-6199-30a3-7bce-1c82a9e31e21",
  "algorithm": "RSA/ECB/PKCS1Padding",
  "spki_hash_base64": "EUVOiaJF1j3cfQnp6IaGjmFr5bSdarcicOAoSG9RJWI=",
  "spki_hash_algorithm": "SHA-256",
  "private_key_used_algorithm": "RSA/ECB/PKCS1Padding",
  "private_key_supported_algorithms": "
```



```
[ "RSA/ECB/PKCS1Padding", "SHA1withRSA", "SHA256withRSA" ],  
"private_key_mode": "private-key-pem|private-key-name"  
}
```

### 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 *privatekeydecrypt* 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	Mandatory/ Optional
tenant_id	Tenant identifier. Example: <i>025f02fe-bee2-444b-bf76-b5ead30327c0</i>	String in uuid v4 format	Mandatory
reason	Additional context about the operation. Example: <i>Reason of the request</i>	String	Mandatory
email	User's email address. Example: <i>alice.dupont@gmail.com</i>	String	Mandatory
google_email	User's Google account email address. This field is always absent in the case of a <i>digest</i> action. Example: <i>alice.google@gmail.com</i>	String	Optional
google_application	Google Workspace application concerned by the operation. Prescribed values: <ul style="list-style-type: none"><li>• <i>gmail</i></li></ul>	String	Mandatory
resource_name	Resource identifier. Example: <i>//googleapis.com/drive/files/10JsaKJM5JES1yi79QCKx-13w0R1i8JPU"</i>	String	Mandatory
kek_id	Identifier of the KEK used. Example: <i>ed7e4c13-6199-30a3-7bce-1c82a9e31e21</i>	String	Mandatory
perimeter_id	Identifier for additional verification of authentication and authorization requests. Example: <i>Perimeter_id of the request</i>	String	Mandatory
message_id	Identifier of the message on which the signature or decryption operation has been performed. Example: <i>&lt;CADBpGcUzg2iGuYyRoGkQg4F8sHXNoQtxbSxS70iyJgvpDb0g@mail.gmail.com&gt;</i>	String	Mandatory
spki_hash_base64	Base64 digest of the private key. Example: <i>EUV0iaJF1j3cfQnp6laGjmFr5bSdarcic0AoSG9RJWI=</i>	String	Mandatory



Field	Description	Type	Mandatory/Optional
spki_hash_algorithm	Encryption algorithm used. Prescribed value: <ul style="list-style-type: none"> <li>SHA-256</li> </ul>	String	Mandatory
private_key_used_algorithm	Encryption algorithms used in this operation. Example: <i>RSA/ECB/PKCS1Padding</i>	String	Mandatory
private_key_supported_algorithms	Encryption and signature algorithms supported by this key. Example: <i>["RSA/ECB/PKCS1Padding", "SHA1withRSA", "SHA256withRSA"]</i>	String	Mandatory
private_key_mode	Type of private key used during the operation. Prescribed values: <ul style="list-style-type: none"> <li><i>private-key-pem</i>: Users' private keys are stored encrypted at Google,</li> <li><i>private-key-name</i>: Users' private keys are stored in a KMS and never removed. Only the names of the private keys are stored at Google.</li> </ul>	String	Mandatory

Example of logs for the successful *privatekeysign* action:

```
{
  "tenant_id": "025f02fe-bee2-444b-bf76-b5ead30327c0",
  "reason": "reason of the request",
  "google_application": "gmail",
  "email": "alice@gmail.com",
  "google_email": "alice.google@gmail.com",
  "resource_name": "resource name for this request",
  "perimeter_id": "perimeter id for the request",
  "kek_id": "ed7e4c13-6199-30a3-7bce-1c82a9e31e21",
  "spki_hash_base64": "EUVOiaJF1j3cfQnp6IaGjmFr5bSdarcicOAoSG9RJWI=",
  "spki_hash_algorithm": "SHA-256",
  "message_id": "Message id of the request",
  "private_key_used_algorithm": "SHA256withRSA",
  "private_key_supported_algorithms": [
    "RSA/ECB/PKCS1Padding", "SHA1withRSA", "SHA256withRSA"
  ],
  "private_key_mode": "private-key-pem|private-key-name"
}
```

Example of logs for the successful *privatekeydecrypt* action:

```
{
  "tenant_id": "025f02fe-bee2-444b-bf76-b5ead30327c0",
  "reason": "reason of the request",
  "google_application": "gmail",
  "email": "alice@gmail.com",
  "google_email": "alice.google@gmail.com",
  "resource_name": "resource name for this request",
  "perimeter_id": "perimeter id for the request",
  "kek_id": "ed7e4c13-6199-30a3-7bce-1c82a9e31e21",
  "spki_hash_base64": "EUVOiaJF1j3cfQnp6IaGjmFr5bSdarcicOAoSG9RJWI=",
  "spki_hash_algorithm": "SHA-256",
  "message_id": "Message id of the request",
  "private_key_used_algorithm": "RSA/ECB/PKCS1Padding",
  "private_key_supported_algorithms": [
    "RSA/ECB/PKCS1Padding", "SHA1withRSA", "SHA256withRSA"
  ],
  "private_key_mode": "private-key-pem|private-key-name"
}
```



### 3.1.7 wrapprivatkey action

The *wrapprivatkey* action means that a *wrapprivatkey* 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	Mandatory/Optional
tenant_id	Tenant identifier. Example: <i>025f02fe-bee2-444b-bf76-b5ead30327c0</i>	String in uuid v4 format	Mandatory
kek_id	Identifier of the KEK used. Example: <i>ed7e4c13-6199-30a3-7bce-1c82a9e31e21</i>	String	Mandatory
perimeter_id	Identifier for additional verification of authentication and authorization requests. Example: <i>Perimeter_id of the request</i>	String	Mandatory
private_key_supported_algorithms	Encryption and signature algorithms supported by this key. Example: " [ <i>"RSA/ECB/PKCS1Padding"</i> , <i>"SHA1withRSA"</i> , <i>"SHA256withRSA"</i> ]	String	Mandatory
private_key_mode	Type of private key used during the operation. Prescribed values: <ul style="list-style-type: none"><li><i>private-key-pem</i>: Users' private keys are stored encrypted at Google,</li><li><i>private-key-name</i>: Users' private keys are stored in a KMS and never removed. Only the names of the private keys are stored at Google.</li></ul>	String	Mandatory

Example of logs for the successful *wrapprivatkey* action:

```
{
  "tenant_id": "025f02fe-bee2-444b-bf76-b5ead30327c0",
  "perimeter_id": "perimeter id for the request",
  "kek_id": "ed7e4c13-6199-30a3-7bce-1c82a9e31e21",
  "private_key_supported_algorithms": "[\"RSA/ECB/PKCS1Padding\", \"SHA1withRSA\", \"SHA256withRSA\"]",
  "private_key_mode": "private-key-pem|private-key-name"
}
```

### 3.1.8 delegate action

The *delegate* action means that a *delegate* request has been made. This is the case every time an authentication token for delegation is generated.

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	Mandatory/Optional
tenant_id	Tenant identifier. Example: <i>025f02fe-bee2-444b-bf76-b5ead30327c0</i>	String in uuid v4 format	Mandatory
reason	Additional context about the operation. Example: <i>Reason of the request</i>	String	Mandatory
email	User's email address. Example: <i>alice.dupont@gmail.com</i>	String	Mandatory
google_email	User's Google account email address. Example: <i>alice.google@gmail.com</i>	String	Optional
google_application	Google Workspace application concerned by the operation. Prescribed values: <ul style="list-style-type: none"><li>• <i>meet</i></li></ul>	String	Mandatory
resource_name	Resource identifier. Example: <i>//googleapis.com/drive/files/10JsaKJM5JES1yi79QCKx-13w0R1i8JPU"</i>	String	Mandatory
perimeter_id	Identifier for additional verification of authentication and authorization requests. Example: <i>Perimeter_id of the request</i>	String	Mandatory
delegated_to	Identifier of the entity to which authentication is delegated. Example: "Authentication delegated to Alice Dupont"	String	Mandatory

## 3.2 kmaas category

This category of logs contains all the business requests concerning key management as a service [KMaaS].

### 3.2.1 Encrypt and decrypt actions On Prem Only

- The *encrypt* action means that an encrypt request has been made. This is the case whenever data is encrypted using the KMaaS service.
- The *decrypt* action means that a decrypt request has been made. This is the case every time data is decrypted using the KMaaS service.

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	Mandatory/Optional
tenant_id	Tenant identifier. Example: <i>025f02fe-bee2-444b-bf76-b5ead30327c0</i>	String in uuid v4 format	Mandatory



Field	Description	Type	Mandatory/Optional
kek_id	Identifier of the KEK used. Example: <i>ed7e4c13-6199-30a3-7bce-1c82a9e31e21</i>	String	Mandatory

### 3.3 kek category

This category of logs contains all the business requests concerning KEK keys.

#### 3.3.1 Load action

The *load* action means that a KEK key has just been loaded into the memory for use by the SDS encryption service for Google Workspace. It 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	Mandatory/Optional
tenant_id	Tenant identifier. Example: <i>025f02fe-bee2-444b-bf76-b5ead30327c0</i>	String in uuid v4 format	Mandatory
kek_id	Identifier of the KEK used. Example: <i>ed7e4c13-6199-30a3-7bce-1c82a9e31e21</i>	String	Mandatory
is_active_kek	Indicates whether the KEK key loaded is the one used for encryption. Prescribed values: <ul style="list-style-type: none"><li>• true</li><li>• false</li></ul>	Boolean	Mandatory
is_encrypted_kek	Indicates whether the KEK key loaded is encrypted by an MKEK. Prescribed values: <ul style="list-style-type: none"><li>• true</li><li>• false</li></ul>	Boolean	Mandatory

### 3.4 authentication category

This category of logs contains all the business requests concerning JWT authentication tokens. These are generated by a third-party tool and guarantee the user's identity.

#### 3.4.1 Verify action On Prem Only

The *verify* action means that a JWT authentication token has just been validated. It generates an "info" severity log if the token is valid, or a "notice" severity log if it is invalid.

The log fields for this action are as follows:



Field	Description	Type	Mandatory/Optional
tenant_id	Tenant identifier. Example: <i>025f02fe-bee2-444b-bf76-b5ead30327c0</i>	String in uuid v4 format	Mandatory
jwk	Information concerning the JWK used to validate the token. See <a href="#">JWK object description</a> .	Object	Mandatory
jwt	Token content. See <a href="#">JWT object description</a> .	Object	Mandatory
valid	Checking token legitimacy. Prescribed values: <ul style="list-style-type: none"><li>• <i>true</i></li><li>• <i>false</i></li></ul>	Boolean	Mandatory
source	JWK configuration source. Prescribed values: <ul style="list-style-type: none"><li>• <i>local_configuration</i></li><li>• <i>remote_well_known_cse_configuration</i></li></ul>	String	Mandatory
type	Token type. Prescribed values: <ul style="list-style-type: none"><li>• <i>user_authentication</i></li><li>• <i>admin_authentication</i></li><li>• <i>kacsl-to-kacsl_authentication</i></li><li>• <i>wrappivatekey_authentication</i></li><li>• <i>delegate_authentication</i></li></ul>	String	Mandatory
details	Additional message describing the cause of the token refusal. Present only when the token is invalid: Example: <i>JWT expired</i>	String	Optional

### JWK object description

Field	Description	Type	Mandatory/Optional
kid	Key identifier. Example: <i>87bbe0815b064e6d449cac999f0e50e72a3e4374</i>	String	Mandatory
alg	Algorithm used. Prescribed value: <ul style="list-style-type: none"><li>• <i>RS256</i></li></ul>	String	Mandatory/

### JWT object description

Field	Description	Type	Mandatory/Optional
email	Email address of the user concerned by the token. Example: <i>alice.dupont@gmail.com</i>	String	Mandatory



Field	Description	Type	Mandatory/Optional
google_email	User's Google account email address. This field is always absent in the case of a <i>digest</i> action. Example: <i>alice.google@gmail.com</i>	String	Optional
iss	Service that generates the token (issuer). Example: <i>https://google.onelogin.com/</i>	String	Mandatory
aud	Token recipient (audience). Example: <i>a7cb5600-cbb0-023b-531e-02449949762c38534</i>	String array	Mandatory
exp	Expiry time after which the JWT must no longer be accepted. In the form of a timestamp in seconds. Example: <i>1720542398</i>	Integer	Mandatory
iat	Token creation date (issued at). In the form of a timestamp in seconds. Example: <i>1720535198</i>	Integer	Mandatory
number_of_custom_claims	Number of custom claims contained in the token. Example: <i>1</i>	Integer	Mandatory
kacls_url	KACLS URL, for <i>kacls_to_kacls</i> tokens only. Example: <i>https://cse.mysds.io/api/v1/f438ae27-f33d-1fa3-b1e2-efc4d7635684</i>	String	Optional
resource_name	Token resource identifier, for <i>kacls_to_kacls</i> tokens only. Example: <i>//googleapis.com/drive/files/10JsaKJM5JES1yi79QCKx-13w0R1i8JPU</i>	String	Optional

### 3.5 authorization category

This log category contains all business requests concerning JWT authorization tokens that enable checks to be run to see whether the user is authorized or not.

#### 3.5.1 Verify action On Prem Only

The *verify* action means that an authorization token has just been validated. It generates an "info" severity log if the token is valid, or a "notice" severity log if it is invalid.

The log fields for this action are as follows:

Field	Description	Type	Mandatory/Optional
tenant_id	Tenant identifier. Example: <i>025f02fe-bee2-444b-bf76-b5ead30327c0</i>	String in uuid v4 format	Mandatory
jwk	Information concerning the JWK used to validate the token. See <a href="#">JWKS object description</a> .	Object	Mandatory
jwt	Token content. See <a href="#">JWT object description</a> .	Object	Mandatory



Field	Description	Type	Mandatory/Optional
valid	Checking token legitimacy. Prescribed values: <ul style="list-style-type: none"><li>• <i>true</i></li><li>• <i>false</i></li></ul>	Boolean	Mandatory
type	Token type. Prescribed values: <ul style="list-style-type: none"><li>• <i>standard_authorization</i></li><li>• <i>gmail_smime_authorization</i></li><li>• <i>migration_authorization</i></li><li>• <i>delegate_authorization</i></li></ul>	String	Mandatory
details	Additional message describing the cause of the token refusal. Present only when the token is invalid: Example: <i>JWT expired</i>	String	Optional

### JWKS object description

Field	Description	Type	Mandatory/Optional
kid	Key identifier. Example: <i>87bbe0815b064e6d449cac999f0e50e72a3e4374</i>	String	Mandatory
alg	Algorithm used. Prescribed value: <ul style="list-style-type: none"><li>• <i>RS256</i></li></ul>	String	Mandatory

### JWT object description

Field	Description	Type	Mandatory/Optional
email	Email address of the user concerned by the token. Example: <i>alice.dupont@gmail.com</i>	String	Mandatory
iss	Service that generates the token (issuer). Example: <i>https://google.onelogin.com/</i>	String	Mandatory
aud	Token recipient (audience). Example: <i>a7cb5600-cbb0-023b-531e-02449949762c38534</i>	String array	Mandatory
exp	Expiry time after which the JWT must no longer be accepted. In the form of a timestamp in seconds. Example: <i>1720542398</i>	Integer	Mandatory
role	Role of the user. Example: <i>reader</i>	String	Mandatory
iat	Token creation date (issued at). In the form of a timestamp in seconds. Example: <i>1720535198</i>	Integer	Optional



Field	Description	Type	Mandatory/Optional
resource_name	Token resource identifier, for <i>kacls_to_kacls</i> tokens only. Example: <i>//googleapis.com/drive/files/10JsaKJM5JES1yi79QCKx-13w0R1i8JPU</i>	String	Optional
perimeter_id	Identifier to perform a check on authorization requests. Example: <i>22041999</i>	String	Optional
kacls_url	KACLS URL, for <i>kacls_to_kacls</i> tokens only. Example: <i>https://cse.mysds.io/api/v1/f438ae27-f33d-1fa3-b1e2-efc4d7635684</i>	String	Optional
email_type	Origin of the user's email address. Example: "google"	String	Optional
message_id	Identifier of the message on which the signature or decryption operation has been performed. Example: <i>&lt;CADBpGcUzg2iGuYyRoGkQg4F8sHXNoQtxbSxS70iyJg@mail.gmail.com&gt;</i>	String	Optional
spki_hash_algorithm	Algorithm used to produce the <i>spki_hash</i> . Example: <i>SHA-256</i>	String	Optional
spki_hash	base64 digest of the public key. Example: <i>YSBzcGtpIGhhc2ggb2YgdGhlIHBB1YmxpYyBrZXk=</i>	String	Optional
number_of_custom_claims	Number of custom claims contained in the token. Example: <i>1</i>	Integer	Mandatory



## 4. System - Environment logs

The log fields described below relate to the operations concerning the environment (e.g., operating system, server, cache, KMS, etc.). They belong to the *System* log family [Kind:system].

In the event of an erroneous request, some fields marked as mandatory may not be displayed.

### 4.1 server category

This category of logs contains all web server related operations.

#### 4.1.1 Starting action On Prem Only

The *starting* action means that a web server is about to start. It generates a "debug" severity log.

Field	Description	Type	Mandatory/Optional
type	Web server type. Prescribed value: <ul style="list-style-type: none"><li>kmaas</li></ul>	String	Mandatory

#### 4.1.2 Started action On Prem Only

The *started* action means that a web server is fully started and listening on a port. It generates an "info" severity log.

Field	Description	Type	Mandatory/Optional
port	Server listening port. Example: 3000	Integer	Mandatory
type	Web server type. Prescribed value: <ul style="list-style-type: none"><li>kmaas</li></ul>	String	Mandatory
<b>https:</b> A json object containing information about the HTTPS configuration of the server.			
enabled	Specifies whether the service uses HTTPS.	Boolean	Mandatory
ca_path	Path to the certificate authority if specified in the <i>config.json</i> file.	String	Optional
privatekey_path	Path to the private key if specified in the <i>config.json</i> file.	String	Optional
certificate_path	Path to the certificate if specified in the <i>config.json</i> file.	String	Optional

### 4.2 kms category

This log category contains all operations related to the Key Management System [KMS].



#### 4.2.1 connect action On Prem Only

The *connect* action means that a connection is established with a KMS. It generates an "info" severity log, or "warning" or "critical" severity log in the event of an error.

Field	Description	Type	Mandatory/Optional
port	KMS port	Integer	Mandatory
host	Machine hosting the KMS.	String	Mandatory
protocol	Information about the protocol used to connect to the KMS: <ul style="list-style-type: none"><li>• type: "rest_api" or "kmip"</li><li>• kmip: [optional] information on the connection if KMIP<ul style="list-style-type: none"><li>- version: version of the KMIP used</li><li>- supported_versions: version list</li></ul></li><li>• authentication:<ul style="list-style-type: none"><li>- ca: path to the certification authority file</li><li>- cert: path to the certificate file</li><li>- key: path to the private key file</li></ul></li></ul>	json object	Mandatory
kms_version	KMS version.	String	Optional

#### 4.2.2 Disconnect action On Prem Only

The *disconnect* action means that the connection to the KMS has been closed. It generates an "info" severity log, or "warning" in the event of an error.

Field	Description	Type	Mandatory/Optional
host	Machine hosting the KMS.	String	Mandatory

#### 4.2.3 Operation action On Prem Only

The *operation* action means that an operation has been performed with the KMS. It generates an "info" severity log, or "warning" or "critical" severity log in the event of an error.

Field	Description	Type	Mandatory/Optional
operation_name	Type of operation performed on the KMS (possible value: extract_keys, sign, decrypt).	String	Mandatory
host	Machine hosting the KMS.	String	Mandatory
key_labels	List of labels used to extract keys from the KMS.	List of strings	Optional
tenant_id	Tenant identifier. Example: 025f02fe-bee2-444b-bf76-b5ead30327c0	String in uuid v4 format	Optional





### 4.3 resource category

This category of logs contains all the external resource access operations.

#### 4.3.1 get action On Prem Only

The *get* action means that an external resource has been accessed. It generates an "info" severity log, or "warning" in the event of an error.

Field	Description	Type	Mandatory/Optional
resource	URL of the retrieved resource. Example: <i>https://localhost:4000/static/one-login/.well-known/jwks.json</i>	String	Mandatory
type	Type of request made. Example: <i>http</i>	String	Mandatory
status	Request status Examples: <i>200, 403, ECONNREFUSED</i>	String	Mandatory
method	Request method. Examples: <i>POST, GET, OPTIONS</i>	String	Mandatory



## 5. HTTP- HTTP request logs

The log fields described below relate to the HTTP requests managed by the SDS encryption service for Google Workspace. They belong to the *http* log family (Kind:http).

### 5.1 request category

This category of logs contains all the incoming HTTP requests sent to the SDS encryption service for Google Workspace.

#### 5.1.1 receive action On Prem Only

The *receive* action means that an HTTP request has been received by the SDS encryption service for Google Workspace. It generates an "info" severity log.

The log fields for this action are as follows:

Field	Description	Type	Mandatory/Optional
endpoint	URL of the retrieved resource. Example: <i>https://localhost:4000/static/one-login/.well-known/jwks.json</i>	String	Mandatory
method	Request method. Examples: <i>POST, GET, OPTIONS</i>	String	Mandatory
remote_user_agent	Information about the request issuer contained in the request header. Example: <i>Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/27.0.1453 Safari/537.36</i>	String	Mandatory
remote_address	Address of request issuer. Example: <i>172.16.16.212</i>	String	Mandatory
content_length	Size of received request body, in bytes. Only present when body size is greater than zero.	Integer	Optional



**STORMSHIELD**

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

*Copyright © Stormshield 2025. All rights reserved. All other company and product names contained in this document are trademarks or registered trademarks of their respective companies.*