GUIDE

SERVICE DE CHIFFREMENT SDS POUR GOOGLE WORKSPACE

GUIDE DES LOGS

Dernière mise à jour du document : 4 septembre 2024

Référence : sds-fr-sds-for-gw-guide_des_los

Table des matières

1. Avant de commencer

Le service de chiffrement SDS pour Google Workspace génère des logs pour chaque opération, ce qui permet de tracer toutes les actions effectuées et les problèmes potentiels. Les logs sont au format JSON et sont hébergés chez Stormshield.

Un identifiant unique au format UUIDV4 est généré automatiquement à chaque requête. Il s'agit de l'identifiant de corrélation permettant de lier tous les logs qui concernent la même requête ou le même événement.

Pour consulter vos logs, faites une demande d'export à Stormshield à l'adresse *data-security-business-unit@stormshield.eu*.

Ce document décrit tous les logs susceptibles d'être générés par le service de chiffrement SDS pour Google Workspace dans un environnement Saas.

2. Champs communs à tous les logs

Les champs suivants sont affichés pour tous des logs générés par le service de chiffrement SDS pour Google Workspace en mode Saas, dans l'ordre indiqué dans le tableau.

- Les champs **obligatoires** sont systématiquement présents dans les logs émis en cas de requête réussie, mais peuvent être absents en cas de requête en échec.
- Les champs **optionnels** peuvent être présents ou absents dans les deux cas.

Champ	Description	Type	Obligatoire/Optionnel
timestamp	Date et heure à laquelle le log a été créé. Au format UTC. Exemple : "2023-12-05T09:27:58.936Z"	Chaîne de caractères au format ISO 8601	Obligatoire
severity	Niveau de gravité du log. Valeurs possibles : • *emerg* : Le système est inutilisable, • *alert* : Le problème doit être corrigé immédiatement, • *crit* : Erreur critique, • *err* : Erreur non critique, • *warning* : L'opération a réussi mais a généré un avertissement, • *notice* : Événement inhabituel ne nécessitant pas d'action corrective, • *info* : Message d'information d'opération normale, • *debug* : Information utile aux développeurs pour le dépannage de l'application.	Chaîne de caractères	Obligatoire
application_version	Version de l'application. Exemple : "4.3.0.2354"		Obligatoire
kind	Famille de logs à laquelle appartient le log. Valeur possible : • *domain* : Logs concernant les opérations métier du service de chiffrement SDS pour Google Workspace.	Chaîne de caractères	Obligatoire
category	Catégorie du log. Valeurs possibles : • *cse* : Logs sur les requêtes métier effectuées par le service de chiffrement SDS pour Google Workspace. • *authentication* : Logs sur les actions de vérification des jetons d'authentification.	Chaîne de caractères	Obligatoire

Champ	Description	Type	Obligatoire/Optionnel
action	Événement qui s'est produit. Valeurs possibles : • unwrap, • privilegedwrap, • takeout, • privilegedunwrap, • rewrap, • digest, • certs, • wrapprivatekey, • privatekeysign, • privatekeydecrypt, • privilegedprivatekeydecrypt	Chaîne de caractères	Obligatoire
log_version	Version actuelle du format de logs. Valeur possible : *2*	Entier	Obligatoire
process_id	Identifiant du processus. Exemple : *4031*	Entier	Obligatoire
correlation_id	Identifiant unique permettant de lier l'ensemble des logs qui concernent la même requête ou le même événement. Exemple : "*146f73b6-c15d-4488-984c-97726cf86587*"	Chaîne de caractères	Obligatoire

Les champs du bloc *error* décrits ci-dessous sont affichés pour tous les logs générés par le service de chiffrement SDS pour Google Workspace en cas d'erreur lors de l'exécution de l'action :

Champ	Description	Type	Obligatoire/Optionnel
code	Numéro de l'erreur. Exemple : *2006003*	Entier	Obligatoire
message	Message de l'erreur. Exemple : *Unauthorized request*	Chaîne de caractères	Obligatoire

3. Domain - Logs liés aux opérations métier

Les logs dont les champs sont décrits ci-dessous informent sur les opérations métier effectuées par le service de chiffrement SDS pour Google Workspace. Ils appartiennent à la famille de logs *Domain* (Kind:domain).

3.1 Catégorie *cse*

Dans cette catégorie de logs se trouvent toutes les requêtes métier effectuées par le service de chiffrement SDS pour Google Workspace.

3.1.1 Actions wrap, unwrap, privilegedwrap et digest

- *wrap* : une requête *wrap* a été effectuée. C'est le cas chaque fois qu'une clé est chiffrée.
- *unwrap* : une requête *unwrap* a été effectuée. C'est le cas chaque fois qu'une clé est déchiffrée.
- *privilegedwrap* : une requête *privilegedwrap* a été effectuée. C'est le cas chaque fois qu'un import de fichiers en masse est en cours.
- *digest* : une requête *digest* a été effectuée. C'est le cas chaque fois qu'une opération de migration ou de chiffrement vers un KACLS de secours est en cours.

Toutes ces actions génèrent un log de gravité "info" en cas de succès, ou de gravité "crit" en cas d'erreur.

Les champs des logs pour ces actions sont les suivants :

Champ	Description	Type	Obligatoire/Optionnel
tenant_id	Identifiant du tenant. Exemple : *025f02fe-bee2-444b-bf76-b5ead30327c0*	Chaîne de caractères au format uuid v4	Obligatoire
reason	Contexte supplémentaire sur l'opération. Exemple : *Reason of the request*	Chaîne de caractères	Obligatoire
email	Adresse e-mail de l'utilisateur. Exemple : *alice.dupont@gmail.com*	Chaîne de caractères	Obligatoire
google_email	Adresse e-mail du compte Google de l'utilisateur. Ce champ est toujours absent dans le cas d'une action *digest*. Exemple : *alice.google@gmail.com*	Chaîne de caractères	Optionnel
google_application	Application Google Workspace concernée par l'opération. Valeurs possibles : • *meet*, • *drive*, • *calendar*	Chaîne de caractères	Obligatoire
resource_name	Identifiant de la ressource. Exemple : *//googleapis.com/drive/files/10JsaKJM5JES1yi79QCKx-13w0R1i8JPU"*	Chaîne de caractères	Obligatoire

Champ	Description	Type	Obligatoire/Optionnel
perimeter_id	Identifiant permettant d'effectuer une vérification supplémentaire des demandes d'authentification et d'autorisation. Exemple : *Perimeter_id of the request*	Chaîne de caractères	Obligatoire
kek_id	Identifiant de la clé KEK utilisée. Exemple : *ed7e4c13-6199-30a3-7bce-1c82a9e31e21*	Chaîne de caractères	Obligatoire

3.1.2 Action rewrap

L'action *rewrap* signifie qu'une requête *rewrap* a été effectuée. C'est le cas chaque fois qu'une opération de migration ou de chiffrement vers un KACLS de secours est en cours.

Cette action génère un log de gravité "info" en cas de succès, ou de gravité "crit" en cas d'erreur.

Les champs des logs pour cette action sont les suivants :

Champ	Description	Type	Obligatoire/Optionnel
tenant_id	Identifiant du tenant. Exemple : *025f02fe-bee2-444b-bf76-b5ead30327c0*	Chaîne de caractères au format uuid v4	Obligatoire
reason	Contexte supplémentaire sur l'opération. Exemple : *Reason of the request*	Chaîne de caractères	Obligatoire
email	Adresse e-mail de l'utilisateur. Exemple : *alice.dupont@gmail.com*	Chaîne de caractères	Obligatoire
google_application	Application Google Workspace concernée par l'opération. Valeurs possibles : • *meet*, • *drive*, • *calendar*	Chaîne de caractères	Obligatoire
resource_name	Identifiant de la ressource. Exemple : *//googleapis.com/drive/files/10JsaKJM5JES1yi79QCKx-13w0R1i8JPU"*	Chaîne de caractères	Obligatoire
perimeter_id	Identifiant permettant d'effectuer une vérification supplémentaire des demandes d'authentification et d'autorisation. Exemple : *Perimeter_id of the request*	Chaîne de caractères	Obligatoire
kek_id	Identifiant de la clé KEK utilisée. Exemple : *ed7e4c13-6199-30a3-7bce-1c82a9e31e21*	Chaîne de caractères	Obligatoire
original_kacls_url	URL du KACLS qui sera migré. Exemple : *https://cse.mysds.io/api/v1/f438ae27-f33d-1fa3-b1e2-efc4d7635684*	Chaîne de caractères (URL)	Obligatoire

3.1.3 Action certs

L'action *certs* signifie qu'une requête *certs* a été effectuée. C'est le cas chaque fois qu'une opération de migration ou de chiffrement vers un KACLS de secours est en cours et qu'une demande de certificats est émise par un autre KACLS.

Cette action génère un log de gravité "info" en cas de succès, ou de gravité "crit" en cas d'erreur.

Les champs des logs pour cette action sont les suivants :

Champ	Description	Type	Obligatoire/Optionnel
tenant_id	Identifiant du tenant. Exemple : *025f02fe-bee2-444b-bf76-b5ead30327c0*	Chaîne de caractères au format uuid v4	Obligatoire
keys	Certificat public du KACLS au format JSON Web Key Set comme défini dans la RFC 7517. Exemple fourni par Google.	Objet de type JSON Web Key Set	Obligatoire

Autre exemple de certificat public :

```
"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 Action privilegedunwrap

L'action *privilegedunwrap* signifie qu'une requête *privilegedunwrap* a été effectuée. C'est le cas chaque fois qu'une opération de migration ou de chiffrement vers un KACLS de secours est en cours.

Cette action génère un log de gravité "info" en cas de succès, ou de gravité "crit" en cas d'erreur.

Les champs des logs pour cette action sont les suivants :

Champ	Description	Type	Obligatoire/Optionnel
tenant_id	Identifiant du tenant. Exemple : *025f02fe-bee2-444b-bf76-b5ead30327c0*	Chaîne de caractères au format uuid v4	Obligatoire
reason	Contexte supplémentaire sur l'opération. Exemple : *Reason of the request*	Chaîne de caractères	Obligatoire

Champ	Description	Type	Obligatoire/Optionnel
resource_name	Identifiant de la ressource. Exemple : *//googleapis.com/drive/files/10JsaKJM5JES1yi79QCKx-13w0R1i8JPU"*	Chaîne de caractères	Obligatoire
perimeter_id	Identifiant permettant d'effectuer une vérification supplémentaire des demandes d'authentification et d'autorisation. Exemple : *Perimeter_id of the request*	Chaîne de caractères	Obligatoire
kek_id	Identifiant de la clé KEK utilisée. Exemple : *ed7e4c13-6199-30a3-7bce-1c82a9e31e21*	Chaîne de caractères	Obligatoire

3.1.5 Action takeout

L'action *takeout* signifie qu'un document chiffré est exporté depuis Google.

Cette action génère un log de gravité "info" en cas de succès, ou de gravité "crit" en cas d'erreur.

Application Drive

L'action *takeout* liée à l'application Google Drive, signifie qu'une requête *privilegedunwrap* a été effectuée. C'est le cas chaque fois qu'un document chiffré est exporté depuis Google.

Les champs des logs pour cette action sont les suivants :

Champ	Description	Type	Obligatoire/ Optionnel
tenant_id	Identifiant du tenant. Exemple : *025f02fe-bee2-444b-bf76-b5ead30327c0*	Chaîne de caractères au format uuid v4	Obligatoire
reason	Contexte supplémentaire sur l'opération. Exemple : *Reason of the request*	Chaîne de caractères	Obligatoire
email	Adresse e-mail de l'utilisateur. Exemple : *alice.dupont@gmail.com*	Chaîne de caractères	Obligatoire
google_email	Adresse e-mail du compte Google de l'utilisateur. Ce champ est toujours absent dans le cas d'une action *digest*. Exemple : *alice.google@gmail.com*	Chaîne de caractères	Optionnel
google_application	Application Google Workspace concernée par l'opération. Valeurs possibles : • *meet* • *drive* • *calendar*	Chaîne de caractères	Obligatoire
resource_name	Identifiant de la ressource. Exemple : *//googleapis.com/drive/files/10JsaKJM5JES1yi79QCKx-13w0R1i8JPU"*	Chaîne de caractères	Obligatoire

Champ	Description	Type	Obligatoire/ Optionnel
perimeter_id	Identifiant permettant d'effectuer une vérification supplémentaire des demandes d'authentification et d'autorisation. Exemple : *Perimeter_id of the request*	Chaîne de caractères	Obligatoire
kek_id	Identifiant de la clé KEK utilisée. Exemple : *ed7e4c13-6199-30a3-7bce-1c82a9e31e21*	Chaîne de caractères	Obligatoire

Application Gmail

L'action *takeout* liée à l'application Gmail, signifie qu'une requête *privilegedprivatekydecrypt* a été effectuée. C'est le cas chaque fois qu'un e-mail chiffré est exporté depuis Google.

Les champs des logs pour cette action sont les suivants :

Champ	Description	Type	Obligatoire/ Optionnel
tenant_id	Identifiant du tenant. Exemple : *025f02fe-bee2-444b-bf76-b5ead30327c0*	Chaîne de caractères au format uuid v4	Obligatoire
reason	Contexte supplémentaire sur l'opération. Exemple : *Reason of the request*	Chaîne de caractères	Obligatoire
email	Adresse e-mail de l'utilisateur. Exemple : *alice.dupont@gmail.com*	Chaîne de caractères	Obligatoire
google_email	Adresse e-mail du compte Google de l'utilisateur. Ce champ est toujours absent dans le cas d'une action *digest*. Exemple : *alice.google@gmail.com*	Chaîne de caractères	Optionnel
google_application	Application Google Workspace concernée par l'opération. Valeurs possibles : • *gmail*	Chaîne de caractères	Obligatoire
kek_id	Identifiant de la clé KEK utilisée. Exemple : *ed7e4c13-6199-30a3-7bce-1c82a9e31e21*	Chaîne de caractères	Obligatoire
spki_hash_base64	Digest en base64 de la clé privée. Exemple : *EUV0iaJF1j3cfQnp6IaGjmFr5bSdarcic0AoSG9RJWI=*	Chaîne de caractères	Obligatoire
spki_hash_algorithm	Algorithme de chiffrement utilisé. Valeur possible : • *SHA-256*	Chaîne de caractères	Obligatoire
private_key_used_algorithm	Algorithmes de chiffrement utilisé lors de cette opération. Exemple : *RSA/ECB/PKCS1Padding*	Chaîne de caractères	Obligatoire

Champ	Description	Type	Obligatoire/ Optionnel
private_key_ supported_ algorithms	Algorithmes de chiffrement et de signature supportés par cette clé. Exemple : *"["RSA/ECB/PKCS1Padding","SHA1withRSA", "SHA256withRSA"]*	Chaîne de caractères	Obligatoire
private_key_mode	Type de clé privée utilisée lors de l'opération. Valeurs possibles : • *private-key-pem* : Les clés privées des utilisateurs sont stockées chiffrées chez Google, • *private-key-name* : Les clés privées des utilisateurs sont stockées dans un KMS et n'en sortent jamais. Seul le nom des clés privées est stocké chez Google.	Chaîne de caractères	Obligatoire

3.1.6 Actions privatekeysign et privatekeydecrypt

- *privatekeysign* : une requête *privatekeysign* a été effectuée. C'est le cas chaque fois qu'un e-mail est signé pour être chiffré.
- *privatekeydecrypt* : une requête *privatekydecrypt* a été effectuée. C'est le cas chaque fois qu'un e-mail chiffré est déchiffré.

Ces actions génèrent un log de gravité "info" en cas de succès, ou de gravité "crit" en cas d'erreur.

Les champs des logs pour ces actions sont les suivants :

Champ	Description	Type	Obligatoire/ Optionnel
tenant_id	Identifiant du tenant. Exemple : *025f02fe-bee2-444b-bf76-b5ead30327c0*	Chaîne de caractères au format uuid v4	Obligatoire
reason	Contexte supplémentaire sur l'opération. Exemple : *Reason of the request*	Chaîne de caractères	Obligatoire
email	Adresse e-mail de l'utilisateur. Exemple : *alice.dupont@gmail.com*	Chaîne de caractères	Obligatoire
google_email	Adresse e-mail du compte Google de l'utilisateur. Ce champ est toujours absent dans le cas d'une action *digest*. Exemple : *alice.google@gmail.com*	Chaîne de caractères	Optionnel
google_ application	Application Google Workspace concernée par l'opération. Valeurs possibles : • *gmail*	Chaîne de caractères	Obligatoire
kek_id	Identifiant de la clé KEK utilisée. Exemple : *ed7e4c13-6199-30a3-7bce-1c82a9e31e21*	Chaîne de caractères	Obligatoire

Champ	Description	Type	Obligatoire/ Optionnel
perimeter_id	Identifiant permettant d'effectuer une vérification supplémentaire des demandes d'authentification et d'autorisation. Exemple : *Perimeter_id of the request*	Chaîne de caractères	Obligatoire
message_id	Identifiant du message sur lequel l'opération de signature ou de déchiffrement a été effectuée. Exemple : *<CADBpGcUzg2iGuYyRoGkQg4F8sHXNoQtxbSxS70iyJgvpDb0g@mail.gmail.com>*	Chaîne de caractères	Obligatoire
spki_hash_base64	Digest en base64 de la clé privée. Exemple : *EUV0iaJF1j3cfQnp6IaGjmFr5bSdarcic0AoSG9RJWI=*	Chaîne de caractères	Obligatoire
spki_hash_algorithm	Algorithme de chiffrement utilisé. Valeur possible : • *SHA-256*	Chaîne de caractères	Obligatoire
private_key_used_algorithm	Algorithmes de chiffrement utilisés lors de cette opération. Exemple : *RSA/ECB/PKCS1Padding*	Chaîne de caractères	Obligatoire
private_key_supported_algorithms	Algorithmes de chiffrement et de signature supportés par cette clé. Exemple : *"["RSA/ECB/PKCS1Padding","SHA1withRSA", "SHA256withRSA"]*	Chaîne de caractères	Obligatoire
private_key_mode	Type de clé privée utilisée lors de l'opération. Valeurs possibles : • *private-key-pem* : Les clés privées des utilisateurs sont stockées chiffrées chez Google, • *private-key-name* : Les clés privées des utilisateurs sont stockées dans un KMS et n'en sortent jamais. Seul le nom des clés privées est stocké chez Google.	Chaîne de caractères	Obligatoire

3.1.7 Action wrapprivatekey

L'action *wrapprivatekey* signifie qu'une requête *wrapprivatekey* a été effectuée. C'est le cas chaque fois qu'une clé privée d'un utilisateur est chiffrée pour Gmail.

Cette action génère un log de gravité "info" en cas de succès, ou de gravité "crit" en cas d'erreur.

Les champs des logs pour ces actions sont les suivants :

Champ	Description	Type	Obligatoire/ Optionnel
tenant_id	Identifiant du tenant. Exemple : *025f02fe-bee2-444b-bf76-b5ead30327c0*	Chaîne de caractères au format uuid v4	Obligatoire
kek_id	Identifiant de la clé KEK utilisée. Exemple : *ed7e4c13-6199-30a3-7bce-1c82a9e31e21*	Chaîne de caractères	Obligatoire

Champ	Description	Type	Obligatoire/ Optionnel
perimeter_id	Identifiant permettant d'effectuer une vérification supplémentaire des demandes d'authentification et d'autorisation. Exemple : *Perimeter_id of the request*	Chaîne de caractères	Obligatoire
private_key_supported_ algorithms	Algorithmes de chiffrement et de signature supportés par cette clé. Exemple : "*["RSA/ECB/PKCS1Padding","SHA1withRSA", "SHA256withRSA"]*	Chaîne de caractères	Obligatoire
private_key_mode	Type de clé privée utilisée lors de l'opération. Valeurs possibles : • *private-key-pem* : Les clés privées des utilisateurs sont stockées chiffrées chez Google, • *private-key-name* : Les clés privées des utilisateurs sont stockées dans un KMS et n'en sortent jamais. Seul le nom des clés privées est stocké chez Google.	Chaîne de caractères	Obligatoire

Les images de ce document ne sont pas contractuelles, l'aspect des produits présentés peut éventuellement varier.