GUIDE

SERVICE DE CHIFFREMENT SDS POUR GOOGLE WORKSPACE

GUIDE DE DÉPLOIEMENT SAAS

Dernière mise à jour du document : 8 octobre 2024

Référence : sds-fr-sds-for-gw-guide_de_déploiement_saas

Table des matières

Ce document n'est pas exhaustif et d'autres modifications mineures ont pu être incluses dans cette version.

1. Avant de commencer

Le service de chiffrement SDS pour Google Workspace est une solution de protection, d'édition et de consultation des données de l'entreprise gérées dans l'écosystème de Google Workspace. Google Workspace est la suite d'applications Google dans le cloud destinée aux professionnels. Pour plus d'informations, reportez-vous à la documentation Google Workspace.

Le service de chiffrement SDS pour Google Workspace s'appuie sur Google Client Side Encryption (CSE), la méthode de chiffrement de bout en bout proposée par Google pour ses applications Google Workspace. La configuration s'effectue dans la console d'administration Google. Cette technologie est disponible uniquement pour le navigateur Chrome. Pour plus d'informations, reportez-vous à la documentation Google Client Side Encryption.

Google génère des clés DEK (Data Encryption Key) pour chiffrer les fichiers. Ces clés sont elles-même chiffrées par le service de chiffrement SDS pour Google Workspace au moyen de clés KEK (Key Encryption Key) avant d'être stockées sur les serveurs de Google. Pour plus d'informations, reportez-vous à la documentation Google sur le fonctionnement du chiffrement.

Le service de chiffrement SDS pour Google Workspace est installé dans votre infrastructure Cloud : les clés KEK ne sont jamais transmises aux serveurs Google.

Avant d'effectuer les opérations cryptographiques, le service de chiffrement SDS pour Google Workspace procède à une double vérification :

- Authentification : Contrôle de l'identité de l'utilisateur qui demande l'opération,
- Autorisation : Contrôle des droits d'accès de l'utilisateur sur le fichier à chiffrer/déchiffrer.

Le service de chiffrement SDS pour Google Workspace génère des logs pour toutes les opérations qu'il réalise.

NOTE
Tout autre usage que celui décrit dans la documentation n'est pas supporté ou doit faire l'objet d'une prise de contact avec le Support Stormshield.

Ce guide décrit comment déployer le service de chiffrement SDS pour Google Workspace en tant que solution SaaS. Si vous souhaitez mettre en place la solution sur site, contactez votre référent commercial Stormshield.

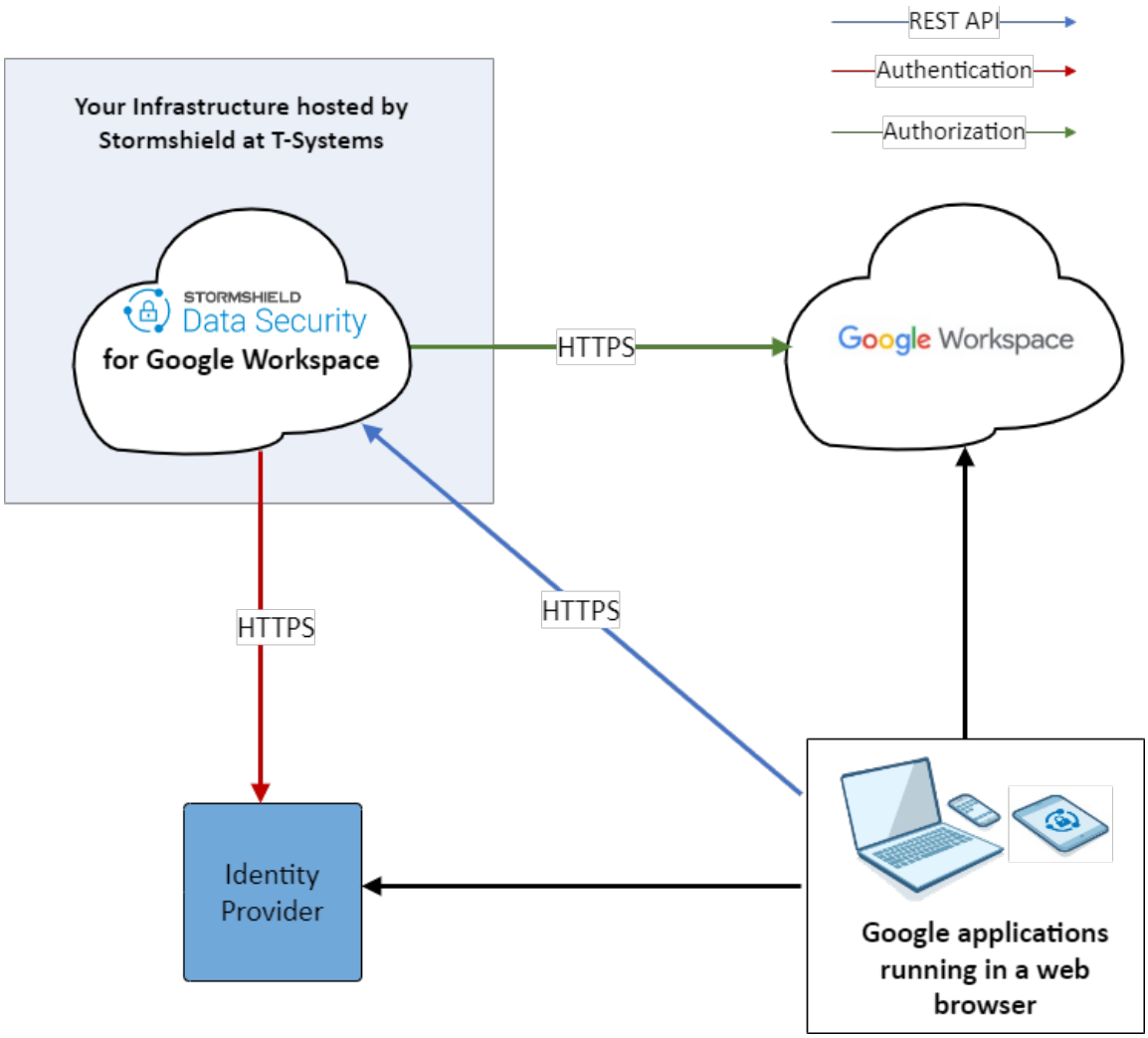
2. Comprendre les prérequis

Vous devez mettre en place les composants suivants dans votre environnement pour utiliser le service de chiffrement SDS pour Google Workspace :

- Un domaine Google et un tenant Google Workspace opérationnels,
- La fonctionnalité Client Side Encryption (CSE) activée sur le tenant Google Workspace. Elle est compatible uniquement avec Google Enterprise Plus et Google Education. Pour plus d'informations, reportez-vous à la **Documentation Google**.
- Un fournisseur d'identité (IdP) pour authentifier les utilisateurs finaux. Le service de chiffrement SDS pour Google Workspace est compatible avec Google Identity et les solutions IdP basées sur le protocole OpenID. Seul Google Identity est évoqué dans ce document.
- Un compte administrateur du domaine Google est nécessaire pour effectuer les opérations de configuration dans la console d'administration Google et la console GCP.
- Un compte Stormshield dont vous devez saisir les informations sur la page **https://mysds.io/fr/**. Pour toute question relative à ce formulaire, contactez votre référent commercial Stormshield.

3. Comprendre l'architecture

Le schéma ci-dessous décrit les différents composants de l'architecture du service de chiffrement SDS pour Google Workspace.



4. Comprendre l'accès aux données

Le tableau ci-dessous liste les différents types de données dans l'infrastructure du service de chiffrement SDS pour Google Workspace et indique si elles sont accessibles par Stormshield et Google.

Type de données	Accessibles par Stormshield	Accessibles dans Google Chrome	Accessibles dans Google Workspace (GCP)
Données utilisateurs chiffrées par une DEK	✗	✓	✓
DEK	✓	✓	✗
DEK chiffrée par une KEK	✓	✓	✓
KEK	✓	✗	✗
Configuration IDP	✓	✓	✓

Pour plus d'informations sur la définition des acronymes DEK et KEK, reportez-vous à la section Avant de commencer et à la documentation Google sur le fonctionnement du chiffrement.

5. Configurer le fournisseur d'identité

Le service de chiffrement SDS pour Google Workspace s'appuie sur un fournisseur d'identité (IdP) pour authentifier les utilisateurs finaux, gérer leurs accès et leur cycle de vie. Il est compatible avec Google Identity et les fournisseurs d'identité tiers basés sur le protocole OpenID.

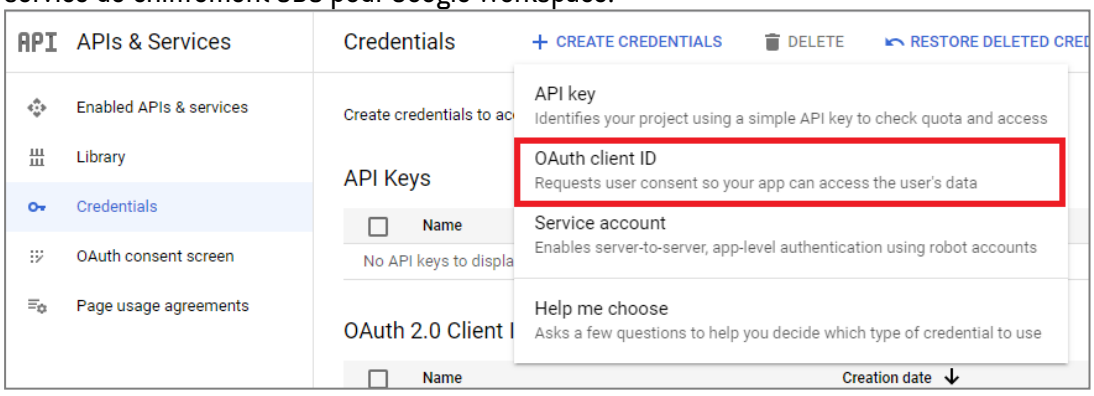
La procédure ci-dessous décrit la configuration avec Google Identity. Pour plus d'informations, reportez-vous à la documentation Google.

Si vous utilisez un IdP tiers, récupérez l'ID client du service de chiffrement SDS pour Google Workspace. Reportez-vous à la documentation de votre IdP.

Si vous souhaitez que des utilisateurs externes invités puissent accéder à votre contenu chiffré, vous devez créer un IdP spécifique pour les authentifier. Pour plus d'informations, reportez-vous à la documentation Google sur la configuration d'un IdP invités pour tous les utilisateurs externes.

5.1 Créer un ID client pour les applications web

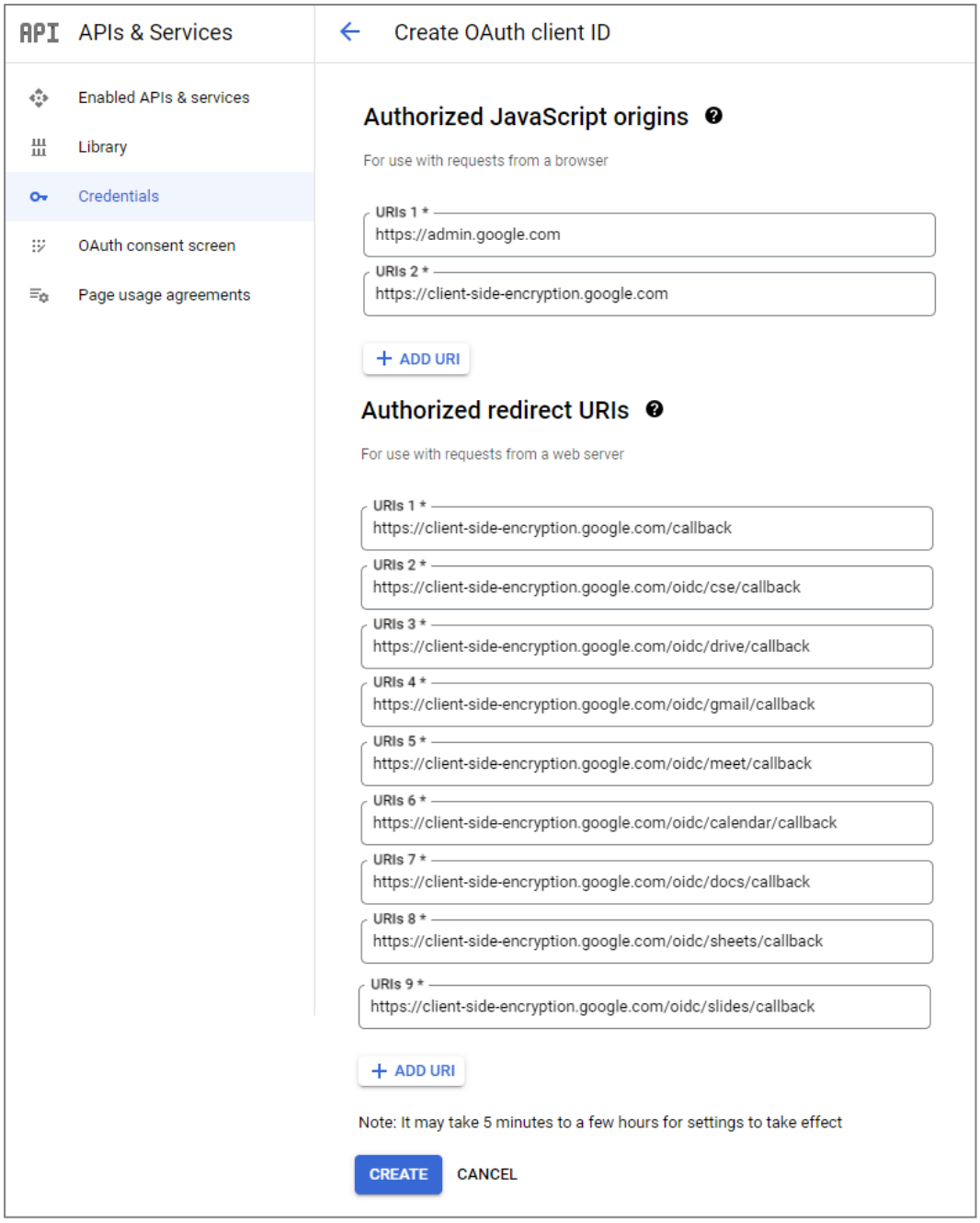
1. Connectez-vous à Google Cloud Platform avec un compte administrateur.
2. Créez un nouveau projet en spécifiant un nom de projet et l'organisation à laquelle il se rattache.
3. Dans le panneau **API et services > Identifiants**, cliquez sur **Créer des identifiants > ID client OAuth** afin de créer un identifiant pour la nouvelle application que vous allez utiliser avec le service de chiffrement SDS pour Google Workspace.



4. Cliquez sur **Configurer l'écran de consentement**, puis choisissez le **Type d'utilisateur Interne**.
5. Cliquez sur **Créer**.
6. Dans le panneau **Modifier l'enregistrement de l'application**, renseignez les paramètres, puis cliquez sur **Enregistrer et continuer**.
   Il n'est pas utile de configurer des champs d'application ni la bibliothèque des API Google, car vous souhaitez uniquement récupérer un identifiant pour configurer la section IdP sur la console d'administration Google.
7. Cliquez de nouveau sur **Créer des identifiants > ID client OAuth**, et dans le champ **Type d'application**, choisissez **Application Web**.
8. Saisissez un **Nom**, par exemple le même que celui du projet.

9. Dans la zone **Origines Javascript autorisées**, saisissez les origines HTTP hébergeant votre application :
   - https://admin.google.com
   - https://client-side-encryption.google.com

10. Dans la zone **URI de redirection autorisés**, saisissez les chemins vers lesquels sont redirigés les utilisateurs après l'authentification Google :
    - 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. Cliquez sur **Créer**.
    Le client OAuth est créé. Vous pouvez récupérer son ID et télécharger le JSON correspondant.

5.2 Créer un ID client pour les applications mobiles et Drive pour ordinateur

Pour les applications mobiles Drive, Agenda et Meet, ainsi que Google Drive pour ordinateur, les ID Client sont les suivantes :

- Drive pour ordinateur :
  947318989803-k88lapdik9bledfml8rr69ic6d3rdv57.apps.googleusercontent.com,
- Drive sur Android :
  313892590415-6lbccuf47cou4q45vanraqp3fv5jt9do.apps.googleusercontent.com,

- Drive sur iOS :
  313892590415-d3h1l7kl4htab916r6jevqdtu8bfmh9m.apps.googleusercontent.com,
- Agenda sur Android :
  313892590415-q84luo8fon5pn5vl8a6rppo1qvcd3qvn.apps.googleusercontent.com,
- Agenda sur iOS :
  313892590415-283b3nilr8561tedgu1n4dcm9hd6g3hr.apps.googleusercontent.com,
- Meet sur Android :
  313892590415-i06v47su4k03ns7ot38akv7s9ari5oa5.apps.googleusercontent.com,
- Meet sur iOS :
  313892590415-32ha2bvs0tr1b12s089i33o58hjvqt55.apps.googleusercontent.com.

6. Se connecter au fournisseur d'identité

Il existe deux options pour authentifier les utilisateurs via le fournisseur d'identité (IdP), ainsi que décrit dans la Documentation Google **Choisir le mode de connexion au fournisseur d'identité pour le chiffrement côté client :**

- Via un fichier .well-known,
- Via la console d'administration Google Workspace.

Utilisez de préférence l'option du fichier .well-known, ce qui vous permet de mettre à jour votre configuration sans l'intervention de Stormshield.

6.1 Se connecter au fournisseur d'identité via un fichier .well-known

Vous devez placer un fichier *.well-known/cse-configuration* sur le site web public de votre société, à la racine du domaine. Ce fichier identifie l'IdP que vous utilisez et permet à vos collaborateurs externes de connaître vos paramètres d'IdP.

Pour le fournisseur d'identité de Google, le contenu du fichier est le suivant :

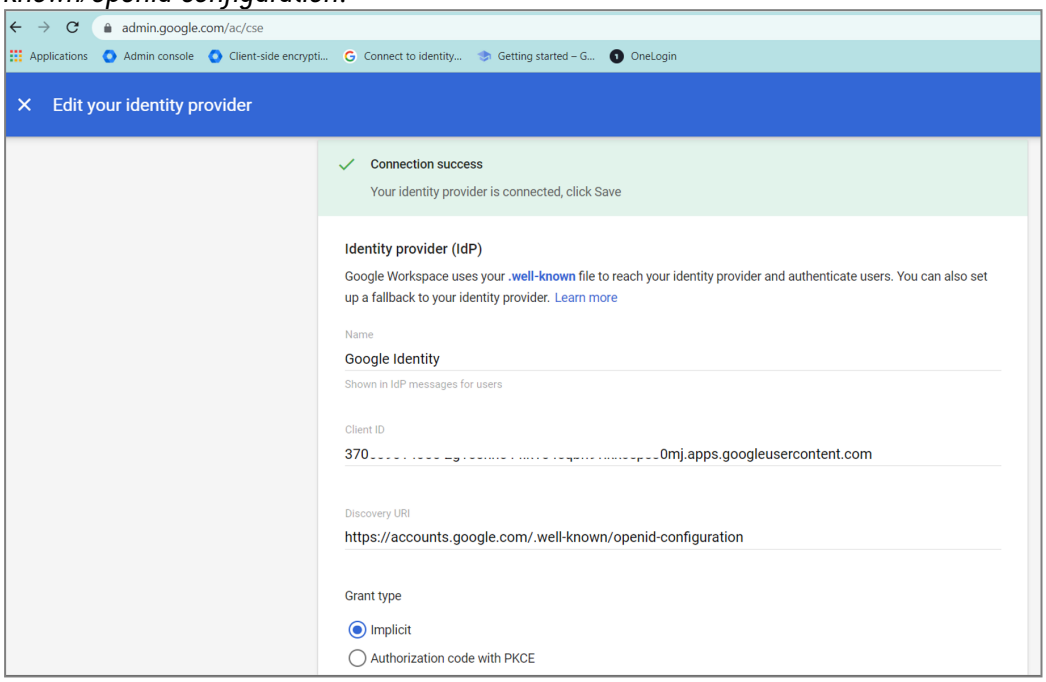
```
{
"name": "https://accounts.google.com",
"client_id": "37*********",
"discovery_uri": "https://accounts.google.com/.well-known/openid-configuration"
}
```

Pour plus d'informations, reportez-vous à la section *Utiliser une authentification distante* du *Guide d'administration* du service de chiffrement SDS pour Google Workspace.

6.2 Se connecter au fournisseur d'identité via la console d'administration

1. Connectez-vous à la console d'administration Google en tant que super-administrateur.
2. Choisissez le menu **Sécurité > Contrôle des accès et des données > Chiffrement côté client**.

3. Configurez le fournisseur d'identité en saisissant les informations concernant votre IdP.
   Nom : Nom de votre choix,
   ID client : ID client OAuth que vous avez créé dans votre projet Google Cloud Platform,
   URI de découverte : Pour Google Identity, il s'agit de *https://accounts.google.com/.well-known/openid-configuration*.

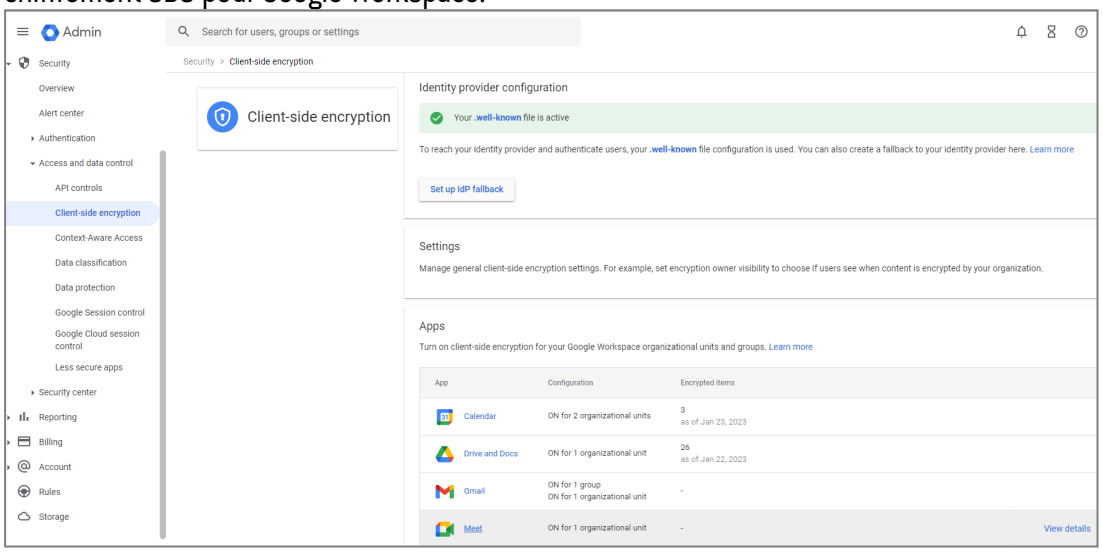


4. Transmettez à Stormshield les informations concernant votre IdP afin que la configuration soit finalisée.

7. Activer le chiffrement pour Google Drive, Meet et Agenda

Afin que les utilisateurs puissent chiffrer les données des services Google Drive, Meet et Agenda, vous devez activer le service de chiffrement SDS pour Google Workspace dans la console d'administration Google.

1. Connectez-vous à la console d'administration Google en tant que super-administrateur.
2. Choisissez le menu **Sécurité > Contrôle des accès et des données > Chiffrement côté client**.
3. Dans la section **Applications**, pour chaque service Google, sélectionnez l'unité organisationnelle (OU) ou le groupe pour lequel vous souhaitez activer le service de chiffrement SDS pour Google Workspace.



NOTE

La fonctionnalité Client Side Encryption de Google comporte des limitations pour Drive, ainsi que pour la version mobile de Meet et Agenda. Pour plus d'informations, reportez-vous à la Documentation Google.

8. Configurer le chiffrement pour Gmail

Afin de configurer et d'activer le chiffrement pour Gmail, reportez-vous à la Documentation Google.

Pour vous aider dans la mise en œuvre du chiffrement pour Gmail, Stormshield développe une solution permettant de gérer les clés de chiffrement et de signature : Stormshield Orchestrator. Pour plus d'informations sur la mise à disposition de cette solution, veuillez contacter votre référent commercial Stormshield, puis remplir ce formulaire.

STORMSHIELD

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