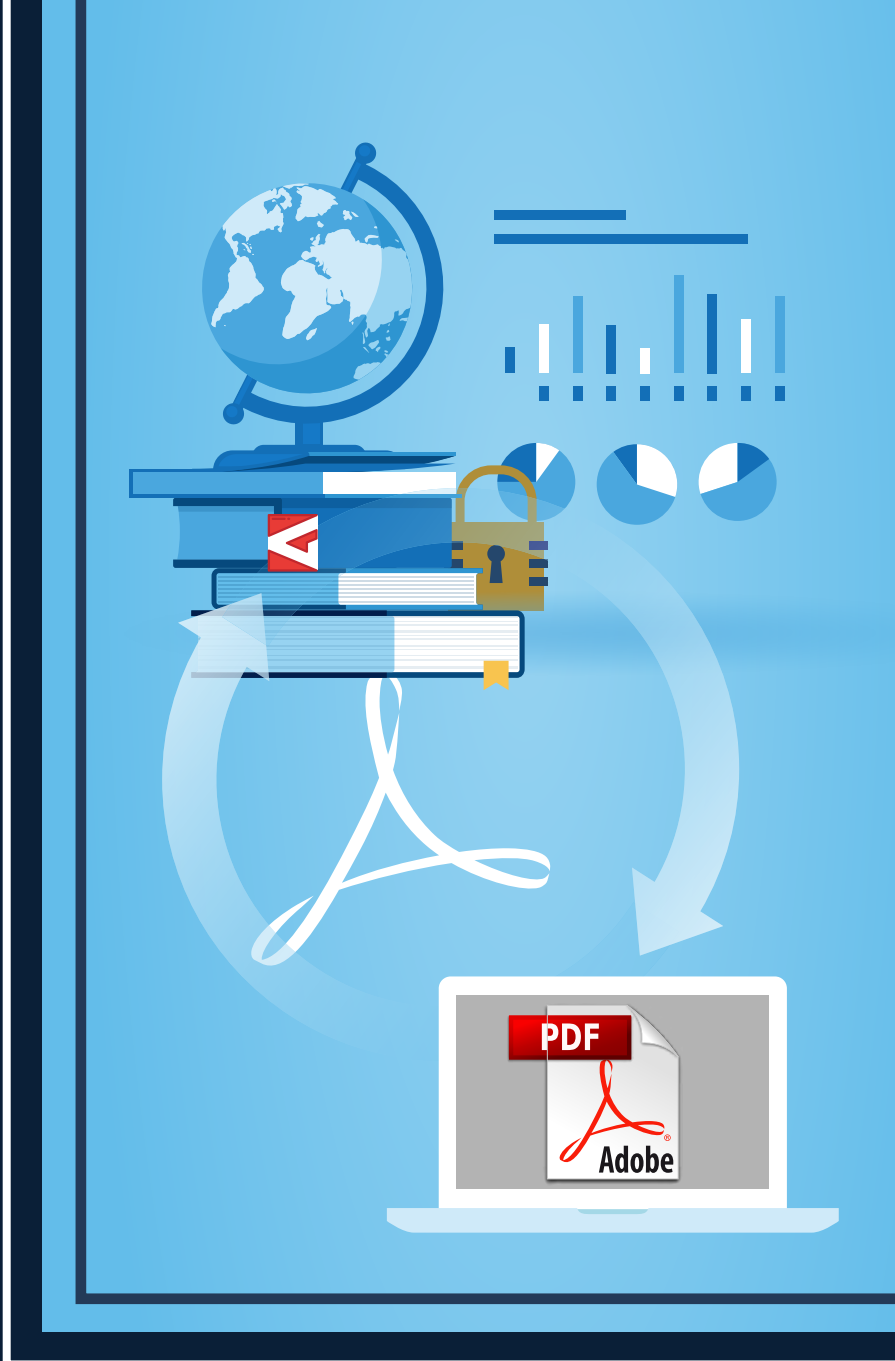


# CCN-CERT BP/16



## Recommandations de sécurité d'Adobe Acrobat Reader DC

RAPPORT DE BONNES PRATIQUES

MARS 2022

**ccn-cert**  
centro criptológico nacional

**CCN**  
centro criptológico nacional

Édité par :



Paseo de la Castellana 109, 28046 Madrid

© Centre national de cryptologie, 2022

Date de publication : mars 2022

### **LIMITATION DE RESPONSABILITÉ**

Ce document est fourni conformément aux termes contenus dans le présent document, rejetant expressément tout type de garantie implicite qui pourrait y être liée. En aucun cas, le Centre national de cryptologie ne peut être tenu responsable des dommages directs, indirects, fortuits ou extraordinaires dérivés de l'utilisation des informations et des logiciels indiqués, même s'il a été averti d'une telle possibilité.

### **AVIS LÉGAL**

La reproduction de tout ou partie de ce document par quelque moyen ou procédé que ce soit, y compris la reprographie et le traitement informatique, ainsi que la diffusion de copies par location ou prêt public, sont strictement interdites sans l'autorisation écrite du Centre national de cryptologie, sous peine des sanctions prévues par la loi.

# Index

<b>1. À propos du CCN-CERT, cert gouvernemental espagnol</b>	4
<b>2. Introduction</b>	5
<b>3. Installation et securisation renforcee d'adobe Reader dc piste continue sur Windows</b>	6
3.1. Telecharger et installer Adobe Reader dc piste continue	7
3.2. Versions	8
3.3. Configuration requise	9
3.4. Emplacement de l'installation	10
3.5. Telechargement et installation de Reader	11
3.5.1. Acrobat Reader DC (Enterprise)	11
3.5.2. Acrobat Reader DC (particuliers)	12
3.6. Appliquer les valeurs de securite	13
3.6.1. Client Windows	13
3.6.2. Serveur Windows : comment creer et gerer le magasin central des modeles d'administration des strategies de groupe	14
3.7. Valeurs de registre	15
3.8. Desactiver la tache de mise a jour d'Adobe Acrobat	29
3.9. Desactiver le service Adobearmservice	30
<b>4. Liste de contrôle (évaluation)</b>	31
<b>5. Décalogue de recommandations</b>	33
<b>ANNEXE. Scripts de configurations securisees</b>	34

# 1. À propos du CCN-CERT, CERT gouvernemental espagnol

Le CCN-CERT est la capacité de réponse aux incidents de sécurité informatique du Centre national de cryptologie, CCN, rattaché au Centre National de Renseignement, CNI. Ce service a été créé en 2006 en tant que **CERT gouvernemental espagnol** et ses fonctions sont définies dans la loi 11/2002 réglementant le CNI, le RD 421/2004 réglementant le CCN et dans le RD 3/2010, du 8 janvier, réglementant le schéma national de sécurité (ENS), modifié par le RD 951/2015 du 23 octobre.

Sa mission est donc de contribuer à l'amélioration de la cybersécurité espagnole, en tant que centre national d'alerte et de réponse qui coopère et aide à réagir rapidement et efficacement aux cyberattaques et à faire face activement aux cybermenaces, y compris la coordination au niveau national des différentes capacités de réponse aux incidents ou des centres opérationnels de cybersécurité existants.

L'objectif étant de disposer d'un cyberspace plus sécurisé et fiable, par la préservation de l'information classifiée (comme le stipule l'art. 4. F de la loi 11/2002) et des informations sensibles, la défense du patrimoine technologique espagnol, la formation du personnel spécialisé, l'application de politiques et de procédures de sécurité, ainsi que l'utilisation et le développement des technologies les plus appropriées à cette fin.

Conformément à ce règlement et à la loi 40/2015 sur le régime juridique du secteur public, le CCN-CERT est responsable de la gestion des cyberincidents affectant tout organisme ou entreprise publique. Dans le cas des opérateurs critiques du secteur public, la gestion des cyberincidents sera assurée par le CCN-CERT en coordination avec le CNPIC.

**Le CCN-CERT est la capacité de réponse aux incidents de sécurité informatique du Centre national de cryptologie**

# 2. Introduction

Ce document fait partie de la documentation émise par le Centre national de cryptologie dont l'objectif est de préserver la sécurité des systèmes TIC des administrations publiques.

À cette fin, un mécanisme est fourni pour appliquer des mesures de sécurité de manière automatisée et non surveillée sur un logiciel de visualisation de fichiers PDF, afin de faciliter la possibilité de mettre en œuvre la sécurité dans les systèmes TIC d'une manière simple et agile.

## Objet

L'objectif de ce document est de définir les procédures et les utilitaires nécessaires pour mettre en œuvre et assurer la sécurité dans la version continue d'Adobe Reader DC.

## Périmètre

Le présent document définit une procédure visant à renforcer la sécurité et à protéger Adobe Acrobat Reader DC afin de limiter les vulnérabilités et les risques potentiels auxquels il peut être exposé.

Les utilisateurs de ce guide peuvent renforcer la sécurité de cette application par le biais de l'interface utilisateur et des paramètres du registre, ainsi que configurer les fonctions de ce produit pour protéger l'intégrité du contenu PDF.

**Ce document fait partie de la documentation émise par le Centre national de cryptologie dont l'objectif est de préserver la sécurité des systèmes TIC des administrations publiques**



Adobe Acrobat DC

# 3. Installation et securisation renforcee d'Adobe Reader DC piste continue sur Windows

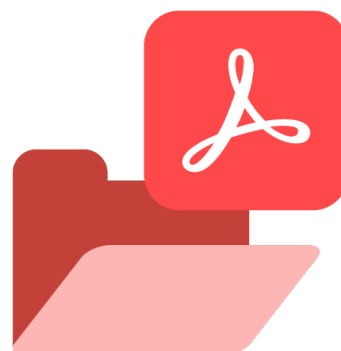
Adobe Reader peut être téléchargé gratuitement sur le site web d'Adobe et permet de visualiser et d'imprimer des documents PDF.

Ce manuel est conçu pour Adobe Acrobat Reader DC Piste Continue, mais peut également être utilisé pour les versions ultérieures.

Les dernières mises à jour logicielles relatives à la sécurité doivent être installées sur Adobe Reader DC. Pour ce faire, déterminez la méthode de mise à jour (par exemple, connexion à un serveur WSUS, procédure locale, mise à jour automatique, etc.)

Pour déterminer la version que vous avez installée, cliquez sur **Aide >>** **À propos d'Adobe Acrobat Reader DC**. Vérifiez que vous avez appliqué la dernière mise à jour du logiciel. Si les dernières mises à jour des logiciels de sécurité d'Adobe ne sont pas appliquées, cela constitue une faille de sécurité critique.

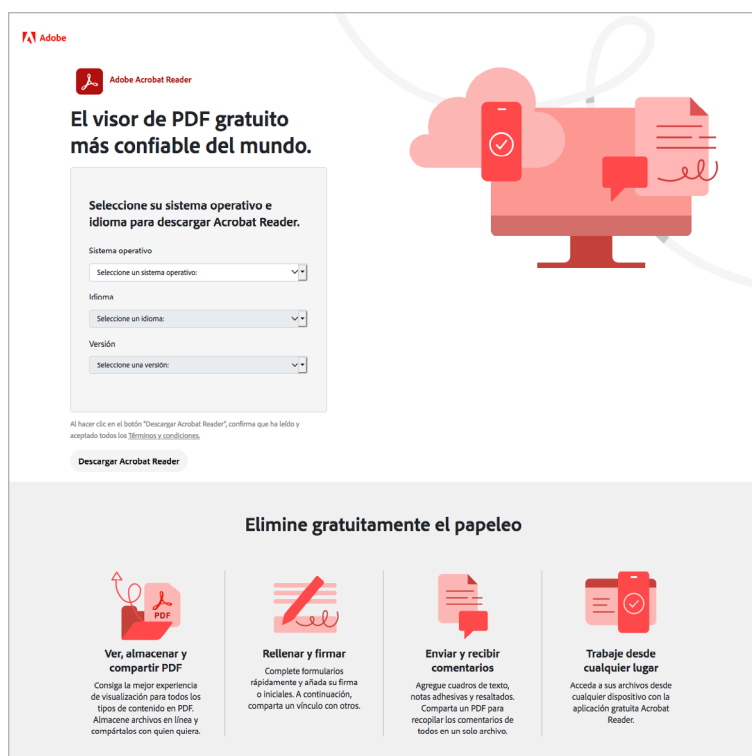
**Adobe Reader peut être téléchargé gratuitement sur le site web d'Adobe et permet de visualiser et d'imprimer des documents PDF**



## 3.1. Télécharger et installer Adobe Reader DC piste continue

Le programme doit être téléchargé à partir d'un ordinateur connecté à Internet.

Avant de télécharger le programme, veuillez noter les informations suivantes.





## 3.2. Versions

Le logiciel de bureau Acrobat Reader DC est disponible pour le déploiement des versions Classique et Continue.

La version Continue fournit des outils basés sur les services, ainsi que de nouvelles fonctionnalités, des améliorations de la sécurité et de la plate-forme, et des corrections des bogues les plus fréquents. La cadence de mise à jour de la piste continue est plus fréquente que celle de la piste classique.

La version Continue est similaire au modèle 10.X - 11.X et ne fournit pas de nouvelles fonctionnalités dans les mises à jour. Les services gratuits sont disponibles, mais facultatifs. La cadence des mises à jour est trimestrielle et fournit des améliorations de la sécurité et de la plate-forme ainsi que des corrections de bogues.

Ci-dessous, nous pouvons voir le format générique d'affichage de la version finale d'Adobe Reader DC (majeur.mineur.mineur\_mineur).

**Le logiciel de bureau Acrobat Reader DC est disponible pour le déploiement des versions Classique et Continue**

DESCRIPTION		
<div><div>Année de publication</div><div>ID de suivi</div><div>Champ caché dans la liste des modifications</div><div>15.006.20456.1110321</div><div>numéro de version interne</div><div>numéro de version interne</div></div>		
VERSION	RANG	NOTES
Majeure	1-255	Les deux derniers chiffres de l'année de publication
Mineure	1-255	Un numéro interne indiquant quand le code est passé de Trunk à Beta.
Mineur_minor	1-65535	Les deux premiers chiffres indiquent la version : 20=Continu ; 30=Classique
4ème champ caché	Modifier le numéro de liste	Ce numéro n'est visible que si l'utilisateur clique sur le numéro de version dans la boîte « À propos ».



## 3.3. Configuration requise

Voici la configuration minimale requise pour installer Adobe Acrobat Reader DC.

<b>Acrobat Reader DC (32 bits)</b>	<ul style="list-style-type: none"><li>• Processeur Intel® ou AMD de 1,5 GHz ou plus rapide</li><li>• Windows 11 (64 bits), Windows 10 (32 bits et 64 bits) version 1809 ou ultérieure, Windows 8, 8.1 (32 bits et 64 bits)*, Windows 7 SP1 (32 bits et 64 bits) ou Windows Server - 2008 R2 (64 bits), 2012 (64 bits), 2012 R2 (64 bits) *, 2016 (64 bits) ou 2019 (64 bits)</li><li>• 2 Go de RAM</li><li>• 450 Mo d'espace disponible sur le disque dur</li><li>• Résolution d'écran 1024 × 768</li><li>• Internet Explorer 11</li></ul>
------------------------------------	--

[\*] Avec la mise à jour Windows 2919355 installée.

<b>Acrobat Reader DC (64 bits)</b>	<ul style="list-style-type: none"><li>• Processeur Intel® ou AMD de 1,5 GHz ou plus rapide</li><li>• Windows 11 (64 bits), Windows 10 (64 bits) version 1809 ou ultérieure, Windows Server 2016 (64 bits) ou Windows Server 2019 (64 bits)</li><li>• 2 Go de RAM</li><li>• 900 Mo d'espace disponible sur le disque dur pour l'anglais</li><li>• 1 Go d'espace disponible sur le disque dur pour les autres langues</li><li>• Résolution d'écran 1024 × 768</li><li>• Internet Explorer 11</li></ul>
------------------------------------	--

## 3.4. Emplacement de l'installation

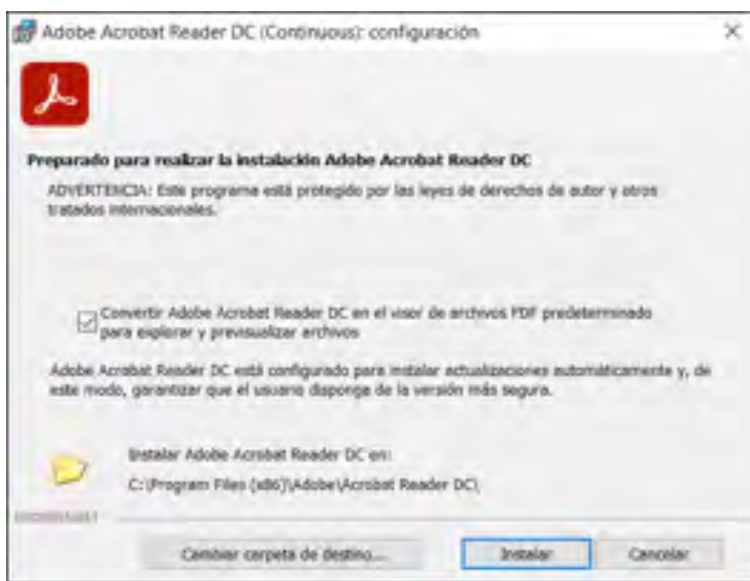
Les chemins d'installation d'Adobe Reader DC sont décrits ci-dessous :

- ▶ **Chemin d'installation sous Windows (32bits)**  
C:\Program Files (x86)\Adobe\Acrobat Reader DC\
- ▶ **Chemin d'installation sous Windows (64bits)**  
C:\Program Files\Adobe\Acrobat Reader DC\
- ▶ **Chemin de registre**  
HKCU\Software\Adobe\Acrobat Reader\DC\
- ▶ **Chemin des données de l'application**  
%Appdata%\Roaming\Adobe\Acrobat\DC\

**Pour une surveillance continue, tous les services sont visibles**

Pour une surveillance continue, tous les services sont visibles. Les services Adobe Document Cloud gratuits sont fonctionnels par défaut et les services payants nécessitent une mise à niveau ou un achat.

Pour la version Acrobat DC Enterprise, le paramètre par défaut d'Adobe Acrobat Reader DC comme visionneur PDF par défaut est coché pendant le processus d'installation.



**REMARQUE :**

Il est possible de personnaliser le chemin d'accès où l'installation du programme a lieu dans le processus d'installation du programme.

## 3.5. Téléchargement et installation de Reader

### 3.5.1. Acrobat Reader DC (Enterprise)

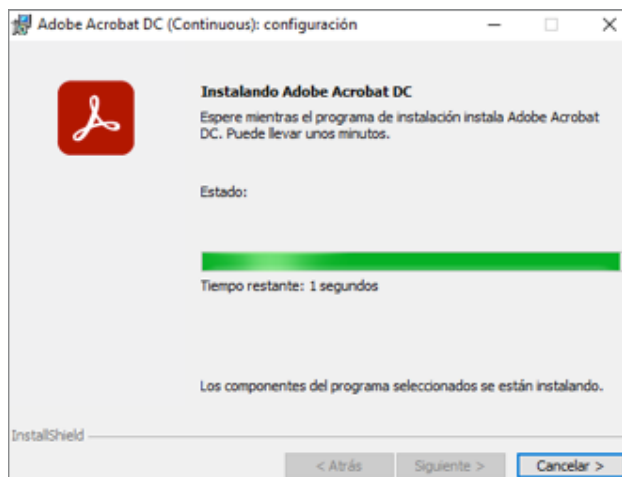
Via l'URL suivante :

<https://get.adobe.com/es/reader/enterprise/>

Toutes les versions d'Adobe Acrobat Reader DC disponibles au téléchargement sur ce lien utilisent un suivi continu.

#### DESCRIPTION

- ▶ Dans cette fenêtre, sélectionnez le système d'exploitation dans lequel vous installerez ce téléchargement « **Étape 1** », la langue « **Étape 2** » et enfin la version « **Étape 3** ». Ensuite, cliquez sur le bouton « **Télécharger maintenant** » pour lancer le téléchargement du programme. Une fois cette étape terminée, double-cliquez sur le fichier d'installation et attendez que le processus d'installation soit terminé.
- ▶ Le fichier d'installation que vous téléchargez sera utilisé pour installer ou mettre à jour la version d'Acrobat Reader.
- ▶ Redémarrez le système et vous êtes prêt à utiliser le programme.



### 3. Installation et sécurisation renforcée d'Adobe Reader DC piste continue sur Windows

#### 3.5.2. Acrobat Reader DC (particuliers)

Via l'URL suivante :

<https://get.adobe.com/es/reader/>

Adobe Acrobat Reader DC est installé directement sur votre ordinateur.

Une connexion à Internet est nécessaire pour compléter le processus d'autorisation au premier lancement et tous les 30 jours afin de valider votre abonnement.

##### DESCRIPTION

Dans cette fenêtre, sélectionnez le système d'exploitation dans lequel vous installerez ce téléchargement « **Étape 1** », la langue « **Étape 2** » et enfin la version « **Étape 3** ».

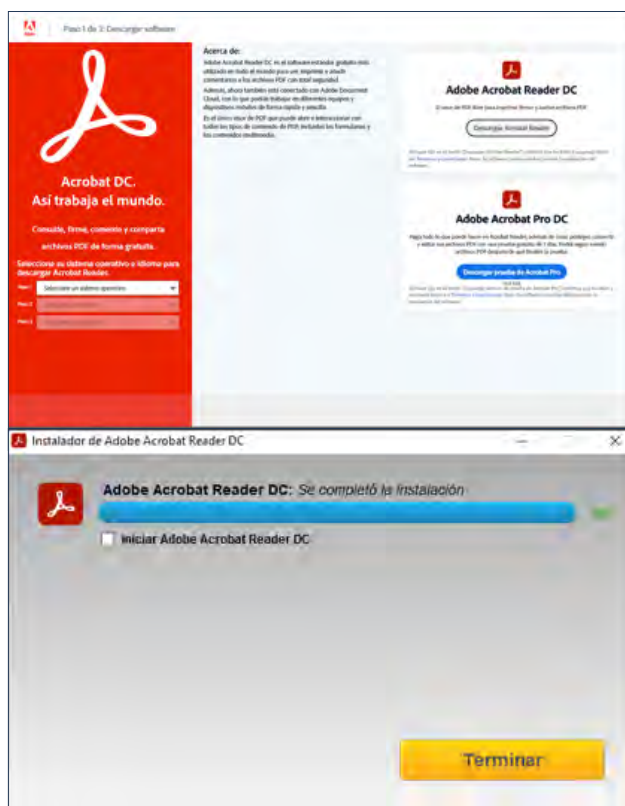
Ensuite, cliquez sur le bouton « **Télécharger Acrobat Reader** » pour lancer le téléchargement du fichier d'installation d'Adobe Acrobat, appelé « **reader[xxx]\_install.exe** ».

Une fois cette étape terminée, double-cliquez sur le fichier d'installation pour finaliser l'installation.

##### REMARQUE :

l'installation d'Acrobat Reader DC se fait en deux étapes : vous téléchargez le programme d'installation, puis vous installez Reader.

Cliquez sur **Terminer** et **redémarrez le système**. Vous êtes maintenant prêt à utiliser le programme.



## 3.6. Appliquer les valeurs de sécurité

Voici une description étape par étape de la procédure d'ajout des fichiers .admx et .adml et des paramètres pour la sécurisation renforcée d'Adobe Reader DC sur un ordinateur Windows.

### 3.6.1. Client Windows

Dans cet exemple, on suppose que l'ordinateur sur lequel les scripts doivent être exécutés est équipé du système d'exploitation Windows et d'Adobe Reader DC.

DESCRIPTION	
1.	Ouvrez une session avec un utilisateur qui a des droits d'administrateur et qui est membre du groupe « Utilisateur Shell » sur la machine où vous voulez exécuter les scripts.
2.	Copiez les fichiers et les dossiers qui accompagnent ce guide dans le répertoire « C:\Scripts » de l'ordinateur.
3.	Assurez-vous qu'au minimum les fichiers suivants ont été copiés dans le répertoire « C:\scripts » : <ul style="list-style-type: none"><li>– GP Report</li><li>– GPOs</li><li>– PolicyDefinitions</li><li>– Scripts_local</li></ul>
4.	Ensuite, allez dans le dossier « C:\Scripts_local » et exécutez le fichier « Import ADMX - Install GPO.bat » en tant qu'administrateur (option Exécuter en tant qu'administrateur).
5.	Les modèles d'administration seront ajoutés correctement et les valeurs des GPO seront importées.
6.	Lorsque l'exécution est terminée, appuyez à nouveau sur une touche pour fermer la fenêtre.
7.	Redémarrez le système.
<b>REMARQUE :</b> L'importation des paramètres de la stratégie de groupe locale à partir de la sauvegarde de la GPO contenue dans le dossier Scripts se fait à l'aide de l'outil gratuit LGPO.exe qui est un utilitaire de ligne de commande pour automatiser la gestion de la stratégie de groupe locale et qui fait partie du Microsoft Security Compliance Toolkit. URL de téléchargement : <a href="https://www.microsoft.com/download/details.aspx?id=55319">https://www.microsoft.com/download/details.aspx?id=55319</a>	

### 3.6.2. Serveur Windows : comment créer et gérer le magasin central des modèles d'administration des stratégies de groupe

Voici comment utiliser les fichiers .admx et .adml pour créer et gérer les paramètres de stratégie basés sur le registre dans Windows. Et aussi comment utiliser le magasin central pour stocker et répliquer les fichiers de stratégie de groupe d'Adobe Reader DC, qui accompagnent ce guide, dans un environnement de domaine.

#### LE MAGASIN CENTRAL

Pour tirer parti des fichiers .admx, vous devez créer un magasin central dans le dossier SYSVOL d'un contrôleur de domaine. Le magasin central est un emplacement de fichier qui est protégé par les outils de stratégie de groupe. Les outils de stratégie de groupe utilisent tous les fichiers .admx qui se trouvent dans le magasin central. Par la suite, les fichiers trouvés dans le magasin central sont répliqués sur tous les contrôleurs de domaine du domaine.

Pour créer un magasin central pour les fichiers .admx et .adml, créez un dossier nommé PolicyDefinitions à l'emplacement suivant :

**\\FQDN\SYSVOL\FQDN\policies**

**REMARQUE :** FQDN est un nom de domaine entièrement qualifié.

Par exemple, pour créer un magasin central pour le domaine contoso.com, créez un dossier PolicyDefinitions à l'emplacement suivant :

**\\contoso.com\SYSVOL\contoso.com\policies**

Copiez tous les fichiers du dossier PolicyDefinitions, qui accompagne ce guide, vers le dossier PolicyDefinitions du contrôleur de domaine. Le dossier PolicyDefinitions, qui accompagne ce guide, contient les fichiers .admx et .adml pour la langue espagnole (es-ES).

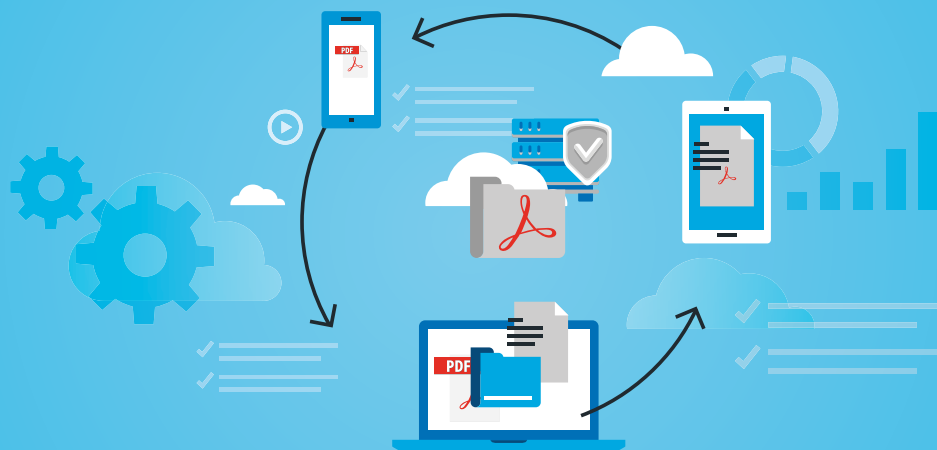
Maintenant, si vous ouvrez une GPMC et modifiez une politique existante, vous verrez que le nouveau type de modèle que vous avez activé avec le répertoire PolicyDefinitions apparaît dans les modèles administratifs, et aussi dans notre langue.

Dans le dossier GPO de ce guide, vous trouverez une GPO de sauvegarde avec les paramètres de sécurité.

## 3.7. Valeurs de registre



Voici les modifications de sécurité mises en œuvre au niveau du registre dans le cadre du processus d'amélioration de la sécurité exposé à la section « 3.6 Appliquer les paramètres de sécurité ».

<p>► <b>Adobe Reader DC doit empêcher l'ouverture de fichiers autres que PDF ou FDF</b></p>	<p>Les pièces jointes représentent un risque potentiel pour la sécurité car elles peuvent contenir des contenus malveillants, ouvrir d'autres fichiers dangereux ou lancer des applications.</p> <p>Les fichiers portant l'extension .bin, .exe, .bat, etc. seront reconnus comme des menaces.</p> <p>Cette fonction empêche les utilisateurs d'ouvrir ou de lancer des types de fichiers autres que PDF ou FDF et désactive l'option de menu.</p> <p>La valeur de « <b>iFileAttachmentPerms</b> » doit être définie sur « 1 » et le type défini sur « <b>REG_DWORD</b> ».</p>
<p><b>VÉRIFICATION</b></p>	<p><b>Chemin d'accès :</b> Édition&gt; Préférences&gt; Trust Manager&gt; Dans la section « PDF file attachments »&gt; Assurez-vous que la case pour « Allow opening non-PDF files with external applications » ne soit pas cochée et soit grisée (verrouillée)..</p> <p>REG QUERY HKEY_LOCAL_MACHINE\Software\Policies\Adobe\Acrobat Reader\DC\FeatureLockDown /v iFileAttachmentPerms</p>





### 3. Installation et sécurisation renforcée d'Adobe Reader DC piste continue sur Windows

 <b>Adobe Reader DC doit bloquer le contenu Flash</b>	<p>Adobe Reader et Acrobat ne sont plus livrés avec un lecteur Flash dédié depuis la version 9.5.1. Depuis lors, le rendu du contenu Flash dans un PDF exige que le lecteur Flash soit déjà sur la machine de l'utilisateur.</p> <p>Cette stratégie simplifie les déploiements d'Acrobat et de Reader en réduisant le nombre de mises à jour futures nécessaires en cas de problème de sécurité.</p> <p>Le contenu Flash peut être intégré dans les PDF et être utilisé pour installer un logiciel malveillant sur l'ordinateur d'un utilisateur.</p> <p>La valeur de « <b>bEnableFlash</b> » doit être fixée à « 0 » et le type configuré sur « REG_DWORD ».</p>
<b>VÉRIFICATION</b>	REG QUERY HKEY_LOCAL_MACHINE\Software\Policies\Adobe\Acrobat Reader\DC\FeatureLockDown /v bEnableFlash
 <b>Adobe Reader DC doit désactiver tout accès aux services Document Cloud Services</b>	<p>Par défaut, les services en ligne d'Adobe sont étroitement intégrés à Adobe Reader DC.</p> <p>Avec l'intégration d'<b>Adobe Document Cloud</b>, la désactivation de cette fonctionnalité évite le risque de vecteurs d'attaque supplémentaires.</p> <p>Dans Adobe Reader DC, les ressources Adobe Cloud nécessitent un abonnement payant pour chaque service.</p> <p>La valeur de « <b>bToggleAdobeDocumentServices</b> » doit être définie sur « 1 » et le type défini sur « REG_DWORD ».</p>
<b>VÉRIFICATION</b>	REG QUERY HKEY_LOCAL_MACHINE\Software\Policies\Adobe\Acrobat Reader\DC\FeatureLockDown\cServices /v bToggleAdobeDocumentServices
	<b>REMARQUE :</b> Le nom de clé <b>cServices</b> n'est pas créé par défaut dans l'installation d'Adobe Reader DC et doit être créé.

### 3. Installation et sécurisation renforcée d'Adobe Reader DC piste continue sur Windows

<p>▶ <b>Adobe Reader DC doit activer la sécurité renforcée dans une application distincte</b></p>	<p>Les fichiers PDF ont évolué, passant de pages statiques à des documents complexes dotés de fonctionnalités telles que des formulaires interactifs, du contenu multimédia, des scripts et d'autres fonctions.</p> <p>Ces caractéristiques rendent les fichiers PDF vulnérables aux scripts ou actions malveillantes qui peuvent endommager le système ou voler des données.</p> <p>La fonction de sécurité renforcée protège le système contre ces menaces en bloquant ou en autorisant sélectivement des actions pour des emplacements et des fichiers de confiance.</p> <p>La sécurité renforcée détermine si un PDF est visualisé dans une application autonome. L'ouverture d'un fichier PDF contenant un contenu exécutable malveillant constitue une menace pour les utilisateurs d'Adobe Reader DC.</p> <p>La sécurité renforcée « durcit » l'application contre les actions risquées telles que la prévention de l'accès multi-domaine, l'interdiction de l'injection de données et de scripts, le blocage de l'accès des scripts aux <b>XObjects</b>, l'impression silencieuse et l'exécution de JavaScript à haut privilège.</p> <p>La valeur de « <b>bEnhancedSecurityStandalone</b> » doit être définie sur « 1 » et le type défini sur « REG_DWORD ».</p>
<p><b>VÉRIFICATION</b></p>	<p><b>Chemin d'accès :</b> Édition&gt; Préférences&gt; Sécurité (renforcée)&gt; Dans la section 'Sécurité renforcée' &gt; La case pour 'Activer la sécurité renforcée' est cochée et grisée (verrouillée).</p> <p>REG QUERY <b>HKEY_LOCAL_MACHINE\Software\Policies\Adobe\Acrobat Reader\DC\FeatureLockDown /v bEnhancedSecurityStandalone</b></p>
<p>▶ <b>Adobe Reader DC doit désactiver les connecteurs web tiers</b></p>	<p>Lorsque les connecteurs web tiers sont désactivés, cela empêche la configuration d'Adobe Reader DC d'accéder à des services tiers pour le stockage de fichiers.</p> <p>La valeur de « <b>bToggleWebConnectors</b> » doit être définie sur « 1 » et le type défini sur « REG_DWORD ».</p>
<p><b>VÉRIFICATION</b></p>	<p>REG QUERY <b>HKEY_LOCAL_MACHINE\Software\Policies\Adobe\Acrobat Reader\DC\FeatureLockDown\cServices /v bToggleWebConnectors</b></p> <p><b>REMARQUE :</b> Le nom de clé <b>cServices</b> n'est pas créé par défaut dans l'installation d'Adobe Reader DC et doit être créé.</p>

### 3. Installation et sécurisation renforcée d'Adobe Reader DC piste continue sur Windows

<b>▶ Adobe Reader DC doit désactiver la synchronisation avec le cloud</b>	<p>Par défaut, les services en ligne d'Adobe sont étroitement intégrés à Adobe Reader DC.</p> <p>Lorsque la synchronisation <b>Adobe Cloud</b> est désactivée, elle empêche la synchronisation des préférences de bureau sur les appareils sur lesquels l'utilisateur est connecté avec un ID Adobe (y compris les téléphones).</p> <p>La valeur de « <b>bTogglePrefsSync</b> » doit être définie sur « 1 » et le type défini sur « REG_DWORD ».</p>
<b>VÉRIFICATION</b>	<p>REG QUERY HKEY_LOCAL_MACHINE\Software\Policies\Adobe\Acrobat Reader\DC\FeatureLockDown\cServices /v bTogglePrefsSync</p> <p><b>REMARQUE :</b> Le nom de clé cServices n'est pas créé par défaut dans l'installation d'Adobe Reader DC et doit être créé.</p>
<b>▶ Adobe Reader DC doit activer le mode FIPS</b>	<p>L'utilisation d'algorithmes de cryptage faibles ou non testés compromet l'objectif de la protection des données par cryptage.</p> <p>L'application doit mettre en œuvre des modules cryptographiques conformes aux normes les plus élevées approuvées par les entités, car cela garantit qu'ils ont été testés et validés.</p> <p>La valeur de « <b>bFIPSMODE</b> » doit être définie sur « 1 » et le type défini sur « REG_DWORD ».</p>
<b>VÉRIFICATION</b>	<p>REG QUERY HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral /v bFIPSMODE</p>
<b>▶ Adobe Reader DC doit désactiver l'accès à Webmail</b>	<p>Lorsque la messagerie Web est désactivée, l'utilisateur ne peut pas configurer un compte de messagerie Web pour envoyer un document PDF ouvert en tant que pièce jointe.</p> <p>Les utilisateurs doivent avoir la possibilité d'envoyer des documents en tant que pièces jointes de Microsoft Outlook.</p> <p>La différence est qu'Outlook doit être configuré par l'administrateur sur la machine locale.</p> <p>La valeur de « <b>bDisableWebmail</b> » doit être définie sur « 1 » et le type défini sur « REG_DWORD ».</p>
<b>VÉRIFICATION</b>	<p>REG QUERY HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral /v bFIPSMODE</p> <p><b>REMARQUE :</b> Le nom de clé cWebmailProfiles n'est pas créé par défaut dans l'installation d'Adobe Reader DC et doit être créé.</p>



### 3. Installation et sécurisation renforcée d'Adobe Reader DC piste continue sur Windows

<p>▶ <b>Adobe Reader DC doit désactiver la possibilité d'approuver (<i>trust</i>) les documents certifiés en tant qu'emplacement privilégié</b></p>	<p>Les emplacements privilégiés permettent à l'utilisateur de faire confiance de manière sélective aux fichiers, dossiers et hôtes pour contourner certaines restrictions de sécurité, telles que la sécurité renforcée et l'affichage protégé.</p> <p>Par défaut, l'utilisateur peut créer des emplacements privilégiés via la GUI.</p> <p>La désactivation des documents certifiés désactive et bloque la capacité de l'utilisateur final à élever les documents certifiés au rang d'emplacement privilégié.</p> <p>La valeur de « <b>bEnableCertificateBasedTrust</b> » doit être définie sur « 0 » et le type défini sur « REG_DWORD ».</p>
<p><b>VÉRIFICATION</b></p>	<p><b>Chemin d'accès :</b> Édition&gt; Préférences&gt; Sécurité (renforcée)&gt; Dans la section « Emplacement privilégié », vérifiez que l'option « Approuver automatiquement les documents avec une certification valide » est désactivée et grisée (verrouillée).</p> <p>REG QUERY <b>HKEY_LOCAL_MACHINE\Software\Policies\Adobe\Acrobat Reader\DC\FeatureLockDown /v bEnableCertificateBasedTrust</b></p>
<p>▶ <b>Adobe Reader DC doit bloquer les sites web</b></p>	<p>Cliquer sur un lien vers l'Internet représente un risque potentiel pour la sécurité.</p> <p>Les sites web malveillants peuvent transférer des contenus nuisibles ou collecter des données en silence.</p> <p>Les documents Acrobat Reader peuvent se connecter à des sites web qui peuvent représenter une menace potentielle pour les systèmes et cette fonctionnalité doit être bloquée.</p> <p>Cependant, les flux de documents PDF de confiance peuvent bénéficier d'un accès légitime aux sites Web avec un risque minimal.</p> <p>Par conséquent, il est possible d'approuver l'accès à des sites web et accepter le risque si l'accès offre un avantage et s'il s'agit d'un site de confiance ou si le risque associé à l'accès au site a été atténué.</p> <p>La valeur de « <b>iURLPerms</b> » doit être définie sur « 1 » et le type défini sur « REG_DWORD ».</p>

### 3. Installation et sécurisation renforcée d'Adobe Reader DC piste continue sur Windows

<b>VÉRIFICATION</b>	<p><b>Chemin d'accès :</b> Édition&gt; Préférences&gt; Gestionnaire d'approbations&gt; Dans la section « Accès Internet des fichiers PDF en dehors du navigateur Web »&gt; Sélectionnez l'option « Modifier les paramètres »&gt; Dans la section « Les fichiers PDF peuvent se connecter à des sites Web pour partager ou obtenir des informations »&gt; Vérifiez que le bouton radio « Bloquer l'accès des fichiers PDF à tous les sites Web » est sélectionné et désactivé (verrouillé).</p> <p>REG QUERY HKEY_LOCAL_MACHINE\Software\Policies\Adobe\Acrobat Reader\DC\FeatureLockDown\cDefaultLaunchURLPerms /v "iURLPerms"</p>
<p>▶ <b>Adobe Reader DC doit activer le mode protégé</b></p>	<p>L'ouverture d'un fichier PDF contenant un contenu exécutable malveillant constitue une menace pour les utilisateurs d'Adobe Reader DC.</p> <p>Le sandboxing est une technique permettant de créer un environnement d'exécution isolé, qui autorise l'exécution de programmes non fiables.</p> <p>Dans le contexte d'Adobe Reader, un « programme non fiable » est un PDF et les processus qu'il invoque.</p> <p>Lorsque le sandboxing est activé, Reader part du principe que tous les fichiers PDF sont potentiellement malveillants et limite tout traitement en l'invoquant.</p> <p>Cette isolation des fichiers PDF réduit le risque de failles de sécurité dans les zones situées en dehors du bac à sable.</p> <p>La valeur de « <b>bProtectedMode</b> » doit être définie sur « 1 » et le type défini sur « REG_DWORD ».</p>
<b>VÉRIFICATION</b>	<p><b>Chemin d'accès :</b> Édition&gt;Préférences&gt; Sécurité (renforcée)&gt; Protections du site de test&gt; Activer le mode protégé au démarrage.</p> <p>REG QUERY HKEY_LOCAL_MACHINE\Software\Policies\Adobe\Acrobat Reader\DC\FeatureLockDown /v bProtectedMode</p>

### 3. Installation et sécurisation renforcée d'Adobe Reader DC piste continue sur Windows

 <b>Adobe Reader DC doit activer l'affichage protégé</b>	<p>Il s'agit essentiellement d'un mode de lecture seule. Cette fonction est basée sur la technique sandbox.</p> <p>Dans Reader, l'affichage protégé n'est pris en charge que lorsque le « mode protégé » est activé. Si une clé de registre <b>HKCU</b> ou <b>HKLM Protected Mode</b> est définie sur 0 (désactivé), l'affichage protégé ne peut pas être activé.</p> <p>La valeur de « <b>iProtectedView</b> » doit être définie sur « 2 » et le type défini sur « REG_DWORD ».</p>
<b>VÉRIFICATION</b>	<p><b>Chemin d'accès</b> : Edition&gt; Préférences&gt; Sécurité (Renforcée)&gt; Affichage protégé (Tous les fichiers).</p> <p>REG QUERY <b>HKEY_LOCAL_MACHINE\Software\Policies\Adobe\Acrobat Reader\DC\FeatureLockDown /v iProtectedView</b></p>
 <b>Adobe Reader DC doit activer la sécurité renforcée dans un navigateur</b>	<p>Les fichiers PDF ont évolué, passant de pages statiques à des documents complexes dotés de fonctionnalités telles que des formulaires interactifs, du contenu multimédia, des scripts et d'autres fonctions.</p> <p>La sécurité renforcée bloque des comportements spécifiques tels que : l'injection de données, l'injection de scripts, l'impression silencieuse, les liens web (s'ils ne sont pas autorisés par les paramètres du <b>Trust Manager</b>), l'accès inter-domaines et l'accès à des flux externes.</p> <p>La valeur de « <b>bEnhancedSecurityInBrowser</b> » doit être définie sur « 1 » et le type défini sur « REG_DWORD ».</p>
<b>VÉRIFICATION</b>	<p><b>Chemin d'accès</b> : Édition&gt; Préférences&gt; Sécurité (renforcée)&gt; Sécurité renforcée &gt; Activer la sécurité renforcée.</p> <p>REG QUERY <b>HKEY_LOCAL_MACHINE\Software\Policies\Adobe\Acrobat Reader\DC\FeatureLockDown /v bEnhancedSecurityInBrowser</b></p>

### 3. Installation et sécurisation renforcée d'Adobe Reader DC piste continue sur Windows

<p>▶ <b>Adobe Reader DC doit bloquer l'accès aux sites web inconnus</b></p>	<p>Étant donné que l'accès à l'Internet constitue un risque potentiel pour la sécurité, le fait de cliquer sur un lien vers un site Web inconnu représente un risque potentiel pour la sécurité. Les sites web malveillants peuvent transférer des contenus nuisibles ou collecter silencieusement des données.</p> <p>La valeur de « <b>iUnknownURLPerms</b> » doit être fixée à « 3 » et le type à « REG_DWORD ».</p>
<p><b>VÉRIFICATION</b></p>	<p><b>Chemin d'accès :</b> Édition&gt; Préférences&gt; Gestionnaire d'approbations&gt; Accès Internet des fichiers PDF en dehors du navigateur Web&gt; Modifier les paramètres&gt; Bloquer l'accès des fichiers PDF à tous les sites Web.</p> <p>REG QUERY <b>HKEY_LOCAL_MACHINE\Software\Policies\Adobe\Acrobat Reader\DC\FeatureLockDown\cDefaultLaunchURLPerms /v iUnknownURLPerms</b></p>
<p>▶ <b>Adobe Reader DC doit désactiver Online SharePoint Access</b></p>	<p>Désactive les fonctions d'intégration de SharePoint et d'Office 365.</p> <p>Contrôle la capacité de l'application à détecter qu'un fichier provient d'un serveur SharePoint. Désactive la demande d'extraction et supprime les éléments de menu spécifiques à SharePoint.</p> <p>La valeur de « <b>bDisableSharePointFeatures</b> » doit être définie sur « 1 » et le type défini sur « REG_DWORD ».</p>
<p><b>VÉRIFICATION</b></p>	<p>REG QUERY <b>HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Adobe\Acrobat Reader\DC\FeatureLockDown\cSharePoint /v bDisableSharePointFeatures</b></p> <p><b>REMARQUE :</b> Le nom de clé <b>cSharePoint</b> n'est pas créé par défaut dans l'installation d'Adobe Reader DC et doit être créé.</p>



### 3. Installation et sécurisation renforcée d'Adobe Reader DC piste continue sur Windows

<p>▶ <b>Adobe Reader DC doit désactiver la possibilité d'approuver les confiances d'IE à des emplacements privilégiés</b></p>	<p>Les emplacements privilégiés permettent à l'utilisateur de faire confiance de manière sélective aux fichiers, dossiers et hôtes pour contourner certaines restrictions de sécurité, telles que la sécurité renforcée et l'affichage protégé.</p> <p>La désactivation de la confiance d'IE dans les emplacements privilégiés désactive et bloque la capacité de l'utilisateur final à traiter les sites de confiance d'IE comme un emplacement privilégié.</p> <p>La valeur de « <b>bDisableTrustedSites</b> » doit être définie sur « 1 » et le type défini sur « REG_DWORD ».</p>
<p><b>VÉRIFICATION</b></p>	<p><b>Chemin d'accès :</b> Édition&gt; Préférences&gt; Sécurité (renforcée)&gt; Emplacements privilégiés &gt; Ajouter hôte. Cette option doit être grisée et désactivée.</p> <p>REG QUERY <b>HKEY_LOCAL_MACHINE\Software\Policies\Adobe\Acrobat Reader\DC\FeatureLockDown /v bDisableTrustedSites</b></p>
<p>▶ <b>Adobe Reader DC doit désactiver la possibilité d'ajouter des fichiers et des dossiers de confiance</b></p>	<p>Désactive les dossiers et fichiers de confiance et empêche les utilisateurs de spécifier un emplacement privilégié pour les répertoires.</p> <p>La valeur de « <b>bDisableTrustedFolders</b> » doit être définie sur « 1 » et le type défini sur « REG_DWORD ».</p>
<p><b>VÉRIFICATION</b></p>	<p><b>Chemin d'accès :</b> Édition &gt; Préférences &gt; Sécurité (renforcée) &gt; Emplacements privilégiés &gt; Ajouter un chemin de dossier. Cette option doit être grisée et désactivée.</p> <p>REG QUERY <b>HKEY_LOCAL_MACHINE\Software\Policies\Adobe\Acrobat Reader\DC\FeatureLockDown /v bDisableTrustedFolders</b></p>
<p>▶ <b>Adobe Reader DC doit désactiver la possibilité de spécifier des emplacements privilégiés basés sur l'hôte</b></p>	<p>Désactive et bloque la possibilité de spécifier des emplacements privilégiés basés sur l'hôte.</p> <p>La valeur de « <b>bDisableOSTrustedSites</b> » doit être définie sur « 1 » et le type défini sur « REG_DWORD ».</p>
<p><b>VÉRIFICATION</b></p>	<p><b>Chemin d'accès :</b> Édition &gt; Préférences &gt; Sécurité (renforcée) &gt; Emplacements privilégiés &gt; Faire automatiquement confiance aux sites de mes zones de sécurité Win OS. Cette option doit être désactivée.</p> <p>REG QUERY <b>HKEY_LOCAL_MACHINE\Software\Policies\Adobe\Acrobat Reader\DC\FeatureLockDown /v bDisableOSTrustedSites</b></p>

### 3. Installation et sécurisation renforcée d'Adobe Reader DC piste continue sur Windows

<p>▶ <b>Adobe Reader DC doit désactiver la possibilité de modifier le pilote par défaut</b></p>	<p>Désactive la possibilité de changer le pilote spécifique par défaut (visionneur de PDF).</p> <p>La valeur de « <b>bDisablePDFHandlerSwitching</b> » doit être définie sur « 1 » et le type défini sur « REG_DWORD ».</p>
<p><b>VÉRIFICATION</b></p>	<p><b>Chemin d'accès :</b> Édition &gt; Préférences &gt; Général &gt; Sélectionner comme pilote PDF par défaut. Cette option doit être grisée et désactivée.</p> <p>REG QUERY HKEY_LOCAL_MACHINE\Software\Policies\Adobe\Acrobat Reader\DC\FeatureLockDown /v bDisablePDFHandlerSwitching</p>
<p>▶ <b>Adobe Reader DC doit désactiver le module complémentaire Adobe Send and Track pour Outlook</b></p>	<p>Lorsqu'il est activé, un bouton Adobe « Envoyer et suivre » apparaît dans Outlook lors de la rédaction d'un courrier électronique.</p> <p>Permet d'envoyer des fichiers volumineux en tant que liens publics via Outlook.</p> <p>Les pièces jointes sont téléchargées sur Adobe Document Cloud et des liens publics vers les fichiers sont insérés dans le corps du courriel.</p> <p>Les destinataires peuvent cliquer sur le lien pour prévisualiser le fichier dans une fenêtre de navigateur et peuvent le télécharger si nécessaire.</p> <p>La valeur de « <b>bAdobeSendPluginToggle</b> » doit être définie sur « 1 » et le type défini sur « REG_DWORD ».</p>
<p><b>VÉRIFICATION</b></p>	<p>REG QUERY HKEY_LOCAL_MACHINE\Software\Policies\Adobe\Acrobat Reader\DC\FeatureLockDown\cServices /v bAdobeSendPluginToggle</p> <p><b>REMARQUE :</b> le nom de la clé cCloud n'est pas créé par défaut dans l'installation d'Adobe Reader DC et doit être créé.</p>

### 3. Installation et sécurisation renforcée d'Adobe Reader DC piste continue sur Windows

<p>▶ <b>Adobe Reader DC doit désactiver Adobe Send for Signature (Adobe Sign)</b></p>	<p>Désactivez <b>Adobe Send for Signature</b> (Adobe Sign).</p> <p>Le service de signature <b>Adobe Document Cloud</b> permet aux utilisateurs d'envoyer des documents en ligne pour signature et de signer depuis n'importe quel endroit ou appareil.</p> <p>Les documents signés sont stockés dans le cloud Adobe.</p> <p>Le service de signature <b>Adobe Document Cloud</b> fonctionne sur la base d'un abonnement.</p> <p>Lorsqu'<b>Adobe Send for Signature</b> est désactivé, les utilisateurs ne peuvent pas utiliser la fonction de signature d'<b>Adobe Document Cloud</b>.</p> <p>La valeur de « <b>bToggleAdobeSign</b> » doit être définie sur « 1 » et le type défini sur « REG_DWORD ».</p>
<p><b>VÉRIFICATION</b></p>	<p>REG QUERY HKEY_LOCAL_MACHINE\Software\Policies\Adobe\Acrobat Reader\DC\FeatureLockDown\cServices /v bToggleAdobeSign</p> <p><b>REMARQUE :</b> le nom de la clé cCloud n'est pas créé par défaut dans l'installation d'Adobe Reader DC et doit être créé.</p>
<p>▶ <b>Adobe Reader DC doit désactiver la fonction de réparation d'Adobe</b></p>	<p>Lorsque la fonction de réparation est désactivée, l'utilisateur n'a pas l'option (menu Aide) ou la fonctionnalité pour réparer une installation d'Adobe Reader DC.</p> <p>La valeur de « <b>DisableMaintenance</b> » doit être définie sur « 1 » et le type défini sur « REG_DWORD ».</p>
<p><b>VÉRIFICATION</b></p>	<p><b>Chemin d'accès :</b> Aide&gt; Réparer l'installation. Cette option doit être grisée et désactivée.</p> <p><b>Pour 32 bits:</b> REG QUERY HKEY_LOCAL_MACHINE\Software\Adobe\Acrobat Reader\DC\Installer /v DisableMaintenance</p> <p><b>Pour 64 bits:</b> REG QUERY HKEY_LOCAL_MACHINE\Software\Wow6432Node\Adobe\Acrobat Reader\DC\Installer /v DisableMaintenance</p>

### 3. Installation et sécurisation renforcée d'Adobe Reader DC piste continue sur Windows

<p>▶ <b>Adobe Reader DC doit désactiver le téléchargement périodique des certificats Adobe</b></p>	<p>Indique si les certificats approuvés peuvent être téléchargés périodiquement depuis Adobe.</p> <p>La valeur de « <b>bLoadSettingsFromURL</b> » doit être définie sur « 0 » et le type défini sur « REG_DWORD ».</p>
<p><b>VÉRIFICATION</b></p>	<p><b>Chemin d'accès :</b> Édition&gt; Préférences&gt; Gestionnaire d'approbations&gt; Mises à jour automatiques de Adobe Approved Trust List (AATL)&gt; Charger les certificats approuvés à partir d'un serveur AATL d'Adobe. La case doit être décochée.</p> <p>REG QUERY HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\Security\cDigSig\cAdobeDownload /v bLoadSettingsFromURL</p> <p><b>REMARQUE :</b> les noms de clés cDigSig et cAdobeDownload ne sont pas créés par défaut dans l'installation d'Adobe Reader DC et doivent être créés.</p>
<p>▶ <b>Adobe Reader DC doit désactiver le téléchargement périodique des certificats européens</b></p>	<p>Indique si les certificats de confiance peuvent être téléchargés périodiquement depuis Adobe.</p> <p>La valeur de « <b>bLoadSettingsFromURL</b> » doit être définie sur « 0 » et le type défini sur « REG_DWORD ».</p>
<p><b>VÉRIFICATION</b></p>	<p><b>Chemin d'accès :</b> Modifier &gt; Préférences&gt; Gestionnaire d'approbations &gt; Mises à jour automatiques de listes européennes (EUTL)&gt; Charger les certificats approuvés depuis un serveur EUTL d'Adobe. La case ne doit pas être cochée.</p> <p>REG QUERY HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\Security\cDigSig\cEUTLDownload /v bLoadSettingsFromURL</p> <p><b>REMARQUE :</b> les noms de clés cDigSig et cEUTLDownload ne sont pas créés par défaut dans l'installation d'Adobe Reader DC et doivent être créés.</p>
<p>▶ <b>Adobe Reader DC doit désactiver Acrobat Upsell</b></p>	<p>Pour les produits DC, désactivez les messages qui encouragent l'utilisateur à mettre à niveau le produit. Par exemple, les utilisateurs de Reader peuvent acheter des outils et des fonctionnalités supplémentaires.</p> <p>La valeur de « <b>bLoadSettingsFromURL</b> » doit être définie sur « 1 » et le type défini sur « REG_DWORD ».</p>
<p><b>VÉRIFICATION</b></p>	<p>REG QUERY HKEY_LOCAL_MACHINE\Software\Policies\Adobe\Acrobat Reader\DC\FeatureLockDown /v bAcroSuppressUpsell</p>

### 3. Installation et sécurisation renforcée d'Adobe Reader DC piste continue sur Windows

 <b>Adobe Reader DC doit désactiver l'écran de bienvenue d'Adobe</b>	<p>Désactive l'écran de bienvenue au démarrage de l'application.</p> <p>La valeur de « <b>bShowWelcomeScreen</b> » doit être définie sur « 0 » et le type défini sur « REG_DWORD ».</p>
<b>VÉRIFICATION</b>	<p><b>Chemin d'accès :</b> Édition &gt; Préférences &gt; Général &gt; Démarrage de l'application &gt; Afficher l'écran d'accueil. La case doit être décochée.</p> <p>REG QUERY HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Adobe\Acrobat Reader\DC\FeatureLockDown\cWelcomeScreen /v bShowWelcomeScreen</p> <p><b>REMARQUE :</b> Le nom de clé cWelcomeScreen n'est pas créé par défaut dans l'installation d'Adobe Reader DC et doit être créé.</p>
 <b>Adobe Reader DC doit désactiver à la fois les mises à jour des composants du plug-in web du produit et tous les services</b>	<p>Par défaut, les services en ligne d'Adobe sont intégrés de manière transparente dans Adobe Reader DC.</p> <p>La désactivation des mises à jour des services désactive les mises à jour des composants du plug-in web du produit et de tous les services sans exception, y compris les écrans de connexion en ligne.</p> <p>La valeur de « <b>bUpdater</b> » doit être définie sur « 0 » et le type défini sur « REG_DWORD ».</p>
<b>VÉRIFICATION</b>	<p>REG QUERY HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Adobe\Acrobat Reader\DC\FeatureLockDown\cServices /v bUpdater</p> <p><b>REMARQUE :</b> Le nom de clé cServices n'est pas créé par défaut dans l'installation d'Adobe Reader DC et doit être créé.</p>
 <b>Adobe Reader DC doit désactiver les mises à jour du produit</b>	<p>Désactiver les mises à jour du produit.</p> <p>La valeur de « <b>bUpdater</b> » doit être définie sur « 0 » et le type défini sur « REG_DWORD ».</p>
<b>VÉRIFICATION</b>	<p>REG QUERY HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Adobe\Acrobat Reader\DC\FeatureLockDown /v bUpdater</p>

### 3. Installation et sécurisation renforcée d'Adobe Reader DC piste continue sur Windows

#### Valeurs de registre supplémentaires

##### Options du lecteur

Apple ne fournit plus de mises à jour de sécurité pour les anciens logiciels QuickTime pour Windows, ce qui rend ces logiciels vulnérables à l'exploitation. Par conséquent, pour protéger Reader, Adobe a également supprimé la prise en charge de QuickTime sous Windows. Reader DC utilise désormais le lecteur vidéo intégré de Windows pour lire les anciennes vidéos QuickTime, c'est-à-dire les vidéos intégrées dans les documents PDF créés avec Acrobat 9 et les versions antérieures. Si cette option n'est pas sélectionnée et que QuickTime Player n'est pas disponible, Windows utilise son lecteur intégré.

**Chemin d'accès :** Édition > Préférences > Multimédia (ancien) > sous « Options du lecteur », vérifiez que « Ne pas utiliser QuickTime Player pour les éléments multimédias » est coché.

##### JavaScript

Permet d'ajuster le comportement de l'application afin que JavaScript s'exécute au niveau de sécurité souhaité. Cela permet de limiter l'accès de l'application aux API JavaScript et d'isoler les flux de travail qui ne nécessitent pas d'API JavaScript.

Décochez cette option pour désactiver complètement JavaScript ou restreindre JavaScript via les API.

**Chemin d'accès :** Édition > Préférences > JavaScript > sous « JavaScript » vérifiez que « Enable Javascript for Acrobat » est décoché.

##### Documents dans la liste des fichiers récents

La liste des fichiers récents fournit des raccourcis vers vos fichiers récemment ouverts. Il s'agit d'un manque de confidentialité si vous partagez l'appareil avec quelqu'un.

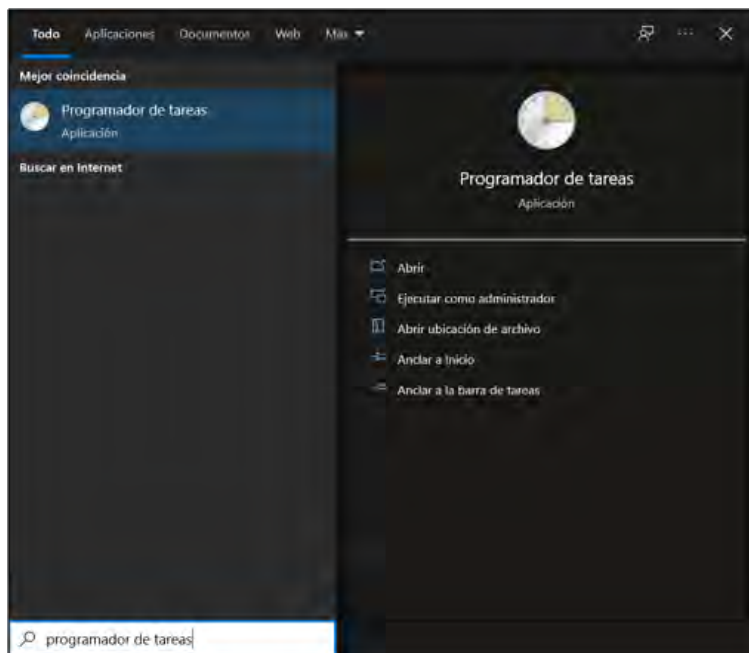
En réduisant cette option à zéro, la liste récente est désactivée.

**Chemin d'accès :** Édition > Préférences > Documents > sous « Paramètres d'ouverture » vérifiez que « Documents dans la liste des fichiers récents » : est réglé sur zéro (0).

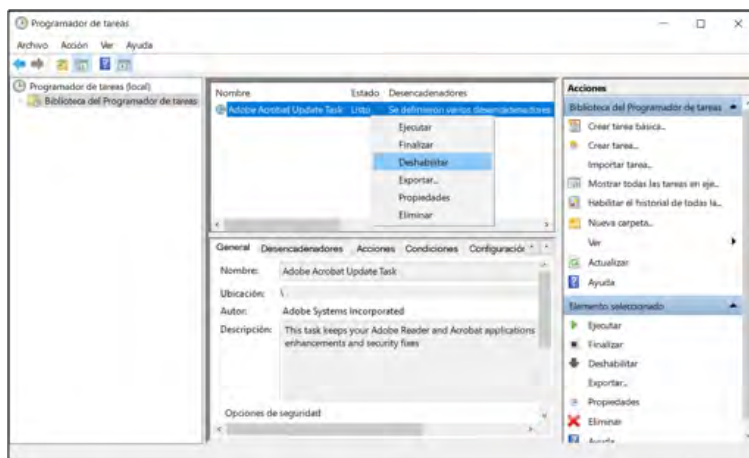
## 3.8. Desactiver la tache de mise a jour d'Adobe Acrobat

La première étape pour désactiver la mise à jour automatique d'Adobe Reader consiste à désactiver la « tâche de mise à jour d'Adobe Acrobat » dans le planificateur de tâches. Pour ce faire :

- ▶ Dans la boîte de recherche, tapez : **planificateur de tâches**
- ▶ Ouvrez le planificateur de tâches et exécutez en tant qu'administrateur



- ▶ Cliquez sur **Bibliothèque de planification des tâches** dans la partie gauche, puis dans le volet de droite, cliquez avec le bouton droit de la souris sur la **tâche de mise à jour d'Adobe Acrobat** et sélectionnez **Désactiver**.





## 3.9. Désactiver le service AdobeARMservice

Voici une description étape par étape de la manière de configurer le service AdobeARMservice sur une machine Windows autonome.

Dans cet exemple, on suppose que l'ordinateur sur lequel cette fonctionnalité doit être désactivée est équipé du système d'exploitation Windows et d'Adobe Reader DC.

DESCRIPTION	
1.	Connectez-vous avec un utilisateur qui a des privilèges d'administrateur et qui est membre du groupe « <b>Utilisateurs Shell</b> » sur la machine où vous voulez désactiver AdobeARMservice.
2.	Copiez les fichiers et dossiers accompagnant ce guide dans le répertoire « <b>C:\scripts</b> » de votre ordinateur.
3.	Assurez-vous qu'au minimum les fichiers suivants ont été copiés dans le répertoire « <b>C:\Scripts_local_Scripts</b> » : – <b>AdobeARMservice.bat</b> – <b>AdobeARMservice.inf</b>
4.	Ensuite, allez dans le dossier « <b>C:\Scripts_local</b> » et exécutez le fichier « <b>AdobeARMservice.bat</b> » en tant qu'administrateur (option Exécuter en tant qu'administrateur).
5.	Vous devrez saisir à nouveau les informations d'identification de l'utilisateur avec des privilèges d'administrateur.
6.	Dans la fenêtre pop-up, appuyez sur une touche pour lancer l'exécution du script. Lorsque l'exécution est terminée, appuyez à nouveau sur une touche pour fermer la fenêtre.
7.	Le service « <b>AdobeARMservice</b> » a été désactivé avec succès.
<b>REMARQUE :</b> Pour les machines clientes reliées à un domaine, il est recommandé de désactiver le service <b>AdobeARMservice</b> via les stratégies de groupe définies dans le domaine	

# 4. Liste de contrôle (évaluation)

CRITICITÉ	VÉRIFICATION
Élevée	Les dernières mises à jour logicielles relatives à la sécurité doivent être installées sur Adobe Reader DC.
Moyenne	Adobe Reader DC doit désactiver le service de mise à jour « <b>AdobeARMservice</b> ».
Moyenne	Adobe Reader DC doit éviter d'ouvrir des fichiers autres que des fichiers PDF ou FDF.
Moyenne	Adobe Reader DC doit bloquer le contenu Flash.
Moyenne	Adobe Reader DC doit désactiver tout accès aux services de <b>Document Cloud Services</b> .
Moyenne	Adobe Reader DC doit activer la sécurité renforcée dans une application distincte.
Moyenne	Adobe Reader DC doit désactiver les connecteurs web tiers.
Moyenne	Adobe Reader DC doit désactiver la synchronisation avec le cloud.
Moyenne	Adobe Reader DC doit activer le mode FIPS.
Moyenne	Adobe Reader DC doit désactiver l'accès au <b>Webmail</b> .
Moyenne	Adobe Reader DC doit désactiver la possibilité d'approuver ( <b>trust</b> ) les documents certifiés en tant qu'emplacement privilégié.
Moyenne	Adobe Reader DC doit bloquer les sites web.
Moyenne	Adobe Reader DC doit activer Protected View.

#### 4. Liste de contrôle (évaluation)

CRITICITÉ	VÉRIFICATION
Moyenne	Adobe Reader DC doit activer le mode protégé.
Moyenne	Adobe Reader DC doit activer la sécurité renforcée dans un navigateur.
Moyenne	Adobe Reader DC doit bloquer l'accès aux sites web inconnus.
Moyenne	Adobe Reader DC doit désactiver <b>Online SharePoint Access</b> .
Moyenne	Adobe Reader DC doit désactiver la possibilité d'approuver les confiances d'IE à des emplacements privilégiés.
Moyenne	Adobe Reader DC doit désactiver la possibilité d'ajouter des fichiers et des dossiers approuvés.
Moyenne	Adobe Reader DC doit désactiver la possibilité de spécifier des emplacements privilégiés basés sur l'hôte.
Faible	Adobe Reader DC doit désactiver la possibilité de modifier le pilote par défaut.
Faible	Adobe Reader DC doit désactiver le module complémentaire Adobe Send and Track pour Outlook.
Faible	Adobe Reader DC doit désactiver <b>Adobe Send for Signature</b> .
Faible	Adobe Reader DC doit désactiver la fonction de réparation d'Adobe.
Faible	Adobe Reader DC doit désactiver le téléchargement périodique des certificats Adobe.
Faible	Adobe Reader DC doit désactiver le téléchargement périodique des certificats européens.
Faible	Adobe Reader DC doit désactiver Acrobat <b>Upsell</b> .
Faible	Adobe Reader DC doit désactiver l'écran de bienvenue d'Adobe.
Faible	Adobe Reader DC doit désactiver les mises à jour de service.

# 5. Décalogue de recommandations

## Décalogue de sécurité pour Acrobat Reader DC

- 1 Utilisez toujours la dernière version d'Adobe.
- 2 Il est conseillé d'examiner toutes les fonctions de sécurité du logiciel, car elles constituent une défense supplémentaire contre les attaques.
- 3 Il est recommandé de verrouiller l'interface utilisateur afin que l'utilisateur final ne puisse pas modifier les paramètres.
- 4 Le nettoyage des métadonnées est recommandé lorsque les fichiers PDF sont accessibles au public.
- 5 Il est recommandé d'utiliser Adobe Reader DC uniquement pour ouvrir les fichiers PDF ou FDF.
- 6 Il est recommandé d'utiliser un certificat numérique pour signer les documents PDF afin d'en garantir la paternité contre d'éventuelles manipulations ou modifications par des tiers.
- 7 Il est recommandé de ne pas utiliser de **plugins** tiers.
- 8 Il est recommandé de bloquer les liens vers l'internet dans les fichiers PDF.
- 9 Il est recommandé d'activer le mode et l'affichage protégés.
- 10 Il est recommandé de bloquer tout type de connexion Internet depuis les fichiers PDF.

# ANNEXE. Scripts de configurations securisees

Pour faciliter la mise en œuvre du correctif de sécurité Acrobat Reader DC, un dossier script est inclus dans ce document, qui contient les fichiers nécessaires à la sécurisation renforcée du programme.

L'objectif des scripts est d'exécuter automatiquement des scripts, en atténuant autant que possible les défaillances causées lors de la sécurisation d'un système ou d'un programme spécifique.

Les fichiers ou dossiers inclus dans le dossier « **Scripts** » sont énumérés ci-dessous.

GP Report	<ul style="list-style-type: none"><li>Adobe Reader DC Continuo - equipo.htm</li><li>Adobe Reader DC Continuo - usuario.htm</li></ul>
GPOs	<ul style="list-style-type: none"><li>{5FDCB222-F465-4C7C-864B-E5EE4E8BFA09}</li><li>{CD465C95-EA48-4901-A8F1-41A65B64ECFA}</li></ul>
PolicyDefinitions	<ul style="list-style-type: none"><li>fr-FR<ul style="list-style-type: none"><li>AcrobatReaderDC.adml</li></ul></li><li>AcrobatReaderDC.admx</li></ul>
Scripts_local	<ul style="list-style-type: none"><li>Outils<ul style="list-style-type: none"><li>LGPO.exe</li></ul></li><li>Import ADMX - Install GPO.bat</li><li>Import ADMX - Install GPO.ps1</li><li>AdobeARMservice.bat</li><li>AdobeARMservice.ps1</li></ul>



[www.ccn.cni.es](http://www.ccn.cni.es)

[www.ccn-cert.cni.es](http://www.ccn-cert.cni.es)

[oc.ccn.cni.es](mailto:oc.ccn.cni.es)

