



**STORMSHIELD**



GUIDE

**SDS ENCRYPTION PORTAL**

# GUIDE D'ADMINISTRATION ET D'UTILISATION

Dernière mise à jour du document : 02 avril 2025

Référence : sds-fr-sdse\_guide\_encryption\_portal



# Table des matières

1. Avant de commencer .....	3
1.1 Modes d'utilisation .....	3
1.2 Pré-requis pour l'utilisation de SDS Encryption Portal .....	4
2. Choisir le mode d'utilisation de SDS Encryption Portal .....	5
2.1 Comprendre le mode "PKI externe" .....	5
2.1.1 Caractéristiques .....	5
2.1.2 Prérequis .....	5
2.1.3 Fonctionnement .....	5
2.2 Comprendre le mode "PKI interne" .....	6
2.2.1 Caractéristiques .....	6
2.2.2 Fonctionnement .....	6
3. Créer un tenant pour votre organisation .....	8
4. Créer le compte de l'administrateur de la sécurité .....	9
5. Créer les comptes des utilisateurs .....	10
5.1 Créer des comptes via l'API publique .....	10
5.2 Créer un compte de façon individuelle .....	10
6. Se connecter à SDS Encryption Portal .....	11
6.1 Connexion des utilisateurs en mode "PKI externe" .....	11
6.2 Connexion des utilisateurs en mode "PKI interne" .....	11
6.3 Connexion des utilisateurs externes .....	11
7. Importer les clés de chiffrement .....	13
8. Protéger un document .....	14
9. Consulter un document protégé .....	15
10. Gérer son mot de passe .....	16
10.1 Réinitialiser son mot de passe .....	16
10.2 Modifier son mot de passe .....	16
11. Administrer les utilisateurs .....	17
11.1 Attribuer des droits d'administration .....	17
11.2 Donner les accès d'un utilisateur à un autre .....	17
11.3 Attribuer un nouveau mot de passe à un utilisateur .....	18
11.4 Supprimer des utilisateurs .....	18
12. Pour aller plus loin .....	19
13. Contact .....	20

Dans la documentation, Stormshield Data Management Center est désigné sous la forme abrégée : SDMC.



# 1. Avant de commencer

Bienvenue dans le *Guide d'administration et d'utilisation* de [SDS Encryption Portal](#).

Ce guide s'adresse aux administrateurs de SDS Encryption Portal.

SDS Encryption Portal permet aux utilisateurs de votre organisation de protéger (chiffrer) et télécharger en clair (déchiffrer) des documents confidentiels avec un navigateur internet. Ils peuvent échanger ces documents au sein de leur organisation ou avec des partenaires externes, garantissant ainsi la protection des données sensibles. SDS Encryption Portal est accessible depuis des postes de travail ou des appareils mobiles.

Pour utiliser le portail, vous devez demander à Stormshield la création d'un tenant pour votre organisation.

Les membres de votre tenant pourront ensuite protéger des documents pour eux-mêmes, mais aussi pour toute autre personne, qu'elle soit membre ou non d'un tenant Stormshield.

## **i** NOTE

Un utilisateur qui ne dispose pas de tenant, et donc de clés de chiffrement, peut utiliser SDS Encryption Portal uniquement pour déchiffrer des documents chiffrés pour lui. Dans ce cas, SDS Encryption Portal est gratuit.

L'administrateur de la sécurité du portail tient les rôles d'assistance et de recouvrement. Il peut également les attribuer à d'autres utilisateurs.

## 1.1 Modes d'utilisation

SDS Encryption Portal offre deux modes d'utilisation :

- **Le mode "PKI externe"**. Ce mode permet d'utiliser les clés de chiffrement existantes des utilisateurs si votre organisation possède une solution de PKI. Dans ce mode, l'authentification des utilisateurs auprès du portail fonctionne exclusivement avec la solution de gestion des identités Microsoft Entra ID. Ce mode est actuellement disponible en version Bêta. Contactez votre commercial Stormshield si vous souhaitez mettre en place cette solution.

**i** Ce mode est compatible avec la solution SDS Enterprise.

- **Le mode "PKI interne"**. Si votre organisation ne possède pas de solution de PKI pour la génération des clés de chiffrement de vos utilisateurs, ce mode permet de générer automatiquement des clés lorsque les utilisateurs utilisent le portail pour la première fois. Les clés restent stockées dans la base de données du portail et ne peuvent être récupérées. Dans ce mode, les utilisateurs se connectent au portail via leur adresse e-mail et un mot de passe spécifique.

**i** Ce mode n'est pas compatible avec la solution SDS Enterprise.

Pour plus d'informations sur ces modes, reportez-vous à la section [Choisir le mode d'utilisation de SDS Encryption Portal](#).

Vous choisissez le mode d'utilisation au moment où Stormshield crée le tenant de votre organisation. Une fois le tenant créé, il n'est pas possible de changer de mode d'utilisation.



## 1.2 Pré-requis pour l'utilisation de SDS Encryption Portal

- Stormshield doit créer au préalable un tenant pour votre organisation, en configurant le mode "PKI externe" ou "PKI interne".
- Vous devez disposer d'un navigateur web, d'une connexion internet, et d'une adresse e-mail. Le navigateur doit supporter TLS 1.2 ou supérieur.
- Les flux doivent être autorisés vers le site <https://sds.stormshieldcs.eu>.
- L'exécution de JavaScript doit être autorisée pour le serveur <https://sds.stormshieldcs.eu> ou le domaine [stormshieldcs.eu](https://sds.stormshieldcs.eu).
- La taille des documents à protéger ne doit pas dépasser 20 Mo. Pour pouvoir consulter ou protéger des documents plus volumineux, les utilisateurs doivent disposer de la solution SDS Enterprise.
- Vous allez recevoir des e-mails en provenance de l'adresse [noreply@stormshieldcs.eu](mailto:noreply@stormshieldcs.eu). Autorisez cette adresse dans votre messagerie afin que les e-mails ne soient pas considérés comme du courrier indésirable.



## 2. Choisir le mode d'utilisation de SDS Encryption Portal

Veillez prendre connaissance des sections suivantes pour comprendre la différence entre les deux modes d'utilisation de SDS Encryption Portal.

### ! AVERTISSEMENT

Le mode "PKI externe" est actuellement disponible en version Bêta. Contactez votre commercial Stormshield si vous souhaitez mettre en place cette solution.

### 2.1 Comprendre le mode "PKI externe"

Ce mode d'utilisation est recommandé pour les organisations qui disposent d'une solution de PKI pour générer leurs clés de chiffrement. SDS Encryption Portal peut alors utiliser les clés des utilisateurs existantes.

#### 2.1.1 Caractéristiques

Le mode "PKI externe" possède les caractéristiques suivantes :

- Les utilisateurs se connectent au portail via la solution Microsoft Entra ID,
- Vous utilisez les clés de chiffrement générées par votre PKI et déjà en service dans l'organisation. Les utilisateurs les importent dans le portail pour chiffrer et déchiffrer des documents pour eux ou pour d'autres utilisateurs du même tenant.
- Les utilisateurs d'un tenant peuvent partager des documents chiffrés avec des utilisateurs externes, c'est-à-dire n'appartenant pas à leur tenant, grâce à des clés générées à la volée.
- L'interopérabilité avec la solution SDS Enterprise est assurée par l'utilisation des mêmes clés de chiffrement : les documents chiffrés via le portail, au format *.sdsx*, peuvent être déchiffrés via l'agent SDS Enterprise et inversement,

#### 2.1.2 Prérequis

- Vous devez disposer de la solution de gestion des identités Microsoft Entra ID,
- Vous devez disposer d'une solution de PKI au sein de votre organisation.

#### 2.1.3 Fonctionnement

Une fois le tenant créé, les utilisateurs se connectent à SDS Encryption Portal via Microsoft Entra ID, utilisant ainsi leurs identifiants habituels. A la première connexion, nous leur recommandons d'importer dans le portail leur couple clé privée / certificat au format *.p12* afin d'utiliser les clés déjà existantes. La clé privée est stockée de manière sécurisée dans la section "IndexedDB" du navigateur internet, et le certificat est publié dans la base de données du tenant.

Une fois les clés importées, elles sont utilisées pour les opérations de chiffrement et déchiffrement réalisées sur le portail par les utilisateurs d'un même tenant. Les mêmes fichiers peuvent ainsi être chiffrés ou déchiffrés indifféremment depuis SDS Encryption Portal ou depuis SDS Enterprise.



Les utilisateurs peuvent également chiffrer pour des destinataires externes, c'est-à-dire appartenant à un autre tenant que le leur ou n'appartenant à aucun tenant, grâce à un système de génération à la volée de clés publiques spécifiques.

Pour utiliser SDS Encryption Portal en mode "PKI externe", consultez les sections suivantes :

- [Se connecter à SDS Encryption Portal](#)
- [Importer les clés de chiffrement](#)
- [Protéger un document](#)
- [Consulter un document protégé](#)

## 2.2 Comprendre le mode "PKI interne"

Ce mode d'utilisation est recommandé pour les entreprises et organisations qui n'utilisent pas de clés de chiffrement issues d'une solution de PKI.

### 2.2.1 Caractéristiques

Le mode "PKI interne" possède les caractéristiques suivantes :

- Les utilisateurs se connectent au portail avec leur adresse e-mail et un mot de passe spécifique,
- La génération à la première connexion et l'utilisation des clés sont transparentes pour les utilisateurs,
- Les clés leur permettent de chiffrer et déchiffrer des documents pour eux ou pour d'autres utilisateurs du même tenant,
- Les clés de chiffrement étant stockées par le portail, les utilisateurs peuvent l'utiliser depuis n'importe quel appareil, navigateur ou réseau,
- Les utilisateurs d'un tenant peuvent partager des documents chiffrés avec des utilisateurs externes, c'est-à-dire n'appartenant pas à leur tenant, grâce à des clés générées à la volée. Ces clés sont également stockées par le portail.

### 2.2.2 Fonctionnement

Chaque utilisateur membre d'un tenant doit posséder un compte sur le portail. Pour plus d'informations, reportez-vous à la section [Créer les comptes des utilisateurs](#).

La première fois que chaque utilisateur se connecte au portail, ses clés de chiffrement privée et publique sont automatiquement générées et stockées dans la base de données du portail.

Les clés sont ensuite utilisées pour les opérations de chiffrement et déchiffrement réalisées sur le portail par les utilisateurs.

Les utilisateurs peuvent également chiffrer pour des destinataires externes, c'est-à-dire appartenant à un autre tenant que le leur ou n'appartenant à aucun tenant, grâce à un système de génération à la volée de clés publiques spécifiques.

Pour utiliser SDS Encryption Portal en mode "PKI interne", consultez les sections suivantes :

- [Créer le compte de l'administrateur de la sécurité](#)
- [Créer les comptes des utilisateurs](#)
- [Se connecter à SDS Encryption Portal](#)



- Protéger un document
- Consulter un document protégé



## 3. Créer un tenant pour votre organisation

SDS Encryption Portal est un service cloud hébergé par Stormshield.

Stormshield crée un tenant pour chacune des organisations utilisatrices du portail afin de réserver un espace sécurisé aux utilisateurs d'une même organisation. Ce tenant est configuré selon les besoins des administrateurs de la sécurité et des utilisateurs.

Contactez Stormshield afin qu'un tenant soit créé pour votre organisation.

Les informations suivantes sont nécessaires lors de la création de votre tenant :

Identification de l'organisation	<ul style="list-style-type: none"><li>• Nom</li><li>• Secteur d'activité</li><li>• Taille</li><li>• Adresse</li><li>• Complément d'adresse (optionnel)</li><li>• Pays</li><li>• État/Province/Région (optionnel)</li><li>• Code postal</li><li>• Ville</li></ul>
Mode d'utilisation	Choisissez le mode d'utilisation du portail que vous souhaitez mettre en place : mode "PKI interne" ou mode "PKI externe". Pour plus d'informations sur les modes d'utilisation, reportez-vous à la section <a href="#">Choisir le mode d'utilisation de SDS Encryption Portal</a> . Ce choix ne peut être modifié par la suite. En cas de doute, prenez conseil auprès de Stormshield.
Informations de contact	Si vous choisissez le mode "PKI externe", vous devez fournir des informations de contact à Stormshield lors de la création du tenant. Votre commercial Stormshield vous indiquera le détail des informations à fournir.
Partage de documents avec des utilisateurs externes	Vous devez également indiquer à Stormshield si vous souhaitez que vos utilisateurs puissent partager des documents chiffrés avec des utilisateurs externes, c'est-à-dire appartenant à un autre tenant ou ne disposant pas de tenant.





## 4. Créer le compte de l'administrateur de la sécurité

### ! ATTENTION

Cette section s'applique au mode d'utilisation "PKI interne" seulement. En mode "PKI externe", le système de recouvrement est assuré par votre solution de PKI et l'assistance (perte du mot de passe) est assurée par votre solution de gestion des identités.

Sur SDS Encryption Portal, le premier compte utilisateur créé devient compte d'assistance et de recouvrement et son détenteur est administrateur de la sécurité. Ce compte est indispensable au bon fonctionnement et à la sécurisation de la solution et ne peut donc être supprimé.

Les rôles de l'administrateur de la sécurité sont les suivants :

- **Assistance** : Il attribue un nouveau mot de passe à un utilisateur si le mot de passe est perdu ou si sa confidentialité est compromise.
- **Recouvrement** : Il donne à un utilisateur les accès à tous les documents protégés d'un autre utilisateur, au cas où ce dernier quitterait l'organisation sans déchiffrer ses données par exemple.

Pour créer le premier compte utilisateur, consultez la section [Créer un compte utilisateur de façon individuelle](#).

Pour plus d'informations, reportez-vous à la section [Assistance et recouvrement](#) du guide [Architecture et Sécurité](#).

L'administrateur de la sécurité peut également déléguer ces rôles à d'autres utilisateurs. Pour plus d'informations, reportez-vous à la section [Administrer les utilisateurs](#).

### i NOTE

Si l'administrateur de la sécurité est également un utilisateur du portail, il doit créer un compte avec une adresse e-mail différente du compte administrateur pour l'utiliser.



## 5. Créer les comptes des utilisateurs

### ! ATTENTION

Cette section s'applique au mode d'utilisation "PKI interne" seulement.

Pour créer les comptes des utilisateurs sur le portail, deux solutions sont possibles. Vous pouvez utiliser l'API publique de Stormshield Data Management Center (SDMC) pour créer vous-même les comptes de vos utilisateurs. Ou bien chaque utilisateur peut créer son compte en se rendant sur le portail.

### 5.1 Créer des comptes via l'API publique

L'**API publique** de SDMC permet de créer une liste d'utilisateurs prédéfinis :

- Utilisez la route <https://sds.stormshieldcs.eu/doc/api/#operation/createUsers> pour saisir l'adresse e-mail des utilisateurs. Chaque utilisateur reçoit alors un e-mail l'invitant à activer son compte sur le portail. Si l'e-mail ne se trouve pas dans sa boîte de réception, il doit vérifier son courrier indésirable. Le lien de confirmation expire au bout de 48 heures.

### 5.2 Créer un compte de façon individuelle

Indiquez la procédure suivante à vos utilisateurs :

1. Rendez-vous sur [SDS Encryption Portal](#) et cliquez sur **Créer un compte**.
2. Saisissez vos prénom, nom et adresse e-mail professionnelle, puis acceptez les conditions d'utilisation et cliquez sur **Suivant**.
3. Dans la fenêtre **Mot de passe**, saisissez et confirmez un mot de passe de votre choix respectant les critères énoncés, puis cliquez sur **Suivant**.
4. Un e-mail est envoyé à l'adresse que vous venez de spécifier. Consultez votre messagerie pour confirmer votre adresse e-mail et activer votre compte SDS Encryption Portal. Si l'e-mail ne se trouve pas dans votre boîte de réception, vérifiez votre courrier indésirable. Le lien de confirmation expire au bout de 48 heures, mais vous pouvez demander à votre administrateur de vous le renvoyer si besoin.
5. Lorsque votre compte est créé, [connectez-vous à SDS Encryption Portal](#). Vous devez vous connecter au moins une fois pour qu'un autre utilisateur puisse partager des documents protégés avec vous.



## 6. Se connecter à SDS Encryption Portal

Selon la situation de l'utilisateur, la procédure de connexion diffère.

### 6.1 Connexion des utilisateurs en mode "PKI externe"

Si vous avez choisi le mode "PKI externe", vos utilisateurs se connectent au portail via la solution Microsoft Entra ID, avec leurs identifiants habituels. Indiquez la procédure suivante à vos utilisateurs :

1. Rendez-vous sur [SDS Encryption Portal](#).
2. Saisissez votre adresse e-mail et cliquez sur **Suivant**.
3. Cliquez sur **Se connecter avec Microsoft**.  
La fenêtre de connexion Microsoft s'ouvre.
4. Si nécessaire, saisissez à nouveau votre adresse e-mail, puis saisissez votre mot de passe et cliquez sur **Se connecter**.

Vous pouvez maintenant [Consulter un document protégé](#) ou [Protéger un document](#).

### 6.2 Connexion des utilisateurs en mode "PKI interne"

Si vous avez choisi le mode "PKI interne", vos utilisateurs se connectent avec leur adresse e-mail et leur mot de passe spécifique à SDS Encryption Portal. Indiquez la procédure suivante à vos utilisateurs :

1. Rendez-vous sur [SDS Encryption Portal](#).
2. Saisissez votre adresse e-mail et cliquez sur **Suivant**.
3. Saisissez votre mot de passe et cliquez sur **Se connecter**.

Vous pouvez maintenant [Consulter un document protégé](#) ou [Protéger un document](#).

### 6.3 Connexion des utilisateurs externes

Lorsque des utilisateurs de SDS Encryption Portal protègent un document pour des destinataires externes, qui ne détiennent pas de compte sur le portail, ces derniers doivent suivre la procédure ci-dessous pour consulter le document :

1. Rendez-vous sur [SDS Encryption Portal](#).
2. Saisissez votre adresse e-mail et cliquez sur **Suivant** pour obtenir votre code d'accès unique.
3. Consultez votre messagerie. Vous avez reçu un e-mail de Stormshield ([noreply@stormshieldcs.eu](mailto:noreply@stormshieldcs.eu)) contenant le code. Si l'e-mail ne se trouve pas dans votre boîte de réception, vérifiez votre courrier indésirable. Cliquez sur **Saisir le code**.
4. Saisissez le code dans le champ prévu à cet effet, puis cliquez sur **Se connecter**.  
La page de sélection du document s'affiche.  
Le code ne peut être utilisé qu'une seule fois et est valide pour une durée de deux heures. Si votre code a expiré, demandez un nouveau code en recommençant la procédure à l'étape 2. Assurez-vous de saisir le dernier code reçu, car la génération d'un nouveau code invalide les précédents.
5. Une fois connecté à SDS Encryption Portal, vous pouvez [Consulter un document protégé](#).



Les utilisateurs externes ne détenant pas de compte sur SDS Encryption Portal ne peuvent pas protéger de document.



## 7. Importer les clés de chiffrement

### ! ATTENTION


Cette section s'applique au mode d'utilisation "PKI externe" seulement.

Si vous utilisez une solution de PKI, SDS Encryption Portal permet d'utiliser les clés générées par votre solution pour les opérations de chiffrement et déchiffrement sur le portail, entre utilisateurs d'un même tenant.

Lors de leur première connexion à SDS Encryption Portal, les utilisateurs peuvent importer leur couple clé privée / certificat au format *.p12*.

Si votre organisation utilise également la solution SDS Enterprise, l'utilisation des mêmes clés pour SDS Encryption Portal et pour SDS Enterprise permet l'interopérabilité entre les deux solutions. Les mêmes fichiers peuvent ainsi être chiffrés ou déchiffrés indifféremment depuis SDS Encryption Portal ou depuis SDS Enterprise.

Pour importer les clés dans le portail, indiquez la procédure suivante à vos utilisateurs :

1. Rendez-vous sur [SDS Encryption Portal](#) et connectez-vous.
2. Cliquez sur  en haut à droite, et choisissez **Importer un fichier .p12**.  
Le fichier *.p12* doit contenir :
  - une seule clé privée et un seul certificat,
  - l'attribut E correspondant à l'adresse e-mail de l'utilisateur.
3. Importez le fichier et saisissez son mot de passe.  
La clé privée est stockée de manière sécurisée dans la section "IndexedDB" du navigateur internet, et le certificat est publié dans la base de données du tenant.

Veuillez noter les principes suivants :

- Si un utilisateur n'importe pas ses clés de chiffrement lors de sa première connexion au portail, des clés sont générées à la volée et stockées par le portail. Dans ce cas, l'interopérabilité avec la solution SDS Enterprise n'est pas possible. Si finalement vous souhaitez que l'utilisateur utilise ses propres clés de chiffrement, veuillez contacter votre commercial Stormshield.
- Si un utilisateur souhaite se connecter au portail depuis un autre navigateur ou un autre appareil, il devra importer de nouveau ses clés de chiffrement.
- En cas de changement de clé privée ou de certificat, l'utilisateur peut réimporter ses clés en suivant la même procédure. Le nouveau fichier *.p12* remplace le précédent.
- Lorsqu'un utilisateur a importé ses clés de chiffrement dans le portail via un navigateur, si un utilisateur différent utilise le même navigateur pour se connecter au portail, la clé privée stockée par le navigateur est automatiquement supprimée. Le nouvel utilisateur peut alors importer ses clés de chiffrement.



## 8. Protéger un document

Lorsque l'utilisateur protège l'accès à un document qui contient des informations confidentielles, seuls lui-même et les personnes autorisées peuvent le consulter.

Pour donner l'accès à d'autres personnes, les cas varient :

Les destinataires appartiennent au même tenant que l'utilisateur	Les adresses e-mail des destinataires utilisées pour le partage sont contenues dans la base de données du tenant. Elles sont automatiquement proposées lors de la sélection des destinataires.
Les destinataires appartiennent à un autre tenant que celui de l'utilisateur	L'utilisateur entre manuellement leurs adresses e-mail.
Les destinataires ne détiennent pas de compte sur SDS Encryption Portal	L'utilisateur entre manuellement leurs adresses e-mail. Les destinataires accèdent au document protégé à l'aide d'un code temporaire. Pour plus d'informations, reportez-vous à la section <a href="#">Connexion des utilisateurs externes</a> .

Pour protéger un document, indiquez la procédure suivante à vos utilisateurs :

1. Connectez-vous à SDS Encryption Portal. Pour plus d'informations, reportez-vous à la section [Se connecter à SDS Encryption Portal](#).  
La page de sélection du document s'affiche.
2. Cliquez sur le cadre au centre de la page pour sélectionner le document à protéger sur votre disque.  
- ou -  
Faites un glisser-déposer du document à protéger vers le cadre au centre de la page.
3. Si vous souhaitez que d'autres personnes puissent consulter ce document, saisissez leur adresse e-mail dans le champ **E-mails**. Vous pouvez spécifier jusqu'à 30 adresses.
4. Cliquez sur **Protéger**.  
Le document protégé est enregistré au format `.sdsx` dans votre dossier de téléchargement par défaut. Il peut être consulté uniquement par vous-même et par les personnes que vous avez autorisées en saisissant leur adresse e-mail.
5. Si votre navigateur bloque l'enregistrement, cliquez sur **Sauvegarder le document**.

### ! ATTENTION

La version non protégée du document se trouve toujours à son emplacement initial. Il est recommandé de la supprimer afin que seule la version protégée soit présente sur votre disque. Pensez aussi à supprimer le document de la corbeille pour plus de sécurité.

6. Mettez le document protégé à disposition des personnes autorisées par exemple en le partageant sur un espace collaboratif ou en l'envoyant par e-mail. Elles pourront le consulter via SDS Encryption Portal, ou via SDS Enterprise si votre mode d'utilisation du portail l'autorise. Pour plus d'informations, reportez-vous à la section [Consulter un document protégé](#).
7. Si vous souhaitez protéger un autre document confidentiel, cliquez sur **Nouveau document** et reprenez à partir de l'étape 2.



## 9. Consulter un document protégé

1. Connectez-vous à SDS Encryption Portal. Pour plus d'informations, reportez-vous à la section [Se connecter à SDS Encryption Portal](#).  
La page de sélection du document s'affiche.
2. Cliquez sur le cadre au centre de la page pour sélectionner le document protégé sur votre disque. Ce document doit avoir l'extension `.sdsx`.  
- ou -  
Faites un glisser-déposer du document protégé vers le cadre au centre de la page.  
Si vous possédez les droits sur ce document, alors il est déchiffré et enregistré dans votre dossier de téléchargement par défaut.
3. Si votre navigateur bloque l'enregistrement, cliquez sur **Sauvegarder le document**.
4. Si vous souhaitez consulter un autre document protégé, cliquez sur **Nouveau document** et répétez l'étape 2.



## 10. Gérer son mot de passe

### ! ATTENTION

Cette section s'applique au mode d'utilisation "PKI interne" seulement.

Si vous utilisez SDS Encryption Portal en mode "PKI interne" les utilisateurs disposent d'un compte protégé par un mot de passe spécifique au portail. En cas d'oubli du mot de passe, les utilisateurs peuvent demander sa réinitialisation auprès de leur administrateur.

L'utilisateur peut aussi modifier son mot de passe aussi souvent qu'il le souhaite en fournissant l'ancien mot de passe et le nouveau.

Indiquez les procédures suivantes à vos utilisateurs.

### 10.1 Réinitialiser son mot de passe


En cas d'oubli de votre mot de passe, pour le réinitialiser :

1. Contactez votre administrateur pour qu'il vous transmette un mot de passe temporaire.
2. Connectez-vous à SDS Encryption Portal en utilisant ce mot de passe. Pour plus d'informations, reportez-vous à la section [Se connecter à SDS Encryption Portal](#).  
La page **Mot de passe expiré** s'affiche.
3. Dans le champ **Ancien mot de passe**, saisissez le mot de passe temporaire.
4. Dans les champs **Mot de passe** et **Confirmer le mot de passe**, saisissez un nouveau mot de passe respectant les critères énoncés.
5. Cliquez sur **Modifier le mot de passe**.  
Votre nouveau mot de passe est enregistré et vous êtes automatiquement connecté au SDS Encryption Portal avec ce nouveau mot de passe.

En tant qu'administrateur, pour savoir comment générer un mot de passe temporaire pour un utilisateur, reportez-vous à la section [Administrer les utilisateurs](#).

### 10.2 Modifier son mot de passe

Si vous craignez que votre mot de passe ne soit plus suffisamment sécurisé et que vous souhaitez le modifier :

1. Connectez-vous à SDS Encryption Portal. Pour plus d'informations, reportez-vous à la section [Se connecter à SDS Encryption Portal](#).
2. Cliquez sur l'icône  en haut à droite, et choisissez **Modifier mot de passe**.
3. Remplissez les champs **Ancien mot de passe**, **Mot de passe**, et **Confirmer le mot de passe**. Respectez les critères énoncés pour le nouveau mot de passe.
4. Cliquez sur **Modifier**.  
Votre nouveau mot de passe est enregistré.





# 11. Administrer les utilisateurs


## ! ATTENTION

Cette section s'applique au mode d'utilisation "PKI interne" seulement.

Si vous êtes **administrateur de la sécurité**, vous pouvez utiliser SDS Encryption Portal pour effectuer les tâches d'administration suivantes :

- Attribuer des droits d'administration à d'autres utilisateurs : Assistance, Recouvrement, Suppression d'utilisateurs.
- Donner les accès d'un utilisateur à un autre (Recouvrement) et attribuer un nouveau mot de passe à un utilisateur (Assistance).
- Supprimer des utilisateurs.

## 11.1 Attribuer des droits d'administration

1. Connectez-vous à SDS Encryption Portal en tant qu'administrateur de la sécurité. Pour plus d'informations, reportez-vous à la section [Se connecter à SDS Encryption Portal](#).
2. Cliquez sur l'icône  en haut à droite, et choisissez **Administrer les utilisateurs**.
3. Dans le menu **Utilisateurs**, cliquez sur l'utilisateur auquel vous souhaitez attribuer des droits.
4. Dans la zone **Droits d'administration de la sécurité**, activez ou désactivez ces différents droits selon vos besoins :
  - **Donner les accès d'un utilisateur à un autre (rôle Recouvrement)**. Ce rôle permet de donner à un utilisateur les accès à tous les documents protégés d'un autre utilisateur, au cas où ce dernier quitterait la société par exemple.
  - **Modifier le mot de passe des utilisateurs (rôle Assistance)**. Ce rôle permet d'attribuer un nouveau mot de passe à un utilisateur ayant oublié le mot de passe associé à son compte SDS Encryption Portal.
  - **Supprimer un utilisateur**
5. Cliquez sur **Appliquer**.

Un cartouche s'affiche sur la page de l'utilisateur indiquant son rôle *Recouvrement* et / ou *Assistance*.

Après s'être reconnecté à SDS Encryption Portal, l'utilisateur peut maintenant effectuer les opérations correspondant à son rôle.


En revanche, cet utilisateur n'est pas autorisé à attribuer ces rôles à d'autres utilisateurs.

## 11.2 Donner les accès d'un utilisateur à un autre


### EXEMPLE

Si Paul quitte la société, cette opération permettra à sa collègue Alice d'accéder à tous les documents protégés de Paul après le départ de celui-ci. Alice conservera ses propres accès et détiendra également les accès de Paul.





1. Connectez-vous à SDS Encryption Portal avec un compte utilisateur possédant le rôle *Recouvrement*. Pour plus d'informations, reportez-vous à la section [Se connecter à SDS Encryption Portal](#).
  2. Cliquez sur l'icône  en haut à droite, et choisissez **Administrer les utilisateurs**.
  3. Dans le menu **Utilisateurs**, cliquez sur l'utilisateur dont vous souhaitez recouvrer le compte (Paul dans notre exemple).  
Les informations concernant cet utilisateur s'affichent.
  4. Cliquez sur le bouton **Donner les accès**.
  5. Saisissez tout ou partie du nom de l'utilisateur à qui vous souhaitez donner les accès (Alice dans notre exemple). La liste des correspondances s'affiche.
  6. Choisissez votre utilisateur, puis cliquez sur **Donner les accès**.
- Après s'être reconnecté à SDS Encryption Portal, Alice peut maintenant accéder à tous les documents protégés de Paul en héritant de ses droits.

### 11.3 Attribuer un nouveau mot de passe à un utilisateur

1. Connectez-vous à SDS Encryption Portal avec un compte utilisateur possédant le rôle *Assistance*. Pour plus d'informations, reportez-vous à la section [Se connecter à SDS Encryption Portal](#).
2. Cliquez sur l'icône  en haut à droite, et choisissez **Administrer les utilisateurs**.
3. Dans le menu **Utilisateurs**, cliquez sur l'utilisateur dont vous souhaitez modifier le mot de passe.  
La page de cet utilisateur s'affiche.
4. Cliquez sur le bouton **Modifier le mot de passe**.
5. Saisissez le nouveau mot de passe temporaire et confirmez-le, puis cliquez sur **Modifier le mot de passe**.
6. Transmettez de manière sécurisée le mot de passe temporaire à l'utilisateur. Il devra le modifier.

### 11.4 Supprimer des utilisateurs

Avant de supprimer un utilisateur, assurez-vous de donner l'accès à ses documents protégés à un autre utilisateur le cas échéant, en suivant la procédure de recouvrement [ci-dessus](#).

1. Connectez-vous à SDS Encryption Portal avec un compte utilisateur possédant le droit de supprimer des utilisateurs. Pour plus d'informations, reportez-vous à la section [Se connecter à SDS Encryption Portal](#).
2. Cliquez sur l'icône  en haut à droite, et choisissez **Administrer les utilisateurs**.
3. Dans le menu **Utilisateurs**, cliquez sur l'icône  de l'utilisateur à supprimer, et sélectionner **Supprimer définitivement**.
4. Confirmez la suppression.



## 12. Pour aller plus loin

---

Des informations complémentaires et réponses à vos éventuelles questions sont disponibles dans la [base de connaissances Stormshield](#) (authentification nécessaire).



## 13. Contact

---

Pour contacter notre Technical Assistance Center (TAC) Stormshield :

- <https://mystormshield.eu/>  
La soumission d'une requête auprès du TAC doit se faire par le biais du gestionnaire d'incidents dans l'espace privé <https://mystormshield.eu/>, menu **Support technique** > **Gestion des tickets**.
- +33 (0) 9 69 329 129  
Afin d'assurer un service de qualité, veuillez n'utiliser ce mode de communication que pour le suivi d'incidents auparavant créés par le biais de l'espace <https://mystormshield.eu/>.



**STORMSHIELD**

[documentation@stormshield.eu](mailto:documentation@stormshield.eu)

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

*Copyright © Stormshield 2025. Tous droits réservés. Tous les autres produits et sociétés cités dans ce document sont des marques ou des marques déposées de leur détenteur respectif.*