GUIDE

STORMSHIELD KEY MANAGEMENT AS A SERVICE

LOG GUIDE (V1 FORMAT)

Document last updated: October 16, 2025

Reference: sds-en-sds_kmaas-v1_log_guide

Table of contents

In the documentation, Stormshield Key Management as a service is referred to in its short form: Stormshield KMaaS.

This document is not exhaustive and minor changes may have been included in this version.

1. Getting started

The Stormshield KMaaS generates logs for every operation, making it possible to trace all operations performed and potential issues. Logs are generated in JSON format. In RPM mode, the logs are managed by the *systemd* service.

There are two different log formats:

- Refer to this guide for more information on logs in the old format.
- Refer to the to the *Stormshield KMaaS Log Guide* for more information on logs in the new format.

2. Logging requirements

Logging is a technical activity essential to the security of information systems. To meet the logging requirements for the Stormshield KMaaS, you must :

- Follow the security recommendations for logging systems issued by ANSSI in their document *ANSSI-PA-012*,
- Set up a partition dedicated to logs, with restricted access rights,
- Formalize and implement a log rotation policy for all logging system equipment.
- In Docker mode, follow the recommendations issued by ANSSI in their document ANSSI-FT-082 relating to Docker container deployment.

3. Accessing logs

3.1 In Docker mode

Access the logs of the Stormshield KMaaS by running the Docker standard command:

```
docker logs <containerID> -f
```

3.2 In RPM mode

Logs are stored in the *systemd* standard folder. The following commands can be used to show and export logs.

Command	Description
cat /var/log/messages	Shows all logs of all services.
journalctl -u cse	Shows all logs relating to the Stormshield KMaaS.
journalctl -u cse -b	Shows all logs relating to the Stormshield KMaaS since the last time the machine was started.
journalctl -u cse > cse.log	Exports all logs relating to the Stormshield KMaaS into a *cse.log* file.

4. Understanding the contents of logs

The Stormshield KMaaS generates two types of logs:

- Configuration logs, which provide information about the status and running of the Stormshield KMaaS. Such logs belong to either the *server_status*, *kmip_status*, or *kmip_decrypt* categories.
- API logs, which provide information on API calls to the Stormshield KMaaS. Such logs belong to the *api_route* category.

The following tables describe the fields for each log type.

In these tables:

- **JWT** means JSON web token,
- **KACLS** is the name that Google gives to the Stormshield KMaaS (i.e., Key Access Control List Service).

4.1 Generic log fields

The fields described in the table below appear in all Stormshield KMaaS logs.

Field	Type Description	Type	Examples
severity	Log severity: • *info*: standard severity used for most logs, • *warning*: indicates that the operation was successful but generated a warning, • *critical*: indicates that the operation ended in an error.	String	Prescribed values: "info", "warning", "critical"
kind	Log group to which the log belongs, for example: • domain: logs concerning Stormshield KMaaS business operations This field is only present in logs in the new format.	Character string	Prescribed values: "domain", "system"
category	Log category, for instance: • *server_status*: configuration log that provides information about the startup of the Stormshield KMaaS and its status, • *api_route*: log of the API that provides information about API routes (e.g., "/wrap").	String	Prescribed values: "server_status", "api_route", "kmip_status", "kmip_extract", "kek_reading", "policy_status", "jwks", "open_id", "keks", "kek"
action	Event that occurred, for instance for the "keks" category: • *setup*: KEK persistence and refresh mode has been configured. • *load*: A KEK retrieval has been triggered. This field is only present in logs in the new format.	Character string	
version	Current version of the service.	String	"4.3.0.2354"

Field	Type Description	Type	Examples
timestamp	Date and time at which the log was created. In ISO-8601 format.	String	"2021-03-05T16:53:28Z"
hostname	Host name.	String	"cseserver13"
process	Node.js worker PID.	Integer	4031
tenant_id	Tenant identifier.	String (uuid v4)	"025f02fe-bee2-444b-bf76-b5ead30327c0"
errors	Optional	Array	

4.2 Logs relating to the status of the service (start, stop, failure)

The fields described below belong to logs that contain errors which appear when the Stormshield KMaaS starts.

Field	Description	Type	Examples
name	Service name.	String	"Stormshield SDS CSE #13"
status	Server status.	String	Prescribed values: "started", "stopped", "failure"
host	Server address.	String	"172.16.16.240", "cse13.stormshield.eu"
port	Port on which the Stormshield KMaaS listens.	Integer	4333
persistence_type	Persistence mode of KEK data.	String	Prescribed values: "json_file", "kms"
https	Server startup mode: HTTP or HTTPS.	Boolean	Prescribed values: "true" (HTTPS), "false" (HTTP)
cache	Activation status of the cache.	Boolean	Prescribed values: "true", "false"
proxy	Information relating to the activation of the proxy It contains the information below:	Object	Mandatory
	proxy.enabled: Activation status of the proxy	Boolean	Prescribed values: "true", "false"
	proxy.https_url: URL used for the HTTP proxy	String	"http://myhttpsproxyurl"

4.3 Logs relating to configurations retrieved from the identity provider

The log fields described below provide information on the retrieval status of configurations. These logs are issued when the service is started.

These logs can be generated when data is retrieved from the application cache or when a request is made.

If you use *discoveryUri* to retrieve the identity provider configuration, the logs displayed will be as follows:

Field	Type Description	Type	Examples
category	Log category.	String	Prescribed value: "open_id"
status	Status of the request.	String	Prescribed values: "fetching", "unreachable", "fetch success"
discovery_uri	URI used for retrieving the configuration.	String	"https://localhost:3001/static/one-login/.well-known/openid-configuration"
token_type	Function of the token to retrieve.	String	Prescribed values: "authorization", "authentication"
role	Role associated with the token to retrieve.	String	Prescribed values: "user", "admin", "wrapprivatekey"
source	Source of the configuration used.	String	Prescribed values: "local_configuration", "remote_well_known_cse_configuration"

If you use *discoveryUri* to retrieve the identity provider configuration, the logs displayed will be as follows:

Field	Type Description	Type	Examples
category	Log category.	String	Prescribed value: "jwks"
status	Status of the request.	String	Prescribed values: "checking reachability", "unreachable", "reachable"
jwks_uri	JWKS used for retrieving the configuration.	String	"https://localhost:3001/static/one-login/.well-known/jwks.json"
token_type	Function of the token to retrieve.	String	Prescribed values: "authorization", "authentication"
role	Role associated with the token to retrieve.	String	Prescribed values: "user", "admin", "wrapprivatekey

4.4 Logs relating to KEK management

The log fields described below relate to KEK management.

4.4.1 *keks* category

connect action

The connect action means that a connection to the KMS in REST mode has been tested. It generates an "info" severity log. The fields in this log are as follows:

Field	Description	Examples
persistence_type	Mode used for storing KEKs.	"kms", "json_file"

auto_refresh	Information on automatic KEK refresh: enabled/disabled, and refresh frequency in seconds.	"auto_refresh": {
		"enabled": true,
		"interval_seconds":86400,
		}

resource	IP address of the KMS, or URI of the *keks.json* file where the KEKs are located.	"file:///etc/stormshield/cse/keks.json"

load action

The load action means that KEK retrieval has been triggered. It generates an "info" severity log. The fields in this log are as follows:

Field	Description	Examples
persistence_type	Mode used for storing KEKs.	"kms", "json_file"
resource	IP address of the KMS, or URI of the *keks.json* file where the KEKs are located.	"file:///etc/stormshield/cse/keks.json"
reason	Reason for triggering KEK retrieval. The possible values are: • "initialization" if the KEKs are loaded at application startup • "scheduled" if the KEKs are loaded following a scheduled refresh	

setup action

The setup action means that KEK refresh and KEK storing mode have been configured. It generates an "info" severity log. The fields in this log are as follows:

Field	Description	Examples
persistence_type	Mode used for storing KEKs.	"kms", "json_file"
resource	IP address of the KMS, or URI of the *keks.json* file where the KEKs are located.	"file:///etc/stormshield/cse/keks.json"

Field	Description	Examples

auto_refresh	Information about:
	• Periodic KEK refresh: enabled/disabled, and refresh frequency in seconds.
	• Minimum interval between two refresh operations, whether periodic or one-off.
		"auto_refresh": {
		"scheduled": {
		"enabled": true,
		"interval_seconds":86400
		}
		"minimum_interval_seconds": 1800
		}

4.4.2 *kek* category

load action

The load action means that a KEK has been loaded in the Stormshield KMaaS memory. It generates an "info" severity log. The fields in this log are as follows:

Field	Description	Examples
kek_id	Unique identifier of the KEK used.	"bbc9cd0b-803c-4d9c-93f9-b43bdfc0bf96"
is_active_kek	Indicates if the KEK is the active encryption key for the tenant. The possible values are "true" and "false".	
persistence_type	Mode used for storing KEKs.	"kms", "json_file"
resource	IP address of the KMS, or URI of the *keks.json* file where the KEKs are located.	"file:///etc/stormshield/cse/keks.json"

4.5 Logs relating to the retrieval of key encryption keys (KEKs)

The log fields described below provide information on the retrieval status of KEKs. These logs are shown when the service starts and when the KEKs are refreshed.

Field	Description	Type	Examples
kek_id	Identifier of the KEK used.	String	"bbc9cd0b-803c-4d9c-93f9-b43bdfc0bf96"
is_active_kek	Active KEK used for encryption.	String	Prescribed values: "true", "false"
source	Source of the KEK.	String	Prescribed values: "kms", "local"

4.6 Logs relating to the connection to the KMS

The log fields described below provide information on the connection to the key management system (KMS) and the status of key encryption key (KEK) extraction.

These logs vary according to the type of cryptographic backend used: KMS REST API, or the Stormshield KMaaS.

4.6.1 KMS REST API

kms category

connect action

The connect action means that a connection to the KMS in REST mode has been tested. It generates an "info" severity log if the KMS is reachable, or a "warning" log if the KMS is unreachable. The fields in this log are as follows:

Field	Description	Examples
context.ca	Path to the certification authority	/etc/stormshield/cse/ca_kms.pem
context.cert	Path to the KMS client certificate	/etc/stormshield/cse/cert_kms.pem
context.host	URL of the KMS	https://web.ciphertrustmanager
context.port	KMS port	443
context.current_version	KMS API version	2.2.1
context.minimum_version	Minimum version supported by the Stormshield KMaaS	2.2
context.status	Connection status	Prescribed values: "true", "false"

4.6.2 Stormshield KMaaS

These logs are shown when the service starts and when the KEKs are refreshed.

Field	Description	Type	Examples
host	KMS address	String	"https://10.1.1.24"
port	KMS port	Integer	"5696"
supported_version	List of KMIP protocol versions supported by the KMS on which the user is connected.	String	Prescribed values: ["1.4","1.3","1.2","1.1","1.0"]
kmip_version	Version of the KMIP protocol used	String	"1.4"
status	Status of KEK extraction	String	Prescribed values: "started","starting", "stopped", "failure"

4.7 Logs relating to the *health* API route

The fields described below belong to logs about the *health* API route. This route is used to check that the Stormshield KMaaS is operating correctly.

Field	Description	Type	Examples
api_route	Name of the API route. Here "/health".	String	Prescribed values: "/health", "/status", "/wrap", "/unwrap", "/privilegedunwrap", "/digest", "/rewrap"
user_agent	User agent used in the request.	String	"Chrome/27.0.1453.110"
source_address	Network traffic source (client requesting the connection).	String	"172.16.16.212"
http_status	HTTP response code that indicates the status of the request to the proxy.	Integer	"200", "404", "413", "500"
response_payload	Data relating to the HTTP response.	Object	
name	Server name.	String	"SDS CSE"

4.8 Logs relating to the *status* API route

The fields described below belong to logs about the *status* API route. This route makes it possible to get information on the Stormshield KMaaS installed.

Field	Description	Type	Examples
api_route	URL slug of the API route.	String	"/api/v1/{tenantId}/status"
user_agent	User agent used in the request.	String	"Chrome/27.0.1453.110"
source_address	Network traffic source (client requesting the connection).	String	"172.16.16.212"
http_status	HTTP response code that indicates the status of the request to the proxy.	Integer	"200", "405", "413", "500"
response_payload	Data relating to the HTTP response.	Object	
name	Server name.	String	"Preprod SDS CSE"
server_type	Server type.	String	"KACLS"
vendor_id	Vendor ID of the server.	String	"SDS_CSE"
operations_supported	Operations supported by the service.	Array	['wrap', 'unwrap', 'privilegedwrap', 'privilegedunwrap', 'digest', 'rewrap', 'privatekeysign', 'privatekeydecrypt', 'privilegedprivatekeydecrypt']

4.9 Logs relating to the *wrap* API route

The fields described below belong to logs about the *wrap* API route. This route enables key wrapping.

Field	Description	Type	Examples
api_route	URL slug of the API route.	String	"/api/v1/{tenantId}/wrap"
user_agent	User agent used in the request.	String	"Chrome/27.0.1453.110"
source_address	Network traffic source (client requesting the connection).	String	"172.16.16.212"
http_status	HTTP response code that indicates the status of the request to the proxy.	Integer	Prescribed values: "200", "400", "401", "405", "413", "415", "500"
request_payload	Data relating to the HTTP request.	Object	
reason	JSON string providing additional context about the operation.	String	"{client:'drive' op:'update'}"
authorization_token	JWT guaranteeing that the user is allowed to wrap a key for 'resource_name'. It contains the information below:	Object	
	email: e-mail address of the user that the authorization token concerns.	String	"alice@domain.eu"
	email_type: Origin of the user's email address. • google: Google accounts (default value), • google-visitor: account verified by Google, • customer-idp: IDP account.	String	
	role: role requested in the authorization token. Prescribed value: "writer"	String	
	resource_name: resource identifier.	String	"6Bhds6BhdRkqt3Rkqt36Bhd"
	perimeter_id: identifier to conduct verifications of authentication and authorization requests.	String	"s6Bhds6BhdRkqt3Rkqt3"
	kacls_url: URL of the KACLS.	String	"https://someserver.eu"
	iss: identifies the service that generates the JWT (issuer).	String	"www.google.com"
	aud: identifies the recipient of the JWT (audience).	String array	"s6BhdRkqt3"

Field	Description	Type	Examples
	exp: identifies the expiry time after which the JWT must no longer be accepted.	Integer (timestamp in seconds)	"1694617320"
	iat: identifies the date on which the JWT was created (issued at).	Integer (timestamp in seconds)	"1694617320"
authentication_ token	JWT generated by a third-party tool that guarantees the user's identity. It contains the information below:	Object	
	claims: standard user data provided by the IDP. • email: e-mail address of the user that the authentication token concerns. • google_email: email address of the Google account of the user that the authentication token concerns. • iss: identifies the service that generates the JWT (issuer). • aud: identifies the recipient of the JWT (audience). • exp: identifies the expiry time after which the JWT must no longer be accepted. • iat: identifies the date on which the JWT was created (issued at).	String String String array Integer (timestamp in seconds) Integer (timestamp in seconds)	"username@domain.eu" "www.onelogin.com" "s6BhdRkqt3" "1694617320" "1694617320"
	number_of_custom_claims: number of custom claims included in the authentication token.	Integer	2
additional_data	Additional data. It contains the information below:	Object	
	wrap_properties: data relating to the wrap operation.	Object	
	kek_id: identifier of the KEK used.	String	"bbc9cd0b-803c-4d9c-93f9-b43bdfc0bf96"
	version: Version of the wrap operation.	Integer	1
	mode: Mode used for the wrap operation. • persistence: Persistence mode used	Object String	"json_file"
	cse_version: version of the service during the wrap operation.	String	"1.0.23458"

Field	Description	Type	Examples
	authentication_mode: authentication mode used for the wrap operation.	String	"local-configuration", "admin-configuration", "cse-configuration"
	authentication_domain: domain used for authentication.	String	"domain.com"

4.10 Logs relating to the certs API route

The fields described below belong to logs concerning the certs API route. This route is called by another KACLS, as part of a migration or backup operation: it returns the KACLS public certificate.

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"
          }
    ]
```

4.11 Logs relating to the *unwrap* API route

The fields described below belong to logs about the *unwrap* API route. This route enables key unwrapping.

Field	Description	Type	Examples
api_route	URL slug of the API route.	String	"/api/v1/{tenantId}/unwrap"
user_agent	User agent used in the request.	String	"Chrome/27.0.1453.110"
source_address	Network traffic source (client requesting the connection).	String	"172.16.16.212"
http_status	HTTP response code that indicates the status of the request to the proxy.	Integer	Prescribed values: "200", "400","401", "405", "413", "415", "500"
request_payload	Data relating to the HTTP request.	Object	

Field	Description	Type	Examples
reason	JSON string providing additional context about the operation.	String	"{client:'drive' op:'update'}"
authorization_token	JWT attesting that the user is allowed to wrap a key for 'resource_name'. It contains the information below:	Object	
	email: e-mail address of the user that the authorization token concerns.	String	"alice@domain.eu"
	email_type: Origin of the user's email address. • google: Google accounts (default value), • google-visitor: account verified by Google, • customer-idp: IDP account.	String	
	role: role requested in the authorization token.	String	Prescribed values: "reader", "writer"
	resource_name: resource identifier.	String	"6Bhds6BhdRkqt3Rkqt36Bhd"
	perimeter_id: identifier to conduct verifications of authentication and authorization requests.	String	"s6Bhds6BhdRkqt3Rkqt3"
	kacls_url: URL of the KACLS.	String	"https://someserver.eu"
	iss: identifies the service that generates the JWT (issuer).	String	"www.google.com"
	aud: identifies the recipient of the JWT (audience).	String array	"s6BhdRkqt3"
	exp: identifies the expiry time after which the JWT must no longer be accepted.	Integer (timestamp in seconds)	"1694617320"
	iat: identifies the date on which the JWT was created (issued at).	Integer (timestamp in seconds)	"1694617320"
authentication_token	JWT generated by a third-party tool that guarantees the user's identity.	Object	

Field	Description	Type	Examples
	claims: standard user data provided by the IDP. • email: e-mail address of the user that the authentication token concerns. • google_email: email address of the Google account of the user that the authentication token concerns. • iss: identifies the service that generates the JWT (issuer). • aud: identifies the recipient of the JWT (audience). • exp: identifies the expiry time after which the JWT must no longer be accepted. • iat: identifies the date on which the JWT was created (issued at).	String String String array Integer (timestamp in seconds) Integer (timestamp in seconds)	"username@domain.eu" "www.onelogin.com" "s6BhdRkqt3" "1694617320" "1694617320"
	number_of_custom_claims: number of custom claims included in the authentication token.	Integer	2
additional_data	Additional data. It contains the information below:	Object	
	wrap_properties: data relating to the wrap operation.	Object	
	kek_id: identifier of the KEK used.	String	"bbc9cd0b-803c-4d9c-93f9-b43bdfc0bf96"
	version: version of the wrap operation.	Integer	1
	mode: mode used for the wrap operation. • persistence: persistence mode used	Object String	Prescribed values: "json_file"
	cse_version: version of the service during the wrap operation.	String	"1.0.23458"
	authentication_mode: authentication mode used for the wrap operation.	String	"local-configuration", "admin-configuration", "cse-configuration"
	authentication_domain: domain used for authentication.	String	"domain.com"

4.12 Logs relating to the *digest* API route

The fields described below belong to logs about the *digest* API route. Such routes make it possible to check whether the migration to another KACLS was successful.

Field	Description	Type	Examples
api_route	URL slug of the API route.	String	"/api/v1/{tenantId}/digest"
user_agent	User agent used in the request.	String	"Chrome/27.0.1453.110"
source_address	Network traffic source (client requesting the connection).	String	"172.16.16.212"
http_status	HTTP response code that indicates the status of the request to the proxy.	Integer	Prescribed values: "200", "400","401", "405", "413", "415", "500"
request_payload	Data relating to the HTTP request.	Object	
reason	JSON string providing additional context about the operation.	String	"{client:'drive' op:'update'}"
authorization_token	JWT attesting that the user is allowed to wrap a key for 'resource_name'. It contains the information below:	Object	
	email: e-mail address of the user that the authorization token concerns.	String	"alice@domain.eu"
	role: role requested in the authorization token.	String	Prescribed value: "check"
	resource_name: resource identifier.	String	"6Bhds6BhdRkqt3Rkqt36Bhd"
	kacls_url: URL of the KACLS.	String	"https://someserver.eu"
	iss: identifies the service that generates the JWT (issuer).	String	"www.google.com"
	aud: identifies the recipient of the JWT (audience).	String array	"s6BhdRkqt3"
	exp: identifies the expiry time after which the JWT must no longer be accepted.	Integer (timestamp in seconds)	"1694617320"
	iat: identifies the date on which the JWT was created (issued at).	Integer (timestamp in seconds)	"1694617320"
additional_data	Additional data. It contains the information below:	Object	
	wrap_properties: data relating to the wrap operation.	Object	
	kek_id: identifier of the KEK used.	String	"bbc9cd0b-803c-4d9c-93f9-b43bdfc0bf96"

Field	Description	Type	Examples
	version: version of the wrap operation.	Integer	1
	mode: mode used for the wrap operation. • persistence: persistence mode used	Object String	Prescribed values: "json_file"
	cse_version: version of the service during the wrap operation.	String	"1.0.23458"
	authentication_mode: authentication mode used for the wrap operation.	String	"local-configuration", "admin-configuration", "cse-configuration"
	authentication_domain: domain used for authentication.	String	"domain.com"

4.13 Logs relating to the *rewrap* API route

The fields described below belong to logs about the *rewrap* API route. Such routes make it possible to migrate from one KACLS to another.

Field	Description	Type	Examples
api_route	URL slug of the API route.	String	"/api/v1/{tenantId}/rewrap"
user_agent	User agent used in the request.	String	"Chrome/27.0.1453.110"
source_address	Network traffic source (client requesting the connection).	String	"172.16.16.212"
http_status	HTTP response code that indicates the status of the request to the proxy.	Integer	Prescribed values: "200", "400", "401", "405", "413", "415", "500"
request_payload	Data relating to the HTTP request.	Object	
reason	JSON string providing additional context about the operation.	String	"{client:'drive' op:'update'}"
authorization_token	JWT guaranteeing that the user is allowed to wrap a key for 'resource_name'. It contains the information below:	Object	
	email: e-mail address of the user that the authorization token concerns.	String	"alice@domain.eu"
	role: role requested in the authorization token.	String	Prescribed value: "migrator"
	resource_name: resource identifier.	String	"6Bhds6BhdRkqt3Rkqt36Bhd"
	kacls_url: URL of the KACLS.	String	"https://someserver.eu"

Field	Description	Type	Examples
	iss: identifies the service that generates the JWT (issuer).	String	"www.google.com"
	aud: identifies the recipient of the JWT (audience).	String array	"s6BhdRkqt3"
	exp: identifies the expiry time after which the JWT must no longer be accepted.	Integer (timestamp in seconds)	"1694617320"
	iat: identifies the date on which the JWT was created (issued at).	Integer (timestamp in seconds)	"1694617320"
authentication_token	JWT generated by a third-party tool that guarantees the user's identity. It contains the information below:	Object	
	claims: standard user data provided by the IDP. • email: e-mail address of the user that the authentication token concerns. • google_email: email address of the Google account of the user that the authentication token concerns. • iss: identifies the service that generates the JWT (issuer). • aud: identifies the recipient of the JWT (audience). • exp: identifies the expiry time after which the JWT must no longer be accepted. • iat: identifies the date on which the JWT was created (issued at).	String String String array Integer (timestamp in seconds) Integer (timestamp in seconds)	"username@domain.eu" "www.onelogin.com" "s6BhdRkqt3" "1694617320" "1694617320"
	number_of_custom_claims: number of custom claims included in the authentication token.	Integer	2
additional_data	Additional data. It contains the information below:	Object	
	wrap_properties: data relating to the wrap operation.	Object	
	kek_id: identifier of the KEK used.	String	"bbc9cd0b-803c-4d9c-93f9-b43bdfc0bf96"
	version: Version of the wrap operation.	Integer	1

Field	Description	Type	Examples
	mode: Mode used for the wrap operation. • persistence: Persistence mode used	Object String	"json_file"
	cse_version: version of the service during the wrap operation.	String	"1.0.23458"
	authentication_mode: authentication mode used for the wrap operation.	String	"local-configuration", "admin-configuration", "cse-configuration"
	authentication_domain: domain used for authentication.	String	"domain.com"

4.14 Logs relating to the *privilegedwrap* API route

The fields described below belong to logs about the *privilegedwrap* API route. This route allows the administrator to perform bulk file import.

Field	Description	Type	Example
api_route	URL slug of the API route.	String	"/api/v1/{tenantId}/privilegedwrap"
user_agent	User agent used in the request.	String	"Chrome/27.0.1453.110"
source_address	Network traffic source (client requesting the connection).	String	"172.16.16.212"
http_status	HTTP response code that indicates the status of the request to the proxy.	Integer	Prescribed values: "200", "400", "401", "405", "413", "415", "500"
request_payload	Data relating to the HTTP request.	Object	
reason	JSON string providing additional context about the operation.	String	"{client:'drive' op:'update'}"
authentication_token	JWT generated by a third-party tool that guarantees the user's identity. It contains the information below:	Object	
	claims: standard user data provided by the IDP. • email: e-mail address of the user that the authentication token concerns. • iss: identifies the service that generates the JWT (issuer). • aud: identifies the recipient of the JWT (audience). • exp: identifies the expiry time after which the JWT must no longer be accepted. • iat: identifies the date on which the JWT was created (issued at).	String String String array Integer (timestamp in seconds) Integer (timestamp in seconds)	"username@domain.eu" "www.onelogin.com" "s6BhdRkqt3" "1694617320" "1694617320"
	number_of_custom_claims: number of custom claims included in the authentication token.	Integer	2
additional_data	Additional data. It contains the information below:	Object	
	wrap_properties: data relating to the wrap operation.	Object	
	kek_id: identifier of the KEK used.	String	"bbc9cd0b-803c-4d9c-93f9-b43bdfc0bf96"

Field	Description	Type	Example
	version: version of the wrap operation.	Integer	1
	mode: mode used for the wrap operation. • persistence: persistence mode used	Object String	"json_file"
	cse_version: version of the service during the wrap operation.	String	"1.0.23458"
	authentication_mode: authentication mode used for the wrap operation.	String	"local-configuration", "admin-configuration", "cse-configuration"
	authentication_domain: domain used for authentication.	String	"domain.com"

4.15 Logs relating to the *privilegedunwrap* API route

The fields described below belong to logs about the *privilegedunwrap* API route. This route allows:

- An administrator to decrypt exported user data with the *decrypter.exe* Google utility,
- An encryption service to migrate data from another KACLS to itself.

Field	Description	Type	Examples
api_route	URL slug of the API route.	String	"/api/v1/{tenantId}/privilegedunwrap"
user_agent	User agent used in the request.	String	"Chrome/27.0.1453.110"
source_address	Network traffic source (client requesting the connection).	String	"172.16.16.212"
http_status	HTTP response code that indicates the status of the request to the proxy.	Integer	Prescribed values: "200", "400", "401", "405", "413", "415","500"
request_payload	Data relating to the HTTP request.	Object	
reason	JSON string providing additional context about the operation.	String	"{client:'drive' op:'update'}" In a migration, the value is set: "KACLS migration"
resource_name	Resource identifier.	String	"6Bhds6BhdRkqt3Rkqt36Bhd"
authentication_token	JWT generated by a third-party tool that guarantees the user's identity. It contains the information below:	Object	

Field	Description	Type	Examples
	Only for user use cases email: e-mail address of the user that the authentication token concerns.	String	"alice@domain.eu"
	Only for migration use cases kaclsUrl: URL of the KACLS that initiates the privileged unwrap request.	String	"https://cse.mysds.io/api/v1/0995624d-13f5-40a9-9c59-fee6fe3ef3f4"
	iss: identifies the service that generates the JWT (issuer).	String	URL of the issuing KACLS
	aud: identifies the recipient of the JWT (audience).	String array	In a migration, the value is set: "kacls-migration"
	exp: identifies the expiry time after which the JWT must no longer be accepted.	Integer (timestamp in seconds)	"1694617320"
	iat: identifies the date on which the JWT was created (issued at).	Integer (timestamp in seconds)	"1694617320"
additional_data	Additional data. It contains the information below:	Object	
	wrap_properties: data relating to the wrap operation.	Object	
	kek_id: identifier of the KEK used.	String	"bbc9cd0b-803c-4d9c-93f9-b43bdfc0bf96"
	version: version of the wrap operation.	Integer	1
	mode: mode used for the wrap operation. • persistence: persistence mode used (*none*)	String	Prescribed values: • *kms* or *json file* for persistence
	cse_version: version of the service during the wrap operation.	String	"1.0.23458"
	authentication_mode: authentication mode used for the wrap operation.	String	"local-configuration", "admin-configuration", "cse-configuration" In a migration, the value is set: "migration"
	authentication_domain: domain used for authentication.	String	"domain.com"

4.16 Logs relating to the *wrapprivatekey* API route

The fields described below belong to logs about the *wrapprivatekey* API route. This internal route makes it possible for Stormshield to encrypt user keys for Gmail. It is never called by Google.

Field	Description	Type	Example
api_route	URL slug of the API route.	String	"/api/v1/{tenantId}/wrapprivatekey"
user_agent	User agent used in the request.	String	"Chrome/27.0.1453.110"
source_address	Network traffic source (client requesting the connection).	String	"172.16.16.212"
http_status	HTTP response code that indicates the status of the request to the proxy.	Integer	Prescribed values: "200", "400", "401", "405", "413", "415", "500"
request_payload	Data relating to the HTTP request.	Object	
authentication_token	JWT generated by a third-party tool that guarantees the user's identity. It contains the information below:	Object	
	claims: standard user data provided by the IDP. • email: e-mail address of the user that the authentication token concerns. • iss: identifies the service that generates the JWT (issuer). • aud: identifies the recipient of the JWT (audience). • exp: identifies the expiry time after which the JWT must no longer be accepted. • iat: identifies the date on which the JWT was created (issued at).	String String String array Integer (timestamp in seconds) Integer (timestamp in seconds)	"username@domain.eu" "www.onelogin.com" "s6BhdRkqt3" "1694617320" "1694617320"
	number_of_custom_claims: number of custom claims included in the authentication token.	Integer	2
additional_data	Additional data. It contains the information below:	Object	
	wrap_properties: data relating to the wrap operation.	Object	
	kek_id: identifier of the KEK used.	String	"80c65a46-33db-4f26-bfe3-cefbbb4f16d8"

Field	Description	Type	Example
	version: version of the wrap operation.	Integer	1
	mode: Mode used for the wrap operation. • persistence: Persistence mode used	Object String	"json_file", "kms""
	cse_version: version of the service during the wrap operation.	String	"4.1.1637-0.2.beta"
	supported_algorithms: encryption and signature algorithms used with this key.	String array	["RSA/ECB/PKCS1Padding", "RSA/ECB/OAEPwithSHA-1andMGF1Padding","RSA/ECB/OAEPwithSHA-256andMGF1Padding","RSA/ECB/OAEPwithSHA-512andMGF1Padding","SHA1withRSA","SHA256withRSA","SHA512withRSA","SHA1withRSA/PSS","SHA256withRSA/PSS","SHA512withRSA/PSS"]

4.17 Logs relating to the *privatekeysign* API route

The fields described below belong to logs concerning the *privatekeysign* API route. Google calls up this route when it encrypts and sends encrypted emails.

Field	Description	Type	Example
api_route	URL slug of the API route.	String	"/api/v1/{tenantId}/privatekeysign"
user_agent	User agent used in the request.	String	"Chrome/27.0.1453.110"
source_address	Network traffic source (client requesting the connection).	String	"172.16.16.212"
http_status	HTTP response code that indicates the status of the request to the proxy.	Integer	Prescribed values: "200", "400", "401", "405", "413", "415", "500"
request_payload	Data relating to the HTTP request.	Object	
reason	JSON string providing additional context about the operation.	String	"sign email"
authorization_token	JWT guaranteeing that the user is allowed to wrap a key for 'resource_name'. It contains the information below:	Object	
	email: e-mail address of the user that the authorization token concerns.	String	"username@domain.eu"
	role: role requested in the authorization token.	String	Prescribed value: "signer"
	resource_name: resource identifier.	String	"6Bhds6BhdRkqt3Rkqt36Bhd"
	perimeter_id: identifier to conduct verifications of authentication and authorization requests.	String	"s6Bhds6BhdRkqt3Rkqt3"
	kacls_url: URL of the KACLS.	String	"https://someserver.eu"
	iss: identifies the service that generates the JWT (issuer).	String	"gsuitecse-tokenissuer-gmail@system.gserviceaccount.com"
	aud: identifies the recipient of the JWT (audience).	String array	"cse-authorization"
	exp: identifies the expiry time after which the JWT must no longer be accepted.	Integer (timestamp in seconds)	"1694617320"
	iat: identifies the date on which the JWT was created (issued at).	Integer (timestamp in seconds)	"1694617320"
	spki_hash: digest of the private key in Base64.	String	"saEz24IohD0HIGjddhscQsdjCQfFBqNHs1crLUE+Kt4="

Field	Description	Type	Example
	spki_hash_algorithm: encryption algorithm used	String	"SHA-256"
	message_id: optional ID of the message to which the signature applies.	String	
authentication_token	JWT generated by a third-party tool that guarantees the user's identity. It contains the information below:	Object	
	claims: standard user data provided by the IDP. • email: e-mail address of the user that the authentication token concerns. • google_email: email address of the Google account of the user that the authentication token concerns. • iss: identifies the service that generates the JWT (issuer). • aud: identifies the recipient of the JWT (audience). • exp: identifies the expiry time after which the JWT must no longer be accepted. • iat: identifies the date on which the JWT was created (issued at).	String String String array Integer (timestamp in seconds) Integer (timestamp in seconds)	"username@domain.eu" "www.onelogin.com" "s6BhdRkqt3" "1694617320" "1694617320"
	number_of_custom_claims: number of custom claims included in the authentication token.	Integer	2
additional_data	Additional data. It contains the information below:	Object	
	wrap_properties: data relating to the wrap operation.	Object	
	kek_id: identifier of the KEK used.	String	"80c65a46-33db-4f26-bfe3-cefbbb4f16k8"
	version: version of the wrap operation.	Integer	"2"
	mode: Mode used for the wrap operation. • persistence: Persistence mode used	Object String	"json_file", "kms"

Field	Description	Type	Example
	cse_version: version of the service during the wrap operation.	String	"4.1.1637-0.2.beta"
	key_name : name of the private key used by the KMS to sign in 'kms' mode.	String	38cf0196-1fbf-11ee-be56-0242ac120002
	crypto_mode: type of cryptographic backend used to decrypt session keys.	String	"kms" or "node"
	supported_algorithms: encryption and signature algorithms used with this key.	String array	["RSA/ECB/PKCS1Padding","RSA/ECB/OAEPwithSHA-1andMGF1Padding","RSA/ECB/OAEPwithSHA-256andMGF1Padding","RSA/ECB/OAEPwithSHA-512andMGF1Padding","SHA1withRSA","SHA256withRSA","SHA512withRSA","SHA1withRSA/PSS","SHA256withRSA/PSS","SHA512withRSA/PSS"]

4.18 Logs relating to the *privatekeydecrypt* API route

The fields described below belong to logs about the *privatekeydecrypt* API route. Google calls up this route when it decrypts an encrypted email.

	Description	Type	
api_route	URL slug of the API route.	String	"/api/v1/{tenantId}/privatekeydecrypt"
user_agent	User agent used in the request.	String	"Chrome/27.0.1453.110"
source_address	Network traffic source (client requesting the connection).	String	"172.16.16.212"
http_status	HTTP response code that indicates the status of the request to the proxy.	Integer	Prescribed values: "200", "400", "401", "405", "413", "415", "500"
request_payload	Data relating to the HTTP request.	Object	
reason	JSON string providing additional context about the operation.	String	"unpack request"
authorization_token	JWT guaranteeing that the user is allowed to wrap a key for 'resource_name'. It contains the information below:	Object	
	email: e-mail address of the user that the authorization token concerns.	String	"username@domain.eu"
	role: role requested in the authorization token.	String	Prescribed value: "decrypter"
	resource_name: resource identifier.	String	"6Bhds6BhdRkqt3Rkqt36Bhd"
	perimeter_id: identifier to conduct verifications of authentication and authorization requests.	String	"s6Bhds6BhdRkqt3Rkqt3"
	kacls_url: URL of the KACLS.	String	"https://someserver.eu"
	iss: identifies the service that generates the JWT (issuer).	String	"gsuitecse-tokenissuer-gmail@system.gserviceaccount.com"
	aud: identifies the recipient of the JWT (audience).	String array	"cse-authorization"
	exp: identifies the expiry time after which the JWT must no longer be accepted.	Integer (timestamp in seconds)	"1694617320"
	iat: identifies the date on which the JWT was created (issued at).	Integer (timestamp in seconds)	"1694617320"

	Description	Type	
	spki_hash: hash of the private key in Base64.	String	"saEz24lohDOHIGjddhscQsdjCQfFBqNHs1crLUE+Kt4="
	spki_hash_algorithm: algorithm used to produce the spki_hash hash.	String	"SHA-256"
	message_id: optional ID of the message to which the signature applies.	String	
authentication_token	JWT generated by a third-party tool that guarantees the user's identity. It contains the information below:	Object	
	claims: standard user data provided by the IDP. • email: email address of the user that the authentication token concerns. • google_email: email address of the Google account of the user that the authentication token concerns. • iss: identifies the service that generates the JWT (issuer). • aud: identifies the recipient of the JWT (audience). • exp: identifies the expiry time after which the JWT must no longer be accepted. • iat: identifies the date on which the JWT was created (issued at).	String String String array Integer (timestamp in seconds) Integer (timestamp in seconds)	"username@domain.eu" "www.onelogin.com" "s6BhdRkqt3" "1694617320" "1694617320"
	number_of_custom_claims: number of custom claims included in the authentication token.	Integer	2
additional_data	Additional data. It contains the information below:	Object	
	wrap_properties: data relating to the wrap operation.	Object	
	kek_id: identifier of the KEK used.	String	"80c65a46-33db-4f26-bfe3-cefbbb4f16d8"
	version: version of the wrap operation.	Integer	1

	Description	Type	
	mode: mode used for the wrap operation. • persistence: persistence mode used	Object String	 "json_file", "kms""
	cse_version: version of the service during the wrap operation.	String	"4.1.1637-0.2.beta"
	key_name : name of the public key used by the KMS to sign in 'kms' mode.	String	38cf0196-1fbf-11ee-be56-0242ac120002div>
	crypto_mode: type of cryptographic backend used to decrypt session keys.	String	"kms" or "node"
	supported_algorithms: encryption and signature algorithms used with this key.	String array	["RSA/ECB/PKCS1Padding","RSA/ECB/OAEPwithSHA-1andMGF1Padding","RSA/ECB/OAEPwithSHA-256andMGF1Padding","RSA/ECB/OAEPwithSHA-512andMGF1Padding","SHA1withRSA","SHA256withRSA","SHA512withRSA","SHA1withRSA/PSS","SHA256withRSA/PSS","SHA512withRSA/PSS"]

4.19 Logs relating to the *privilegedprivatekeydecrypt* API route

The fields described below belong to logs concerning the *privilegedprivatekeydecrypt* API route. A Google administrator calls up this privileged route to decrypt an encrypted email, for example via the Google *decrypter.exe* utility.

Field	Description	Type	Example
api_route	URL slug of the API route.	String	"/api/v1 {tenantId}/privilegedprivatekeydecrypt"
user_agent	User agent used in the request.	String	"Chrome/27.0.1453.110"
source_address	Network traffic source (client requesting the connection).	String	"172.16.16.212"
http_status	HTTP response code that indicates the status of the request to the proxy.	Integer	Prescribed values: "200", "400", "401", "405", "413", "415", "500"
request_payload	Data relating to the HTTP request.	Object	
reason	JSON string providing additional context about the operation.	String	"Command-line decrypter"
authentication_token	JWT generated by a third-party tool that guarantees the user's identity. It contains the information below:	Object	
	claims: standard user data provided by the IDP. • email: e-mail address of the user that the authentication token concerns. • google_email: email address of the Google account of the user that the authentication token concerns. • iss: identifies the service that generates the JWT (issuer). • aud: identifies the recipient of the JWT (audience). • exp: identifies the expiry time after which the JWT must no longer be accepted. • iat: identifies the date on which the JWT was created (issued at).	String String String array Integer (timestamp in seconds) Integer (timestamp in seconds)	"username@domain.eu" "www.onelogin.com" "s6BhdRkqt3" "1694617320" "1694617320"
	number_of_custom_claims: number of custom claims included in the authentication token.	Integer	2
additional_data	Additional data. It contains the information below:	Object	

Field	Description	Type	Example
	wrap_properties: data relating to the wrap operation.	Object	
	kek_id: identifier of the KEK used.	String	"80c65a46-33db-4f26-bfe3-cefbbb4f16d8"
	version: version of the wrap operation.	Integer	1
	mode: mode used for the wrap operation. • persistence: persistence mode used	Object String	"json_file", "kms""
	cse_version: version of the service during the wrap operation.	String	"4.1.1637-0.2.beta"
	key_name : name of the private key used by the KMS to sign in 'kms' mode.	String	38cf0196-1fbf-11ee-be56-0242ac120002div>
	crypto_mode: type of cryptographic backend used to decrypt session keys.	String	"kms" or "node"
	supported_algorithms: encryption and signature algorithms used with this key.	String array	["RSA/ECB/PKCS1Padding", "RSA/ECB/OAEPwithSHA-1andMGF1Padding","RSA/ECB/OAEPwithSHA-256andMGF1Padding","RSA/ECB/OAEPwithSHA-512andMGF1Padding","SHA1withRSA","SHA256withRSA","SHA1withRSA/PSS","SHA256withRSA/PSS","SHA512withRSA/PSS"]

4.20 Logs relating to the application of an OPA policy

The log fields described below relate to the application of an OPA policy. For more information, see the section Customizing authorization rules of the *Administration Guide*.

The *policy.wasm* and *policy.data.json* files are optional. If one of the files is not present, the service starts and no policies are applied. A log is issued to indicate that the policy is disabled.

Field	Description	Type	Examples
status	Status of the policy.	String	Prescribed values: "enabled", "disabled", "loading"
loadingFile	File is being loaded.	String	Prescribed values: "policy", "data"
type	Type of the applied policy.	String	Prescribed value: "opa"

5. Further reading

Additional information and answers to questions you may have about Stormshield KMaaS are available on the Documentation website and in the Stormshield knowledge base (authentication required).

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