GUIDE

SDS ENCRYPTION SERVICE FOR GOOGLE WORKSPACE

SAAS DEPLOYMENT GUIDE

Document last updated: October 8, 2024

Reference: sds-en-sds_for_gw-saas_deployment_guide

Table of contents

In the documentation, SDS encryption service for Google Workspace is referred to in its short form: SDS encryption service for Google Workspace.

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

1. Getting started

The SDS encryption service for Google Workspace is a solution in which corporate data managed in the Google Workspace ecosystem can be protected, edited and consulted. Google Workspace is Google's cloud-based application suite for professionals. For more information, refer to the Google Workspace documentation.

The SDS encryption service for Google Workspace relies on Google Client Side Encryption (CSE), the end-to-end encryption method that Google offers for its Google Workspace applications. CSE is configured in the Google administration console. This technology is available only on Chrome browsers. For more information, refer to the Google Client Side Encryption documentation.

Google generates DEKs (Data Encryption Keys) to encrypt files. These keys are also encrypted by the SDS encryption service for Google Workspace using KEKs (Key Encryption Key) before being stored on the Google servers. For more information, refer to the Google documentation on encryption operation.

The SDS encryption service for Google Workspace is installed in your Cloud infrastructure: KEKs are never transmitted to the Google servers.

Before performing cryptographic operations, the SDS encryption service for Google Workspace first conducts a double check:

- Authentication: checks the identity of the user requesting the operation,
- Authorization: checks the user's access privileges for the file to encrypt/decrypt.

The SDS encryption service for Google Workspace generates logs for all the operations that it performs.

NOTE
The use of the solution in any way other than as described in the documentation is not managed. Alternatively, get in touch with Stormshield Support for clarification.

This guide describes how to deploy the SDS encryption service for Google Workspace as an SaaS solution. To implement the solution on site, contact your commercial referent Stormshield.

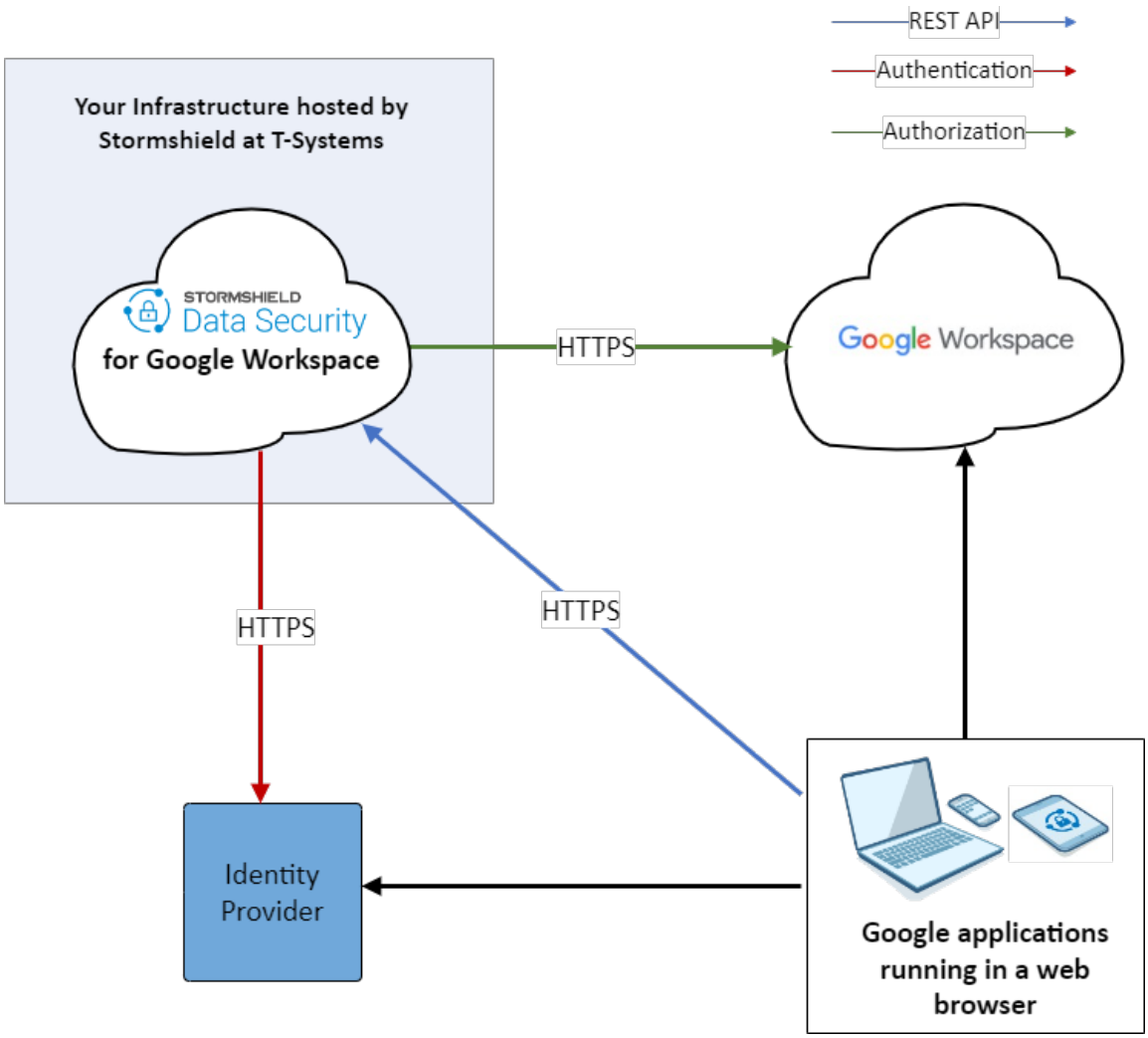
2. Understanding the requirements

The following components must be implemented in your environment to use the SDS encryption service for Google Workspace:

- A Google domain and a Google Workspace tenant both operational,
- The Client Side Encryption (CSE) feature activated on the Google Workspace tenant. It is compatible only with Google Enterprise Plus and Google Education. For more information, refer to the Google documentation.
- An identity provider (IdP) to authenticate end users. The SDS encryption service for Google Workspace is compatible with Google Identity and IdP solutions based on the OpenID protocol. Only Google Identity is mentioned in this document.
- An administrator account of the Google domain is necessary to perform the configuration operations in the Google administration console and the GCP console.
- A Stormshield account of which you must enter the information in the https://mysds.io/en/ page. For any question regarding this form, contact your Stormshield sales representative.

3. Understanding the architecture

The following diagram describes the different components of the architecture of the SDS encryption service for Google Workspace.



4. Understanding access to the data

The following table lists the different types of data in the infrastructure of the SDS encryption service for Google Workspace and indicates whether they are accessible by Stormshield and Google.

Data type	Accessible by Stormshield	Accessible in Google Chrome	Accessible in Google Workspace (GCP)
Encrypted user data by a DEK	✗	✓	✓
DEK	✓	✓	✗
DEK encrypted by a KEK	✓	✓	✓
KEK	✓	✗	✗
IDP configuration	✓	✓	✓

For more information on the definition of the DEK and KEK acronyms, refer to the Getting started section and the Google documentation on encryption operation.

5. Configuring the identity provider

The SDS encryption service for Google Workspace uses an identity provider (IdP) to authenticate end users, manage their access and life cycle. It is compatible with Google Identity and third party identity providers based on the OpenID protocol.

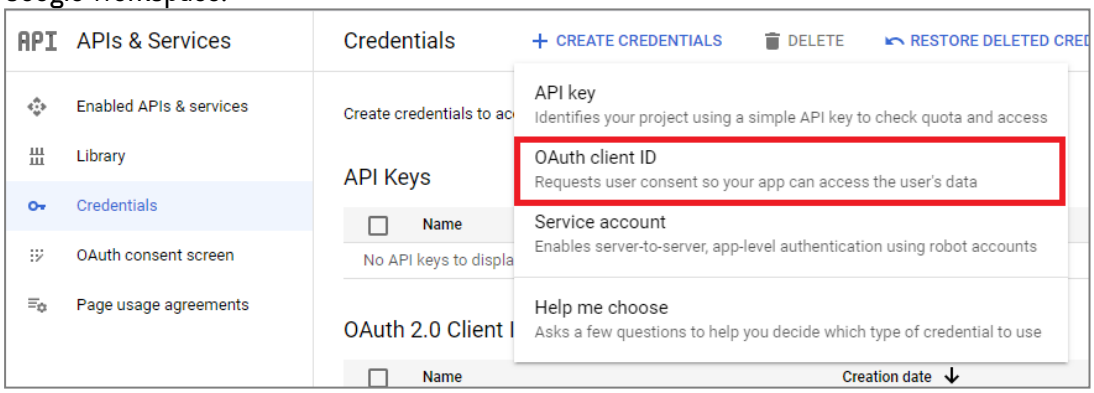
The following procedure describes the configuration with Google Identity. For more information, refer to the Google documentation.

When using a third party IdP, get the client ID from the SDS encryption service for Google Workspace. Refer to the documentation of your IdP.

To provide your external guest users with access to your encrypted content, you must create a specific IdP to authenticate them. For more information, refer to the Google documentation on configuring a guest IdP for al external users.

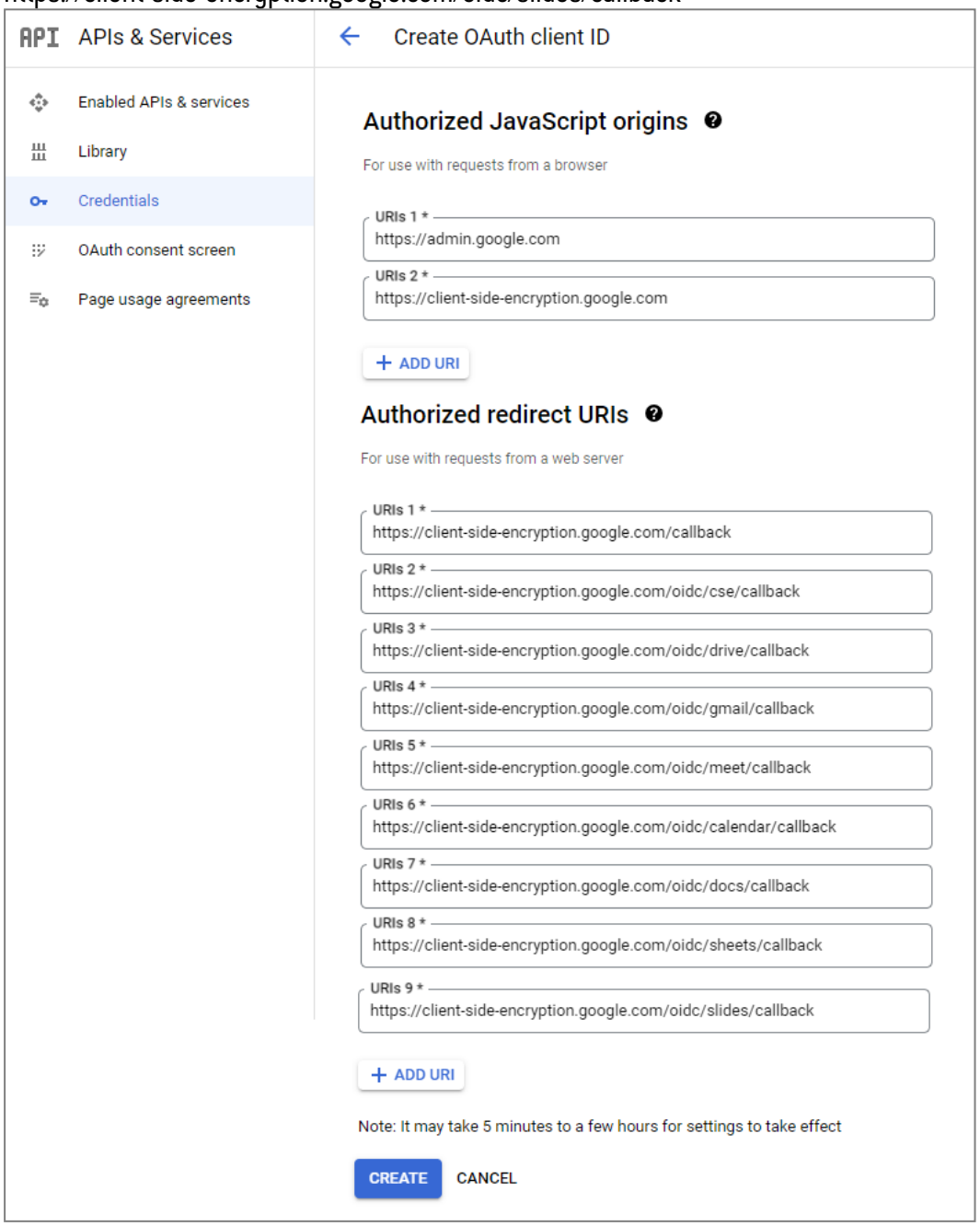
5.1 Creating a client ID for web applications

1. Log into the Google Cloud Platform using an administrator account.
2. Create a new project by specifying a project name and the organization it is connected to.
3. In the **APIs and services** > **Credentials** pane, click **Create credentials** > **OAuth client ID** to create a credential for the new application to be used with the SDS encryption service for Google Workspace.



4. Click **Configure the consent screen**, then choose the **Internal User type**.
5. Click on **Create**.
6. In the **Edit app registration** pane, enter the parameters, then click on **Save and continue**. You do not need to configure the scopes or the Google API library, as you only wish to get a credential to configure the IdP section on the Google administration console.
7. Click **Create credentials** > **OAuth client ID** again, and in the **Application type** field, choose **Web application**.
8. Enter a **Name**, for example the name of the project.
9. In the **Authorized Javascript origins** area, enter the HTTP origins hosting your application:
   - https://admin.google.com
   - https://client-side-encryption.google.com

10. In the **Authorized redirect URIs** area, enter the paths the users are redirected to after Google authentication:
    - https://client-side-encryption.google.com/callback
    - https://client-side-encryption.google.com/oidc/cse/callback
    - https://client-side-encryption.google.com/oidc/drive/callback
    - https://client-side-encryption.google.com/oidc/gmail/callback
    - https://client-side-encryption.google.com/oidc/meet/callback
    - https://client-side-encryption.google.com/oidc/calendar/callback
    - https://client-side-encryption.google.com/oidc/docs/callback
      https://client-side-encryption.google.com/oidc/sheets/callback
    - https://client-side-encryption.google.com/oidc/slides/callback



11. Click on **Create**.
    The OAuth client is created. You can get its ID and download the corresponding JSON.

5.2 Creating a client ID for mobile apps and Drive for desktop

For Drive, Calendar and Meet mobile applications, as well as Google Drive for desktop, the Client IDs are as follows:

- Drive for desktop:
  947318989803-k88lapdik9bledfml8rr69ic6d3rdv57.apps.googleusercontent.com,
- Drive on Android:
  313892590415-6lbccuf47cou4q45vanraqp3fv5jt9do.apps.googleusercontent.com,
- Drive on iOS:
  313892590415-d3h1l7kl4htab916r6jevqdtu8bfmh9m.apps.googleusercontent.com,
- Calendar on Android:
  313892590415-q84luo8fon5pn5vl8a6rppo1qvcd3qvn.apps.googleusercontent.com,
- Calendar on iOS:
  313892590415-283b3nilr8561tedgu1n4dcm9hd6g3hr.apps.googleusercontent.com,
- Meet on Android:
  313892590415-i06v47su4k03ns7ot38akv7s9ari5oa5.apps.googleusercontent.com,
- Meet on iOS:
  313892590415-32ha2bvs0tr1b12s089i33o58hjvqt55.apps.googleusercontent.com.

6. Connect to the identity provider

There are two options to authenticate users via the identity provider (IdP), as described in the Google Documentation **Choose how to connect to your IdP for CSE:**

- Via a .well-known file,
- Via the Google Workspace administration console.

Use the .well-known file option whenever possible. It allows you to update your configuration without Stormshield intervention.

6.1 Connect to the identity provider via a .well-known file

Place a *.well-known/cse-configuration* file in your company's public website, at the domain root. This file identifies the IdP used and provides your external users with your IdP parameters.

For the Google identity provider, the file content is as follows:

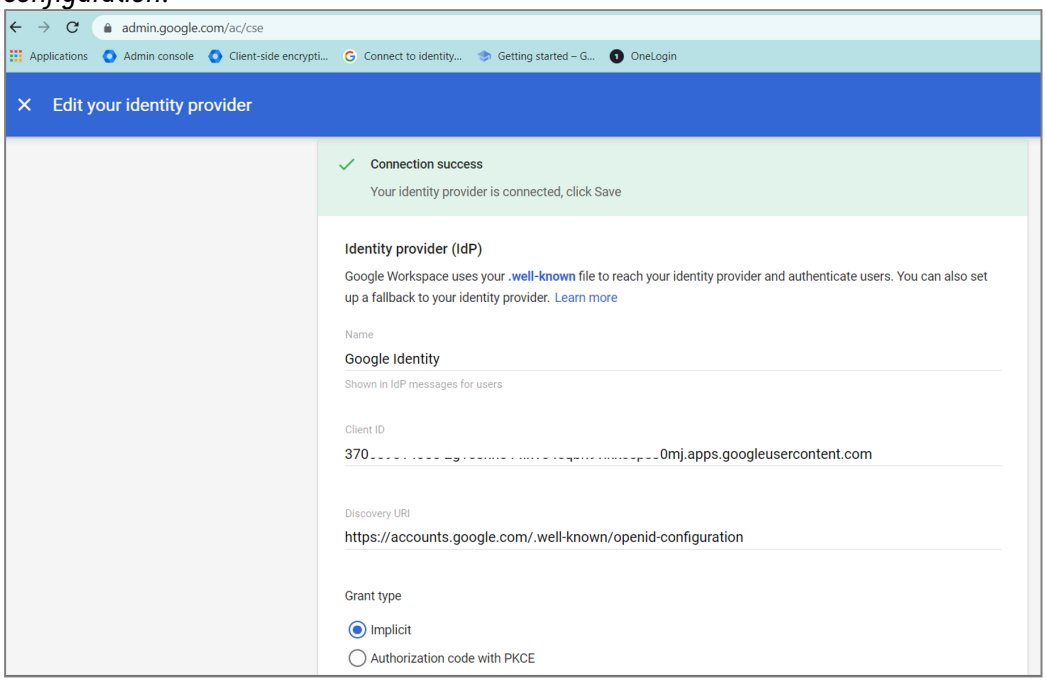
```
{
"name": https://accounts.google.com
"client_id": "37*********",
"discovery_uri": "https://accounts.google.com/.well-known/openid-configuration"
}
```

For more information, go to the *Using remote authentication* section of the *Administration guide* of the SDS encryption service for Google Workspace.

6.2 Connect to the identity provider via the administration console

1. Log into the Google administration console as a super-administrator.
2. Choose the **Security > Access and data control > Client side encryption** menu.

3. Configure the identity provider by entering the information relative to your IdP.
Name: Name of your choice,
Client ID: OAuth client ID you created in your Google Cloud Platform project,
Discovery URI: For Google Identity, it is *https://accounts.google.com/.well-known/openid-configuration*.

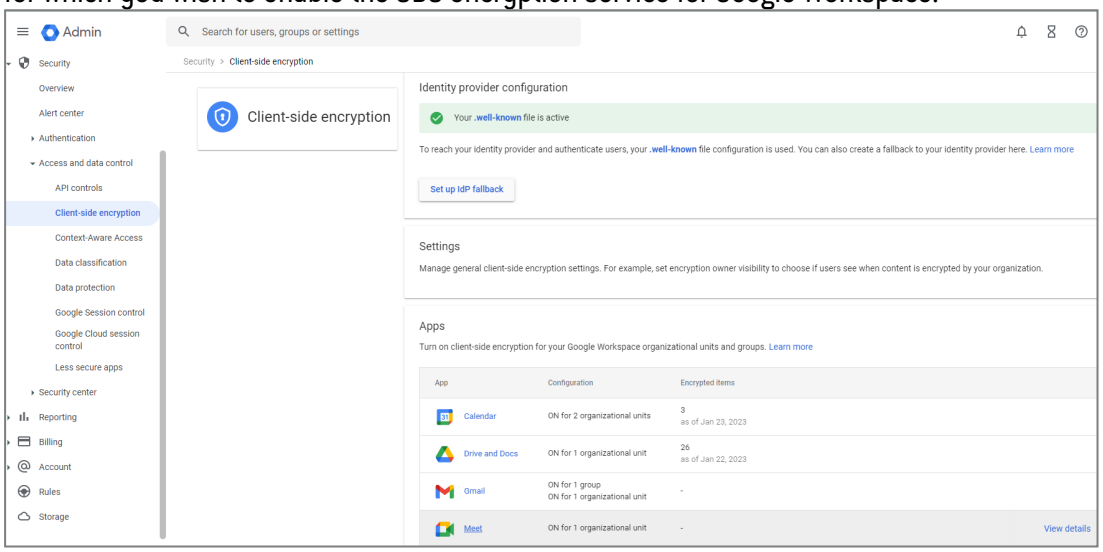


4. Send your IdP information to Stormshield so that we can complete the configuration.

7. Enabling encryption for Google Drive, Meet and Calendar

To allow the users to encrypt Google Drive, Meet and Calendar services, you must enable SDS encryption service for Google Workspace in the Google administration console.

1. Log into the Google administration console as a super-administrator.
2. Choose the **Security > Access and data control > Client side encryption** menu.
3. In the **Apps** section, for each Google service, select the organizational unit (OU) or the group for which you wish to enable the SDS encryption service for Google Workspace.



NOTE
Google's Client Side Encryption feature has limitations for Drive, as well as for the mobile version of Meet and Calendar. For more information, refer to the Google documentation.

8. Configuring encryption for Gmail

To configure and enable encryption for Gmail, refer to the Google Documentation.

To help you in implementing encryption for Gmail, Stormshield develops a solution allowing encryption and signature keys to be managed: Stormshield Orchestrator. For more information on the availability of this solution, contact your Stormshield sales representative, then fill in this form.

STORMSHIELD