GUIDE

STORMSHIELD KEY MANAGEMENT AS A SERVICE

LOG GUIDE

Document last updated: October 16, 2025

Reference: sds-en-kmaas-v2_log_guide

Table of contents

1. Getting started

The Stormshield KMaaS 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, if the operation request does not provide it through the specific *x-request-id* header. This is the correlation ID linking all logs related to the same request or event.

If you are using Stormshield KMaaS in SaaS mode, to view your logs, submit an export request to Stormshield at *data-security-business-unit@stormshield.eu*.

In On Premise mode, refer to the Stormshield KMaaS Administration Guide for more information on log locations.

This document describes all the logs likely to be generated by the Stormshield KMaaS. The vast majority of logs are common to both SaaS and On Premises modes of Stormshield KMaaS. 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 Stormshield KMaaS 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 values: • *domain*: Stormshield KMaaS business operation logs. • *system*: Logs relating to the operations concerning the environment. • *http*: Logs relating to the HTTP operations of the Stormshield KMaaS.	String	Mandatory
category	Log category. Examples of possible values: • *cse*: Logs of business requests issued by the Stormshield KMaaS. • *authentication*: Logs of authentication token verification actions.	String	Mandatory

Field	Description	Type	Mandatory/Optional
action	Event that occurred. Examples of possible 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
hostname On Prem Only	Host name. Example: *MyCSEServer*	String	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 Stormshield KMaaS in the event of an error when executing the action:

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

3. Domain- Business operation logs

The log fields described below relate to business operations performed by the Stormshield KMaaS. They belong to the *Domain* log family (Kind:domain).

3.1 *kacls* category

This category of logs contains all the business requests made by the KACLS.

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: *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
perimeter_id	Identifier for additional verification of authentication and authorization requests. Example: *Perimeter_id of the request*	String	Mandatory

Field	Description	Type	Mandatory/Optional
kek_id	Identifier of the KEK used. Example: *ed7e4c13-6199-30a3-7bce-1c82a9e31e21*	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: *025f02fe-bee2-444b-bf76-b5ead30327c0*	String in uuid v4 format	Mandatory
reason	Additional context about the operation. Example: *Reason of the request*	String	Mandatory

Field	Description	Type	Mandatory/Optional
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

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

Field	Description	Type	Mandatory/Optional
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"
      }
    ]
```

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_
FwSmxu2AeDkCVXpLwbRXkbOKc83MHC8czp80RuGjy3I6vhNocdZBhnJ5H7fAFNOmtd_C3xVFtdOO6H7sd2AQQ_
zoEwV0qISSLS_
uZbr6gwsiyxRUUARsvEmGUUqt0lOnXniE1cKMu1mdbcCmhfZH3g5n2Z1bcq8u86KlIcZ8T0Wnu1PGMhXML4mhe6z
3KH3PWqvoeYj4ILzz5KEI6zrMun-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: *025f02fe-bee2-444b-bf76-b5ead30327c0*	String in uuid v4 format	Mandatory
reason	Additional context about the operation. Example: *Reason of the request*	String	Mandatory

Field	Description	Type	Mandatory/Optional
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

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: *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

Field	Description	Type	Mandatory/ 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
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

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": "xUVOgaJF1j6dfQnp6IaGmmFr5bSdarcicOAoSG9RkzI=",
"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": "xUVOgaJF1j6dfQnp6IaGmmFr5bSdarcicOAoSG9RkzI=",
"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 *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	Mandatory/ Optional
tenant_id	Tenant identifier. Example: *025f02fe-bee2-444b-bf76-b5ead30327c0*	String in uuid v4 format	Mandatory

Field	Description	Type	Mandatory/ Optional
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: *EUVOiaJF1j3cfQnp6IaGjmFr5bSdarcicOAoSG9RJWI=*	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

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 *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	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: • *gmail*	String	Mandatory
resource_ name	Resource identifier. Example: *//googleapis.com/drive/files/10JsaKJM5JES1yi79QCKx-13w0R1i8JPU"*	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: *EUV0iaJF1j3cfQnp6IaGjmFr5bSdarcic0AoSG9RJWI=*	String	Mandatory

Field	Description	Type	Mandatory/ Optional
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

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 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	Mandatory/ 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

Example of logs for the successful *wrapprivatekey* 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: *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. Example: *alice.google@gmail.com*	String	Optional
google_application	Google Workspace application concerned by the operation. Prescribed values: • *meet*	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
delegated_to	Identifier of the entity to which authentication is delegated. Example: "Authentication delegated to Alice Dupont"	String	Mandatory

3.1.9 status action

The *status* action means that a *status* request has been made. This request is used to check the KACLS configuration status. It can be made either manually or automatically by Google on a regular basis.

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: *025f02fe-bee2-444b-bf76-b5ead30327c0*	String in uuid v4 format	Mandatory
server_type	Type of the service, as defined by Google. Prescribed value: • *KACLS*	String	Mandatory

Field	Description	Type	Mandatory/ Optional
vendor_id	Name of the provider of theStormshield KMaaS. Prescribed value: • Stormshield	String	Mandatory
version	Version of the Stormshield KMaaS. Example: *4.5.0.2435*	String	Mandatory
name	Name of the Stormshield KMaaS instance as defined in the "name" field of the *config.json* configuration file.	String	Mandatory
operations_supported	Array containing the list of operations supported by the tenant. Examples: *certs, delegate, privatekeydecrypt, priviledgedwrap, wrap*, etc.	Array	Mandatory

3.2 *crypto_api* category

This category of logs contains all the business requests concerning the Crypto API feature.

3.2.1 setup action On Prem Only

The *setup* action means that the Crypto API configuration is checked. It generates an "info" severity log if it is configured properly, or an "err" 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
enabled	Specify if the Crypto API feature is enabled.	Boolean	Mandatory

Field	Description	Type	Mandatory/Optional
errors	If the Crypto API feature cannot be enabled due to an incorrect configuration, this JSON object contains an error list with an error code and a message: • If the severity level is "info", the error list is empty, the Crypto API feature is enabled. • If the severity level is "err", the list contains at least one error. *Example: [* *{* *code: 2002010,* *message: 'Feature: CryptoAPI not enabled for tenantId bc337abd-0d4f-43f9-aaf6-54ef7268d2e5. Reason: Validation failed. Reasons are: [Wrong type error: <tenant>/crypto_api/authentication property must be array]'* *}* *]*	Object	Mandatory if enabled is set to true

3.2.2 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: *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

3.3 *kek* category

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

3.3.1 Load action On Prem Only

The *load* action means that a KEK key has just been loaded into the memory for use by the Stormshield KMaaS. 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: *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
is_active_kek	Indicates whether the KEK key loaded is the one used for encryption. Prescribed values: • true • false	Boolean	Mandatory
is_encrypted_kek	Indicates whether the KEK loaded is encrypted by an MKEK. Prescribed values: • true • false	Boolean	Mandatory

3.3.2 load_asym action On Prem Only

The *load_asym* action means that a KEK key has just been loaded into the memory for use by the KAS rewrap operation. 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: *025f02fe-bee2-444b-bf76-b5ead30327c0*	String in uuid v4 format	Mandatory
kid	Identifier of the KEK used. Example: *ed7e4c13-6199-30a3-7bce-1c82a9e31e21*	String	Mandatory
is_encrypted_kek	Indicates whether the KEK loaded is encrypted by an MKEK. Prescribed values: • true • false	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 or an API key has 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: *025f02fe-bee2-444b-bf76-b5ead30327c0*	String in uuid v4 format	Mandatory
method	Method used for authentication. Prescribed values: • *jwt* • *api_key*	String	Mandatory
jwk	Information concerning the JWK used to validate the token. See JWK object description.	Object	Mandatory if method is set to jwt
jwt	Token content. See JWT object description.	Object	Mandatory if method is set to jwt
valid	Checking JWT token or API key legitimacy. Prescribed values: • *true* • *false*	Boolean	Mandatory
source	JWK configuration source. Prescribed values: • *local_configuration* • *remote_well_known_cse_configuration* Only *local_configuration* if method is set to api_key.	String	Mandatory
type	Token type if method is set to jwt. Prescribed values: • *user_authentication* • *admin_authentication* • *kacsl-to-kacls_authentication* • *wrapprivatekey_authentication* • *delegate_authentication* • *crypto_api_authentication* Authenticated feature if method is set to api_key. Prescribed values: • *crypto_api_authentication* • *pki_authentication*	String	Mandatory

Field	Description	Type	Mandatory/Optional
details	Additional message describing the cause of the token refusal. Present only when the token is invalid: Example: *JWT expired*	String	Optional

JWK object description

Field	Description	Type	Mandatory/Optional
kid	Key identifier. Example: *87bbe0815b064e6d449cac999f0e50e72a3e4374*	String	Mandatory
alg	Algorithm used. Prescribed value: • *RS256*	String	Mandatory/

JWT object description

Field	Description	Type	Mandatory/Optional
email	Email address of the user concerned by the token. 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
iss	Service that generates the token (issuer). Example: *https://google.onelogin.com/*	String	Mandatory
aud	Token recipient (audience). Example: *a7cb5600-cbb0-023b-531e-02449949762c38534*	String array	Mandatory
exp	Expiry time after which the JWT must no longer be accepted. In the form of a timestamp in seconds. Example: *1720542398*	Integer	Mandatory
iat	Token creation date (issued at). In the form of a timestamp in seconds. Example: *1720535198*	Integer	Mandatory
number_of_custom_claims	Number of custom claims contained in the token. Example: *1*	Integer	Mandatory
kacls_url	KACLS URL, for *kacls_to_kacls* tokens only. Example: *https://cse.mysds.io/api/v1/f438ae27-f33d-1fa3-b1e2-efc4d7635684*	String	Optional
resource_name	Token resource identifier, for *kacls_to_kacls* tokens only. Example: *//googleapis.com/drive/files/10JsaKJM5JES1yi79QCKx-13w0R1i8JPU*	String	Optional

Field	Description	Type	Mandatory/Optional
delegated_to	Identifier of the entity to which authentication is delegated. Example: "Authentication delegated to Alice Dupont"	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: *025f02fe-bee2-444b-bf76-b5ead30327c0*	String in uuid v4 format	Mandatory
jwk	Information concerning the JWK used to validate the token. See JWKS object description.	Object	Mandatory
jwt	Token content. See JWT object description.	Object	Mandatory
valid	Checking token legitimacy. Prescribed values: • *true* • *false*	Boolean	Mandatory
type	Token type. Prescribed values: • standard_authorization • gmail_smime_authorization • migration_authorization • delegate_authorization	String	Mandatory
details	Additional message describing the cause of the token refusal. Present only when the token is invalid: Example: *JWT expired*	String	Optional

JWKS object description

Field	Description	Type	Mandatory/Optional
kid	Key identifier. Example: *87bbe0815b064e6d449cac999f0e50e72a3e4374*	String	Mandatory

Field	Description	Type	Mandatory/Optional
alg	Algorithm used. Prescribed value: • *RS256*	String	Mandatory

JWT object description

Field	Description	Type	Mandatory/Optional
email	Email address of the user concerned by the token. Example: *alice.dupont@gmail.com*	String	Mandatory
iss	Service that generates the token (issuer). Example: *https://google.onelogin.com/*	String	Mandatory
aud	Token recipient (audience). Example: *a7cb5600-cbb0-023b-531e-02449949762c38534*	String array	Mandatory
exp	Expiry time after which the JWT must no longer be accepted. In the form of a timestamp in seconds. Example: *1720542398*	Integer	Mandatory
role	Role of the user. Example: *reader*	String	Mandatory
iat	Token creation date (issued at). In the form of a timestamp in seconds. Example: *1720535198*	Integer	Optional
resource_name	Token resource identifier, for *kacls_to_kacls* tokens only. Example: *//googleapis.com/drive/files/10JsaKJM5JES1yi79QCKx-13w0R1i8JPU*	String	Optional
perimeter_id	Identifier to perform a check on authorization requests. Example: *22041999*	String	Optional
kacls_url	KACLS URL, for *kacls_to_kacls* tokens only. Example: *https://cse.mysds.io/api/v1/f438ae27-f33d-1fa3-b1e2-efc4d7635684*	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: *<CADBpGcUzg2iGuYyRoGkQg4F8sHXNoQtxbSxS70iyJg@mail.gmail.com>*	String	Optional
spki_hash_algorithm	Algorithm used to produce the spki_hash. Example: *SHA-256*	String	Optional
spki_hash	base64 digest of the public key. Example: *YSBzcGtpIGhhc2ggb2YgdGhlIHB1YmxpYyBrZXk=*	String	Optional

Field	Description	Type	Mandatory/Optional
number_of_custom_claims	Number of custom claims contained in the token. Example: *1*	Integer	Mandatory
delegated_to	Identifier of the entity to which authentication is delegated. Example: "Authentication delegated to Alice Dupont"	String	Optional

3.6 *pki* category

This category of logs contains all the requests concerning the PKI feature.

3.6.1 setup action On Prem Only

The *setup* action means that a *setup* request has been made. This is the case every time the PKI feature configuration has been loaded for a given tenant. It generates an "info" severity log in the event of success, or an "err" 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
enabled	Indicate if the PKI feature is enabled.	Boolean	Mandatory
default_pki_id	ID of the PKI engine.	String	Mandatory if "enabled" is "true"
errors	List of configuration errors where each error is a JSON object with a code and a message. If the log severity is "info", the list is empty. *Example: [{ code: 2002010, message: 'Feature: Pki not enabled for tenantId bc337abd-0d4f-43f9-aaf6-54ef7268d2e5. Reason: Validation failed. Reasons are: [Wrong type error: <tenant>/pki/authentication property must be array]' }]*	String	Mandatory if "enabled" is "true"

3.6.2 load_pki action On Prem Only

The *load_pki* action means that a PKI engine has been loaded for a given tenant. This step may occur during a call to the */simpleenroll* endpoint. It generates an "info" severity log in the event of success, or an "err" 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
pki_name	Name of the PKI engine.	String	Mandatory
pki_id	ID of the PKI engine.	String	Mandatory
ra.type	Type of the Registration Authority (RA).	String	Mandatory
ca.type	Type of the Certification Authority (CA).	String	Mandatory
ca.certificate_chain	File containing the CA certificate chain.	String	Mandatory
ca.key	File containing the CA private key.	String	Mandatory
ca.key_algo	CA signature algorithm.	String	Mandatory only if "info" severity
errors	JSON object containing an error code and a message indicating why the PKI engine could not be loaded. Example: *error: {* *code: 2024002,* *message: 'No pem data found in file /etc/stormshield/cse/key.pem'* *},*	Object	Mandatory only if "err" severity

3.6.3 issue_cert action

The *issue_cert* action means that a certificate has been issued following a Certificate Signing Request (CSR). This action occurs when calling the */simpleenroll* endpoint. It generates an "info" severity log in the event of success, or an "err" 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
pki_id	ID of the PKI engine.	String	Mandatory only if "info" severity
spki_hash	Hash of the Subject Public Key Information.	String	Mandatory only if "info" severity
algo	Signature algorithm and hash. Example: *rsassa_pkcs1_v1_5.sha-512*	String	Mandatory only if "info" severity
public_key.type	Type of algorithm used for public keys.	String	Mandatory only if "info" severity

Field	Description	Type	Mandatory/Optional
csr.DN	List of the Distinguished Names attributes in the CSR.	Object	Mandatory only if "info" severity
issued_certificate.serial_number	Serial number of the certificate issued.	String	Mandatory only if "info" severity
issued_certificate.DN	List of the Distinguished Names attributes in the certificate issued.	Object	Mandatory only if "info" severity

errors	JSON object containing an error code and a message indicating why the certificate could not be issued.
	Example:
	
	error: {
	code: 2026011,
	message: 'Unable to decode certification request"
	}
		Object	Mandatory only if "err" severity

3.7 *proxy* category

This category of logs contains all the business requests concerning the proxy feature.

3.7.1 setup action On Prem Only

The *setup* action means that the configuration of the proxy was completed. It generates an "info" severity log in the event of success, or an "err" severity log in the event of an error.

The log fields for this action are as follows:

Field	Description	Type	Mandatory/Optional
enabled	Indicate whether a proxy has been configured.	Boolean	Mandatory
proxy_url	URL of the proxy.	String	Optional
exclusion_list	List of excluded addresses.	Array	Optional
errors	JSON object containing an error code and a message indicating why the proxy configuration could not be loaded. *Example:* *error: {* *code: 1005001,* *message: 'Validation failed ..."* *},*	Object	Optional

3.8 *logs* category

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

3.8.1 setup action On Prem Only

The *setup* action means that the configuration of the logs was completed. It generates an "info" severity log in the event of success, or an "warning" severity log in the event of an error.

The log fields for this action are as follows:

Field	Description	Type	Mandatory/Optional
formats	Version of the displayed log. Prescribed values: • ["v1", "v2"]: all logs are displayed • ["v2"]: only v2 logs are displayed	String array	Mandatory
kinds	Log family to which the log belongs. Prescribed values: • *domain*: logs related to business operations performed by the KMaaS, • *http*: logs related to HTTP requests received and sent by the KMaaS, • *system*: logs related to system operations performed by the KMaaS.	String	Mandatory
severities	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.	String	Mandatory
errors	JSON object containing an error code and a message indicating why the proxy configuration could not be loaded. *Example:* *error: {* *code: 1005001,* *message: 'Validation failed ..."* *},*	Object	Mandatory

3.9 *tenant* category

This category of logs contains the configuration of the tenant and of the applications enabled on this tenant.

3.9.1 setup action On Prem Only

The *setup* action means that the configuration of the tenant was completed. It generates an "info" severity log in the event of success, or an "warning" 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
features	Names of the features enabled. Prescribed values: • *kacls* • *crypto_api* • *pki* • *kas*	String	Mandatory
errors	If a feature cannot be enabled due to an incorrect configuration, this JSON object contains an error list with an error code and a message: • If the severity level is "info", the error list is empty, the feature is enabled. • If the severity level is "err", the list contains at least one error. *Example: [* *{* *code: 2002010,* *message: 'Feature: Kas not enabled for tenantId bc337abd-0d4f-43f9-aaf6-54ef7268d2e5. Reason: Validation failed. Reasons are: [Wrong type error: <tenant>/kas/authentication property must be array]'* *}* *]*	String	Optional

3.10 *policy* category

This category of logs contains the configuration concerning the OPA policy enabled in a tenant and a feature.

3.10.1 setup action On Prem Only

The *setup* action means that a policy is correctly configured for a given tenant and feature. It generates an "info" severity log if it is successful, or an "err" 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
enable	Specify if the policy is enabled.	Boolean	Mandatory
engine	Prescribed value: • *opa*		Mandatory
type	Type of policy. Prescribed values: • *local* • *remote*	String	Mandatory
feature	Feature concerned by the policy. Prescribed values: • *kacls* • *crypto_api*	String	Mandatory
policy_uri	URL of the remote policy or file path of the local policy.	String	Mandatory
local_data_path	Path to the policy configuration file.	String	Mandatory if type is set to local and engine set to opa
authentication	Authentication type in case of a remote policy.	Object	Mandatory if type is set to remote and engine set to opa
error	If the policy cannot be enabled due to an incorrect configuration, this JSON object contains an error with an error code and a message. *Example: [* *{* *code: 2017004,* *message: "Unable to load policy'* *}* *]*	Object	Optional

3.10.2 Verify action

The *verify* action means that the OPA policy has been verified on the called API route. It generates an "info" severity log if the request was verified, even if the policy is not allowed. It generates an "err" severity log if it was not possible to verify the request.

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

Field	Description	Type	Mandatory/Optional
feature	Feature concerned by the policy. Prescribed values: • *kacls* • *crypto_api*	String	Mandatory
operation	API route concerned by the policy. Example: • *wrap* • *encrypt* ...	String	Mandatory
allow	Specify if the policy is allowed. Prescribed values: • *true* • *false*	Boolean	Mandatory

3.11 *kas* category

This category of logs contains all the business requests concerning the Key Access Management feature (KAS).

3.11.1 setup action On Prem Only

The *setup* action means that the KAS configuration is checked. It generates an "info" severity log if it is configured properly, or an "err" 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
enabled	Specify if the KAS feature is enabled.	Boolean	Mandatory

Field	Description	Type	Mandatory/Optional

errors	If the KAS feature cannot be enabled due to an incorrect configuration, this JSON object contains an error list with an error code and a message:
	• If the severity level is "info", the error list is empty, the KAS feature is enabled.
	• If the severity level is "err", the list contains at least one error.
	*Example: [
	{
	code: 2002010,
	message: 'Feature: Kas not enabled for tenantId bc337abd-0d4f-43f9-aaf6-54ef7268d2e5. Reason: Validation failed. Reasons are: [Wrong type error: <tenant>/kas/authentication property must be array]'
	}
	]*
		Object	Mandatory if enabled is set to true

3.11.2 rewrap action On Prem Only

The *rewrap* action means that a *rewrap* request has been made. This is the case whenever data is decrypted using Key Access Management.

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
kek_id	Identifier of the KEK used. Example: *ed7e4c13-6199-30a3-7bce-1c82a9e31e21*	String	Mandatory

3.11.3 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 Key Access Management.
- The *encrypt* action means that an *encrypt* request has been made. This is the case whenever data is decrypted using Key Access Management.

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
kek_id	Identifier of the KEK used. Example: *ed7e4c13-6199-30a3-7bce-1c82a9e31e21*	String	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: • kmaas	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: • kmaas • metrics	String	Mandatory
https: 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 *config.json* file.	String	Optional
privatekey_path	Path to the private key if specified in the *config.json* file.	String	Optional
certificate_path	Path to the certificate if specified in the *config.json* 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: • type: “rest_api” or “kmip” • kmip: (optional) information on the connection if KMIP - version: version of the KMIP used - supported_versions: version list • authentication: - ca: path to the certification authority file - cert: path to the certificate file - key: path to the private key file	json object	Mandatory
kms_version	KMS version.	String	Optional
domain_id	KMS domain ID used if connecting to the KMS with the REST API. It is not displayed if the root domain is used.	String in UUID v4 format	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 "notice" 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

Field	Description	Type	Mandatory/Optional
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
domain_id	KMS domain ID used if connecting to the KMS with the REST API. It is not displayed if the root domain is used.	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: *https://localhost:4000/static/one-login/.well-known/jwks.json*	String	Mandatory
type	Type of request made. Example: *http*	String	Mandatory
status	Request status Examples: *200*, *403*, *ECONNREFUSED*	String	Mandatory
method	Request method. Examples: *POST*, *GET*, *OPTIONS*	String	Mandatory

5. HTTP- HTTP request logs

The log fields described below relate to the HTTP requests managed by the Stormshield KMaaS. 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 Stormshield KMaaS.

5.1.1 receive action On Prem Only

The *receive* action means that an HTTP request has been received by the Stormshield KMaaS. 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: *https://localhost:4000/static/one-login/.well-known/jwks.json*	String	Mandatory
method	Request method. Examples: *POST*, *GET*, *OPTIONS*	String	Mandatory
remote_user_agent	Information about the request issuer contained in the request header. Example: *Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/27.0.1453 Safari/537.36*	String	Mandatory
remote_address	Address of request issuer. Example: *172.16.16.212*	String	Mandatory
content_length	Size of received request body, in bytes. Only present when body size is greater than zero.	Integer	Optional

STORMSHIELD