

ARTICLE TECHNIQUE

Présentation de la sécurité d'Adobe Acrobat avec services Document Cloud



Sommaire

| | |
|--|----|
| Sécurité Adobe | 3 |
| Présentation d'Acrobat avec services Document Cloud | 3 |
| Expériences utilisateur Acrobat | 3 |
| Services Document Cloud | 4 |
| Fonctionnalités de sécurité des documents Acrobat | 4 |
| Sécurité des services Adobe Document Cloud | 7 |
| Intégrations Microsoft | 8 |
| Conclusion | 10 |

Sécurité Adobe

Adobe sait combien la sécurité des expériences digitales est importante. Les pratiques de sécurité sont profondément ancrées dans nos processus opérationnels et de développement logiciel, ainsi que dans nos outils, et sont scrupuleusement suivies par nos équipes pluridisciplinaires pour prévenir, détecter et résoudre rapidement les incidents. De plus, notre collaboration avec des partenaires, chercheurs, instituts de recherche en sécurité et autres acteurs sectoriels nous permet de mieux cerner les dernières menaces et vulnérabilités en date, et nous intégrons régulièrement des techniques de sécurité renforcées aux produits et services que nous proposons.

Cet article technique décrit l'approche de « défense en profondeur » et les procédures mises en œuvre par Adobe pour renforcer la sécurité d'Adobe Acrobat avec les services Document Cloud, ainsi que des données associées.

Présentation d'Acrobat avec services Document Cloud

L'application Acrobat avec services Document Cloud constitue la solution PDF complète pour l'univers connecté et multi-écran actuel. En utilisant la version ordinateur d'Acrobat et l'application mobile Adobe Acrobat Reader (avec fonctionnalités mobiles avancées) avec les services Document Cloud, les entreprises peuvent mettre en place des workflows documentaires plus fluides et répondre à la demande de solutions mobiles, tout en contribuant à garantir la sécurité des documents sur l'ensemble des appareils.

La solution Acrobat avec services Document Cloud permet de convertir la quasi-totalité des contenus en document électronique à partager, ainsi que d'automatiser la création, la manipulation et la transformation des fichiers PDF depuis n'importe quel service cloud ou n'importe quelle application (mobile ou ordinateur) Acrobat.

Expériences utilisateur Acrobat

Les membres de la clientèle peuvent utiliser les services Document Cloud dans le cadre de diverses expériences utilisateur Acrobat :

- Acrobat Pro, l'application pour ordinateur ;
- Acrobat en ligne, une application web accessible sur ordinateur et appareils mobiles via les navigateurs compatibles, notamment Chrome, Microsoft Edge, Firefox et Safari ;
- Le client mobile Acrobat Reader, une application à télécharger gratuitement sur smartphone et tablette via l'Apple App Store et Google Play.

Adobe a également intégré Acrobat à plusieurs outils de productivité Microsoft. Dans le cadre de ces intégrations, le mécanisme de stockage des documents diffère des versions autonomes d'Acrobat. Les informations sur la sécurité relatives à chaque intégration sont détaillées à la section [Intégrations Microsoft](#).

Services Document Cloud

Les services Adobe Document Cloud sont les suivants :

- Envoyer un PDF : envoyez un PDF à un destinataire via un client de messagerie électronique.
- Organiser un PDF : insérez, supprimez, réagencez et faites pivoter des pages dans un PDF.
- Créer un fichier PDF : convertissez des documents Word, Excel et PowerPoint, ainsi que des images et des photos en fichiers PDF.
- Exporter un fichier PDF : convertissez des PDF en fichiers Microsoft Word, Excel, PowerPoint ou RTF modifiables.
- Modifier un fichier PDF : modifiez des PDF depuis un appareil mobile ou ordinateur portable.
- Combiner en PDF : regroupez plusieurs fichiers dans un seul et même PDF et assemblez des liasses de documents, où que vous soyez.
- Remplir et signer : renseignez un formulaire et signez-le.
- Adobe Scan : capturez du contenu et convertissez-le en fichier PDF indexé de qualité.
- [Adobe Acrobat Sign](#) : préparez et envoyez des documents en vue d'y apposer des signatures électroniques fiables sur tout type d'appareil moderne, des signatures simples aux signatures numériques dans le cloud.

Adobe enrichit régulièrement les services Document Cloud. La liste à jour de l'ensemble des services Document Cloud est disponible sur [Adobe.com](https://adobe.com).

Fonctionnalités de sécurité des documents Acrobat

Biffure

Les services Adobe Document Cloud incluent un ensemble d'outils de biffure permettant à chaque membre de la clientèle de protéger les informations sensibles ou confidentielles, et notamment de supprimer définitivement du texte et des images d'un document avant sa distribution. De plus, les utilisateurs et les utilisatrices peuvent rechercher et biffer certaines informations sur la base de modèles, tels que des adresses e-mail et des numéros de téléphone ou de carte bancaire. Les informations sélectionnées sont entièrement supprimées du fichier, et pas simplement masquées, comme c'est le cas avec d'autres outils ou d'autres méthodes. Grâce à la fonction d'assainissement des documents, chaque membre de la clientèle peut également supprimer les informations cachées et les objets non graphiques, comme les métadonnées éventuellement présentes dans le document PDF.

Partage de fichiers

Les fichiers Document Cloud stockés dans le cloud portent la mention « Privé », ce qui signifie que le contenu n'est visible que pour l'utilisateur ou l'utilisatrice qui l'a chargé. Ce dernier doit d'ailleurs prendre des mesures explicites pour partager ce contenu qui, à défaut, demeurera privé. Les fichiers Document Cloud peuvent être partagés en envoyant un lien aux destinataires.

Les utilisateurs et les utilisatrices des services Document Cloud ont le choix entre deux options de partage : Afficher le fichier ou Réviser le fichier. Si l'utilisateur ou l'utilisatrice envoie le lien en activant l'option Afficher le fichier, le destinataire n'aura accès au contenu qu'en lecture seule. En revanche, s'il ou elle envoie le document pour révision, le destinataire pourra l'annoter, mais en aucun cas le modifier. Les liens peuvent être envoyés par e-mail, par SMS ou via une application de collaboration.

Paramètres des actifs et restrictions de partage

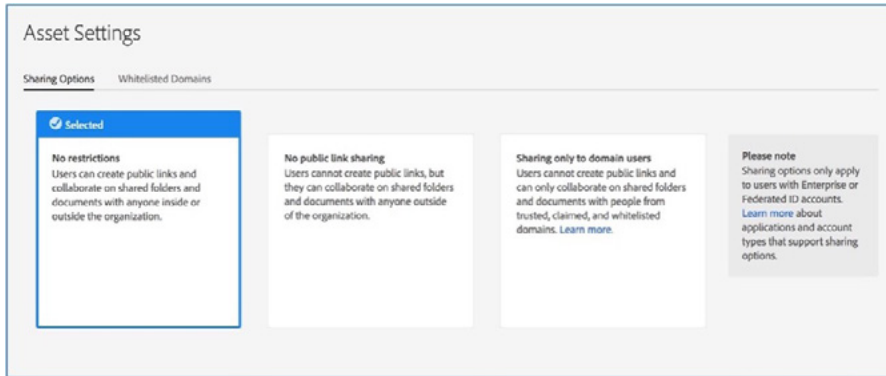


Figure 1 : Paramètres des actifs des services Document Cloud

Des restrictions de partage peuvent être appliquées au contenu stocké dans Document Cloud via la fonctionnalité Paramètres des actifs d'Adobe Admin Console. Le service IT peut ainsi désactiver le partage des liens publics et restreindre la collaboration dans Document Cloud au domaine réservé de l'entreprise et aux autres domaines autorisés. Lorsque les restrictions de partage sont activées, les destinataires doivent s'identifier. De plus, si le mode « Partage limité aux utilisateurs du domaine » est activé, le contenu ne peut être partagé qu'avec les membres de l'entreprise ou des personnes utilisant d'autres domaines de confiance ; le partage avec l'extérieur est totalement désactivé.

Microsoft Purview Information Protection

Microsoft Purview Information Protection (MPIP) est une solution de gestion des droits Microsoft. Les utilisateurs et les utilisatrices d'Azure Information Protection et d'autres solutions Microsoft Purview Information Protection peuvent utiliser Acrobat ou Acrobat Reader pour accéder au contenu libellé et protégé. Avec les versions les plus récentes d'Acrobat Pro/Standard sur ordinateur (22.003.20258 et ultérieures), il est désormais possible [d'appliquer en mode natif des règles et des étiquettes de sensibilité Information Protection](#) aux PDF et de les modifier, sans aucun plug-in ni aucune installation supplémentaire.

Mode protégé

Afin de protéger chaque membre de la clientèle des tentatives d'écriture ou de lecture malveillantes des fichiers PDF à partir du système de fichier d'un ordinateur, Adobe propose un mode protégé mettant en œuvre la technologie de pointe « sandbox » (bac à sable).

Dans Acrobat Reader, le mode protégé offre une protection élargie contre les pirates qui tentent d'installer des programmes malveillants sur un système informatique, mais aussi contre les utilisateurs malintentionnés en les empêchant d'accéder aux données confidentielles et à la propriété intellectuelle et de les extraire du réseau d'entreprise.

Activé par défaut à chaque lancement d'Acrobat Reader, ce mode restreint le niveau d'accès octroyé aux programmes, protégeant ainsi les postes sous Microsoft Windows des fichiers PDF malveillants qui essaieraient d'effectuer des opérations en écriture ou en lecture dans le système de fichiers de l'ordinateur, de supprimer des fichiers ou de modifier les informations système.

Le mode protégé d'Acrobat Reader (sous Windows 8.1 et versions ultérieures) peut s'exécuter de manière isolée dans l'environnement [AppContainer](#).

Vue protégée

Très prisée des professionnels de la sécurité, la technologie « sandbox » permet de créer un environnement confiné pour l'exécution de programmes assortis de droits ou d'autorisations restreints. Cette solution aide à protéger les systèmes des utilisateurs et des utilisatrices contre les dommages susceptibles d'être provoqués par des documents non fiables contenant du code exécutable. Dans le contexte d'Acrobat Reader, le contenu non fiable désigne tout fichier PDF et les processus qu'il met en œuvre. Reader traite tous les fichiers PDF comme s'ils étaient corrompus et isole les traitements invoqués dans le bac à sable. Semblable au mode protégé d'Acrobat Reader, la vue protégée est une mise en œuvre de la technologie « sandbox » pour les riches fonctionnalités d'Acrobat.

Dans Acrobat, Adobe étend les fonctionnalités de la vue protégée en bloquant non seulement les attaques en écriture dans le système de l'ordinateur par du code malveillant utilisant le format PDF, mais aussi les attaques en lecture visant à dérober des données confidentielles ou de la propriété intellectuelle via des fichiers PDF. À l'instar du mode protégé, la vue protégée confine l'exécution des programmes non fiables (par exemple, tout fichier PDF et les processus qu'il invoque) dans une sandbox restreinte afin d'empêcher les opérations en écriture ou en lecture dans le système de fichiers de l'ordinateur par du code malveillant utilisant le format PDF. La vue protégée part du principe que tous les fichiers PDF sont potentiellement malveillants et confine le traitement dans la sandbox, sauf si l'utilisateur ou l'utilisatrice déclare qu'un fichier est fiable.

La vue protégée est prise en charge par les deux scénarios d'ouverture de documents PDF : dans l'application Acrobat autonome ou dans un navigateur. La vue protégée sous Windows 8 et versions ultérieures s'exécute systématiquement dans un conteneur d'application. Résultat : un environnement encore plus solidement verrouillé pour chaque membre de la clientèle qui active la vue protégée. Lorsqu'un utilisateur ou une utilisatrice ouvre un fichier potentiellement malveillant dans la vue protégée, une barre de message jaune s'affiche en haut de la fenêtre Acrobat. Cette barre indique que le fichier n'est pas fiable et rappelle à l'utilisateur ou à l'utilisatrice que la vue protégée, qui désactive plusieurs fonctionnalités d'Acrobat et limite les possibilités d'interaction avec le fichier, est activée. En fait, le fichier est en lecture seule et la vue protégée empêche tout contenu malveillant incorporé ou associé à une balise de modifier le système.

Si l'utilisateur ou l'utilisatrice estime que le fichier est fiable et que toutes les fonctionnalités d'Acrobat peuvent être activées, il ou elle peut cliquer sur le bouton Activer toutes les fonctions dans la barre de message. Cela permet de sortir de la vue protégée. L'application considère alors que le fichier est définitivement fiable en l'ajoutant à la liste des emplacements privilégiés d'Acrobat. Chaque ouverture suivante du fichier PDF fiable désactive les restrictions de la vue protégée.

Sécurité des services

Adobe Document Cloud

Authentification des utilisateurs et des utilisatrices

Avec Adobe Admin Console, les personnes en charge de l'administration peuvent gérer les droits d'accès des utilisateurs et des utilisatrices aux services Adobe Document Cloud à l'aide de licences nominatives. La solution Acrobat avec services Document Cloud prend en charge [quatre \(4\) types de licence nominative](#) : Adobe ID, Business ID, Entreprise ID et Federated ID. Pour en savoir plus sur ces différents types d'identité et sur les services de gestion des identités d'Adobe, consultez la [présentation du système de gestion des identités d'Adobe](#).

Stockage des documents et du contenu créé par l'utilisateur ou l'utilisatrice

Les services Adobe Document Cloud utilisent un stockage mutualisé. Le contenu et documents créés par les utilisateurs ou les utilisatrices font l'objet d'une redondance dans plusieurs centres de données et sur plusieurs équipements dans chaque centre. Tout le trafic réseau fait systématiquement l'objet d'une vérification des données et de calculs de contrôle pour prévenir toute corruption et contribuer à garantir l'intégrité des données. Enfin, le contenu stocké est répliqué automatiquement de manière synchrone dans d'autres centres de données de la zone géographique de la clientèle afin de garantir l'intégrité des données même en cas de perte de données sur deux sites.

Les documents et le contenu UGC transférés dans Document Cloud sont généralement stockés dans le centre de données régional correspondant au code pays de l'utilisateur ou de l'utilisatrice qui charge les données, quel que soit le type d'identité :

- Pour l'Amérique du Nord, l'Amérique centrale et l'Amérique du Sud, les données sont stockées dans l'état de Virginie, aux États-Unis.
- Pour l'Europe et l'Afrique, les données sont stockées à Dublin, en Irlande.
- Pour l'Asie-Pacifique et le Moyen-Orient, les données sont stockées à Tokyo, au Japon.

Si les personnes en charge de l'administration sont habilitées à allouer un espace de stockage dans le cloud à certains comptes Entreprise ID et Federated ID via Adobe Admin Console, ils ne peuvent pas accéder directement aux documents et contenus de l'utilisateur final dans l'espace de stockage des services Document Cloud. Ils peuvent toutefois révoquer l'accès de l'utilisateur ou de l'utilisatrice et devenir propriétaires de son compte. En configuration Services partagés, lorsque ces types de compte avec espace de stockage sont supprimés, les anciens utilisateurs et les anciennes utilisatrices de ces comptes n'ont plus accès aux données de l'espace de stockage qui sont supprimées au bout de 90 jours.

Les administrateurs et les administratrices peuvent également utiliser Admin Console pour allouer un espace de stockage aux comptes associés à un Adobe ID. Bien que n'exerçant aucun contrôle sur ces comptes, ils ont néanmoins la possibilité de révoquer les droits d'accès aux services et applications et de supprimer l'espace de stockage octroyé à l'entreprise, les données étant également supprimées au bout de 90 jours.

Cryptage des données

Par défaut, les contenus et documents de l'utilisateur ou de l'utilisatrice des services Document Cloud sont cryptés « en transmission » via le protocole HTTPS TLS 1.2. Ils sont cryptés « au repos » via des clés de chiffrement symétriques AES 256 bits, différentes pour chaque membre de la clientèle et pour chaque domaine déclaré de chaque entreprise. Ces méthodes de cryptage sont appliquées à la fois pour le stockage permanent et temporaire des documents.

Clés de cryptage dédiées

Outre les fonctions de cryptage standard intégrées, les personnes en charge de l'administration peuvent appliquer une autre couche de contrôle et de sécurité aux documents « au repos » avec une clé de cryptage dédiée pour tout ou partie des domaines de l'entreprise. Le contenu stocké via les services Document Cloud peut alors être crypté « au repos » via cette clé. Si besoin, cette clé peut être révoquée dans Admin Console. Cette révocation a pour effet de rendre le contenu crypté avec cette clé inaccessible aux utilisateurs finaux et d'empêcher le chargement et le téléchargement de contenu jusqu'à réactivation de la clé.

Remarque : les clés de cryptage dédiées permettent de crypter les fichiers Adobe Document Cloud, mais pas les métadonnées correspondantes.

Pour en savoir plus sur la gestion du cryptage à l'aide d'une clé dédiée, [rendez-vous sur Adobe.com](https://adobe.com).

Signatures électroniques et numériques

Dans le cadre des services Document Cloud, différents outils sont disponibles pour la manipulation des signatures :

- L'**outil Remplir et signer** permet d'ouvrir un PDF, de compléter les champs de formulaire et de signer le document par voie électronique.
- L'**outil Certificats** permet d'apposer sur un document une signature électronique associée à un certificat numérique, ce dernier étant lié de manière cryptographique au champ de signature. Identifiant le signataire de manière unique, chaque certificat numérique est émis par un prestataire de services de confiance ou une autorité de certification figurant sur la liste AATL (Adobe Approved Trust List) ou EUTL (European Union Trusted Lists). Avec l'outil Certificats, les utilisateurs et les utilisatrices peuvent aussi appliquer des horodatages sur les documents et les certifier via un sceau infalsifiable.

Intégrations Microsoft

Dans le cadre d'un partenariat entre les deux éditeurs, Adobe a créé des intégrations pour les principaux outils de productivité Microsoft. Acrobat et les services Document Cloud sont ainsi accessibles en mode natif dans les solutions suivantes :

- Microsoft SharePoint et OneDrive
- Microsoft Teams
- Microsoft Word, Excel et PowerPoint (seules les fonctionnalités de création et de protection des PDF sont disponibles)

Dans le cadre de ces intégrations, Adobe ne crée qu'une copie temporaire du document, et ne recueille aucun renseignement sur les entreprises clientes ni aucune information personnelle sur l'utilisateur ou l'utilisatrice.

Acrobat pour SharePoint et OneDrive

Avec cette intégration, les utilisateurs et les utilisatrices ont accès aux workflows PDF dans Microsoft 365. Ils peuvent ainsi consulter, créer et modifier des PDF dans le cloud.

Avec cette version intégrée d'Acrobat, les documents sont stockés à leur emplacement d'origine dans SharePoint ou OneDrive. Les opérations telles que la consultation, l'annotation et la recherche s'effectuent en local, sur la machine de l'utilisateur ou de l'utilisatrice. Lorsqu'un document est modifié, celui-ci est de nouveau stocké dans le compte SharePoint ou OneDrive de l'utilisateur ou de l'utilisatrice.

En cas de création, de réorganisation, de regroupement ou d'exportation de documents, ceux-ci sont transférés sur les serveurs Adobe Document Cloud situés dans la [zone géographique correspondant au code pays de l'utilisateur ou de l'utilisatrice](#) en vue d'un traitement provisoire, puis supprimés dans les 24 heures. Lors de ce processus, les documents sont cryptés en transmission et au repos (voir la section [Cryptage des données](#)). Les documents modifiés sont de nouveau enregistrés sur le compte SharePoint ou OneDrive de l'utilisateur ou de l'utilisatrice.

Pour plus d'informations sur les fonctionnalités spécifiques d'Acrobat pour SharePoint et OneDrive, [rendez-vous sur Adobe.com](#).

Acrobat pour Microsoft Teams

Avec cette intégration, les utilisateurs et les utilisatrices ont accès aux workflows PDF dans Microsoft Teams. Ils peuvent ainsi consulter, créer et modifier des PDF dans le cloud. Les membres de la clientèle peuvent utiliser Acrobat pour Microsoft Teams sous forme d'onglet personnel, de bot, d'onglet, d'action de message ou d'extension de message.

Par défaut, les PDF partagés dans une conversation ou un canal Microsoft Teams sont stockés sur le compte OneDrive ou SharePoint de l'utilisateur ou de l'utilisatrice. Les opérations telles que la consultation, l'annotation et la recherche s'effectuent en local, sur la machine de l'utilisateur ou de l'utilisatrice. Lorsqu'un document est modifié, celui-ci est de nouveau stocké dans le compte SharePoint ou OneDrive de l'utilisateur ou de l'utilisatrice.

En cas de création, de réorganisation, de regroupement ou d'exportation, les documents sont transférés sur les serveurs Adobe Document Cloud situés dans la [zone géographique correspondant au code pays de l'utilisateur ou de l'utilisatrice](#) en vue d'un traitement provisoire, puis supprimés dans les 24 heures. Lors de ce processus, ils sont cryptés en transmission et au repos (voir la section [Cryptage des données](#)). Les documents modifiés sont de nouveau enregistrés sur le compte SharePoint ou OneDrive de l'utilisateur ou de l'utilisatrice.

Pour plus d'informations sur les fonctionnalités spécifiques d'Acrobat pour Microsoft Teams, [rendez-vous sur Adobe.com](#).

Acrobat pour Word, Excel et PowerPoint

Avec le complément Créer un fichier PDF, les utilisateurs et les utilisatrices peuvent facilement convertir un document Microsoft 365 en PDF de qualité, puis enregistrer ce dernier dans OneDrive ou le télécharger pour l'enregistrer localement. Ils peuvent également protéger le PDF par mot de passe pour empêcher tout accès frauduleux au document.

Conclusion

L'approche proactive d'Adobe en matière de sécurité et les procédures rigoureuses décrites dans ce document contribuent à préserver la sécurité d'Acrobat avec les services Document Cloud et de vos données confidentielles. Chez Adobe, nous prenons très au sérieux la sécurité de vos données d'expériences digitales, et surveillons en permanence un environnement où les menaces évoluent constamment, afin de conserver une longueur d'avance sur les activités malveillantes et de garantir la sécurité des données de notre clientèle.

Pour plus d'informations sur la sécurité Adobe (processus de sécurité propres aux opérations, aux produits et à l'entreprise, programme de test, conformité et certifications, programme de résolution des incidents, plan de continuité d'activité et de reprise sur incident, etc.), consultez le [Centre de données Adobe](#).

Les informations contenues dans ce document sont susceptibles d'être modifiées sans préavis. Pour en savoir plus sur les solutions, les contrôles et les formules de licences d'Adobe, contactez votre représentant agréé.



© 2024 Adobe. Tous droits réservés.

Adobe, the Adobe logo, Acrobat, the Adobe PDF logo, Adobe Document Cloud, and Document Cloud are either registered trademarks or trademarks of Adobe in the United States and/or other countries. All other trademarks are the property of their respective owners.