Dell Data Guardian

Guide d'utilisation v1.2

Remarques, précautions et avertissements

REMARQUE : Une REMARQUE indique des informations importantes qui peuvent vous aider à mieux utiliser votre produit.

PRÉCAUTION : Une PRÉCAUTION indique un risque d'endommagement du matériel ou de perte de données et vous indique comment éviter le problème.

AVERTISSEMENT : Un AVERTISSEMENT indique un risque d'endommagement du matériel, de blessures corporelles ou même de mort.

Dell Data Guardian User Guide (Guide d'utilisation de Dell Data Guardian)

2017 - 04

Rév. A01

Table des matières

1

Introduction à Dell Data Guardian

Le *Dell Data Guardian User Guide* (Guide d'utilisation de Dell Data Guardian) contient les informations nécessaires pour installer et utiliser Dell Data Guardian.

Présentation

En fonction des règles définies par un administrateur, Dell Data Guardian protège les données, notamment :

- Systèmes de partage de fichiers basés sur le cloud : les ordinateurs ou périphériques mobiles Windows capturent des données destinées au stockage cloud, cryptent ces données puis les chargent dans le cloud.
- Les documents Office stockés localement, partagés avec d'autres utilisateurs de différentes façons ou stockés sur un média amovible. Vous pouvez protéger les documents Office suivants : .docx, .pptx, .xlsx, .docm, .pptm, .xlsm.

> **REMARQUE :**
> Votre administrateur vous indiquera si votre entreprise utilise Data Guardian avec stockage cloud uniquement, documents Office uniquement ou les deux.

Vous pouvez utiliser Data Guardian sur les plates-formes suivantes :

- Windows
- iOS
- Android
- Ce produit comme Data Guardian pour Mac peut ouvrir les fichiers cryptés par l'autre produit.
  - Ce document concerne Dell Data Guardian pour Windows uniquement.
  - Pour obtenir des informations utilisateur à propos de Dell Data Guardian pour Mac, voir l'aide en ligne dans le logiciel.

Assistance supplémentaire

Si vous avez toujours besoin d'aide après avoir lu ce document, veuillez vous adresser à votre administrateur.

2

Configuration requise pour Dell Data Guardian

Ce chapitre présente la configuration matérielle et logicielle requise pour le client.

REMARQUE :
IPv6 n'est pas pris en charge.

Serveur

Data Guardian nécessite que le client soit connecté à un serveur Dell Enterprise Server ou Dell Enterprise Server - VE, v9.6 ou version ultérieure. Dans ce document, les deux serveurs sont appelés « serveur Dell », sauf lorsqu'il est nécessaire de désigner une version spécifique (par exemple, une procédure varie en cas d'utilisation du serveur d'entreprise Dell - VE).

Client Encryption

- Les meilleures pratiques informatiques doivent être suivies pendant le déploiement. Ceci inclut, sans s'y limiter, les environnements de test contrôlés pour les premiers tests et les déploiements échelonnés pour les utilisateurs.
- Le compte utilisateur servant à l'installation/la mise à jour/la désinstallation doit correspondre à un administrateur local ou de domaine, qui peut être affecté temporairement par un outil de déploiement tel que Microsoft SMS ou Dell KACE. Les utilisateurs non-administrateurs et disposant de privilèges particuliers ne sont pas pris en charge.
- Sauvegardez toutes les données importantes avant de démarrer l'installation/désinstallation.
- Lors de l'installation, n'apportez aucune modification à l'ordinateur, notamment, n'insérez ou ne retirez pas de lecteurs externes (USB).
- Bien que le client de cryptage ne soit pas nécessaire, n'importe quel client de chiffrement utilisé avec Data Guardian doit correspondre à la version v8.12 ou ultérieure.
- Data Guardian n'est pas pris en charge avec Microsoft Office 365.
- Pour le cryptage cloud, l'ordinateur doit disposer d'un lecteur de disque (valeur de lettre) attribuable disponible.
- Vérifiez que les périphériques cibles sont connectés à https://nomdevotreserveurdesécurité.domaine.com:8443/cloudweb/register et https://nomdevotreserveurdesécurité.domaine.com:8443/cloudweb.
- Avant de déployer Data Guardian, il est préférable de ne pas avoir créé de compte de stockage Cloud sur les périphériques cibles.

  Si les utilisateurs décident de conserver leurs comptes existants, ils doivent déplacer tout fichier devant rester *non crypté* en dehors du client de synchronisation avant d'installer Data Guardian.
- L'utilisateur doit être prêt à redémarrer son ordinateur Windows une fois l'installation du client terminée.
- Data Guardian ne perturbe pas le fonctionnement des clients de synchronisation. Les administrateurs et les utilisateurs finals doivent donc se familiariser avec le fonctionnement de ces applications avant de déployer Data Guardian. Pour plus d'informations, reportez-vous au support Box sur https://support.box.com/home, au support Dropbox sur https://www.dropbox.com/help, ou au support OneDrive sur http://windows.microsoft.com/en-us/onedrive/onedrive-help#onedrive=other.
- Si Office 2010 est en cours d'exécution : si des règles ont été définies pour protéger les documents Office et les documents prenant en charge les macros, les utilisateurs doivent disposer d'Office 2010 Service Pack 1 ou version ultérieure (v14.0.6029 ou ultérieure). Voir https://support.microsoft.com/en-us/kb/2121559 pour déterminer si un Service Pack a été appliqué à une suite Microsoft Office 2010. Sans cette mise à jour, les documents protégés ne sont pas accessibles. Les nouveaux documents Office ne sont pas protégés quelle que soit la règle, à moins que la fonctionnalité d'analyse soit activée. La prochaine analyse convertit les documents Office en fichiers protégés, mais les utilisateurs ne peuvent y accéder sans une version d'Office prise en charge.
- Data Guardian ne prend pas en charge l'outil de restauration du système de Windows.
- Consultez régulièrement la rubrique www.dell.com/support pour obtenir la dernière documentation et conseils techniques.

Conditions préalables du client

Le programme d'installation installe le package redistribuable Microsoft Visual C++ 2015 (x86 et x64) s'il n'est pas déjà installé.

REMARQUE :
Pour Windows 7 et Windows 8.1, les dernières mises à jour Windows doivent être installées. Pour plus d'informations, voir https://support.microsoft.com/en-us/help/2919355 et https://support.microsoft.com/en-us/help/2999226.

Microsoft .Net 4.5.2 (ou version ultérieure) est requis pour Data Guardian. Tous les ordinateurs expédiés depuis l'usine Dell sont préinstallés avec .Net 4.5.2. Cependant, si vous n'effectuez pas l'installation sur du matériel Dell ou que vous procédez à une mise à niveau de Data Guardian sur du matériel Dell plus ancien, vous devez vérifier la version de .Net installée et la mettre à jour, si nécessaire, avant d'installer Dell Data Guardian pour éviter tout échec d'installation/de mise à niveau. Pour vérifier la version .Net installée, suivez ces instructions sur l'ordinateur ciblé pour installation : http://msdn.microsoft.com/en-us/library/hh925568(v=vs.110).aspx. Pour installer Microsoft .Net Framework 4.5.2, accédez à https://www.microsoft.com/en-us/download/details.aspx?id=42643.

Matériel client Windows

La configuration minimale requise doit répondre aux spécifications minimales du système d'exploitation. Le tableau suivant répertorie le matériel pris en charge pour le client Windows.

Matériel Windows

- 200 Go d'espace disque disponible, selon le système d'exploitation
- Carte d'interface réseau 10/100/1000 ou Wi-Fi
- TCP/IP installé et activé

Si votre entreprise crypte les données pour un stockage dans le cloud, votre ordinateur doit disposer d'un caractère alphabétique libre pouvant être affecté à un lecteur de disque.

Systèmes d'exploitation

Le tableau suivant répertorie les systèmes d'exploitation pris en charge.

Systèmes d'exploitation Windows (32 bits et 64 bits)

- Windows 7 SP0-SP1
- Windows 8.1
- Windows 10

REMARQUE :
Windows 7 n'est pas pris en charge avec la stratégie de géolocalisation pour les événements d'audit Data Guardian.

Systèmes d'exploitation Android

- 4.4 - 4.4.4 KitKat
- 5.0-5.1.1 Lollipop
- 6.0 -6.0.1 Marshmallow
- 7.0 Nougat

Systèmes d'exploitation iOS

- iOS 8.x
- iOS 9.x
- iOS 10.x - 10.3

Clients de synchronisation Cloud

Le tableau ci-dessous décrit les clients de synchronisation cloud qui fonctionnent avec Data Guardian. Des mises à jour du client de synchronisation sont émises fréquemment. Dell recommande de tester les nouvelles versions du client de synchronisation avec Data Guardian avant de les présenter à l'environnement de production.

Clients de synchronisation Cloud

- Dropbox
- Dropbox for Business (Windows uniquement)

  REMARQUE :
  Selon la version du serveur Dell utilisé par votre société, tous les fichiers et dossiers des comptes personnels Dropbox liés à des comptes professionnels peuvent être cryptés.

- Box

  REMARQUE :
  Box Tools et Box Edit ne sont pas pris en charge dans Data Guardian. L'utilisation de Box Tools peut entraîner une erreur avec écran bleu.

- Google Drive
- OneDrive
- OneDrive for Business
- Unified OneDrive

  REMARQUE :
  Unified OneDrive est un client de synchronisation unifié pour OneDrive et OneDrive for Business.

Navigateurs Web

Vous pouvez utiliser Data Guardian > Cryptage cloud avec Internet Explorer, Mozilla Firefox et Google Chrome.

REMARQUE :
Data Guardian > Cryptage cloud ne prend pas en charge le navigateur Microsoft Edge.

Tâches utilisateur : Cryptage cloud et Office protégé

Votre administrateur a déjà configuré les règles de Data Guardian et vous indiquera si votre entreprise utilise Data Guardian :

- Pour gérer votre client de synchronisation cloud
- Pour gérer votre client de synchronisation cloud et une protection supplémentaire pour les documents Office : si votre entreprise protège seulement les documents Office mais ne gère pas de client de synchronisation cloud, suivez la procédure de la section Tâches utilisateur : Office protégé sans cryptage cloud.

Si votre entreprise utilise Data Guardian avec un stockage cloud :

- Avant de déployer Data Guardian, consultez l'aide en ligne de votre fournisseur de stockage cloud/client de synchronisation cloud pour comprendre le fonctionnement de votre application de stockage cloud. Ce document a pour objectif principal d'expliquer l'utilisation de Data Guardian.
- D'une manière générale, installez et travaillez avec un seul client de synchronisation Cloud. Votre société peut avoir préféré un client de synchronisation Cloud et défini une règle qui vous autorise à n'utiliser que celui-ci.

Présentation des tâches

Cette présentation résume la séquence d'installation et d'utilisation de Data Guardian.

Installer Data Guardian et un client de synchronisation cloud

Tâche	Description	Pour en savoir plus
Si un client de synchronisation cloud est installé avant Data Guardian	Les dossiers et fichiers existants qui se synchronisent vers le cloud ne sont pas cryptés. **REMARQUE :** Les dossiers et fichiers existants qui se synchronisent depuis le cloud sont cryptés.	Voir Dossiers préexistants contenant des fichiers non cryptés.
Installez Data Guardian	Déterminez les éléments suivants : L'utilisateur doit installer Data Guardian L'administrateur a déjà installé Data Guardian : passez à l'étape suivante.	Installation par l'utilisateur : voir Installer Data Guardian sous Windows. Redémarrez le système et passez à l'étape suivante.
Confirmer l'état d'activation	Vérifiez que l'icône Data Guardian de la barre d'état système est dotée d'une coche verte  .	Si l'icône est affublée d'un point d'exclamation orange, voir Problèmes possibles à l'activation : cloud et Office protégé.
Si des règles protègent les documents dans le	Client de synchronisation Business ou	Comptes de client de synchronisation cloud d'entreprise ou

Tâche	Description	Pour en savoir plus
cloud, installez un client de synchronisation cloud	Client de synchronisation Basic	Comptes de client de synchronisation cloud de base

REMARQUE :

Si vous ouvrez un document Office et qu'une page de garde s'affiche avec des informations d'installation ou d'activation, il est possible que votre administrateur ait défini des règles pour protéger les documents Office. Vérifiez que Data Guardian est installé et activé. Voir Problèmes possibles à l'activation : cloud et Office protégé.

Utiliser Data Guardian

Tâche	Description	Pour en savoir plus
Afficher le client de synchronisation Cloud dans l'Explorateur de fichiers.	Après avoir installé Data Guardian et un client de synchronisation cloud, un Lecteur virtuel DDG vDisk s'affiche dans l'explorateur de fichiers.	Travailler avec les dossiers et les fichiers Accéder aux dossiers et fichiers du client de synchronisation sur l'ordinateur local
Travailler avec le client de synchronisation cloud sur le Lecteur virtuel DDG vDisk	Sur le Lecteur virtuel DDG vDisk, vous pouvez ajouter des sous-dossiers dans le client de synchronisation cloud puis faire glisser des fichiers ou en créer dans ces sous-dossiers. Après la synchronisation, les fichiers sont sécurisés dans le cloud : il est possible d'ouvrir les fichiers Office, mais seule une page de garde affiche ; les autres fichiers sont cryptés en tant que fichiers .xen. Cependant, sur le disque virtuel local, ils sont décryptés et affichés en texte clair. Pour plus d'informations, cliquez sur le lien correspondant à votre client de synchronisation Cloud.	**Compte Business :** Dropbox for Business OneDrive Entreprise/OneDrive unifié **Compte Basic :** Dropbox Box Google Drive OneDrive
Afficher le menu de la barre d'état système	Fournit des informations utiles concernant les fichiers, les dossiers et le dépannage.	Présentation des éléments de menu de Data Guardian dans la barre d'état système
Documents Office protégé, prenant en charge les macros et .pdf si la règle est activée	Protégez un document Office (.docx, .pptx, .xlsx, .docm, .pptm, .xlsm, .pdf) dès sa création. Ce document sera protégé si vous le partagez avec d'autres utilisateurs ou l'enregistrez sur un média amovible.	Utiliser les documents Office avec le mode protégé de Data Guardian • Observer l'option de menu Fichier pour déterminer le niveau de sécurité des documents Office • Travailler avec l'option de menu Fichier
Partager un dossier cloud avec d'autres utilisateurs afin de collaborer sur des fichiers	Partager un dossier avec : un utilisateur interne (possédant une adresse e-mail dans le domaine). un utilisateur externe (possédant une adresse e-mail hors domaine) : à déterminer avec votre administrateur.	Utilisateur interne : voir l'aide en ligne relative à votre fournisseur de stockage Cloud. Utilisateur externe : voir Utiliser Data Guardian en tant qu'utilisateur externe.

Installez Data Guardian avec le cloud et Office protégé

Dossiers préexistants contenant des fichiers non cryptés

Avant de déployer Dell Data Protection | Data Guardian (DDG VDisk), il est préférable de ne pas avoir créé de compte fournisseur de stockage cloud sur les périphériques cibles.

Si vous détenez déjà un compte fournisseur de stockage cloud dont les dossiers sont synchronisés avec votre ordinateur local et que vous installez Data Guardian :

- Les dossiers et fichiers existants qui se synchronisent vers le cloud restent en clair
- Les fichiers que vous ajoutez à ces dossiers existants restent en clair
- Les fichiers qui se synchronisent depuis le cloud sont cryptés

  Si vous souhaitez crypter les fichiers existants, accédez au Lecteur virtuel DDG vDisk, créez un nouveau sous-dossier dans le client de synchronisation cloud et déplacez les fichiers existants dans ce dossier.

  ou

  Pour les contenus volumineux, un administrateur ou un gestionnaire peut temporairement demander le menu Gérer les dossiers.

Installer Data Guardian sous Windows

Vous devez disposer des droits d'administrateur sur l'ordinateur local pour installer Data Guardian.

L'ordinateur doit disposer d'une lettre disponible, pouvant être attribuée à un lecteur de disque.

Soyez prêt à redémarrer l'ordinateur après l'installation de Data Guardian.

1. Pour télécharger le programme d'installation de Data Guardian, rendez-vous à l'emplacement spécifié par votre administrateur.
2. En fonction de votre système d'exploitation, sélectionnez le programme d'installation 32 bits ou 64 bits, généralement nommés **setup32.exe** et **setup64.exe**, et le copiez-le sur l'ordinateur local.
3. Double-cliquez sur le fichier pour lancer le programme d'installation.
4. Si vous recevez un avertissement de sécurité, cliquez sur **Exécuter**.
5. Sélectionnez une langue, puis cliquez sur **OK**.
6. Si un message vous invite à installer Microsoft Visual C++ 2010 Redistributable Package ou Microsoft .NET Framework 4.0 Client Profile, cliquez sur **OK**.
7. Dans la page d'accueil, cliquez sur **Suivant**.
8. Lisez le contrat de licence, acceptez les conditions, puis cliquez sur **Suivant**.
9. À l'écran Dossier de destination, cliquez sur **Suivant** pour installer à l'emplacement par défaut suivant **C:\Program Files\Dell\Dell Data Protection\Dell Data Guardian\.**

   Sur **C:**, n'installez pas Data Guardian dans les dossiers Users ou Windows, ou à la racine d'un lecteur. Vous obtiendrez un message d'erreur.
10. Dans le champ *Nom du serveur :*, saisissez le nom du serveur avec lequel cet ordinateur communiquera. Par exemple, serveur.domaine.com. Il n'est pas nécessaire d'inclure www ou http(s). Cette information est fournie par votre administrateur.

    Ne décochez pas la case *Activer la vérification de confiance SSL* sauf si votre administrateur vous le demande.
11. Cliquez sur **Suivant**.
12. Dans l'écran d'information Confirmer le serveur d'activation, confirmez que l'adresse URL du serveur est correcte. Le programme d'installation ajoute www ou http(s) et le port. Cliquez sur **Suivant**.
13. Dans la fenêtre Type de gestion, sélectionnez cette option :
    - Utilisation interne : utilisateur doté d'une adresse e-mail incluse dans le domaine de la société.

14 Cliquez sur **Installer** pour démarrer l'installation.
Une fenêtre affichant l'avancée de l'installation apparaît.

15 Lorsque l'écran Installation terminée s'affiche, cliquez sur **Terminer**.

16 Cliquez sur **Oui** pour redémarrer.
L'installation de Data Guardian est maintenant terminée.

17 Une fois que vous avez redémarré, vérifiez dans la barre d'état système que l'icône Data Guardian est dotée d'une coche verte  .

Data Guardian et cryptage cloud

Si votre entreprise a défini des règles pour protéger les données du cloud, que vous déjà installé un client de synchronisation et que vous y êtes connecté(e), un Lecteur virtuel DDG vDisk s'affiche dans l'Explorateur Windows.

REMARQUE :
Data Guardian ne prend pas en charge le démontage du disque virtuel.

Si vous devez installer et connecter un client de synchronisation, voir Installer un client de synchronisation cloud.

Installer un client de synchronisation cloud

Télécharger et installer

En règle générale, les sociétés conseillent à tous les utilisateurs d'installer le même client de synchronisation Cloud. Le cas échéant, utilisez le client de synchronisation Cloud préféré de votre société.

REMARQUE :
L'ordinateur doit disposer d'une lettre disponible, pouvant être attribuée à un lecteur de disque.

REMARQUE :
Actuellement, Data Guardian ne prend pas en charge les clients de synchronisation installés à un point de montage.

1 Installez un client de synchronisation Cloud Business ou Basic :
- **Comptes de client de synchronisation cloud d'entreprise**
  Si votre entreprise offre la possibilité d'avoir un compte Business, votre administrateur vous fournira un lien vous permettant de le télécharger et de l'installer. Les options sont les suivantes :
  - **Dropbox for Business** : si vous installez Dropbox for Business, vous devez également Authentifier Dropbox for Business.
  - **OneDrive Entreprise/OneDrive unifié** : pour une procédure détaillée, voir https://support.microsoft.com/en-us/kb/2903984.
- **Comptes de client de synchronisation cloud de base**
  - **Dropbox** : voir https://www.dropbox.com/install
  - **Synchronisation Box** : voir https://www.box.com/box-for-devices
  - **Google Drive** : https://www.google.com/drive/download/
  - OneDrive/OneDrive unifié **(Windows 7 et 8)** : voir https://onedrive.live.com/about/en-us/download/
    Dans Windows 8.1 et versions ultérieures, OneDrive est préinstallé. Si vous avez activé les mises à jour Windows, OneDrive unifié remplace OneDrive.

2 Après l'installation et une fois connecté(e), les éléments suivants s'affichent :
- Un Lecteur virtuel DDG vDisk s'ajoute dans l'Explorateur de fichiers. Le dossier du client de synchronisation Cloud est ajouté à ce disque virtuel.
  Si vous installez plusieurs clients de synchronisation Cloud, un dossier par client s'affiche sur ce disque.

REMARQUE :
Data Guardian ne prend pas en charge le démontage du disque virtuel.

- Dans l'Explorateur de fichiers > Favoris, un dossier est ajouté à votre client de synchronisation Cloud.
- Dans la barre d'état système, l'icône Client de synchronisation s'affiche.
- En fonction du fournisseur de stockage Cloud, un raccourci du client de stockage peut être ajouté automatiquement au bureau.
- Avec le mode de protection individuelle uniquement (mais sans le mode de protection forcée) : un dossier Documents sécurisés s'ajoute à la racine du dossier Documents. Voir Documents > dossier Documents sécurisés.

Modifier la lettre de lecteur virtuel ou créer un raccourci

Une fois que vous avez installé Data Guardian et un client de synchronisation cloud, l'icône Lecteur virtuel DDG vDisk s'affiche dans l'Explorateur de fichiers. Une lettre située vers la fin de l'alphabet et disponible est attribuée au disque.

Pour modifier la lettre du disque :

1 Dans la barre d'état système, cliquez sur l'icône de Data Guardian et sélectionnez **Configurer le lecteur**.

2 Sélectionnez une lettre disponible dans la liste *Actuelles*.

3 Cliquez sur **Appliquer** ou sur **OK**.
Pour ajouter l'icône Lecteur virtuel DDG vDisk sur le bureau, cliquez avec le bouton droit sur le lecteur et sélectionnez **Créer un raccourci**.

Authentifier Dropbox for Business

Si vous installez Dropbox for Business, Data Guardian demande une authentification.

Pour vous authentifier :

1 Après avoir installé Data Guardian, une fenêtre Authentification peut s'ouvrir. Autrement, cliquez sur l'icône de Data Guardian et sélectionnez **Dropbox > Connecter.**
La fenêtre Authentification vous notifie que Data Guardian doit avoir accès à votre compte Dropbox et peut donner des instructions à propos des comptes professionnel et personnel.

Ceci fournit des options de menu contextuel à l'intention de l'utilisateur. Ceci est essentiel pour l'entreprise et votre administrateur, car ceci fournit des mesures de sécurité supplémentaires.

2 Dans la fenêtre d'authentification, cliquez sur **Suivant**.

3 Si une fenêtre de Protection contre les menaces du réseau s'ouvre, cliquez sur **Oui**.

4 Dans la fenêtre Authentification, entrez votre e-mail de domaine et mot de passe Dropbox.

5 Cliquez sur **Se connecter**.

6 Si vous avez lié vos comptes Dropbox professionnel et personnel, vous êtes invité à en sélectionner un. Vous devez sélectionner votre compte professionnel.

7 Cliquez sur **Terminer** ou attendez la fermeture de la fenêtre.

Travailler avec les dossiers et les fichiers

Data Guardian fonctionne de manière transparente avec votre client de synchronisation cloud. Lorsque votre administrateur définit une règle pour activer Data Guardian, les fichiers sont cryptés et sécurisés dans le Cloud lorsqu'ils sont synchronisés depuis votre ordinateur local.

Suivez les instructions de l'aide relative au fournisseur de stockage Cloud pour effectuer les tâches suivantes :

- Créer des dossiers
- Charger/télécharger des dossiers et des fichiers

REMARQUE :
Pour charger des fichiers, copiez ou bien faites glisser des fichiers vers les dossiers du Lecteur virtuel DDG vDisk. Data Guardian ne prend pas en charge la fonction de glisser-déposer des fichiers depuis votre ordinateur local vers le Web, ni la création de fichiers directement dans le site Web du fournisseur de stockage cloud.

- Utiliser la synchronisation sélective des dossiers
- Partager des dossiers ou des fichiers avec des utilisateurs internes qui possèdent Data Guardian. Voir Partager un dossier avec un utilisateur interne.
- Partager des dossiers ou des fichiers avec des utilisateurs externes. Voir Utiliser Data Guardian en tant qu'utilisateur externe.
- Annuler le partage de dossiers

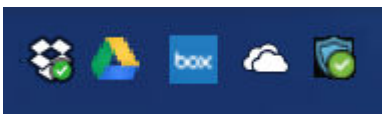
Afficher les dossiers et les fichiers sur l'ordinateur local et dans le Cloud

Accéder aux dossiers et fichiers du client de synchronisation sur l'ordinateur local

Pour accéder aux dossiers et fichiers synchronisés, cliquez sur le **Lecteur virtuel DDG vDisk** dans l'Explorateur de fichiers. Votre client de synchronisation Cloud s'affiche.

Voici d'autres façons d'accéder à votre client de synchronisation Cloud.

- Dans la barre d'état système, sélectionnez l'icône Client de synchronisation et ouvrez le dossier Client de synchronisation. Pour plus d'informations, voir l'aide sur le fournisseur de stockage Cloud.

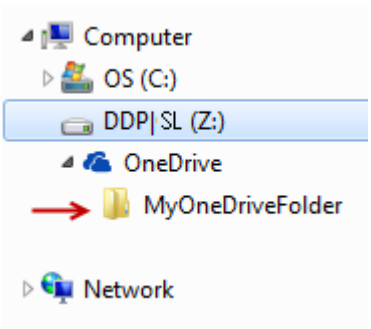


- Dans les favoris, cliquez sur l'icône Client de synchronisation.
  Lorsque vous cliquez sur l'icône Client de synchronisation dans la barre d'état système ou dans les Favoris, vous noterez que le Lecteur virtuel DDG vDisk apparaît en surbrillance. Data Guardian vous redirige vers ce lecteur virtuel, ce qui vous permet d'afficher en texte clair vos dossiers et fichiers localement décryptés.

Vous pouvez également accéder aux dossiers et fichiers du Lecteur virtuel DDG vDisk via un raccourci sur le bureau. Voir Modifier la lettre de lecteur virtuel ou créer un raccourci.

Ajouter des dossiers

Avec Data Guardian, vous devez ajouter des sous-dossiers au dossier de synchronisation du cloud. N'ajoutez pas de fichiers à la racine du Lecteur virtuel DDG vDisk.



Ajouter des fichiers

Lorsque vous ajoutez un fichier à un dossier, Data Guardian ajoute automatiquement un fichier au dossier sur le Web. Data Guardian utilise le fichier Comment accéder aux fichiers sécurisés.html lorsque vous partagez un dossier avec des utilisateurs externes. Il n'est pas nécessaire d'ouvrir ou de télécharger ce fichier. Voir Utiliser Data Guardian en tant qu'utilisateur externe.

Afficher les dossiers et les fichiers du client de synchronisation dans le Cloud

Data Guardian crypte vos données dans le cloud et les noms de fichiers reçoivent une extension .xen. L'icône en regard du fichier peut varier selon le fournisseur de stockage Cloud mais n'affiche pas le contenu. Vous ne pouvez pas ouvrir les fichiers dans le Cloud. Toutefois, si quelqu'un accède à votre compte de stockage Cloud, il ne lui sera pas possible d'ouvrir ou de voir vos fichiers. Ceci augmente la sécurité au sein du Cloud. Vous pouvez uniquement afficher les fichiers en texte clair sur le Lecteur virtuel DDG vDisk.

Il arrive que lorsque vous téléchargez un fichier .xen sur votre bureau et le décryptez, une copie du fichier avec extension .xen demeure. Vous pouvez supprimer la copie téléchargée du fichier .xen.

Si votre entreprise a besoin d'une protection supplémentaire de ses dossiers et de ses fichiers dans le Cloud, votre administrateur peut définir une règle permettant d'obscurcir les noms de fichiers dans le cloud ainsi que la date de téléchargement. Si quelqu'un accède à votre compte de stockage Cloud, il ne lui sera pas possible d'ouvrir les fichiers ou de lire les noms de fichiers.

Afficher les dossiers et les fichiers du client de synchronisation sur un ordinateur local sur lequel sont installés Data Guardian et un disque virtuel

Pour faciliter l'utilisation de Data Guardian sur votre ordinateur local, lorsque vous ouvrez un dossier du Lecteur virtuel DDG vDisk, les fichiers issus du cloud sont automatiquement décryptés et s'affichent en texte clair, même s'ils sont protégés en tant que fichiers cryptés dans le cloud.

Protéger les dossiers et fichiers des appareils dépourvus de Data Guardian

Si une personne non autorisée télécharge un fichier protégé depuis le cloud vers un périphérique **dépourvu** de Data Guardian, cette personne ne peut pas accéder à vos données. Selon les règles définies par votre administrateur :

- Documents Office : le document s'ouvre, mais seule une page de garde s'affiche avec un message spécifique à l'entreprise.
- Documents non Office : le fichier se télécharge en tant que fichier .xen. La personne en question ne peut pas ouvrir ce fichier.

> **REMARQUE :**
> Pour les utilisateurs internes, si vous téléchargez un fichier depuis un ordinateur équipé de Data Guardian vers un périphérique qui en est dépourvu, vous ne pouvez pas afficher ce fichier, sauf si vous installez Data Guardian en tant qu'utilisateur externe.

Il est possible qu'un fichier .xen s'affiche de façon occasionnelle sur un ordinateur équipé de Data Guardian. Par exemple, si la connexion Internet a été interrompue avant la fin du téléchargement, la clé peut ne pas être disponible pour ouvrir le fichier. Une boîte de dialogue signale que le fichier ne peut pas être décrypté.

Data Guardian ne permet pas de modifier des fichiers sans extension. Ces fichiers sont traités comme des fichiers en lecture seule. Pour modifier un fichier sans extension, téléchargez-le depuis le site Web du fournisseur de stockage Cloud, modifiez-le, puis chargez-le via le Lecteur virtuel DDG vDisk.

Rechercher des noms et contenus de fichier sur le Lecteur virtuel DDG vDisk

Si vous souhaitez rechercher des noms de fichiers ou du contenu sur le Lecteur virtuel DDG vDisk, vous devez activer l'indexation de la recherche Windows pour ce lecteur.

> **REMARQUE :**
> L'indexation de la recherche Windows est activée uniquement pour les dossiers des utilisateurs.

Pour activer l'indexation de la recherche Windows pour le Lecteur virtuel DDG vDisk :

1 Dans le Panneau de configuration, saisissez **Indexation de la recherche** dans le champ de recherche.
2 Sélectionnez **Options d'indexation**.
3 Dans *Modifier les emplacements sélectionnés*, cochez la case de ce Lecteur virtuel DDG vDisk.

> **REMARQUE :**
> Les étapes restantes peuvent varier en fonction de votre système d'exploitation.

4 Cliquez sur **OK**.
5 Dans les options d'indexation, cliquez sur **Fermer**.

Vous pouvez désormais effectuer une recherche sur le Lecteur virtuel DDG vDisk.

Partager un dossier avec un utilisateur interne

Un utilisateur interne possède une adresse e-mail dans le domaine de l'entreprise.

Pour partager un dossier avec un utilisateur interne, vous devez accéder au site Web de votre fournisseur de stockage cloud et sélectionner **Partager**. Voir l'aide en ligne de votre fournisseur de stockage Cloud.

Partage d'un dossier à l'aide de Data Guardian et de Box

Sur le site Web de Box, sélectionnez l'une de ces options.

Option du site Web de Box	Options	Description
Partager	Disponible pour les dossiers et les fichiers	Lorsque la fenêtre de partage s'ouvre, assurez-vous que l'option Autoriser le téléchargement est définie sur **Oui**.
	Afficher l'accès	Après le téléchargement des dossiers ou des fichiers, les destinataires de ces partages doivent extraire le dossier compressé puis déplacer le dossier et les fichiers vers le Lecteur virtuel DDG vDisk.
Inviter des collaborateurs	Disponible pour les dossiers	Lorsque la fenêtre d'invitation s'ouvre, vous pouvez sélectionner **Éditeur** ou **Spectateur**.
	Afficher ou modifier l'accès	Les destinataires des partages peuvent synchroniser le dossier vers leur ordinateur. Celui-ci se synchronise alors avec le Lecteur virtuel DDG vDisk.

Utiliser les documents Office avec le mode protégé de Data Guardian

Pour améliorer la sécurité de l'entreprise, votre administrateur peut activer une règle pour protéger les fichiers de ces applications de Bureau :

- .docx, .pptx, .xlsx
- .docm, .pptm, .xlsm

Si une personne non autorisée accède à un fichier protégé, celui-ci reste crypté, par exemple lorsque vous effectuez les actions suivantes :

- Joindre à un e-mail
- Déplacer vers un navigateur : dans certains clients de synchronisation cloud, vous pouvez cliquer avec le bouton droit sur un nom de fichier et sélectionner **Déplacer**.
- Partager sur le réseau

- Charger vers un fournisseur de stockage cloud
- Stocker sur un média amovible

Pour les documents Office, une page de garde peut s'afficher avec des instructions d'installation ou d'activation de Data Guardian, par exemple :

- Vous devez installer Data Guardian.
- Vous devez activer Data Guardian.
- Vous ouvrez un document Office protégé dans le cloud.
- Vous avez téléchargé un fichier Office depuis votre ordinateur équipé de Data Guardian vers un appareil personnel qui n'en dispose pas.
- Un utilisateur non autorisé accède à l'un de vos fichiers Office : la page de garde s'affiche avec un message spécifique à l'entreprise, mais cet utilisateur ne peut pas afficher le contenu du fichier.

Si votre entreprise utilise le mode protégé de Data Guardian, reportez-vous aux sections suivantes :

- Observer l'option de menu Fichier pour déterminer le niveau de sécurité des documents Office
- Travailler avec l'option de menu Fichier
- Déterminer quels documents en mode de protection individuelle sont protégés
- Options de menu supplémentaires pour les documents Office protégés
- Utilisateurs externes et documents Office protégés

Observer l'option de menu Fichier pour déterminer le niveau de sécurité des documents Office

Pour déterminer si votre administrateur a activé les règles Data Guardian, ouvrez un document Office et sélectionnez **Fichier**. Si *Opération Enregistrer sous protégée* s'affiche dans le volet de gauche, vos documents Office bénéficient d'une protection supplémentaire.

Pour déterminer le niveau de sécurité, observez quelles options sont activées ou désactivées :

- **Mode de protection individuelle** : vous permet de déterminer quels documents Office protéger.
  - Les options *Enregistrer sous* et *Opération Enregistrer sous protégée* sont activées : si vous décidez de protéger un document Office, sélectionnez **Opération Enregistrer sous protégée**.
  - Les options *Imprimer* et *Exporter* sont activées ou désactivées selon la règle.
  - L'option *Partager* (*Enregistrer et envoyer* sous Office 2010) est activée.
  - Dossier **Documents > Documents sécurisés** : avec le mode de protection individuelle (mais sans le mode de protection forcée), un dossier Documents sécurisés s'ajoute à la racine du dossier Documents. Les documents Office de ce dossier sont cryptés. Si vous retirez un document Office protégé de ce répertoire, celui-ci reste crypté. Si vous renommez le dossier, le contenu du dossier renommé est crypté. Si vous supprimez le dossier, celui-ci se recrée.
- **Mode de protection forcée** : votre entreprise requiert un niveau élevé de sécurité.
  - L'option *Enregistrer sous* est désactivée et l'option *Opération Enregistrer sous protégée* est activée : vous devez enregistrer tous les documents Office en mode protégé.
  - Les options *Imprimer* et *Exporter* sont activées ou désactivées en fonction de la règle.
  - L'option *Partager* (*Enregistrer et envoyer* sous Office 2010) est désactivée.

    REMARQUE :
    Lorsque le mode Protection forcée est activé, la règle active également des heures spécifiques pour balayer votre ordinateur afin de localiser tous les fichiers Office non protégés et les faire passer en mode Protégé. Vous devez être connecté et relié au réseau pour que Data Guardian puisse balayer et localiser des fichiers Office non protégés.

- Si vous sélectionnez **Opération Enregistrer sous protégée**, la seule option dans le champ *Type d'opération Enregistrer sous* est *Office protégé*.

- **Fichier > Informations** diffère, par exemple :

- Pour le mode de protection individuelle comme pour le mode de protection forcée : l'option *Ajouter une restriction calendaire* s'affiche si l'administrateur a activé cette règle. Voir Optimiser la sécurité en ajoutant des restrictions calendaires.
- Pour le mode de protection individuelle comme pour le mode de protection forcée : les informations liées à la propriété de ce document Office, notamment l'auteur et la date, sont masquées pour une sécurité accrue.
- État de lecture seule : voir ci-dessous pour plus d'informations.

REMARQUE :
L'option *Protéger le document* dans Fichier > Informations est associée au mode protégé de Microsoft Office et non pas de Data Guardian.

Si vous ouvrez un document Office et que celui-ci indique le mode lecture seule, vérifiez les éléments suivants :

- Si l'option *Opération Enregistrer sous protégée* ne s'affiche pas dans le volet de gauche, la lecture seule n'est pas liée aux règles de Data Guardian.
- Si votre administrateur a défini des règles en mode de protection forcée avec un niveau de sécurité plus élevé, les documents Office non protégés s'ouvrent en mode lecture seule.

REMARQUE :
Pour OneDrive, si vous ouvrez un document Office protégé via **Fichier > Ouvrir > OneDrive** et si le document est en lecture seule, assurez-vous d'avoir installé et configuré le client de synchronisation OneDrive.

Travailler avec l'option de menu Fichier

Ce tableau répertorie les options du menu Fichier pour les documents Office. En fonction du niveau de sécurité, certaines options sont grisées.

REMARQUE :
Actuellement, les documents Office intégrés ne sont pas pris en charge par le mode protégé Office.

Menu Fichier	Mode de protection individuelle et documents Office protégés	Mode de protection forcée pour protégés et non protégés
Ouvrez le fichier	**Les fichiers s'ouvrent normalement**	**Les fichiers non protégés s'ouvrent en lecture seule.**
Enregistrer	• Options : Document déjà protégé : permet d'enregistrer avec protection. Non protégé : permet d'enregistrer sans protection. Pour protéger ce document, cliquez sur **Opération Enregistrer sous protégée**. • Document en lecture seule : une boîte de dialogue vous signifie que vous ne pouvez pas enregistrer un document non protégé. Une fenêtre Enregistrer sous s'ouvre alors et vous êtes invité à enregistrer ce document sous un autre nom de fichier. • Fichier .xen : vous pouvez l'ouvrir et l'enregistrer en mode protégé, mais cela entraîne la suppression de ce fichier dans le cloud. Le document Office dispose de son extension habituelle, mais il est protégé. **REMARQUE :** **Sur l'unité virtuelle, si vous cliquez avec le bouton droit pour créer un nouveau document Office, celui-ci est au format .xen. Vous devez l'enregistrer manuellement en tant que document protégé.**	• Le document est protégé. • Document en lecture seule : vous pouvez le modifier, mais pas enregistrer l'original. Lorsque vous cliquez sur Enregistrer, la fenêtre Opération Enregistrer sous protégée s'ouvre et vous devez enregistrer le document en mode protégé sous un nouveau nom. • Documents à distance : si vous ouvrez un document dans un emplacement distant et qu'il n'est pas protégé, vous devez l'enregistrer sur votre disque local pour le modifier et l'enregistrer. Vous ne pouvez pas enregistrer de fichier dans l'emplacement distant. **REMARQUE :** **Cliquer sur Enregistrer déclenche l'ouverture d'une fenêtre Enregistrer sous. L'unique option dans le champ Type d'opération Enregistrer sous est Office protégé (document, présentation, ou classeur).** • Fichier .xen : vous pouvez l'ouvrir et l'enregistrer en mode protégé, mais cela entraîne la suppression de ce fichier dans le cloud. Le document Office dispose de son extension habituelle, mais il est protégé.
Enregistrer sous	**Dispose des options standard (mais pas du mode protégé)**	**Désactivée**
Opération Enregistrer sous protégée	**La seule option dans le champ Type d'opération Enregistrer sous est Office protégé**	**La seule option dans le champ Type d'opération Enregistrer sous est Office protégé**
Impression	**Peut être activée ou grisée en fonction des règles définies par votre administrateur. Si l'option de menu est activée, une règle peut placer un filigrane contenant le nom d'utilisateur, le nom de domaine et l'ID d'ordinateur sur chaque page à l'impression.**	**Selon la règle, cette option peut être activée ou grisée. Si l'option de menu est activée, une règle peut placer un filigrane contenant le nom d'utilisateur, le nom de domaine et l'ID d'ordinateur sur chaque page à l'impression.**
Partager	**Activé**	**Désactivée**
Enregistrer et envoyer (Office 2010)	**Activé**	**Désactivée** **Si l'option Imprimer est activée, vous pouvez sélectionner Imprimer pour imprimer le document au format PDF.**
Exporter (Office 2013 et versions ultérieures)	**Peut être activée ou grisée en fonction des règles définies par votre administrateur.**	**Peut être activée ou grisée en fonction des règles définies par votre administrateur.**
Opération Exporter protégée (Office 2013 et versions ultérieures)	Si l'option de menu Exporter est grisée et Exportation protégée est activée, le document s'exporte avec un filigrane contenant le nom d'utilisateur, le nom de domaine et ID d'ordinateur sur chaque page. **REMARQUE :** Si vous exportez un document en mode protégé vers un utilisateur externe, celui-ci peut l'ouvrir et l'afficher mais pas l'exporter ou l'imprimer.	Si l'option de menu Exporter est grisée et Exportation protégée est activée, le document s'exporte avec un filigrane contenant le nom d'utilisateur, le nom de domaine et ID d'ordinateur sur chaque page. **REMARQUE :** Si vous exportez un document en mode protégé vers un utilisateur externe, celui-ci peut l'ouvrir et l'afficher mais pas l'exporter ou l'imprimer.

Travailler en ligne avec les documents Office protégés

Lors de la création de documents Office protégés, la meilleure pratique consiste à travailler en ligne à cause des clés générées pour ces documents. Si vous avez besoin de réimager votre ordinateur et que vous avez créé des documents Office protégés hors ligne, veillez en avertir votre administrateur.

Travailler en ligne avec les documents protégés prenant en charge les macros

Dans un document prenant en charge les macros, la macro existe mais elle est bloquée. Cependant, actuellement, Data Guardian peut contrôler un document prenant en charge les macros uniquement après que vous avez fermé puis rouvert le document nouvellement protégé (.docm, .pptm, .xlsm). En outre, si vous enregistrez un document protégé avec une macro en tant que document non protégé, vous devez fermer puis rouvrir le document afin d'exécuter la macro.

Joindre un document Office protégé à un e-mail Outlook

Lorsque vous joignez un document Office protégé à un e-mail Outlook, sélectionnez **Insérer** au lieu d'*Insérer comme texte*. *Insérer comme texte* colle le contenu du document directement dans le corps de l'e-mail. Ce contenu n'est alors plus protégé.

Dépannage du mode de protection individuelle

Dans Fichier > Informations, si votre option Imprimer est grisée, une règle Data Guardian a désactivé l'impression des documents Office protégés. Quoiqu'actuellement, lorsque vous cliquez avec le bouton droit sur un fichier Office protégé dans l'Explorateur Windows, l'option d'impression n'est pas grisée. Toutefois, si vous sélectionnez Imprimer, voici ce qui se produit :

- Word : une boîte de dialogue indique que Word a cessé de fonctionner.
- Excel : une boîte de dialogue indique que l'option Imprimer est désactivée par la règle.
- PowerPoint : une boîte de dialogue indique que l'option Imprimer est désactivée par la règle. Si vous cliquez sur OK, une page de garde s'imprime indiquant que le document est protégé.

Déterminer quels documents en mode de protection individuelle sont protégés

Si vous disposez du mode de protection forcée, tous les documents Office sont protégés. Si vous disposez du mode de protection individuelle et souhaitez vérifier si un document est protégé ou non, ouvrez ce document : la barre de titre le désigne comme protégé.

Options de menu supplémentaires pour les documents Office protégés

Le type de document Office, protégé ou non, peut affecter les éléments suivants.

Clic droit > Protéger

Vous pouvez cliquer avec le bouton droit sur un document Office et sélectionner **Protéger**. Vous devez ajouter du contenu pour que l'option de menu s'affiche. Vous ne pouvez pas protéger un document vierge.

Propriétés de fichier > onglet Dell Data Guardian

Avec les documents Office protégés, vous pouvez cliquer avec le bouton droit et sélectionner **Propriétés** et un onglet **Dell Data Guardian** s'affiche avec des informations telles que l'ID de clé de fichier ainsi que les données d'accès et d'embargo.

Coller

Si votre administrateur définit une règle pour protéger les documents Office :

- Vous pouvez copier et coller des données dans le document protégé d'origine.
- Vous ne pouvez pas copier ou coller le contenu d'un document protégé dans un document non protégé. Rien ne s'affiche dans le presse-papiers et un message spécifique à l'entreprise indique que vous ne pouvez pas coller de contenu dans le document non protégé ou non géré.

REMARQUE :
Si vous coupez du texte d'un document protégé et obtenez ce message dans un document non protégé, cliquez sur **Annuler** dans le document protégé pour récupérer le texte.

Glisser-déposer en mode protégé

Vous pouvez faire glisser et déposer du contenu dans un document Word protégé. Actuellement, la fonction de glisser-déposer est désactivée pour les fichiers PowerPoint et Excel protégés.

Imprimer d'enveloppes et d'étiquettes

Si votre administrateur a défini une règle pour ajouter un filigrane lorsque vous imprimez un document Office protégé, procédez comme suit pour imprimer des enveloppes ou des étiquettes :

1 Dans un document Word, sélectionnez l'onglet **Publipostage**.
2 Sélectionnez l'option **Enveloppes** ou **Étiquettes**.
3 Une fois que vous avez saisi l'adresse ou l'adresse de l'expéditeur, cliquez sur **Imprimer**.

REMARQUE : Si vous utilisez une autre option pour imprimer et que votre administrateur a défini une règle pour ajouter un filigrane aux documents Office imprimés, ce filigrane s'affichera sur votre enveloppe ou étiquette.

Altération et documents Office protégés

Data Guardian peut analyser les documents Office protégés pour détecter certaines formes d'altération.

Si un utilisateur interne altère un document Office protégé :

- Data Guardian peut réparer ou restaurer certaines altérations.
- Dans le cas des altérations irréparables, une boîte de dialogue peut s'afficher pour vous avertir que le fichier a été altéré et contacter votre administrateur.

Si un utilisateur non autorisé ouvre un document Office protégé, seule la page de garde s'affiche. Si cet utilisateur non autorisé modifie la page de garde, Data Guardian la restaure lorsqu'un utilisateur autorisé l'enregistre de nouveau au format protégé.

Utilisateurs externes et documents Office protégés

Optimiser la sécurité en ajoutant des restrictions calendaires

Avec Data Guardian, lorsque vous chargez un document Office protégé vers le cloud et le partagez :

- Tous les utilisateurs internes de Data Guardian peuvent l'afficher.
- Selon la règle, les utilisateurs externes peuvent l'afficher.

Si vous le désirez, pour optimiser la sécurité envers les utilisateurs externes, vous pouvez ajouter une restriction calendaire pour limiter la durée d'autorisation d'affichage d'un document Office par un utilisateur externe.

1 Sélectionnez **Fichier > Informations > Restriction calendaire**.
2 Dans le menu déroulant de l'option, sélectionnez une date et une heure de début et de fin d'autorisation d'affichage du document par un utilisateur externe.

REMARQUE :
Vous pouvez choisir une date et une heure de début future si vous souhaitez envoyer le document mais empêcher l'utilisateur externe de l'afficher jusqu'à cette échéance.

3 Cliquez sur **OK**.

Ceci entraînera l'enregistrement, la protection, la fermeture puis la réouverture du document.

REMARQUE :
Si vous modifiez les dates d'un document Office non protégé puis cliquez sur Annuler, Data Guardian continue de protéger ce fichier.

REMARQUE :
Actuellement, lorsque vous ajoutez des restrictions calendaires à un document Office protégé et envisagez de l'enregistrer sur un lecteur réseau, vous devez enregistrer le fichier localement puis le copier sur le réseau.

Si un utilisateur externe ouvre un fichier après l'intervalle calendaire, une boîte de dialogue indique que le fichier est sujet à des restrictions d'accès et que l'utilisateur externe peut contacter l'auteur de ce fichier. La boîte de dialogue n'affiche aucune date pour l'utilisateur externe.

Si vous définissez le champ Date de début sur une date ou une heure future et si l'utilisateur externe ouvre le fichier avant cette échéance, une boîte de dialogue s'affiche et vous informe que vous ne pouvez pas ouvrir ce fichier avant cette échéance en raison de restrictions d'accès.

Opérer sans connexion Internet

Sans connexion Internet, vous pouvez toujours afficher les fichiers de synchronisation cloud sur votre lecteur local via l'explorateur de fichiers. Cependant, le Lecteur virtuel DDG vDisk ne s'affichera pas. Aussi, les modifications ne seront pas synchronisées dans le Cloud tant que vous n'êtes pas connecté à Internet.

Limite du nombre de caractères pour les noms de chemin d'accès aux dossiers

Le nombre limite de caractères autorisés pour les noms de chemin d'accès Windows est 248.

Dans le cloud, cette limite n'existe pas. Vous pouvez donc attribuer des noms de chemin d'accès excédant cette limite aux dossiers et sous-dossiers que vous créez. Cependant, localement, sous Windows, les dossiers ne seront pas créés si les noms de chemin d'accès excèdent cette limite. Assurez-vous donc de limiter à 248 caractères les noms de chemin d'accès aux dossiers et sous-dossiers .

Dropbox for Business

Dropbox for Business a des exigences spécifiques. Voir Installer un client de synchronisation cloud.

Aide relative au fournisseur de stockage Cloud

Avant d'utiliser Data Guardian, familiarisez-vous avec le fournisseur de stockage Cloud. Vous trouverez de l'aide relative à Dropbox for Business à l'adresse :

https://www.dropbox.com/help.

Bien qu'il soit possible de charger des fichiers sur le site Web du fournisseur de stockage Cloud, les meilleures pratiques consistent à travailler à partir de dossiers ou de fichiers situés sur le Lecteur virtuel DDG vDisk.

Connectez Data Guardian et Dropbox for Business

Si votre société utilise Dropbox for Business, vous devez permettre à Data Guardian de rester connecté.

Pour vous connecter :

1 Dans la barre d'état système, cliquez sur l'icône de Data Guardian puis sélectionnez **Dropbox > Connecter**.
2 Dans la fenêtre d'authentification Dropbox, lisez les informations, puis cliquez sur **Suivant**.
3 Si vous avez lié vos comptes Dropbox professionnel et personnel, vous êtes invité à en sélectionner un. Vous devez sélectionner votre compte professionnel.
4 Lorsque vous êtes invité à autoriser Data Guardian à accéder à vos fichiers et dossiers Dropbox, cliquez sur **Autoriser**.
5 Cliquez sur **Terminer**.

Définir la Synchronisation sélective des dossiers

Pour synchroniser des dossiers de manière sélective :

1 Dans la barre d'état système, cliquez sur l'icône **Dropbox for Business**.
2 Cliquez sur l'icône **Paramètres** puis sélectionnez **Préférences**.
3 Cliquez sur l'onglet **Compte** puis sur **Synchronisation sélective**.
4 Sélectionnez uniquement les dossiers ou sous-dossiers de votre ordinateur que vous souhaitez synchroniser.
5 Cliquez sur **Mettre à jour**.
6 Dans la boîte de dialogue Confirmation de mise à jour, cliquez sur **OK**.
7 Dans la fenêtre Préférences de Dropbox, cliquez sur **OK**.
Une fenêtre contextuelle s'affiche dans la barre d'état système et indique que les dossiers sont en cours de synchronisation.

Votre entreprise déterminera si vous pouvez avoir seulement un compte professionnel ou si vous pouvez utiliser à la fois les dossiers professionnels et les dossiers personnels. Pour des dossiers préexistants, qui comportent des fichiers personnels ou des données ne nécessitant pas de cryptage, désélectionnez ces dossiers avant d'installer Data Guardian. Sinon, vos données personnelles pourraient être cryptées.

Utiliser l'icône de la barre d'état système de Dropbox for Business

Dans la barre d'état système, cliquez sur l'icône Dropbox.

- Pour le site Internet : sélectionnez l'icône Globe.

  REMARQUE :
  Si vous utilisez Chrome ou Firefox pour ouvrir Dropbox.com, n'oubliez pas de le fermer après avoir fini de travailler avec des fichiers et des dossiers. Même si vous ouvrez un autre onglet dans le navigateur, le contenu sera crypté. Cela peut inclure le courrier électronique, les pièces jointes ou des chargements à l'aide du navigateur.

- Pour le dossier : sélectionnez l'icône de dossier Dropbox. Ceci vous redirige vers le Lecteur virtuel DDG vDisk.

Utiliser le menu contextuel de Dropbox for Business

Dans l'Explorateur Windows, lorsque vous installez Data Guardian, Dropbox for Business dispose d'un menu contextuel.

REMARQUE :
Vous devez connecter Data Guardian à Dropbox.

Pour accéder au menu contextuel, dans l'Explorateur Windows, ouvrez un dossier Dropbox et effectuez un clic droit sur un fichier. L'icône de Cloud présente ces options :

- Partager une liaison Dropbox sécurisée
- Afficher sur Dropbox.com
- Afficher les versions précédentes

Utiliser les comptes Dropbox professionnel et personnel

Si votre entreprise utilise Dropbox for Business et vous permet de lier un compte Dropbox personnel à votre compte professionnel, assurez-vous de vous familiariser avec les règles définies par votre administrateur pour ces comptes. Par exemple, une société peut définir les règles suivantes :

- Les fichiers professionnels et personnels sont cryptés.

  ou
- Seuls les fichiers et dossiers professionnels sont cryptés. Les fichiers personnels restent non cryptés.

  Pour des raisons de sécurité, votre entreprise peut mettre en place des règles d'audit. Les noms de fichiers contenus dans le dossier personnel sont enregistrés et envoyés au serveur Dell Data Protection.

Si vous utilisez des comptes Dropbox professionnel et personnel, ne stockez pas de fichiers professionnels dans votre dossier Dropbox personnel.

Décryptage des dossiers d'un compte personnel

Si un dossier personnel est accidentellement crypté, l'administrateur peut accorder un accès temporaire pour vous permettre de gérer le cryptage de vos dossiers. Désélectionnez les dossiers qui doivent être non cryptés. De plus, vous pouvez supprimer des dossiers de la synchronisation en dissociant le compte ou en annulant la synchronisation des dossiers personnels qui doivent rester non cryptés.

OneDrive Entreprise/OneDrive unifié

REMARQUE :
Data Guardian n'est pas pris en charge avec Microsoft Office 365.

REMARQUE :
Le partage de données dans OneDrive for Business n'est pas pris en charge.

Aide relative au fournisseur de stockage Cloud

Avant d'utiliser Data Guardian, familiarisez-vous avec le fournisseur de stockage Cloud. L'aide relative à OneDrive for Business est disponible à l'adresse :

http://windows.microsoft.com/en-us/onedrive/onedrive-help#onedrive=other.

Bien qu'il soit possible de charger des fichiers sur le site Web du fournisseur de stockage Cloud, les meilleures pratiques consistent à travailler à partir de dossiers ou de fichiers situés sur le Lecteur virtuel DDG vDisk.

Définir la Synchronisation sélective des dossiers

Pour synchroniser des dossiers de manière sélective :

1 Dans la barre d'état système, cliquez avec le bouton droit sur l'icône **OneDrive Entreprise/OneDrive unifié** et cliquez sur **Synchroniser une nouvelle bibliothèque**.
2 Entrez l'adresse URL de votre bibliothèque.
3 Sélectionnez **Synchroniser maintenant**.
4 Sélectionnez **Afficher mes fichiers**.

Utiliser l'icône de la barre d'état système OneDrive for Business

Dans la barre d'état système :

- Pour le site Web : cliquez avec le bouton droit et sélectionnez **Accéder à OneDrive.com**.
- Pour le dossier : cliquez avec le bouton droit ou gauche et sélectionnez **Ouvrir votre dossier OneDrive Entreprise**. Ceci vous redirige vers le Lecteur virtuel DDG vDisk.

Considérations en matière de sécurité relatives à Data Guardian et OneDrive ou OneDrive Entreprise

Dell Data Guardian crypte les dossiers et fichiers pour sécuriser les données. Étant donné que Data Guardian fonctionne en relation avec les clients de synchronisation, tenez compte des éléments suivants.

- Pendant le téléchargement, ne sélectionnez pas Annuler. Ceci entraînerait un message d'erreur. Si vous souhaitez supprimer un fichier, attendez la fin du téléchargement.
- Pour Windows 8.1, Microsoft OneDrive possède des fichiers d'espace réservé qui semblent exister dans le client de synchronisation mais qui ne sont pas réellement téléchargés Par conséquent, Dell Data Guardian ne peut pas les crypter. Si vous ouvrez un fichier d'espace réservé, Data Guardian affiche une boîte de dialogue indiquant que le fichier ne sera pas protégé. Vous pouvez cliquer avec le bouton droit et sélectionner **Télécharger** puis **Data Guardian** le convertit en fichier .xen.

Dropbox

Aide relative au fournisseur de stockage Cloud

Avant d'utiliser Data Guardian, familiarisez-vous avec le fournisseur de stockage Cloud. Le service clientèle Dropbox est joignable via https://www.dropbox.com/help.

Bien qu'il soit possible de créer des fichiers dans le cloud ou de charger des fichiers vers le site Web du fournisseur de stockage cloud, les meilleures pratiques consistent à travailler à partir de dossiers ou de fichiers situés sur le Lecteur virtuel DDG vDisk.

REMARQUE :
Pour Dropbox et Data Guardian, si vous créez un fichier Office dans le cloud avant de le synchroniser, celui-ci est crypté en tant que fichier .xen. Par conséquent, il s'ouvre en mode lecture seule sur le disque virtuel. Vous ne pouvez pas le modifier.

Si vous supprimez tous les dossiers sur le disque virtuel, les fichiers sont supprimés mais les dossiers peuvent persister. Si c'est le cas, supprimez les dossiers dans le cloud.

Définir la Synchronisation sélective des dossiers

Pour synchroniser des dossiers de manière sélective :

1 Dans la barre d'état système, cliquez sur l'icône **Dropbox**.
2 Cliquez sur l'icône **Paramètres** puis sélectionnez **Préférences**.
3 Cliquez sur l'onglet **Compte** puis sur **Synchronisation sélective**.

4 Sélectionnez uniquement les dossiers ou sous-dossiers de votre ordinateur que vous souhaitez synchroniser.
5 Cliquez sur **Mettre à jour**.
6 Dans la boîte de dialogue Confirmation de mise à jour, cliquez sur **OK**.
7 Dans la fenêtre Préférences de Dropbox, cliquez sur **OK**.
Une fenêtre contextuelle s'affiche dans la barre d'état système et indique que les dossiers sont en cours de synchronisation.

Utiliser l'icône Dropbox de la barre d'état système

Dans la barre d'état système, cliquez sur l'icône Dropbox.

- Pour le site Internet : sélectionnez l'icône Globe.

  REMARQUE :
  Si vous utilisez Chrome ou Firefox pour ouvrir Dropbox.com, n'oubliez pas de le fermer après avoir fini de travailler avec des fichiers et des dossiers. Même si vous ouvrez un autre onglet dans le navigateur, le contenu sera crypté. Cela peut inclure le courrier électronique, les pièces jointes ou des chargements à l'aide du navigateur.

- Pour le dossier : sélectionnez l'icône de dossier Dropbox. Ceci vous redirige vers le Lecteur virtuel DDG vDisk.

Considérations de sécurité liées à Data Guardian et à Dropbox

Si vous êtes en cours d'exécution sur une machine virtuelle, ne faites pas glisser de fichier du bureau du serveur jusqu'au navigateur. Le fichier ne sera pas protégé. Effectuez l'une des actions suivantes : dans le navigateur, utilisez l'option Charger ou, sur le bureau, faites glisser le fichier vers le Lecteur virtuel DDG vDisk.

FAQ concernant Dropbox

Question

Plusieurs fichiers en conflit se trouvent dans mon compte Dropbox. Lorsque je les supprime du Cloud, ils sont automatiquement recréés.

Réponse

Lorsqu'un dossier a déjà été partagé et plusieurs comptes Data Guardian sont activés en même temps, il arrive que les fichiers du dossier soient considérés comme simultanés. Pour préserver l'original, Dropbox crée plusieurs fichiers du même type sous le même nom et les place dans le Cloud. Par conséquent, Data Guardian permet la création de tous ces fichiers sans intervenir.

Solution

1 Tous les utilisateurs qui partagent ce fichier doivent collaborer et retirer ce dossier de la liste des dossiers à synchroniser dans leur application Dropbox. Voir Dropbox for Business.
2 Après la suppression de tous les fichiers et du dossier de chaque ordinateur local, une seule personne doit accéder au Cloud pour effacer les doublons.

Ensuite, chaque utilisateur peut utiliser la synchronisation sélective afin de remettre le dossier dans la liste des dossiers à synchroniser.

Box

Aide relative au fournisseur de stockage Cloud

Avant d'utiliser Data Guardian, familiarisez-vous avec le fournisseur de stockage Cloud. Le service clientèle Box est joignable sur https://support.box.com/home.

Bien qu'il soit possible de charger des fichiers sur le site Web du fournisseur de stockage Cloud, les meilleures pratiques consistent à travailler à partir de dossiers ou de fichiers situés sur le Lecteur virtuel DDG vDisk.

REMARQUE :

Si vous utilisez Internet Explorer pour charger des fichiers vers le fournisseur de stockage cloud Box ou pour ouvrir un fichier, un décalage peut se produire dans la fenêtre de l'Explorateur de fichiers.

REMARQUE :

Box Tools et Box Edit sont pas pris en charge par Data Guardian. L'utilisation de Box Tools peut entraîner la survenue d'un écran bleu.

Définir la Synchronisation sélective des dossiers

Pour synchroniser des dossiers de manière sélective :

1 Dans la barre d'état système, cliquez avec le bouton droit sur l'icône de Box et sélectionnez **Ouvrir le site Web Box**.

2 Sur le site Web du client de synchronisation cloud, cliquez avec le bouton droit sur un dossier et sélectionnez **Synchroniser le dossier avec l'ordinateur**.

3 Dans la fenêtre Synchronisation du dossier, cliquez sur **Synchroniser le dossier**.

L'icône de barre d'état système indique que les paramètres sont appliqués. Ceci peut prendre plusieurs minutes.

4 Une fois terminé, accédez à **Explorateur Windows** > **Synchronisation Box**. Les dossiers synchronisés sont affichés avec une coche.

Utiliser l'icône Box de la barre d'état système

Dans la barre d'état système, cliquez-droit sur l'icône Box.

- Pour le site Web : sélectionnez **Ouvrir le site Web de Box**.
- Pour le dossier : sélectionnez le dossier **Ouvrir la synchronisation de Box**. Ceci vous redirige vers le Lecteur virtuel DDG vDisk.

FAQ concernant le client de synchronisation Box

Question

J'utilise le client de synchronisation Box. J'ai créé un nouveau dossier localement et j'y ai placé quelques fichiers. Le client de synchronisation semble fonctionner, mais rien n'a été créé dans le Cloud.

Réponse

Le client de synchronisation de Box peut prendre un certain temps pour recueillir les informations concernant les nouveaux dossiers et fichiers. Contrairement à ce qui se passe avec d'autres clients de synchronisation, le processus peut prendre plusieurs minutes. Patientez quelques minutes avant de créer de nouveaux dossiers et fichiers, pour laisser au client de synchronisation le temps de terminer l'opération.

Question

J'utilise le client de synchronisation Box. Je n'ai plus de place sur ma partition principale, je l'ai donc déplacé sur un autre lecteur. Je constate que le dossier Mes fichiers Box comprend un ou plusieurs dossiers créés et nommés **Nouveau dossier**.

Réponse

Actuellement, lorsque des fichiers sont synchronisés entre deux ordinateurs sur le même partage de fichiers, si une personne déplace ce dossier vers un autre emplacement, tous les nouveaux dossiers créés par d'autres utilisateurs au sein de ce partage de fichiers créent un dossier vide nommé **Nouveau dossier**.

Solution

Supprimez le nouveau dossier directement dans le Cloud. Il sera supprimé de tous les systèmes qui partagent ce dossier.

Considérations en matière de sécurité relatives à Data Guardian et à Box

Si vous créez un fichier dans le site Web Cloud Box, il sera synchronisé. Cependant, il se téléchargera sous forme de fichier crypté.

Internet Explorer peut provoquer un retard lors du chargement ou de l'ouverture de Box.

Google Drive

Aide relative au fournisseur de stockage Cloud

Avant d'utiliser Data Guardian, familiarisez-vous avec le fournisseur de stockage Cloud. Le service clientèle Google Drive est disponible à l'adresse https://support.google.com/drive/?hl=en#topic=14940.

Bien qu'il soit possible de charger des fichiers sur le site Web du fournisseur de stockage Cloud, les meilleures pratiques consistent à travailler à partir de dossiers ou de fichiers situés sur le Lecteur virtuel DDG vDisk.

Définir la Synchronisation sélective des dossiers

Pour synchroniser des dossiers de manière sélective :

1 Dans la barre d'état système, cliquez sur l'icône **Google Drive**.
2 Sélectionnez l'icône
3 Sélectionnez **Préférences**.
4 Pour effectuer une synchronisation sélective, cliquez sur **Ces dossiers uniquement**.
5 Décochez la case correspondant aux dossiers n'ayant pas besoin de protection dans le Cloud.
6 Cliquez sur **Appliquer**.
7 Pour confirmer, cliquez sur **Continuer**.

Utiliser l'icône Google Drive de la barre d'état système

Dans la barre d'état système, cliquez sur l'icône Google Drive.

- Pour le site Web : sélectionnez **Accéder à Google Drive sur le Web**.
- Pour le dossier : sélectionnez le dossier **Ouvrir Google Drive**. Ceci vous redirige vers le Lecteur virtuel DDG vDisk.

Considérations en matière de sécurité relatives à Data Guardian et à Google Drive

Data Guardian crypte les dossiers et fichiers pour protéger les données. Étant donné que Data Guardian fonctionne en relation avec les clients de synchronisation, tenez compte des éléments suivants.

- La stratégie de sécurité de l'entreprise interdit l'utilisation de Google Documents avec Data Guardian. Lorsque vous installez Data Guardian, une boîte de dialogue vous informe l'existence de cette règle. Pour plus d'informations, contactez votre administrateur informatique.

Google Drive contient une appli Google Docs qui permet aux utilisateurs de collaborer sur des documents en temps réel. Cependant, la collaboration se produit sur un serveur Google et les fichiers ne sont pas cryptés. Pour Windows et Data Guardian, tout document Google que vous créez s'affiche dans les dossiers Google Documents de votre client de synchronisation.

Cependant, si vous ouvrez le dossier, une boîte de dialogue vous avertit que Data Guardian ne peut pas crypter ce document. De plus, pour assurer la sécurité des données, votre administrateur peut exécuter des rapports permettant d'identifier les documents Google en cours de synchronisation afin d'assurer la sécurité.

- Les options Google Drive vous proposent **Supprimer** (déplacer vers la corbeille) et **Effacer**. Avec Data Guardian, Google Drive propose uniquement l'option Effacer par cohérence avec les autres fonctionnalités de Data Guardian.

  REMARQUE :
  Si vous supprimez plusieurs fichiers de l'unité virtuelle de Data Guardian et que certains s'affichent toujours dans le navigateur ou la ligne de commande, supprimez-les dans le navigateur ou depuis la ligne de commande.

- Google Drive peut afficher un avertissement indiquant la suppression des propriétés lors de la copie de fichiers sur le Lecteur virtuel DDG vDisk. Il s'agit d'attributs de sécurité.

OneDrive

REMARQUE :
Data Guardian n'est pas pris en charge avec Microsoft Office 365.

Aide relative au fournisseur de stockage Cloud

Avant d'utiliser Data Guardian, familiarisez-vous avec le fournisseur de stockage Cloud. Support OneDrive sur http://windows.microsoft.com/en-us/onedrive/onedrive-help#onedrive=other.

Bien qu'il soit possible de charger des fichiers sur le site Web du fournisseur de stockage Cloud, les meilleures pratiques consistent à travailler à partir de dossiers ou de fichiers situés sur le Lecteur virtuel DDG vDisk.

Définir la Synchronisation sélective des dossiers

Pour synchroniser des dossiers de manière sélective :

1. Dans la barre d'état système, cliquez avec le bouton droit sur l'icône de **OneDrive** puis sur **Paramètres**.
2. Sélectionnez l'onglet **Choisir les dossiers** puis cliquez sur **Choisir les dossiers**.
3. Ensuite, sélectionnez **Choisir les dossiers à synchroniser**.
4. Une liste de dossiers s'affiche. Cochez ou décochez les cases pour synchroniser ces dossiers. Cliquez sur **OK**.
5. Cliquez sur **OK**.
6. L'icône de barre d'état système indique que les paramètres sont appliqués. Ceci peut prendre plusieurs minutes.
7. Une fois terminé, accédez à **Explorateur Windows** > **OneDrive**. Les dossiers synchronisés sont affichés avec une coche.

Utiliser l'icône OneDrive de la barre d'état système

Dans la barre d'état système :

- Pour le site Web : cliquez avec le bouton droit et sélectionnez **Accéder à OneDrive.com**.
- Pour le dossier : cliquez avec le bouton droit ou gauche et sélectionnez **Ouvrir votre dossier OneDrive**. Ceci vous redirige vers le Lecteur virtuel DDG vDisk.

Considérations en matière de sécurité relatives à Data Guardian et OneDrive ou OneDrive Entreprise

Voir Considérations en matière de sécurité relatives à Data Guardian et aux clients de synchronisation.

Présentation des éléments de menu de Data Guardian dans la barre d'état système

Écran Détails

L'écran Détails de Data Guardian fournit des informations utiles, par exemple :

- Pour le support technique, vous pouvez fournir des informations d'état ou de version.
- Pour voir un nom de fichier non obscurci associé à un fichier .xen, sélectionnez **Fichier** > **État du fichier**.
- Pour rechercher un nom de fichier, sélectionnez Copier en bas à droite et collez le contenu dans un fichier Word.
- Pour voir à qui appartient un dossier, sélectionnez Dossiers et faites défiler jusqu'à la colonne DROITS DE PROPRIÉTÉ DU DOSSIER.

Pour accéder à l'écran Détails :

Cliquez sur l'icône de **Data Guardian** dans la barre d'état système, puis cliquez sur **Détails...**

Les informations suivantes s'affichent dans le coin supérieur gauche de l'écran Infos :

État du service : état du service Windows Data Guardian. Les valeurs disponibles sont les suivantes : Arrêté, Démarrage en attente, Arrêt en attente, Exécution, Poursuite en attente, Pause en attente, En pause.

Statut d'exécution : état d'activation du périphérique. Valeurs possibles : Actif, Réactivation, En suspens, Suspension

Mode utilisateur : utilisateur interne : un utilisateur au sein de cette adresse de domaine

Utilisateur externe : un utilisateur en dehors de cette adresse de domaine

E-mail d'enregistrement : pour les utilisateurs internes, il s'agit de l'adresse e-mail du domaine. Pour les utilisateurs externes, il s'agit de l'e-mail sous lequel ils se sont enregistrés.

URL du serveur : serveur DDP EE/VE qui communique avec ce client.

Dernière modification de règle : date et horodatage correspondant aux modification et utilisation les plus récentes de la règle par le client.

Version de la règle : version de la règle générée par le serveur DDP EE/VE.

La zone **Fichiers** de l'écran Détails affiche les informations suivantes :

Nom : nom du fichier

Cloud : répertorie le nom obscurci du fichier et indique si le fichier est *Non protégé*.

État du fichier : cette valeur indique le propriétaire du dossier. La valeur est déterminée par l'identifiant clé.

État du traitement : indique si le fichier nécessite une clé ou si le traitement est *terminé*.

Entreprise : indique le serveur par défaut. Si un message *Erreur : clé non issue de votre serveur* s'affiche dans cette colonne, cela signifie que la clé n'appartient pas à votre serveur d'entreprise. La clé d'un fichier crypté doit appartenir au serveur de votre entreprise.

Clé : identifiant clé attribué au dossier (le cryptage des nouveaux fichiers se fera à l'aide de cette clé).

Dossier : nom de chemin d'accès complet du dossier.

Dernière modification : la date de modification du fichier.

État de persistance : ceci indique si le fichier est sur disque.

Lecture de fichier XEN : *True* ou *False*.

Créé sous navigateur: *True* ou *False*.

Pour afficher les fichiers journaux, cliquez sur **Afficher le journal** dans l'angle inférieur gauche de l'écran Détails.

REMARQUE :
Vous trouverez également les fichiers journaux sur **C:\ProgramData\Dell\Dell Data Protection\Dell Data Guardian.**

La zone **Fichiers** de l'écran Détails affiche les informations suivantes :

Nom : nom du dossier

Clé : identifiant clé attribué au dossier (le cryptage des nouveaux fichiers se fera à l'aide de cette clé).

Client de synchronisation : le dernier client de synchronisation qui a synchronisé ce dossier (voir Clients de synchronisation cloud).

Propriété du dossier : cette valeur indique le propriétaire du dossier. La valeur est déterminée par l'identifiant clé.

Remplacer : les options sont *Aucun* et *Existant*. Les fichiers préexistants ne sont pas protégés. De plus, si vous avez accès à la fonction de gestion des dossiers et à des fichiers déprotégés, cette colonne indique qu'ils ne sont pas protégés.

Type de masquage : si votre entreprise gère votre stockage cloud, il s'agit d'une règle définie pour chaque dossier qui indique le type de fichiers .xen créés dans le cloud. Cette règle est configurée par votre administrateur. Si votre administrateur sélectionne *Extension uniquement*, le nom de fichier réel s'affichera avec l'extension « .xen ». Si votre administrateur sélectionne *Guid*, un nom de fichier crypté doté de l'extension « .xen » s'affiche. Ce paramètre de règle s'applique uniquement aux nouveaux dossiers. La valeur par défaut est *Extension uniquement*.

Menu Gérer les dossiers

Certains gestionnaires ou administrateurs peuvent avoir besoin de dépanner temporairement les dossiers partagés par plus d'un utilisateur. Vous pouvez demander l'autorisation de votre administrateur pour l'option Gérer les dossiers. En général, il s'agit d'une option temporaire.

Vérifier les mises à jour de règle

Si votre administrateur modifie une règle et vous avertit de sa mise à jour, accédez à la barre d'état système de Windows, cliquez sur l'icône **Dell Data Protection | Data Guardian**, puis sélectionnez **Vérifier les mises à jour de règle**.

Si votre administrateur modifie une règle pour protéger des fichiers créés dans Microsoft Word, vous devez fermer Word pour que la mise à jour soit appliquée.

Localiser les fichiers journaux

Pour tout dépannage, votre administrateur peut demander les fichiers journaux.

Pour localiser les fichiers journaux :

1 Naviguez vers
2 Sélectionnez **Xendow.service.log**.

> **REMARQUE :**
> Lorsque Xendow.Service.log atteint 3 Mo, il est enregistré sous la forme Xendow.Service1.log, puis Xendow.Service2.log.

Mise à niveau de Data Guardian

Les meilleures pratiques consistent à désinstaller la version précédente puis à réinstaller la version actuelle. Voir Désinstaller Data Guardian.

Envoyer des commentaires à Dell

Si votre administrateur a activé une règle de commentaires, vous pouvez envoyer un commentaire à Dell concernant ce produit. Le bref formulaire comprend deux questions concernant votre niveau de satisfaction, avec échelles d'évaluation (dans lesquelles le chiffre 10 représente le plus haut niveau de satisfaction), ainsi qu'un champ réservé au commentaire.

Pour accéder au formulaire, cliquez sur l'icône Data Guardian dans la barre d'état système et sélectionnez **Envoyer des commentaires**.

Si cette fonctionnalité n'est pas activée par une règle, l'option ne s'affiche pas.

Problèmes possibles à l'activation : cloud et Office protégé

Si vous avez installé Data Guardian mais que l'icône Data Guardian de la barre d'état système n'est pas dotée d'une coche verte  , prenez en compte les éléments suivants si vous disposez du cryptage cloud, d'Office protégé ou des deux options :

- L'accès aux sites Web de synchronisation Cloud est bloqué
- La connexion entre les applications de synchronisation Cloud et leurs services Web est bloquée
- Les dossiers de synchronisation locaux ne sont pas mis à jours pendant cette période de temps
- Data Guardian peut convertir des documents Office existants en mode protégé avant l'activation. Si c'est le cas, lorsque vous ouvrez un document Office, une page de garde s'affiche avec des informations sur la méthode d'activation.

Effectuez l'une des opérations suivantes :

- Redémarrez le système puis reconnectez-vous avec un suffixe UPN, par exemple, nom_utilisateur@domaine.com.
- Demandez à votre administrateur de vous confirmer si vous devez cocher la case **Activer la vérification de confiance SSL** lorsque vous installez Data Guardian.
- Contactez votre administrateur système à propos de la configuration de votre ordinateur en vue d'une activation manuelle. Voir Activer Data Guardian.

Activer Data Guardian

En général, Data Guardian s'active automatiquement après l'installation et le redémarrage. Si votre administrateur vous propose une activation manuelle, procédez comme suit :

1 Connectez-vous à Windows.

Dans la barre d'état système, une icône en forme de bouclier assortie d'un point d'exclamation orange s'affiche.

2 Cliquez sur l'icône **Data Guardian** dans la barre d'état système et sélectionnez **Activation par l'utilisateur**.

3 Saisissez l'adresse e-mail de votre domaine et le mot de passe du domaine, puis cliquez sur **Activer**.

Si vous êtes un utilisateur interne (possédant une adresse e-mail dans le domaine), ignorez le bouton S'inscrire. Seuls les utilisateurs externes doivent s'inscrire.

Une fois l'activation terminée, une coche verte s'affiche sur l'icône Data Guardian dans la barre d'état système  .

4 Confirmez l'état de votre mode utilisateur. Cliquez sur l'icône de la barre d'état système et sélectionnez **Détails**.

5 En haut, confirmez le mode utilisateur :

Interne : utilisateur doté d'une adresse e-mail incluse dans le domaine de la société.

Externe : utilisateur doté d'une adresse e-mail extérieure au domaine. Pour plus d'informations, voir Utiliser Data Guardian en tant qu'utilisateur externe.

Tâches utilisateur : Office protégé sans cryptage cloud

Votre administrateur a déjà configuré les règles de Data Guardian pour protéger les documents Office.

REMARQUE :
Si votre entreprise gère également votre client de synchronisation cloud, voir Tâches utilisateur : cryptage cloud et Office protégé.

Présentation des tâches

Cette présentation résume la séquence d'installation et d'utilisation de Data Guardian.

Installez Data Guardian

Tâche	Description	Pour en savoir plus
Installez Data Guardian	Déterminez les éléments suivants : L'utilisateur doit installer Data Guardian L'administrateur a déjà installé Data Guardian : passez à l'étape suivante.	Installation par l'utilisateur : voir Installer Data Guardian sous Windows. Redémarrez le système et passez à l'étape suivante.
Confirmer l'état d'activation	Vérifiez que l'icône Data Guardian de la barre d'état système est dotée d'une coche verte  .	Si l'icône est affublée d'un point d'exclamation orange, voir Problèmes possibles à l'activation : Office protégé.

Utiliser Data Guardian

Tâche	Description	Pour en savoir plus
Afficher le menu de la barre d'état système	Fournit des informations utiles concernant les fichiers, les dossiers et le dépannage.	Présentation des éléments de menu de Data Guardian dans la barre d'état système
Documents Office protégés et prenant en charge les macros, si la règle est activée	Protégez un document Office (.docx, .pptx, .xlsx, .docm, .pptm, .xlsm) dès sa création. Ce document sera protégé si vous le partagez avec d'autres utilisateurs ou l'enregistrez sur un média amovible.	Utiliser les documents Office avec le mode protégé de Data Guardian • Observer l'option de menu Fichier pour déterminer le niveau de sécurité des documents Office • Travailler avec l'option de menu Fichier
Partager un dossier avec d'autres utilisateurs afin de collaborer sur des fichiers	Partager un dossier avec : un utilisateur interne (possédant une adresse e-mail dans le domaine).	Utilisateur interne : voir l'aide en ligne relative à votre fournisseur de stockage Cloud. Utilisateur externe : voir Utiliser Data Guardian en tant qu'utilisateur externe.

Tâche	Description	Pour en savoir plus
	un utilisateur externe (possédant une adresse e-mail hors domaine) : à déterminer avec votre administrateur.	

REMARQUE :

Si vous ouvrez un document Office et qu'une page de garde s'affiche avec des informations d'installation ou d'activation, il est possible que votre administrateur ait défini des règles pour protéger les documents Office. Vérifiez que Data Guardian est installé et activé. Voir Problèmes possibles à l'activation : Office protégé.

Installer Data Guardian pour Office protégé

Installer Data Guardian sous Windows

Vous devez disposer des droits d'administrateur sur l'ordinateur local pour installer Data Guardian.

L'ordinateur doit disposer d'une lettre disponible, pouvant être attribuée à un lecteur de disque.

Soyez prêt à redémarrer l'ordinateur après l'installation de Data Guardian.

1. Pour télécharger le programme d'installation de Data Guardian, rendez-vous à l'emplacement spécifié par votre administrateur.
2. En fonction de votre système d'exploitation, sélectionnez le programme d'installation 32 bits ou 64 bits, généralement nommés **setup32.exe** et **setup64.exe**, et le copiez-le sur l'ordinateur local.
3. Double-cliquez sur le fichier pour lancer le programme d'installation.
4. Si vous recevez un avertissement de sécurité, cliquez sur **Exécuter**.
5. Sélectionnez une langue, puis cliquez sur **OK**.
6. Si un message vous invite à installer Microsoft Visual C++ 2010 Redistributable Package ou Microsoft .NET Framework 4.0 Client Profile, cliquez sur **OK**.
7. Dans la page d'accueil, cliquez sur **Suivant**.
8. Lisez le contrat de licence, acceptez les conditions, puis cliquez sur **Suivant**.
9. À l'écran Dossier de destination, cliquez sur **Suivant** pour installer à l'emplacement par défaut suivant **C:\Program Files\Dell\Dell Data Protection\Dell Data Guardian\.**

   Sur **C:**, n'installez pas Data Guardian dans les dossiers Users ou Windows, ou à la racine d'un lecteur. Vous obtiendrez un message d'erreur.
10. Dans le champ *Nom du serveur :*, saisissez le nom du serveur avec lequel cet ordinateur communiquera. Par exemple, serveur.domaine.com. Il n'est pas nécessaire d'inclure www ou http(s). Cette information est fournie par votre administrateur.

    Ne décochez pas la case *Activer la vérification de confiance SSL* sauf si votre administrateur vous le demande.
11. Cliquez sur **Suivant**.
12. Dans l'écran d'information Confirmer le serveur d'activation, confirmez que l'adresse URL du serveur est correcte. Le programme d'installation ajoute www ou http(s) et le port. Cliquez sur **Suivant**.
13. Dans la fenêtre Type de gestion, sélectionnez cette option :
    - Utilisation interne : utilisateur doté d'une adresse e-mail incluse dans le domaine de la société.
14. Cliquez sur **Installer** pour démarrer l'installation.

    Une fenêtre affichant l'avancée de l'installation apparaît.
15. Lorsque l'écran Installation terminée s'affiche, cliquez sur **Terminer**.
16. Cliquez sur **Oui** pour redémarrer.

    L'installation de Data Guardian est maintenant terminée.
17. Une fois que vous avez redémarré, vérifiez dans la barre d'état système que l'icône Data Guardian est dotée d'une coche verte  .

Utiliser les documents Office avec le mode protégé de Data Guardian

Pour améliorer la sécurité de l'entreprise, votre administrateur peut activer une règle pour protéger les fichiers de ces applications de Bureau :

- .docx, .pptx, .xlsx
- .docm, .pptm, .xlsm

Si une personne non autorisée accède à un fichier protégé, celui-ci reste crypté, par exemple lorsque vous effectuez les actions suivantes :

- Joindre à un e-mail
- Déplacer vers un navigateur : dans certains clients de synchronisation cloud, vous pouvez cliquer avec le bouton droit sur un nom de fichier et sélectionner **Déplacer**.
- Partager sur le réseau
- Charger vers un fournisseur de stockage cloud
- Stocker sur un média amovible

Pour les documents Office, une page de garde peut s'afficher avec des instructions d'installation ou d'activation de Data Guardian, par exemple :

- Vous devez installer Data Guardian.
- Vous devez activer Data Guardian.
- Vous ouvrez un document Office protégé dans le cloud.
- Vous avez téléchargé un fichier Office depuis votre ordinateur équipé de Data Guardian vers un appareil personnel qui n'en dispose pas.
- Un utilisateur non autorisé accède à l'un de vos fichiers Office : la page de garde s'affiche avec un message spécifique à l'entreprise, mais cet utilisateur ne peut pas afficher le contenu du fichier.

Si votre entreprise utilise le mode protégé de Data Guardian, reportez-vous aux sections suivantes :

- Observer l'option de menu Fichier pour déterminer le niveau de sécurité des documents Office
- Travailler avec l'option de menu Fichier
- Déterminer quels documents en mode de protection individuelle sont protégés
- Options de menu supplémentaires pour les documents Office protégés
- Utilisateurs externes et documents Office protégés

Observer l'option de menu Fichier pour déterminer le niveau de sécurité des documents Office

Pour déterminer si votre administrateur a activé les règles Data Guardian, ouvrez un document Office et sélectionnez **Fichier**. Si *Opération Enregistrer sous protégée* s'affiche dans le volet de gauche, vos documents Office bénéficient d'une protection supplémentaire.

Pour déterminer le niveau de sécurité, observez quelles options sont activées ou désactivées :

- **Mode de protection individuelle** : vous permet de déterminer quels documents Office protéger.
  - Les options *Enregistrer sous* et *Opération Enregistrer sous protégée* sont activées : si vous décidez de protéger un document Office, sélectionnez **Opération Enregistrer sous protégée**.
  - Les options *Imprimer* et *Exporter* sont activées ou désactivées selon la règle.
  - L'option *Partager* (*Enregistrer et envoyer* sous Office 2010) est activée.
  - Dossier **Documents > Documents sécurisés** : avec le mode de protection individuelle (mais sans le mode de protection forcée), un dossier Documents sécurisés s'ajoute à la racine du dossier Documents. Les documents Office de ce dossier sont cryptés. Si vous

retirez un document Office protégé de ce répertoire, celui-ci reste crypté. Si vous renommez le dossier, le contenu du dossier renommé est crypté. Si vous supprimez le dossier, celui-ci se recrée.

- **Mode de protection forcée** : votre entreprise requiert un niveau élevé de sécurité.
  - L'option *Enregistrer sous* est désactivée et l'option *Opération Enregistrer sous protégée* est activée : vous devez enregistrer tous les documents Office en mode protégé.
  - Les options *Imprimer* et *Exporter* sont activées ou désactivées en fonction de la règle.
  - L'option *Partager* (*Enregistrer et envoyer* sous Office 2010) est désactivée.

    REMARQUE :
    Lorsque le mode Protection forcée est activé, la règle active également des heures spécifiques pour balayer votre ordinateur afin de localiser tous les fichiers Office non protégés et les faire passer en mode Protégé. Vous devez être connecté et relié au réseau pour que Data Guardian puisse balayer et localiser des fichiers Office non protégés.

- Si vous sélectionnez **Opération Enregistrer sous protégée**, la seule option dans le champ *Type d'opération Enregistrer sous* est *Office protégé*.

- **Fichier > Informations** diffère, par exemple :
  - Pour le mode de protection individuelle comme pour le mode de protection forcée : l'option *Ajouter une restriction calendaire* s'affiche si l'administrateur a activé cette règle. Voir Optimiser la sécurité en ajoutant des restrictions calendaires.
  - Pour le mode de protection individuelle comme pour le mode de protection forcée : les informations liées à la propriété de ce document Office, notamment l'auteur et la date, sont masquées pour une sécurité accrue.
  - État de lecture seule : voir ci-dessous pour plus d'informations.

    REMARQUE :
    L'option *Protéger le document* dans Fichier > Informations est associée au mode protégé de Microsoft Office et non pas de Data Guardian.

Si vous ouvrez un document Office et que celui-ci indique le mode lecture seule, vérifiez les éléments suivants :

- Si l'option *Opération Enregistrer sous protégée* ne s'affiche pas dans le volet de gauche, la lecture seule n'est pas liée aux règles de Data Guardian.
- Si votre administrateur a défini des règles en mode de protection forcée avec un niveau de sécurité plus élevé, les documents Office non protégés s'ouvrent en mode lecture seule.

  REMARQUE :
  Pour OneDrive, si vous ouvrez un document Office protégé via **Fichier > Ouvrir > OneDrive** et si le document est en lecture seule, assurez-vous d'avoir installé et configuré le client de synchronisation OneDrive.

Travailler avec l'option de menu Fichier

Ce tableau répertorie les options du menu Fichier pour les documents Office. En fonction du niveau de sécurité, certaines options sont grisées.

REMARQUE :
Actuellement, les documents Office intégrés ne sont pas pris en charge par le mode protégé Office.

Menu Fichier	Mode de protection individuelle et documents Office protégés	Mode de protection forcée pour protégés et non protégés
Ouvrez le fichier	**Les fichiers s'ouvrent normalement**	**Les fichiers non protégés s'ouvrent en lecture seule.**
Enregistrer	• Options : Document déjà protégé : permet d'enregistrer avec protection. Non protégé : permet d'enregistrer sans protection. Pour protéger ce document, cliquez sur **Opération Enregistrer sous protégée**. • Document en lecture seule : une boîte de dialogue vous signifie que vous ne pouvez pas enregistrer un document non protégé. Une fenêtre Enregistrer sous s'ouvre alors et vous êtes invité à enregistrer ce document sous un autre nom de fichier. • Fichier .xen : vous pouvez l'ouvrir et l'enregistrer en mode protégé, mais cela entraîne la suppression de ce fichier dans le cloud. Le document Office dispose de son extension habituelle, mais il est protégé. **REMARQUE :** **Sur l'unité virtuelle, si vous cliquez avec le bouton droit pour créer un nouveau document Office, celui-ci est au format .xen. Vous devez l'enregistrer manuellement en tant que document protégé.**	• Le document est protégé. • Document en lecture seule : vous pouvez le modifier, mais pas enregistrer l'original. Lorsque vous cliquez sur Enregistrer, la fenêtre Opération Enregistrer sous protégée s'ouvre et vous devez enregistrer le document en mode protégé sous un nouveau nom. • Documents à distance : si vous ouvrez un document dans un emplacement distant et qu'il n'est pas protégé, vous devez l'enregistrer sur votre disque local pour le modifier et l'enregistrer. Vous ne pouvez pas enregistrer de fichier dans l'emplacement distant. **REMARQUE :** **Cliquer sur Enregistrer déclenche l'ouverture d'une fenêtre Enregistrer sous. L'unique option dans le champ Type d'opération Enregistrer sous est Office protégé (document, présentation, ou classeur).** • Fichier .xen : vous pouvez l'ouvrir et l'enregistrer en mode protégé, mais cela entraîne la suppression de ce fichier dans le cloud. Le document Office dispose de son extension habituelle, mais il est protégé.
Enregistrer sous	**Dispose des options standard (mais pas du mode protégé)**	**Désactivée**
Opération Enregistrer sous protégée	**La seule option dans le champ Type d'opération Enregistrer sous est Office protégé**	**La seule option dans le champ Type d'opération Enregistrer sous est Office protégé**
Impression	**Peut être activée ou grisée en fonction des règles définies par votre administrateur. Si l'option de menu est activée, une règle peut placer un filigrane contenant le nom d'utilisateur, le nom de domaine et l'ID d'ordinateur sur chaque page à l'impression.**	**Selon la règle, cette option peut être activée ou grisée. Si l'option de menu est activée, une règle peut placer un filigrane contenant le nom d'utilisateur, le nom de domaine et l'ID d'ordinateur sur chaque page à l'impression.**
Partager	**Activé**	**Désactivée**
Enregistrer et envoyer (Office 2010)	**Activé**	**Désactivée** **Si l'option Imprimer est activée, vous pouvez sélectionner Imprimer pour imprimer le document au format PDF.**
Exporter (Office 2013 et versions ultérieures)	**Peut être activée ou grisée en fonction des règles définies par votre administrateur.**	**Peut être activée ou grisée en fonction des règles définies par votre administrateur.**
Opération Exporter protégée (Office 2013 et versions ultérieures)	Si l'option de menu Exporter est grisée et Exportation protégée est activée, le document s'exporte avec un filigrane contenant le nom d'utilisateur, le nom de domaine et ID d'ordinateur sur chaque page. **REMARQUE :** Si vous exportez un document en mode protégé vers un utilisateur externe, celui-ci peut l'ouvrir et l'afficher mais pas l'exporter ou l'imprimer.	Si l'option de menu Exporter est grisée et Exportation protégée est activée, le document s'exporte avec un filigrane contenant le nom d'utilisateur, le nom de domaine et ID d'ordinateur sur chaque page. **REMARQUE :** Si vous exportez un document en mode protégé vers un utilisateur externe, celui-ci peut l'ouvrir et l'afficher mais pas l'exporter ou l'imprimer.

Travailler en ligne avec les documents Office protégés

Lors de la création de documents Office protégés, la meilleure pratique consiste à travailler en ligne à cause des clés générées pour ces documents. Si vous avez besoin de réimager votre ordinateur et que vous avez créé des documents Office protégés hors ligne, veillez en avertir votre administrateur.

Travailler en ligne avec les documents protégés prenant en charge les macros

Dans un document prenant en charge les macros, la macro existe mais elle est bloquée. Cependant, actuellement, Data Guardian peut contrôler un document prenant en charge les macros uniquement après que vous avez fermé puis rouvert le document nouvellement protégé (.docm, .pptm, .xlsm). En outre, si vous enregistrez un document protégé avec une macro en tant que document non protégé, vous devez fermer puis rouvrir le document afin d'exécuter la macro.

Joindre un document Office protégé à un e-mail Outlook

Lorsque vous joignez un document Office protégé à un e-mail Outlook, sélectionnez **Insérer** au lieu d'*Insérer comme texte*. *Insérer comme texte* colle le contenu du document directement dans le corps de l'e-mail. Ce contenu n'est alors plus protégé.

Dépannage du mode de protection individuelle

Dans Fichier > Informations, si votre option Imprimer est grisée, une règle Data Guardian a désactivé l'impression des documents Office protégés. Quoiqu'actuellement, lorsque vous cliquez avec le bouton droit sur un fichier Office protégé dans l'Explorateur Windows, l'option d'impression n'est pas grisée. Toutefois, si vous sélectionnez Imprimer, voici ce qui se produit :

- Word : une boîte de dialogue indique que Word a cessé de fonctionner.
- Excel : une boîte de dialogue indique que l'option Imprimer est désactivée par la règle.
- PowerPoint : une boîte de dialogue indique que l'option Imprimer est désactivée par la règle. Si vous cliquez sur OK, une page de garde s'imprime indiquant que le document est protégé.

Déterminer quels documents en mode de protection individuelle sont protégés

Si vous disposez du mode de protection forcée, tous les documents Office sont protégés. Si vous disposez du mode de protection individuelle et souhaitez vérifier si un document est protégé ou non, ouvrez ce document : la barre de titre le désigne comme protégé.

Options de menu supplémentaires pour les documents Office protégés

Le type de document Office, protégé ou non, peut affecter les éléments suivants.

Clic droit > Protéger

Vous pouvez cliquer avec le bouton droit sur un document Office et sélectionner **Protéger**. Vous devez ajouter du contenu pour que l'option de menu s'affiche. Vous ne pouvez pas protéger un document vierge.

Propriétés de fichier > onglet Dell Data Guardian

Avec les documents Office protégés, vous pouvez cliquer avec le bouton droit et sélectionner **Propriétés** et un onglet **Dell Data Guardian** s'affiche avec des informations telles que l'ID de clé de fichier ainsi que les données d'accès et d'embargo.

Coller

Si votre administrateur définit une règle pour protéger les documents Office :

- Vous pouvez copier et coller des données dans le document protégé d'origine.

- Vous ne pouvez pas copier ou coller le contenu d'un document protégé dans un document non protégé. Rien ne s'affiche dans le presse-papiers et un message spécifique à l'entreprise indique que vous ne pouvez pas coller de contenu dans le document non protégé ou non géré.

  REMARQUE :
  Si vous coupez du texte d'un document protégé et obtenez ce message dans un document non protégé, cliquez sur **Annuler** dans le document protégé pour récupérer le texte.

Glisser-déposer en mode protégé

Vous pouvez faire glisser et déposer du contenu dans un document Word protégé. Actuellement, la fonction de glisser-déposer est désactivée pour les fichiers PowerPoint et Excel protégés.

Imprimer d'enveloppes et d'étiquettes

Si votre administrateur a défini une règle pour ajouter un filigrane lorsque vous imprimez un document Office protégé, procédez comme suit pour imprimer des enveloppes ou des étiquettes :

1 Dans un document Word, sélectionnez l'onglet **Publipostage**.
2 Sélectionnez l'option **Enveloppes** ou **Étiquettes**.
3 Une fois que vous avez saisi l'adresse ou l'adresse de l'expéditeur, cliquez sur **Imprimer**.

REMARQUE : Si vous utilisez une autre option pour imprimer et que votre administrateur a défini une règle pour ajouter un filigrane aux documents Office imprimés, ce filigrane s'affichera sur votre enveloppe ou étiquette.

Altération et documents Office protégés

Data Guardian peut analyser les documents Office protégés pour détecter certaines formes d'altération.

Si un utilisateur interne altère un document Office protégé :

- Data Guardian peut réparer ou restaurer certaines altérations.
- Dans le cas des altérations irréparables, une boîte de dialogue peut s'afficher pour vous avertir que le fichier a été altéré et contacter votre administrateur.

Si un utilisateur non autorisé ouvre un document Office protégé, seule la page de garde s'affiche. Si cet utilisateur non autorisé modifie la page de garde, Data Guardian la restaure lorsqu'un utilisateur autorisé l'enregistre de nouveau au format protégé.

Utilisateurs externes et documents Office protégés

Optimiser la sécurité en ajoutant des restrictions calendaires

Avec Data Guardian, lorsque vous chargez un document Office protégé vers le cloud et le partagez :

- Tous les utilisateurs internes de Data Guardian peuvent l'afficher.
- Selon la règle, les utilisateurs externes peuvent l'afficher.

Si vous le désirez, pour optimiser la sécurité envers les utilisateurs externes, vous pouvez ajouter une restriction calendaire pour limiter la durée d'autorisation d'affichage d'un document Office par un utilisateur externe.

1 Sélectionnez **Fichier > Informations > Restriction calendaire**.
2 Dans le menu déroulant de l'option, sélectionnez une date et une heure de début et de fin d'autorisation d'affichage du document par un utilisateur externe.

REMARQUE :
Vous pouvez choisir une date et une heure de début future si vous souhaitez envoyer le document mais empêcher l'utilisateur externe de l'afficher jusqu'à cette échéance.

3 Cliquez sur **OK**.
Ceci entraînera l'enregistrement, la protection, la fermeture puis la réouverture du document.

REMARQUE :
Si vous modifiez les dates d'un document Office non protégé puis cliquez sur Annuler, Data Guardian continue de protéger ce fichier.

REMARQUE :
Actuellement, lorsque vous ajoutez des restrictions calendaires à un document Office protégé et envisagez de l'enregistrer sur un lecteur réseau, vous devez enregistrer le fichier localement puis le copier sur le réseau.

Si un utilisateur externe ouvre un fichier après l'intervalle calendaire, une boîte de dialogue indique que le fichier est sujet à des restrictions d'accès et que l'utilisateur externe peut contacter l'auteur de ce fichier. La boîte de dialogue n'affiche aucune date pour l'utilisateur externe.

Si vous définissez le champ Date de début sur une date ou une heure future et si l'utilisateur externe ouvre le fichier avant cette échéance, une boîte de dialogue s'affiche et vous informe que vous ne pouvez pas ouvrir ce fichier avant cette échéance en raison de restrictions d'accès.

Présentation des éléments de menu de Data Guardian dans la barre d'état système

Écran Détails

L'écran Détails de Data Guardian fournit des informations utiles, par exemple :

- Pour le support technique, vous pouvez fournir des informations d'état ou de version.
- Pour voir un nom de fichier non obscurci associé à un fichier .xen, sélectionnez **Fichier** > **État du fichier**.
- Pour rechercher un nom de fichier, sélectionnez Copier en bas à droite et collez le contenu dans un fichier Word.
- Pour voir à qui appartient un dossier, sélectionnez Dossiers et faites défiler jusqu'à la colonne DROITS DE PROPRIÉTÉ DU DOSSIER.

Pour accéder à l'écran Détails :

Cliquez sur l'icône de **Data Guardian** dans la barre d'état système, puis cliquez sur **Détails...**

Les informations suivantes s'affichent dans le coin supérieur gauche de l'écran Infos :

État du service : état du service Windows Data Guardian. Les valeurs disponibles sont les suivantes : Arrêté, Démarrage en attente, Arrêt en attente, Exécution, Poursuite en attente, Pause en attente, En pause.

Statut d'exécution : état d'activation du périphérique. Valeurs possibles : Actif, Réactivation, En suspens, Suspension

Mode utilisateur : utilisateur interne : un utilisateur au sein de cette adresse de domaine

Utilisateur externe : un utilisateur en dehors de cette adresse de domaine

E-mail d'enregistrement : pour les utilisateurs internes, il s'agit de l'adresse e-mail du domaine. Pour les utilisateurs externes, il s'agit de l'e-mail sous lequel ils se sont enregistrés.

URL du serveur : serveur DDP EE/VE qui communique avec ce client.

Dernière modification de règle : date et horodatage correspondant aux modification et utilisation les plus récentes de la règle par le client.

Version de la règle : version de la règle générée par le serveur DDP EE/VE.

La zone **Fichiers** de l'écran Détails affiche les informations suivantes :

Nom : nom du fichier

Cloud : répertorie le nom obscurci du fichier et indique si le fichier est *Non protégé*.

État du fichier : cette valeur indique le propriétaire du dossier. La valeur est déterminée par l'identifiant clé.

État du traitement : indique si le fichier nécessite une clé ou si le traitement est *terminé*.

Entreprise : indique le serveur par défaut. Si un message *Erreur : clé non issue de votre serveur* s'affiche dans cette colonne, cela signifie que la clé n'appartient pas à votre serveur d'entreprise. La clé d'un fichier crypté doit appartenir au serveur de votre entreprise.

Clé : identifiant clé attribué au dossier (le cryptage des nouveaux fichiers se fera à l'aide de cette clé).

Dossier : nom de chemin d'accès complet du dossier.

Dernière modification : la date de modification du fichier.

État de persistance : ceci indique si le fichier est sur disque.

Lecture de fichier XEN : *True* ou *False*.

Créé sous navigateur: *True* ou *False*.

Pour afficher les fichiers journaux, cliquez sur **Afficher le journal** dans l'angle inférieur gauche de l'écran Détails.

REMARQUE :
Vous trouverez également les fichiers journaux sur **C:\ProgramData\Dell\Dell Data Protection\Dell Data Guardian.**

La zone **Fichiers** de l'écran Détails affiche les informations suivantes :

Nom : nom du dossier

Clé : identifiant clé attribué au dossier (le cryptage des nouveaux fichiers se fera à l'aide de cette clé).

Client de synchronisation : le dernier client de synchronisation qui a synchronisé ce dossier (voir Clients de synchronisation cloud).

Propriété du dossier : cette valeur indique le propriétaire du dossier. La valeur est déterminée par l'identifiant clé.

Remplacer : les options sont *Aucun* et *Existant*. Les fichiers préexistants ne sont pas protégés. De plus, si vous avez accès à la fonction de gestion des dossiers et à des fichiers déprotégés, cette colonne indique qu'ils ne sont pas protégés.

Type de masquage : si votre entreprise gère votre stockage cloud, il s'agit d'une règle définie pour chaque dossier qui indique le type de fichiers .xen créés dans le cloud. Cette règle est configurée par votre administrateur. Si votre administrateur sélectionne *Extension uniquement*, le nom de fichier réel s'affichera avec l'extension « .xen ». Si votre administrateur sélectionne *Guid*, un nom de fichier crypté doté de l'extension « .xen » s'affiche. Ce paramètre de règle s'applique uniquement aux nouveaux dossiers. La valeur par défaut est *Extension uniquement*.

Menu Gérer les dossiers

Certains gestionnaires ou administrateurs peuvent avoir besoin de dépanner temporairement les dossiers partagés par plus d'un utilisateur. Vous pouvez demander l'autorisation de votre administrateur pour l'option Gérer les dossiers. En général, il s'agit d'une option temporaire.

Localiser les fichiers journaux

Pour tout dépannage, votre administrateur peut demander les fichiers journaux.

Pour localiser les fichiers journaux :

1 Naviguez vers
2 Sélectionnez **Xendow.service.log**.

> **REMARQUE :**
> Lorsque Xendow.Service.log atteint 3 Mo, il est enregistré sous la forme Xendow.Service1.log, puis Xendow.Service2.log.

Vérifier les mises à jour de règle

Si votre administrateur modifie une règle et vous avertit de sa mise à jour, accédez à la barre d'état système de Windows, cliquez sur l'icône **Dell Data Protection | Data Guardian**, puis sélectionnez **Vérifier les mises à jour de règle**.

Si votre administrateur modifie une règle pour protéger des fichiers créés dans Microsoft Word, vous devez fermer Word pour que la mise à jour soit appliquée.

Mise à niveau de Data Guardian

Les meilleures pratiques consistent à désinstaller la version précédente puis à réinstaller la version actuelle. Voir Désinstaller Data Guardian.

Envoyer des commentaires à Dell

Si votre administrateur a activé une règle de commentaires, vous pouvez envoyer un commentaire à Dell concernant ce produit. Le bref formulaire comprend deux questions concernant votre niveau de satisfaction, avec échelles d'évaluation (dans lesquelles le chiffre 10 représente le plus haut niveau de satisfaction), ainsi qu'un champ réservé au commentaire.

Pour accéder au formulaire, cliquez sur l'icône Data Guardian dans la barre d'état système et sélectionnez **Envoyer des commentaires**.

Si cette fonctionnalité n'est pas activée par une règle, l'option ne s'affiche pas.

Problèmes possibles à l'activation : Office protégé

Si vous avez installé Data Guardian mais que l'icône Data Guardian dans la barre d'état système ne comporte pas de coche verte  , prenez en compte les éléments suivants :

- Data Guardian peut convertir des documents Office existants en mode protégé avant l'activation. Si c'est le cas, lorsque vous ouvrez un document Office, une page de garde s'affiche avec des informations sur la méthode d'activation.

Effectuez l'une des opérations suivantes :

- Redémarrez le système puis reconnectez-vous avec un suffixe UPN, par exemple, nom_utilisateur@domaine.com.
- Demandez à votre administrateur de vous confirmer si vous devez cocher la case **Activer la vérification de confiance SSL** lorsque vous installez Data Guardian.
- Contactez votre administrateur système à propos de la configuration de votre ordinateur en vue d'une activation manuelle. Voir Activer Data Guardian.

Activer Data Guardian

En général, Data Guardian s'active automatiquement après l'installation et le redémarrage. Si votre administrateur vous propose une activation manuelle, procédez comme suit :

1 Connectez-vous à Windows.

Dans la barre d'état système, une icône en forme de bouclier assortie d'un point d'exclamation orange s'affiche.

2 Cliquez sur l'icône **Data Guardian** dans la barre d'état système et sélectionnez **Activation par l'utilisateur**.

3 Saisissez l'adresse e-mail de votre domaine et le mot de passe du domaine, puis cliquez sur **Activer**.

Si vous êtes un utilisateur interne (possédant une adresse e-mail dans le domaine), ignorez le bouton S'inscrire. Seuls les utilisateurs externes doivent s'inscrire.

Une fois l'activation terminée, une coche verte s'affiche sur l'icône Data Guardian dans la barre d'état système  .

4 Confirmez l'état de votre mode utilisateur. Cliquez sur l'icône de la barre d'état système et sélectionnez **Détails**.

5 En haut, confirmez le mode utilisateur :

Interne : utilisateur doté d'une adresse e-mail incluse dans le domaine de la société.

Externe : utilisateur doté d'une adresse e-mail extérieure au domaine. Pour plus d'informations, voir Utiliser Data Guardian en tant qu'utilisateur externe.

Utiliser Data Guardian Mobile sous iOS ou Android

Cette section décrit les informations de base sur l'utilisation de Data Guardian Mobile sur les appareils Android ou iOS. Si votre administrateur définit une règle permettant d'activer Data Guardian, les fichiers sont cryptés et sécurisés dans le cloud. Cependant, vous pouvez utiliser l'application mobile Data Guardian pour les afficher sur votre appareil mobile.

Condition préalable

Avant d'utiliser l'application Data Guardian, vous devez disposer du nom du serveur Dell Data Protection de votre entreprise, par exemple serveur.domaine.com. Cette information est fournie par votre administrateur.

Mise en route de Data Guardian Mobile

Suivez la procédure suivante si vous utilisez Data Guardian Mobile.

Tâche	Description	Voir cette section
Installez Data Guardian	Déterminez les éléments suivants : L'administrateur est déjà installé L'utilisateur doit installer	Installé par l'administrateur : appuyez sur l'application Data Guardian et connectez-vous. Installé par l'utilisateur : voir l'une de ces sections : Installer sur un appareil iOS Installer sur un appareil Android
Accéder au compte fournisseur de votre stockage Cloud	Sur l'appareil, naviguez jusqu'à la page d'accueil de l'application Data Guardian puis appuyez sur votre fournisseur de stockage cloud.	Voir l'une des sections suivantes : Accéder à votre compte de stockage cloud pour iOS Accéder à votre compte de stockage cloud pour Android

L'application Data Guardian Mobile répertorie le client de synchronisation cloud utilisé par votre société et vous permet de le télécharger.

REMARQUE :
Si vous téléchargez l'application client de synchronisation cloud sur votre appareil, Data Guardian ne cryptera aucun dossier ou fichier que vous chargez directement depuis cette application. Pour crypter et protéger des fichiers, vous devez utiliser l'application Data Guardian pour les charger.

Pour protéger vos données dans le cloud, Data Guardian les crypte. Par conséquent, vous devez installer l'application Data Guardian sur votre appareil mobile pour afficher fichiers cryptés.

- Les fichiers Office protégés (.docx, .pptx, .xlsx) conservent leur extension de fichier.
- Les fichiers non Office du cloud portent une extension .xen.

Si une personne non autorisée accède à votre compte de stockage cloud et télécharge un fichier sur un appareil mobile qui ne dispose **pas** de Data Guardian, cette personne ne peut pas ouvrir ou afficher vos fichiers. Si elle ouvre un fichier Office protégé, seule une page de garde s'affiche indiquant que la personne ne peut pas afficher le document sans Data Guardian. Ceci sécurise davantage vos données.

Sur les appareils mobiles, vous pouvez :

- Créer des dossiers
- Charger et télécharger des fichiers

  REMARQUE :
  Avec Data Guardian, vous devez lancer les chargements et téléchargements sur le périphérique. Pour que les fichiers soient cryptés lors de leur téléchargement sur le cloud, vous devez les charger depuis la page d'accueil de Data Guardian et non depuis une application de client de synchronisation cloud. Lorsque vous appuyez sur un fichier, Data Guardian le décrypte automatiquement et l'affiche en texte clair au dans l'application. Cependant, dans le Cloud, le fichier reste sécurisé sous format de fichier .xen.

- Ajouter un fichier aux favoris
  - Pour iOS, voir le menu-tiroir de navigation. Pour Android, appuyez longuement sur le nom du fichier.
- Supprimer des dossiers et des fichiers
- Accepter un fichier partagé par un utilisateur interne

  REMARQUE :
  Si un utilisateur interne partage un dossier avec vous via Data Guardian, vous devez accéder au site Web de stockage cloud et le déplacer vers le dossier racine ou télécharger le dossier partagé afin de l'afficher sur le périphérique.

- Partager un document avec un utilisateur externe (si la règle est activée pour des utilisateurs externes) : pour iOS, voir Afficher les règles de stockage cloud Data Guardian pour votre appareil iOS.
- Modifiez des fichiers Office .docx et .ppt.

  REMARQUE :
  Actuellement, vous ne pouvez pas modifier les fichiers.csv et .csv.xen sur des appareils mobiles.

Documents Office protégés hors ligne

Lorsque vous créez un document Office protégé ou prenant en charge les macros protégé alors que vous êtes hors ligne, ce document se voit attribuer une clé. Lorsque l'appareil se connecte, les clés sont chargées vers le serveur Dell. Si un appareil reste hors ligne pendant trois jours, une notification indique que Data Guardian n'a pas pu contacter le serveur Dell. La notification s'affiche chaque jour jusqu'à ce que vous vous connectiez au réseau. Pour afficher les fichiers cryptés, vous devez connecter l'appareil mobile.

Protection supplémentaire grâce aux limitations géographiques

En fonction des règles définies par votre administrateur, les appareils mobiles peuvent bénéficier d'une protection supplémentaire selon laquelle l'ouverture des documents Office protégés et des fichiers .xen est impossible en dehors d'une région spécifique. Vous devez vous trouver dans une région approuvée pour ouvrir les fichiers protégés. Actuellement, ces régions sont les États-Unis et le Canada. Vous devez activer les services de localisation sur l'appareil pour que ces limitations géographiques fonctionnent. Si la fonction de limitations géographiques est activée par votre administrateur et que les services de localisation sont désactivés, l'accès aux fichiers est refusé.

Utiliser un code PIN

Votre administrateur peut définir une règle exigeant un code PIN.

Data Guardian sur un appareil iOS

Installer sur un appareil iOS

1 Sur votre appareil, appuyez sur **App Store** et recherchez **Data Guardian Mobile**.

2 Sélectionnez et installez l'application **Data Guardian**.

3 Pour le champ Serveur de l'écran de connexion, saisissez le nom d'hôte du serveur Dell Data Protection de votre entreprise ; par ex. : serveur.domaine.com.

4 Entrez votre nom d'utilisateur et votre mot de passe.

5 Appuyez sur **Connexion**.

Accéder à votre compte de stockage cloud pour iOS

Après vous être connecté(e) à Data Guardian, une règle Data Guardian détermine quels fournisseurs de stockage cloud s'affichent sur l'écran d'accueil. Votre administrateur peut désigner un fournisseur de stockage cloud spécifique à utiliser au sein de l'entreprise.

Le menu-tiroir de navigation comporte des options supplémentaires.

Pour accéder au compte :

1 Sur la page d'accueil de Data Guardian, appuyez sur le fournisseur de stockage cloud.

2 Effectuez l'une des actions suivantes en suivant les instructions en ligne :

- Créez un compte auprès du fournisseur de stockage.
- Connectez-vous à un compte fournisseur de stockage Cloud existant.

> **REMARQUE :**
> Pour plus d'informations, voir l'aide relative au fournisseur de stockage Cloud.

Dissocier un fournisseur de stockage Cloud

Si vous détenez plusieurs comptes avec le même fournisseur de stockage, sachez que vous ne pouvez pas vous connecter à plus d'un compte à la fois. Vous devez décocher la case afin de vous dissocier et de vous déconnecter du compte actuel puis vous connecter à l'aide d'autres informations d'identification.

1 Ouvrez le tiroir de navigation de Data Guardian et appuyez sur **Paramètres**.

2 Appuyez sur **Dissocier**.

Afficher les règles de stockage cloud de Data Guardian pour votre appareil iOS

1 Dans le tiroir de navigation de Data Guardian, appuyez sur **Paramètres**.

2 Appuyez sur **Règle**.
Cette liste peut comporter :

- Une révision : nombre de règles ayant été révisées
- Obscurcissement des noms de fichier : la valeur est définie par défaut sur **Non**
- Client de synchronisation cloud : la règle doit être définie sur **Crypter**
- Spectateurs externes : si cette option est définie sur **Oui**, la règle de partage est activée. Lorsque vous ouvrez un document dans l'appli, une option du menu vous permet de partager le fichier.

Désinstallation de l'application Data Guardian

1 Dans le menu-tiroir d'applis iOS, appuyez longuement sur l'icône **Data Guardian**.

2 Appuyez sur **x**.

3 Appuyez sur **Supprimer**.

Dépannage d'iOS et de Data Guardian

Sur un appareil iOS, si vous ouvrez un document Office protégé d'une taille supérieure à 25 Mo et qu'une boîte de dialogue vous avertit d'un niveau de mémoire faible, l'alerte vient de Polaris Office et non de Data Guardian. Si l'appareil dispose de suffisamment de mémoire, fermez le fichier et rouvrez-le.

Avec Dropbox for Business, si vous marquez un fichier comme disponible hors ligne et que renommez ce fichier sur le site Web de Dropbox, le fichier ne s'ouvrira pas sur l'appareil iOS équipé de l'application Data Guardian.

Data Guardian sur un appareil Android

Installer sur un appareil Android

1 Sur votre appareil, accédez à **Google Play** et recherchez **Data Guardian Mobile**.
2 Sélectionnez et installez l'application **Data Guardian**.
3 Pour le champ Serveur de l'écran de connexion, saisissez le nom du serveur Dell Data Protection de votre entreprise, par ex. : serveur.domaine.com.
4 Entrez votre nom d'utilisateur et votre mot de passe.
5 Appuyez sur **Connexion**.

Votre compte est maintenant activé.

Accéder à votre compte de stockage cloud pour Android

Une fois connecté à Data Guardian, une règle Data Guardian détermine quels fournisseurs de stockage cloud s'affichent. Votre administrateur peut désigner un fournisseur de stockage cloud spécifique à utiliser au sein de l'entreprise et bloquer les autres.

Pour accéder au compte :

1 Sur la page d'accueil de Data Guardian, appuyez sur le fournisseur de stockage cloud.
2 Effectuez l'une des actions suivantes en suivant les instructions en ligne :
   - Créez un compte auprès du fournisseur de stockage.
   - Connectez-vous à un compte fournisseur de stockage Cloud existant.

   REMARQUE :
   Pour plus d'informations, voir l'aide relative au fournisseur de stockage Cloud.
3 Après avoir accédé à votre compte, ouvrez le menu-tiroir de navigation et appuyez sur **Paramètres**. Lorsque vous donnez accès à un fournisseur de stockage Cloud, une coche s'affiche dans la case à cocher.

REMARQUE :
Si vous détenez plusieurs comptes avec le même fournisseur de stockage, sachez que vous ne pouvez pas vous connecter à plus d'un compte à la fois. Vous devez décocher la case afin de vous dissocier et de vous déconnecter du compte actuel puis vous connecter à l'aide d'autres informations d'identification.

REMARQUE :
Pour OneDrive et Dropbox, si vous ne parvenez pas à partager un fichier à partir des Applications et si le fichier partage un lien avec l'application Data Guardian, partagez le fichier à partir de l'application d'explorations de fichiers sur l'appareil.

Désinstallation de l'application Data Guardian

1 Dans le menu-tiroir des applications Android, appuyez sur **Paramètres**.
2 Dans **Paramètres**, appuyez sur **Applications**.
3 Appuyez sur l'icône **Data Guardian**.
4 Faites glisser l'icône vers l'option Désinstaller.
5 Cliquez sur **OK**.

Considérations en matière de sécurité relatives à Data Guardian et aux clients de synchronisation

Data Guardian crypte les dossiers et fichiers pour sécuriser les données. Étant donné que Data Guardian fonctionne en relation avec les clients de synchronisation, tenez compte des éléments suivants.

Google Drive

Google Drive contient une appli Google Docs qui permet aux utilisateurs de collaborer sur des documents en temps réel. Cependant, la collaboration se produit sur un serveur Google et non sur un serveur Dell Data Protection EE/VE. De ce fait, les fichiers ne sont pas cryptés. Pour les appareils Android et iOS avec Data Guardian, l'accès à ces Google Docs est bloqué. Il diffère légèrement selon la plateforme :

- Android
- iOS : un message s'affiche.

OneDrive et OneDrive for Business

Avec OneDrive for Business, si vous téléchargez plusieurs fichiers et annulez le téléchargement, OneDrive for Business annulera le téléchargement de ceux qui n'ont pas encore été téléchargés mais poursuivra celui de ceux dont le téléchargement est en cours. Il s'agit d'un problème de Microsoft. De ce fait, laissez le téléchargement des fichiers se terminer avant de procéder à l'annulation.

Journaux

Pour des raisons de sécurité, aucun fichier journal ne sera disponible sur les appareils mobiles.

Envoyer des commentaires à Dell

Si votre administrateur a activé une règle de commentaires, vous pouvez envoyer un commentaire à Dell concernant ce produit. Si cette fonctionnalité n'est pas activée par une règle, l'option ne s'affiche pas.

Pour envoyer un commentaire :

1 Dans le tiroir de navigation Data Guardian, appuyez sur **Commentaires**.
2 De courtes questions vous permettront d'évaluer votre niveau de satisfaction (10 indiquant le niveau de satisfaction le plus haut) et d'apporter un commentaire.

Utiliser Data Guardian en tant qu'utilisateur externe

Un utilisateur externe qui possède une adresse e-mail hors domaine peut aussi utiliser Data Guardian. Voici quelques exemples :

- Vous avez installé et activé Data Guardian en tant que membre de votre entreprise, mais vous devez partager des fichiers protégés ou travailler sur des fichiers protégés avec un utilisateur en dehors de votre entreprise.
- Votre adresse e-mail fait partie du domaine de l'entreprise, mais vous souhaitez aussi installer et activer Data Guardian sur un ordinateur ou un périphérique mobile avec votre adresse personnelle, hors domaine. Ceci vous permet d'interagir avec vos fichiers protégés depuis une adresse e-mail hors du domaine de l'entreprise.

Pour les utilisateurs externes, voir Configuration requise pour le serveur. En outre, le domaine ou l'utilisateur ne doivent pas être sur la liste noire de l'entreprise.

REMARQUE :
Une mise à niveau par l'entreprise entraînera la migration des utilisateurs externes enregistrés auprès de Secure Lifecycle 1.0 ou version ultérieure.

Tâches de l'utilisateur interne

Pour partager des fichiers sécurisés avec un utilisateur externe, vous pouvez envoyer un document Office protégé ou un fichier .xen dans un e-mail Outlook. Une invite de confirmation vous rappelle que vous vous apprêtez à partager la clé attribuée au fichier protégé.

REMARQUE :
Si un utilisateur externe envoie un fichier protégé par e-mail, les clés ne sont pas partagées.

Vous pouvez également utiliser l'option Accorder l'accès pour partager des fichiers sécurisés avec un utilisateur externe. Vous devez alors effectuer les opérations suivantes :

- Rendre un ou plusieurs fichiers sécurisés disponibles pour l'utilisateur externe.
  - Documents Office protégés : accordez l'accès à un ou plusieurs fichiers sécurisés à l'aide d'un des moyens suivants :
    - Dossier local ou lecteur réseau
    - E-mail
    - Média amovible
    - Partage réseau
  - Fichiers .xen non Office : créez un dossier à partager sur le client de synchronisation et ajoutez les fichiers.
- Accordez à l'utilisateur externe l'accès à un ou plusieurs fichiers.

Si vous envisagez de partager des fichiers .xen non Office, vous devez les ajouter à un dossier du client de synchronisation, puis accorder l'accès. Pour les fichiers Office protégés, vous devez accorder l'accès. Les étapes peuvent varier en fonction de la méthode que vous employez ou du client de synchronisation utilisé.

Partager un dossier sur le client de synchronisation pour partager des fichiers .xen

1 Dans Windows l'Explorateur Windows, accédez à votre client de synchronisation, créez un dossier, puis chargez un fichier à partager avec un utilisateur externe. Voir Afficher les dossiers et les fichiers sur l'ordinateur local et dans le cloud.

Les documents Office protégés peuvent se situer sur le Lecteur virtuel DDG vDisk, dans le dossier Data Guardian ou sur le bureau.

> **REMARQUE :**
> Avec les fichiers Office protégés, vous ne pouvez pas sélectionner de dossier.

Une page *Accès partagé à un document protégé* s'ouvre avec une colonne contenant la liste des fichiers sélectionnés.

2 Dans le site Web du client de synchronisation, confirmez que le dossier et le fichier ont été créés et cryptés.

Lorsque vous ajoutez un fichier .xen à un nouveau dossier sur le Lecteur virtuel DDG vDisk, Data Guardian ajoute un document intitulé *Comment accéder aux fichiers sécurisés.html* au dossier du site Web. Ce fichier est utilisé uniquement lors du partage d'un dossier avec un utilisateur externe.

3 Sur le site Web du client de synchronisation, cliquez avec le bouton droit sur le dossier que vous avez créé, puis cliquez sur **Partager**.

Une fenêtre s'ouvre, vous permettant de saisir le compte e-mail d'un utilisateur externe. Les étapes varient en fonction du client de synchronisation utilisé. Pour obtenir des liens vers des informations relatives à votre client de synchronisation, voir Travailler avec le client de synchronisation cloud sur le lecteur virtuel DDG vDisk.

4 Accordez l'accès à des fichiers individuels de ce dossier que vous souhaitez partager.

Accorder l'accès à un ou plusieurs fichiers Office protégés

Vous devez accorder l'accès à chaque fichier que vous partagez avec des utilisateurs externes.

1 Cliquez avec le bouton droit sur un fichier sécurisé et sélectionnez **Accorder l'accès aux fichiers protégés**. Vous pouvez sélectionner jusqu'à 50 fichiers maximum.
2 Dans le champ *E-mail à partager*, saisissez l'adresse e-mail de l'utilisateur hors domaine et cliquez sur **Ajouter**.
3 Répétez cette étape pour ajouter jusqu'à dix adresses e-mail.
4 Cliquez sur **OK**.

Une boîte de dialogue vous informe que le partage a réussi ou que l'adresse e-mail n'est pas autorisée à recevoir des fichiers protégés.

5 Nous vous conseillons d'informer l'utilisateur externe de sa réception d'un e-mail de votre part contenant des instructions d'enregistrement auprès d'un serveur Dell, de téléchargement et d'activation de Dell Data Protection | Data Guardian ainsi que d'affichage des fichiers protégés partagés.

Approuver ou refuser la demande d'accès d'un utilisateur externe

Un utilisateur externe équipé de Data Guardian peut demander l'accès à un document protégé s'il ne dispose pas d'une clé pour ce document.

1 Si vous recevez un e-mail contenant une demande d'accès à un document protégé de la part d'un utilisateur externe, vous pouvez afficher le nom de l'utilisateur externe et du fichier demandé.
2 Sélectionnez **Approuver** ou **Refuser**.

Un e-mail est envoyé à l'utilisateur externe. Si vous approuvez l'accès, vous autorisez le partage de la clé du document protégé.

Si vous n'êtes pas disponible, votre administrateur est également en mesure d'approuver ou de refuser l'accès.

Tâches de l'utilisateur externe

Pour ouvrir et visualiser un document Data Guardian, l'utilisateur externe doit effectuer les actions suivantes :

- S'enregistrer dans Data Guardian
- Installer Data Guardian : l'utilisateur externe doit disposer des droits d'administrateur sur son ordinateur
- Si l'utilisateur interne partage un dossier via un client de synchronisation, l'utilisateur externe doit disposer d'un compte du client de synchronisation. Voir Installer un client de synchronisation cloud , puis Travailler avec le client de synchronisation cloud sur le lecteur virtuel DDG vDisk.

Enregistrer Data Guardian

La première fois qu'un utilisateur interne partage un fichier, l'utilisateur externe doit s'enregistrer.

Pour enregistrer Data Guardian :

1 Dans l'e-mail de vérification de compte du serveur d'entreprise Dell, cliquez sur le lien hypertexte.
2 Continuez vers la page Web.
3 Sur la page Confirmation, cliquez sur **Poursuivre la connexion**.
4 Sur la page Connexion, cliquez sur **Mot de passe oublié**.

> **REMARQUE :**
> Le serveur Dell vous a attribué un mot de passe aléatoire que vous devez réinitialiser.

5 Sur la page Réinitialisation du mot de passe, saisissez et confirmez votre mot de passe, puis cliquez sur **Enregistrer**.
Une boîte de dialogue Confirmation de l'enregistrement s'affiche et un e-mail est envoyé à l'adresse e-mail saisie par l'utilisateur interne.
6 Ouvrez l'e-mail d'activation de compte et cliquez sur le lien.
L'e-mail comporte aussi le nom du serveur à utiliser lors de l'installation de Data Guardian.
7 Sur la page Se connecter, saisissez l'adresse e-mail et le mot de passe utilisés pour vous enregistrer.
8 Cliquez sur **Connexion**.
Une page de téléchargement Data Guardian s'ouvre.
9 Téléchargez et installez Data Guardian.
Une page de téléchargement s'ouvre avec des options pour Windows, iOS, Android et Mac OS X. Dans le cas d'un serveur d'entreprise, la page Téléchargement s'ouvre. Dans le cas d'un serveur Dell Enterprise Server - VE, le fait de cliquer sur Windows vous redirige vers le site dell.com/support.

Les étapes suivantes décrivent l'installation de Data Guardian sous Windows. Voir aussi Tâches utilisateur : Office protégé sans cryptage cloud.

> **REMARQUE :**
> La page de téléchargement comporte aussi le nom du serveur dont vous aurez besoin pour ces étapes.

10 Sous Windows, cliquez sur **Télécharger (32 bits)** ou **Télécharger (64 bits)** selon le système d'exploitation de votre ordinateur.
11 Téléchargez le fichier d'installation sur un répertoire de votre ordinateur.
12 Double-cliquez sur le fichier d'installation pour lancer le programme d'installation.
13 Sélectionnez une langue, puis cliquez sur **OK**.
14 Si vous êtes invité(e) à installer Microsoft Visual C++ 2010 Redistributable Package, cliquez sur **OK**.
15 Dans la page d'accueil, cliquez sur **Suivant**.
16 Lisez le contrat de licence, acceptez les conditions, puis cliquez sur **Suivant**.
17 À l'écran Dossier de destination, cliquez sur **Suivant** pour installer à l'emplacement par défaut suivant **C:\Program Files\Dell\Dell Data Protection\Dell Data Guardian\.**
18 Dans le champ *Nom du serveur :*, saisissez le nom du serveur avec lequel cet ordinateur communiquera. Vous trouverez ce nom dans l'e-mail d'activation que vous avez reçu ou en haut de la page de téléchargement.
19 Cliquez sur **Suivant**.
20 Sur l'écran Confirmer le serveur d'activation, confirmez que l'adresse URL du serveur est correcte. Le programme d'installation ajoute www ou http(s) et le port. Cliquez sur **Suivant**.
21 Dans la fenêtre Type de gestion, sélectionnez cette option :

- Utilisation externe : un utilisateur doté d'une adresse e-mail extérieure au domaine de l'entreprise.

22 Cliquez sur **Installer** pour démarrer l'installation.
Une fenêtre affichant l'avancée de l'installation apparaît.

23 Lorsque l'écran Installation terminée s'affiche, cliquez sur **Terminer**.

24 Cliquez sur **Oui** pour redémarrer.
L'installation de Data Guardian est maintenant terminée.

25 Voir Activer Data Guardian.

Activer Data Guardian

Une fois que Data Guardian est installé et que l'ordinateur redémarre, procédez comme suit pour l'activation :

1 Connectez-vous à Windows.
Dans la barre d'état système, une icône cloud assortie d'un point d'exclamation orange s'affiche.

2 Lorsqu'une boîte de dialogue s'affiche dans la barre d'état système, cliquez sur **Cliquez ici pour activer**.
Si cette boîte de dialogue ne s'affiche pas, cliquez sur l'icône **Data Guardian** dans la barre d'état système et sélectionnez **Activation utilisateur**.

3 Saisissez l'adresse e-mail et le mot de passe utilisés pour vous enregistrer, puis cliquez sur **Activer**.
Une fois l'activation terminée, une coche verte s'affiche sur l'icône Data Guardian dans la barre d'état système  .

4 Confirmez l'état de votre mode utilisateur. Cliquez sur l'icône de la barre d'état système et sélectionnez **Détails**.
En haut, le mode Utilisateur est :

Externe : utilisateur doté d'une adresse e-mail extérieure au domaine.

Si vous déjà installé un client de synchronisation et que vous y êtes connecté(e), le Lecteur virtuel DDG vDisk s'affiche dans l'Explorateur Windows.

Demande d'accès d'un utilisateur interne

Sous Windows et sur mobile, si un utilisateur externe a installé et activé Data Guardian, celui-ci peut demander l'accès d'un fichier à partir d'un utilisateur interne. L'utilisateur externe doit faire une demande séparée pour chaque fichier.

1 Si vous ouvrez un fichier Office protégé et qu'il indique que vous devez faire une demande d'accès, cliquez sur **Oui** ou **Non**.
Une boîte de dialogue confirme l'envoi de la demande. L'utilisateur interne peut approuver ou refuser l'accès. L'utilisateur externe reçoit un e-mail en conséquence. Si l'utilisateur externe ouvre le fichier protégé avant que l'utilisateur interne n'approuve l'accès, un message s'affiche indiquant que la demande est en attente.

2 Après 48 heures, l'utilisateur externe peut à nouveau demander l'accès.
Dans la barre d'état système, l'utilisateur externe peut cliquer avec le bouton droit sur l'icône Data Guardian et sélectionner la page **Détails**. Cliquez sur l'onglet **Sécurité**. Lorsque le délai d'une demande revient à *Aucun*, l'utilisateur externe peut à nouveau demander l'accès.

Afficher un document Office protégé

Si une entreprise active une règle pour protéger ses documents Office et qu'un utilisateur interne envoie un fichier protégé à un utilisateur externe, l'utilisateur externe doit être connecté au serveur Dell lors de la première ouverture du document. Ensuite, cet utilisateur peut ouvrir et afficher le document hors ligne pendant une période donnée, par exemple, une semaine. L'utilisateur externe doit alors se connecter au serveur et rouvrir le document protégé.

Pour des raisons de sécurité, un utilisateur externe ne peut pas effectuer les opérations suivantes avec un document Office protégé.

- Impression

- Exporter
- Enregistrer sous
- Partager

Désinstaller le client de synchronisation ou Data Guardian

Si votre administrateur a installé Data Guardian, lui seul peut le désinstaller. Un utilisateur externe invité à partager un dossier et qui possède des droits d'administrateur sur un ordinateur externe peut également désinstaller Data Guardian de cet ordinateur externe.

Désinstaller un client de synchronisation cloud

Si vous désinstallez votre client de synchronisation cloud mais que vous conservez Data Guardian sur votre ordinateur, vous pouvez toujours afficher vos fichiers en texte clair sur le Lecteur virtuel DDG vDisk.

Toutefois, si vous réinstallez le même client de synchronisation cloud, vous aurez besoin d'une nouvelle clé pour les ouvrir sur le Lecteur virtuel DDG vDisk. Vous devrez également télécharger vos fichiers depuis le site Web du client de synchronisation.

Désinstaller Data Guardian

Vous devez disposer des droits d'administrateur sur l'ordinateur local pour désinstaller Data Guardian.

Copier les fichiers sur votre disque local

Si vous désinstallez Data Guardian de votre ordinateur ou appareil, vous devez tout de même sécuriser les fichiers du site Web du client de synchronisation afin qu'ils restent crypté.

1 Avant la désinstallation, déterminez si vous devez accéder à n'importe lequel des fichiers.
2 Copiez-les à partir du Lecteur virtuel DDG vDisk vers votre disque local.

Ces fichiers, copiés depuis le Lecteur virtuel DDG vDisk, s'affichent en texte clair. Les dossiers et les fichiers présents sur le site Web du client de synchronisation seront cryptés même si vous les téléchargez. Pour les afficher, vous devez réinstaller Data Guardian.

Désinstaller Data Guardian

1 Désinstallez le programme dans le Panneau de configuration Windows.
2 Sélectionnez Dell Data Protection | Data Guardian et cliquez sur **Modifier** dans le menu supérieur.
3 Cliquez sur **Suivant** lorsque l'écran de Bienvenue s'affiche.
4 Sélectionnez **Supprimer** et cliquez sur **Suivant**.
5 Un avertissement s'affiche pour vous demander de confirmer la désinstallation de Dell Data Protection | Data Guardian. Si c'est le cas, cliquez sur **Suivant**.
6 Sur l'écran Supprimer le programme, cliquez sur **Supprimer**.
Une fenêtre d'état affiche la progression.
7 Si vous recevez un message d'erreur du client de synchronisation, cliquez sur **Continuer**.
8 Cliquez sur **Terminer** lorsque l'écran Terminé s'affiche.
9 Cliquez sur **Oui** pour redémarrer.

La désinstallation de Dell Data Protection | Data Guardian est alors terminée.

8

Questions fréquemment posées

FAQ - Général

Question

J'ai déplacé le dossier de synchronisation du fournisseur cloud dans le répertoire Program Files. Depuis, je ne peux plus décrypter les fichiers qui sont téléchargés sur mon dossier de synchronisation à partir du cloud.

Réponse

Le dossier Program Files ou les autres dossiers exclus sont à dessein non protégés, selon la règle établie. Data Guardian ne décrypte aucun fichier téléchargé dans ce dossier ou ses sous-dossiers.

Solution

Dissociez ou désinstallez le client de synchronisation, puis remettez le dossier de synchronisation à son emplacement par défaut ou à un autre emplacement géré.

REMARQUE :
Pour obtenir une liste des emplacements gérés et non gérés, contactez votre administrateur.

Question

J'ai archivé plusieurs fichiers .xen et les ai copiés sur mon bureau. Certains ont été décryptés, mais pas tous.

Réponse

Au cours d'une synchronisation, Data Guardian est conçu pour décrypter directement les fichiers vers l'unité virtuelle ou décrypter lors du téléchargement via un navigateur web. Pour les fichiers qui ont été copiés depuis un autre emplacement, utilisez l'Explorateur Windows et déplacez le fichier .xen dans l'unité virtuelle pour le décrypter.

Solution

Déplacez les fichiers .xen dans le dossier de l'unité virtuelle pour les charger dans le cloud. Ils pourront ainsi être décryptés localement.

Question

J'ai renommé mon ordinateur. Depuis, je ne reçois plus de mises à jour de règles et le cryptage ne s'effectue plus dans le Cloud.

Réponse

Actuellement, le serveur reconnaît uniquement le point final sur lequel vous avez effectué l'activation initiale. Si vous modifiez le nom du point de terminaison, le serveur ne reconnaît plus l'emplacement où il doit envoyer la règle et Data Guardian ne fonctionne pas comme prévu.

Solution

1 Arrêtez la synchronisation des fichiers sur l'ordinateur local.

REMARQUE :
Si vous n'arrêtez pas la synchronisation avant de procéder à la désinstallation, d'importantes données pourront ne plus être protégées dans le Cloud ou même être supprimées.

2 Désinstaller et réinstaller Data Guardian. Vous devez disposer des droits d'administrateur pour désinstaller.

Question

Rien ne se produit lorsque j'essaie de charger des fichiers dans le Cloud à partir d'appareils Windows interrompus. Lorsque je ferme les fenêtres déjà ouvertes, le message d'erreur « Accès refusé » s'affiche.

Réponse

Le message d'erreur ne provient pas de Data Guardian. Vous pouvez accéder aux fichiers localement, mais ne recevrez pas les mises à jour futures des fichiers.

FAQ sur les documents Office et le mode protégé

Question

J'ai essayé d'ouvrir un document Office (.docx, .pptx, .xlsx, .docm, .pptm, .xlsm) lorsqu'une page de garde s'est affichée.

Réponse

Si votre administrateur a défini une règle pour protéger les documents Office, vous ou votre administrateur devez installer Data Guardian. Vérifiez que l'icône Data Guardian de la barre d'état système est dotée d'une coche verte, elle indique que l'application est activée.

Solution

Déterminez si vous avez besoin d'installer ou d'activer Data Guardian. Voir Installer Data Guardian ou Problèmes possibles à l'activation.

Question

Je ne parviens pas à ouvrir un document Office protégé (Word, PowerPoint ou Excel).

Réponse

Vérifiez les éléments suivants :

- Paramètres de blocage de fichiers : si votre administrateur a défini des règles pour protéger les documents Office, n'utilisez pas ce paramètre dans **Fichier > Options**.

Solution

Pour vérifier les paramètres de blocage de fichiers :

1 Dans un document Office, sélectionnez **Fichier > Options**.
2 Dans la liste, sélectionnez **Centre de gestion de la confidentialité**.
3 Sur la droite, cliquez sur **Paramètres du centre de gestion de la confidentialité**.
4 Dans la liste, sélectionnez **Paramètres de blocage de fichiers**.
5 Pour *Documents et modèles Word/Excel/PowerPoint 2007 et versions ultérieures*, assurez-vous que la case *Ouvert* est décochée.
6 Cliquez sur **OK**.