Dell Data Protection | Dell Data Guardian pour Mac

Administrator Guide v1.2 (Guide de l'administrateur v1.2)

GUID-5B8DE7B7-879F-45A4-88E0-732155904029

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.

GUID-559E7DE2-5F31-4AF0-8A01-987470FAB58C

Dell Data Guardian for Mac Administrator Guide (Guide l'administrateur de Dell Data Guardian pour Mac)

2017 - 04

Rév. A01

Table des matières

Introduction à Dell Data Guardian pour Mac

Ce guide fournit les informations nécessaires pour gérer le logiciel client Cloud pour Mac.

GUID-DC905DCF-89A3-4894-B120-B1ED63272AA5

Présentation

Dell Data Guardian pour Mac protège les données dans les systèmes de partage de fichiers basés sur Internet. Les ordinateurs Mac OS X utilisant Data Guardian peuvent afficher, modifier et chiffrer des fichiers sur des systèmes de partage de fichiers basés sur Internet pour un stockage sécurisé.

Data Guardian pour Mac peut ouvrir les fichiers chiffrés pour Windows, et inversement.

Data Guardian pour Mac comprend les éléments suivants :

- Data Guardian :
  - **Chiffrement Cloud** : protège les données dans les systèmes de partage de fichiers basés sur le Cloud, tels que les fichiers .xen.
  - **Documents Office protégés** : protège les documents Office (.docx, .pptx, .xlsx, .docm, .pptm, .xlsm) sur le Cloud et affiche le nom du fichier et son extension d'origine. Les fichiers protégés peuvent uniquement être ouverts à l'aide d'un client Data Guardian. Si ce fichier est ouvert depuis un autre environnement, une page de garde s'affiche pour signaler que le document est protégé et expliquer comment un utilisateur autorisé peut déposer une demande d'accès au fichier crypté.

    Vous pouvez définir des règles pour le chiffrement Cloud uniquement ou pour les groupes de stratégies. Pour plus d'informations, voir l'*Aide de l'administrateur*.

    Data Guardian pour Mac est conçu pour partager des fichiers entre les fournisseurs de chiffrement Cloud. Toutefois, si les règles « Documents Office protégés » sont activées pour les Mac, tous les audits de fichiers et la traçabilité sont perdus si le fichier est enregistré par l'utilisateur final sur le Mac local. Si une traçabilité et un audit de fichiers très stricts sont requis par votre entreprise, définissez la règle d'activation *Autoriser Mac* de *Data Guardian* sur « Non sélectionné » afin d'éviter que Data Guardian ne s'active sur des Mac.
- Serveur d'administration de la sécurité : composant du serveur Dell gérant Data Guardian pour Mac. Le serveur d'administration de la sécurité assure la sécurité des données dans le Cloud, peu importe avec qui elles sont partagées. Le serveur d'administration de la sécurité protège également les périphériques internes de la transmission de données sensibles.
- Console de gestion à distance : fournit une administration centralisée des stratégies de sécurité, s'intègre avec les répertoires d'entreprise existants et crée des rapports.

  Ces composants Dell fonctionnent entre eux de façon transparente pour fournir un environnement sécurisé sans dégrader l'expérience utilisateur.

GUID-B47CD81A-486F-43A5-916B-86A247C276EA

Contacter Dell ProSupport

Appelez le 877-459-7304, poste 4310039, afin de recevoir 24h/24, 7j/7 une assistance téléphonique concernant votre produit Dell Data Protection.

Un support en ligne pour les produits Dell Data Protection est en outre disponible à l'adresse dell.com/support. Le support en ligne englobe les pilotes, les manuels, des conseils techniques et des réponses aux questions fréquentes et émergentes.

Pour les numéros de téléphone en dehors des États-Unis, consultez Numéros de téléphone internationaux Dell ProSupport .

Configuration minimale requise pour Dell Data Guardian pour Mac

Ce chapitre présente la configuration matérielle et logicielle requise pour le client. Avant d'effectuer toute opération de déploiement, assurez-vous que les environnements de déploiement respectent les exigences suivantes.

REMARQUE :
IPv6 n'est pas pris en charge.

GUID-213663B0-B65F-4945-B2F1-5BEF78085BDF

Serveur

Data Guardian pour Mac nécessite que le client soit connecté à Dell Enterprise Server ou Dell Enterprise Server - VE, v9.6 ou version supérieure.

GUID-371FFDE5-7A34-4288-AA88-617E73C0F9A4

Matériel du client Mac

Le tableau suivant répertorie le matériel pris en charge pour le client Mac.

Matériel Mac

- Processeur Intel Core 2 Duo, Core i3, Core i5, Core i7, ou Xeon
- 2 Go de RAM
- 10 Go d'espace disque disponible

GUID-3F5F6005-9FEE-46AE-8400-336215F15DB2

Systèmes d'exploitation

La liste suivante répertorie les systèmes d'exploitation pris en charge.

Systèmes d'exploitation Mac

- Mac OS X Yosemite 10.10.5
- Mac OS X El Capitan 10.11.6

- macOS Sierra 10.12.3 et 10.12.4

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

GUID-C4B253E4F-15E5-42AF-8493-D09F2473A534

Fournisseurs de stockage Cloud

Selon les paramètres de règles, les éléments suivants peuvent s'afficher dans l'interface de Dell Data Guardian. L'utilisateur n'a pas besoin de télécharger ou d'installer le client de synchronisation Cloud.

Fournisseurs de stockage Cloud

- Dropbox
- Box
- Google Drive
- OneDrive
- OneDrive for Business

Tâches d'installation de Data Guardian

GUID-168A1BC7-0DED-43F2-9A99-08FC43099963

Configuration requise

Avant d'effectuer ces tâches, confirmez ce qui suit :

- Installation du serveur Dell et de ses composants. Voir l'une des sections suivantes :
  - *Enterprise Server Installation and Migration Guide (Guide d'installation et de migration d'Enterprise Server)*
  - *Virtual Edition Quick Start Guide and Installation Guide (Guide de démarrage rapide et Guide d'installation de Virtual Edition)*
- Dans la console de gestion à distance, attribuez un Rôle d'administrateur Dell approprié.

GUID-D9C4A912-436F-415D-9499-BAE4F1B53233

Stratégies

Par défaut, Data Guardian chiffre les fichiers des utilisateurs et envoie les événements d'audit à DDP EE Server/VE Server. 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).

Si vous souhaitez que les événements d'audit incluent des données de géolocalisation, vous devez activer le WiFi. Pour plus d'informations sur la géolocalisation et les événements d'audit, voir l'*Aide de l'administrateur*.

Pour modifier le comportement par défaut pour chaque fournisseur de stockage Cloud pris en charge, définissez la règle des *Fournisseurs de protection de stockage Cloud*. Si votre entreprise préfère un fournisseur de stockage Cloud spécifique, configurez cette règle sur **Bloquer** pour les autres fournisseurs. Pour en savoir plus sur les règles, voir l'*Aide de l'administrateur*, disponible à partir de la Console de gestion à distance du serveur Dell.

REMARQUE :
L'option Contournement de cette règle est pour Windows. Si vous sélectionnez Contournement pour Mac, elle affiche Autoriser à l'utilisateur final.

GUID-EE401419-8E85-45A9-9775-2C16EEE3FDB0

Tâches de Dell Enterprise Server

GUID-0E37A5B7-8FF3-4F1E-9A8E-AB49D649C05B

Configurer Security Server pour autoriser les téléchargements du client Cloud

DDP Enterprise Server

1 Sur DDP Enterprise Server, rendez-vous sur <rép. d'install. de Security Server>\webapps\cloudweb\brand\dell\resources\
2 Ouvrez le fichier **messages.properties** dans un éditeur de texte.
3 Vérifiez que les entrées sont conformes aux informations suivantes :
Pour une installation **locale** :

download.deviceWin.mode=local

download.deviceMac.local.filename=Dell-Data-Guardian-0.x.x.xxxx.dmg

Pour une installation **à distance** :

```
download.deviceWin.mode=remote
```

```
download.deviceMac.remote.link=https://[NomMachine:adresseIP]:[port]/yourpath/filename.dmg
```

4 Enregistrez les fichiers, puis fermez-les.
5 Rendez-vous sur <rép. d'install. de Security Server> et créez un nouveau dossier nommé Download (Security Server\Download).
6 Dans le dossier Download (Téléchargement), créez un dossier CloudWeb (Security Server\Download\CloudWeb).
7 Ajoutez les programmes d'installation de Dell Data Guardian dans ce dossier.

Virtual Edition : installez manuellement une version différente du client Cloud

Aucune action n'est nécessaire pour permettre aux utilisateurs de télécharger le dernier programme d'installation de Dell Data Guardian. Le dernier programme d'installation est préinstallé sur VE Security Server.

Pour procéder à l'installation manuelle d'une autre version du programme d'installation de Data Guardian sur VE version du VE Security Server, mettez à jour le fichier message.properties.

1 Rendez-vous sur :
/opt/dell/server/security-server/webapps/root/cloudweb/brand/dell/resources/
2 Ouvrez le fichier **messages.properties** dans un éditeur de texte.
Pour une installation **locale** :

```
download.deviceWin.mode=local
```

```
download.deviceMac.local.filename=Dell-Data-Guardian-0.x.x.xxxx.dmg
```

Pour une installation **à distance** :

download.deviceWin.mode=remote

```
download.deviceMac.remote.link=https://[NomMachine:adresseIP]:[port]/yourpath/filename.dmg
```

3 Enregistrez les fichiers, puis fermez-les.
4 Copiez les fichiers dans /opt/dell/server/security-server/download/cloudweb.
5 Ajoutez les programmes d'installation de Data Guardian à ce dossier.

GUID-40291F18-814A-40EC-9D60-A185154BA6FC

Autoriser/refuser des utilisateurs sur la liste l'accès total/liste noire

Les entrées de la liste d'accès total et la liste noire déterminent les utilisateurs pouvant s'inscrire sur le serveur Dell pour utiliser Data Guardian.

Liste d'accès total

La liste d'accès total permet à des utilisateurs ou groupes d'utilisateurs particuliers de s'inscrire sur le serveur Dell afin d'utiliser Data Guardian.

Les utilisateurs externes doivent être placés sur la liste d'accès total pour pouvoir effectuer un enregistrement. Regardez les exemples suivants pour permettre aux utilisateurs de s'inscrire :

Type d'utilisateur	Entrez
Toutes les adresses e-mail organisation.com	`organization.com`
Un utilisateur spécifique	`jdoe@organization.com`
Tous les utilisateurs Gmail	`gmail.com`

Liste noire

La liste noire empêche des utilisateurs ou groupes d'utilisateurs donnés de s'inscrire auprès du serveur Dell et d'utiliser Data Guardian. Les utilisateurs dont les adresses e-mail sont placées sur la liste noire reçoivent un message indiquant qu'il leur est impossible de s'inscrire auprès de Data Guardian.

REMARQUE :
Si un utilisateur est déjà enregistré, cette liste ne peut **pas** l'empêcher d'utiliser Data Guardian.

Vous pouvez utiliser la liste noire pour exclure des utilisateurs spécifiques appartenant à des groupes approuvés sur la liste d'accès total. En outre, vous pouvez placer l'ensemble d'un domaine sur la liste noire, ce qui empêchera toute personne possédant une adresse e-mail incluse dans ce domaine de s'inscrire. Regardez les exemples suivants pour empêcher un utilisateur ou un groupe de s'inscrire sur le serveur Dell :

Type d'utilisateur	Entrez
Toutes les adresses e-mail organisation.com	`organization.com`
Un utilisateur spécifique et cette adresse e-mail	`jdoe@organization.com`
Tous les utilisateurs Gmail	`gmail.com`

Pour modifier la liste d'accès total ou la liste noire, suivez les instructions ci-dessous :

1 Dans le volet de gauche de la console de gestion à distance, cliquez sur **Gestion > Gestion des utilisateurs externes**.

2 Cliquez sur **Ajouter**.

3 Sélectionnez le type d'accès à l'inscription :

Liste noire : bloque l'inscription d'un utilisateur ou d'un domaine. L'utilisateur ne peut pas ouvrir un document Office protégé ni un fichier .xen.

Liste d'accès total : autorise l'inscription et l'accès aux fichiers d'un utilisateur ou d'un domaine. Si un utilisateur ou un domaine sont également sur la liste noire, aucun accès n'est accordé.

4 Dans le champ Saisir un domaine/e-mail, saisissez le domaine de l'utilisateur pour autoriser l'accès à la totalité du domaine, ou une adresse e-mail pour autoriser l'accès uniquement à cet utilisateur.

5 Cliquez sur **Ajouter**.

Pour plus d'informations sur l'utilisation de la liste d'accès total/liste noire, voir l'*Aide de l'administrateur*, accessible à partir de la console de gestion à distance du serveur Dell.

Un utilisateur externe peut demander l'accès à un utilisateur interne pour obtenir la clé d'un fichier protégé. Si l'utilisateur interne n'est pas disponible, vous pouvez utiliser la console de gestion à distance pour accepter ou refuser l'accès.

1 Sélectionnez **Gestion > Gestion des demandes de clés**.
2 Pour plus d'informations, sélectionnez **?** (Aide).

GUID-038F598E-1FF3-4FC8-A419-2F628C92F934

Effacer à distance le compte d'un membre de l'équipe Dropbox for Business

Si votre entreprise est dotée de Dropbox for Business, vous pouvez supprimer à distance un membre de l'équipe du compte professionnel de l'équipe Dropbox for Business si, par exemple, un utilisateur quitte l'entreprise. Les fichiers et dossiers associés au compte du membre de l'équipe seront supprimés de tous les périphériques utilisés par le compte. Cela révoque l'accès de cet utilisateur à ces fichiers.

Configuration requise

REMARQUE :
Avant d'effectuer cette procédure, vous devez sauvegarder tous les fichiers ou dossiers du compte du membre de l'équipe qui peuvent être utiles pour l'entreprise ou d'autres membres de l'équipe Dropbox for Business.

Seul un administrateur de Dropbox for Business peut effacer à distance un compte Dropbox for Business.

L'utilisateur final doit avoir activé Dell Data Guardian et s'être connecté à Dropbox for Business.

S'inscrire dans la Console de gestion à distance

Un seul administrateur de Dropbox for Business doit s'inscrire.

1 Dans le volet de gauche de la console de gestion à distance, sélectionnez **Gestion** > **Gestion de Dropbox**.
2 Sur la page Dropbox for Business, cliquez sur **S'inscrire**.
Le navigateur s'ouvre sur le site Dropbox for Business.
3 Si vous y êtes invité, connectez-vous à Dropbox avec votre compte d'administrateur de Dropbox for Business.
4 Pour autoriser l'accès à Dell Data Guardian, cliquez sur **Autoriser**.
Une page de confirmation s'affiche pour indiquer que l'autorisation Dropbox est octroyée à DDP Enterprise Server - VE.
5 Dans la console de gestion à distance, revenez à **Gestion** > **Gestion de Dropbox** et cliquez sur **Actualiser**.
Le nom de l'administrateur s'affiche.

REMARQUE :
Généralement, la meilleure pratique consiste à ne pas se désinscrire. Cependant, pour retirer les privilèges de l'administrateur de Dropbox for Business pour supprimer des membres de l'équipe Dropbox for Business, cliquez sur **Désinscrire**.

Effacer à distance le compte d'un membre de l'équipe

REMARQUE :
L'option Effacer à distance est disponible uniquement pour les comptes des membres de l'équipe Dropbox for Business. Si l'option Effacer à distance ne s'affiche pas pour un compte utilisateur, l'utilisateur n'a pas inscrit de compte Dropbox for Business.

1 Dans la Console de gestion à distance, sélectionnez **Populations** > **Utilisateurs** dans le volet gauche.
2 Recherchez l'utilisateur donné.
3 Accédez à la page **Détails de l'utilisateur**.
4 Dans la colonne Commande, cliquez sur **Effacer à distance**.
L'effacement à distance est effectué.

REMARQUE :
Avant de sélectionner Effacer à distance, vous devez sauvegarder tous les fichiers ou dossiers du compte du membre de l'équipe qui peuvent être utiles pour l'entreprise ou d'autres membres de l'équipe Dropbox for Business.

5 Au moment de confirmer l'effacement à distance, cliquez sur **Oui**.
La page Détails de l'utilisateur indique la date à laquelle l'effacement à distance est effectué.

6 Dans votre page Membres de la Console administrateur Dropbox for Business, rafraîchissez la liste des membres de l'équipe.
L'utilisateur est supprimé de la liste. Vous pouvez sélectionner l'onglet **Membres supprimés** pour voir quels utilisateurs ont été supprimés.

GUID-B495F3E1-6516-4DFC-9107-4AA52FE296AB

Tâches client

GUID-88098FA1-F419-45AD-A4BA-F5C30D04DDE3

Configuration requise

- Vérifiez que les périphériques cibles sont connectés à :
  - https://nomdevotresecurityserver.domaine.com:8443/cloudweb/register
  - https://nomdevotresecurityserver.domaine.com:8443/cloudweb
- Veiller à ce que l'utilisateur effectuant l'installation dispose d'un compte d'administrateur local pour l'installation.
- Si l'installation est effectuée à l'aide de la ligne de commande, assurez-vous de disposer du nom de domaine complet de Dell Security Server sur lesquels les utilisateurs vont s'activer.

GUID-5A15F45E-2F97-4EB4-90CD-66CD73275BAB

Meilleures pratiques

Pendant le déploiement, assurez-vous de suivre les meilleures pratiques informatiques. Cela comprend notamment :

- Des environnements de test contrôlés pour effectuer les tests initiaux
- Des déploiements échelonnés pour les utilisateurs

GUID-CF4B88F3-DBAF-4834-B15B-8815EEA72B9D

Installer le client

À ce stade, les utilisateurs qui ont été ajoutés à la liste blanche peuvent s'inscrire sur : https://nomdevotresecurityserver.domaine.com:8443/cloudweb/register.

Après l'inscription, l'utilisateur reçoit un e-mail le dirigeant vers https://nomdevotresecurityserver.domaine.com:8443/cloudweb pour se connecter et télécharger le client approprié.

L'installation du client Mac est facultative pour les administrateurs, car les utilisateurs finaux installent généralement le client Mac eux-mêmes (après l'enregistrement) à partir du site https://yoursecurityservername.domain.com:8443/cloudweb.

Toutefois, vous pouvez installer le client Mac si votre organisation vous oblige à le faire. Installez le client Data Guardian à l'aide de l'interface utilisateur ou de la ligne de commande, par le biais de toute technologie Push disponible dans votre organisation. L'inscription et l'activation par l'utilisateur final restent obligatoires.

Mise à niveau à partir de versions antérieures de Cloud Edition

Si une entreprise dispose d'une version antérieure de Cloud Edition et effectue une mise à niveau de Data Guardian, la précédente version de Cloud Edition est supprimée.

REMARQUE :
Si une entreprise effectue une mise à niveau de Cloud Edition vers Data Guardian, les utilisateurs doivent s'authentifier et lier à nouveau Data Guardian avec leur fournisseur de stockage Cloud. Pour plus d'informations sur l'authentification, voir l'Aide en ligne de Dell Data Guardian.

Options d'installation

Pour installer/mettre à niveau le client, sélectionnez l'une des options suivantes :

- Installation interactive : il s'agit de la méthode la plus simple pour installer Data Guardian pour Mac. Cependant, n'utilisez cette méthode que si vous prévoyez d'installer le client sur un ordinateur à la fois.

  ou

- Installation avec ligne de commande : pour cette méthode d'installation avancée, les administrateurs doivent connaître la syntaxe de la ligne de commande. Cette méthode peut être utilisée pour effectuer une installation à partir d'un script, de fichiers de commandes ou de toute technologie Push disponible dans votre organisation.

Installation interactive

1. Pour le client Data Guardian, localisez le programme d'installation de **Dell-Data-Guardian--0.x.x.xxxx.dmg.**
2. Utilisez le fichier **.pkg** situé dans DDPSL-Explorer-0.x.x.xxxx.dmg pour effectuer une installation ou une mise à niveau. Vous pouvez utiliser une installation à partir d'un script, des fichiers de commandes ou toute technologie Push disponible dans votre organisation.
3. Double-cliquez sur le package **Dell-Data-Guardian-x.x.x**.
4. Cliquez sur **Continuer**.
5. Dans la fenêtre Introduction, cliquez sur **Continuer**.
6. Dans la fenêtre Contrat de licence de logiciel, cliquez sur **Continuer**.
7. Cliquez sur **Accepter** pour continuer.
8. Dans la fenêtre Type d'installation, effectuez l'une des actions suivantes :
   - Cliquez sur **Installer**, puis passez à l'étape 9.
   - Dans la fenêtre Sélection de la destination, choisissez une option ci-dessous, cliquez sur **Continuer l'installation**, puis passez à l'étape 9.
     - Installer pour tous les utilisateurs de cet ordinateur
     - Installez uniquement pour moi
9. Dans la boîte de dialogue, saisissez votre nom et votre mot de passe et cliquez sur **Installer le logiciel**.
10. Dans la page Résumé, cliquez sur **Fermer**.
11. Reportez-vous à Activation de l'utilisateur final.

    REMARQUE :
    Si une entreprise effectue une mise à niveau de Cloud Edition vers Data Guardian, les utilisateurs doivent s'authentifier et lier à nouveau Data Guardian avec leur fournisseur de stockage Cloud. Pour plus d'informations sur l'authentification, voir l'Aide en ligne de Dell Data Guardian.

Installation avec ligne de commande

1. Montez le fichier .dmg.
2. Effectuez une installation du package à partir de la ligne de commande en utilisant la commande installer :
   ```
   sudo installer -pkg/Volumes/Dell\ Data\ Guardian"Dell-Data-Guardian\ 0.x.x.xxxx.pkg" -target /
   ```
3. Demandez aux utilisateurs finaux d'activer Data Guardian. Reportez-vous à Activation de l'utilisateur final.

Activation et expérience utilisateur de Data Guardian

GUID-FCD7AF63-06D4-4D0C-8FA3-369265AB00E2

Activation de l'utilisateur final

Lorsque vous ouvrez Dell Data Guardian sur un Mac pour la première fois, suivez ces étapes :

1 Dans Finder, sélectionnez **Applications** et double-cliquez sur **Dell Data Guardian**.

2 Lorsque la fenêtre du serveur Dell s'affiche, saisissez l'adresse du serveur DDP et cliquez sur **Enregistrer**.

La fenêtre Identifiants s'ouvre.

3 Entrez votre adresse e-mail et mot de passe de domaine.

4 Cliquez sur **Connexion** pour activer Dell Data Guardian.

Une fois l'application Dell Data Guardian ouverte et l'activation réussie, le nom du fournisseur de stockage Cloud est activé dans le volet de gauche.

Si une entreprise souhaite que tous ses utilisateurs collaborent en utilisant le même fournisseur de Cloud, l'administrateur peut définir une règle pour autoriser uniquement ce fournisseur et bloquer l'affichage d'autres fournisseurs.

Si l'activation échoue ou si l'authentification de l'application Dell Data Guardian est révoquée ou expire, le nom du fournisseur de stockage Cloud est grisé.

5 Dans le volet de gauche, sélectionnez le fournisseur de stockage Cloud.

Une fenêtre vous demandant d'entrer vos identifiants s'affiche.

6 Pour plus d'informations sur l'authentification, voir l'Aide en ligne de Dell Data Guardian.

GUID-9917238E-00E5-4F56-909D-C76F09426D53

Interface utilisateur

L'interface de Dell Data Guardian est similaire à l'*affichage en colonnes* du Finder d'OS X. Chaque colonne représente un dossier sur le fournisseur de stockage Cloud sélectionné.

REMARQUE :
la barre de titre peut varier en fonction de votre système d'exploitation.

Pour chiffrer et déchiffrer des fichiers, vous devez utiliser l'interface de Dell Data Guardian et non le site Web du fournisseur de stockage Cloud.

Vous pouvez effectuer les tâches suivantes dans la fenêtre Dell Data Guardian :

- **Fichier** > **Nouveau dossier** : pour créer de nouveaux dossiers.

REMARQUE :
Google Drive et OneDrive ajoutent automatiquement un dossier partagé. Cependant, le partage de données dans OneDrive for Business n'est pas pris en charge.

- Menu contextuel : sélectionnez un ou plusieurs dossiers ou fichiers dans la fenêtre principale. Ensuite, effectuez Ctrl-clic (ou un clic droit) et sélectionnez une option de menu :
  - **Effectuez le téléchargement depuis le site de transfert de fichiers Dell Data Protection (CFT).**
  - **Renommer** : lorsque vous renommez un fichier dans l'interface Dell Data Guardian, Dell Data Guardian synchronise les modifications sur le site Web du fournisseurs de stockage Cloud. Ne pas renommer un fichier .xen sur le site Web du fournisseur de stockage Cloud. Il ne sera pas synchronisé.
  - **Supprimer**

    REMARQUE :
    Google Drive avec Data Guardian n'a pas d'option Remove (Supprimer) (envoie vers la corbeille). Il comprend uniquement l'option Delete (Supprimer), pour des raisons de cohérence avec les autres fonctionnalités de Data Guardian.
- **Dissocier** : pour dissocier Dell Data Guardian d'un fournisseur de stockage Cloud, sélectionnez le fournisseur en question dans le volet de gauche, effectuez Ctrl-Clic (ou cliquez avec le bouton droit), puis sélectionnez Dissocier dans le menu.

Informations supplémentaires sur les fichiers et dossiers :

- Pour ajouter des fichiers et des dossiers aux dossiers s'affichant dans l'interface utilisateur de Dell Data Guardian, faites-les glisser à partir du Finder d'OS X ou d'autres applications prenant en charge la fonction glisser-déposer. Les fichiers seront cryptés en fonction de la règle actuelle.
- Pour déchiffrer et ouvrir des fichiers dans des applications, double-cliquez sur un fichier dans la fenêtre Dell Data Guardian. Si le fichier est modifié dans une application externe, le fichier modifié sera alors crypté et téléchargé en tant que nouvelle révision sur le fournisseur de stockage Cloud.
- Pour créer une copie non chiffrée, faites glisser un fichier ou un dossier de la fenêtre Dell Data Guardian et déposez-le dans le Finder.
- Le *chiffrement Cloud* de 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 l'interface de Dell Data Guardian.
- Les attributs étendus ne sont pas copiés dans le Cloud.

GUID-12885ECF-2D63-4BD1-8719-260F247D161E

Évitez l'option Extraire sur le site Web

Data Guardian ne protège pas et ne chiffre pas les fichiers utilisés avec l'option *Ouvrir et extraire* sur le site Web OneDrive for Business ou n'importe quel site Web de fournisseur de stockage Cloud. Si un fichier est ouvert et extrait, n'utilisez pas la commande Ouvrir de l'interface de Dell Data Guardian car le téléchargement automatique sera bloqué.

Lorsque vous protégez vos fichiers avec Data Guardian, utilisez l'interface de Dell Data Guardian pour travailler sur ces fichiers.

Si vous voulez travailler sur un fichier doté de propriétés spéciales à partir d'un site Web de fournisseur de stockage Cloud :

1 Sur l'interface de Dell Data Guardian, effectuez un Ctrl-clic (ou un clic droit) sur un fichier et sélectionnez **Télécharger**.
2 Sélectionnez et modifiez le fichier.
3 Chargez le fichier via l'interface de Dell Data Guardian.

GUID-B18E3439-4C04-4F3A-AADA-DD5552F902D6

Préférences d'application

Pour lancer les Préférences :

1 Lancez Dell Data Guardian.
2 Dans la barre de menus de Dell Data Guardian, sélectionnez **Préférences**.

REMARQUE :
Ces informations sont également disponibles à partir de l'icône d'aide.

Vous pouvez modifier ces paramètres :

- Masquer les fichiers qui commencent par "." : cette case est cochée par défaut et ces fichiers sont masqués. Pour afficher les fichiers masqués, décochez la case.

  REMARQUE :
  Généralement, les fichiers précédés d'un point de séparation sont masqués dans le Finder d'OS X.

- **Dissocier un fournisseur de stockage Cloud** : répertorie les fournisseurs de stockage Cloud authentifiés par Data Guardian. Pour supprimer un fournisseur de stockage Data Guardian, sélectionnez le nom du fournisseur, et cliquez sur le signe moins (-) en bas à gauche de la fenêtre Préférences.

Règles du serveur : l'administrateur du serveur DDP définit les règles suivantes, qui contrôlent la manière dont Data Guardian gère les fichiers et dossiers :

- **Serveur DDP** : indique l'URL du serveur.
- **Intervalle d'interrogation** : indique l'intervalle (en minutes) au cours duquel le logiciel client recherche des mises à jour de la règle.
- **Chiffrer :** règle de chiffrement principale permettant le chiffrement des dossiers et fichiers sur le site Web de stockage Cloud.
- **Extension uniquement** ou **Camoufler**

  Extension uniquement (paramètre de règle par défaut) affiche le nom de fichier sur le site Web.

  Si une entreprise exige une protection supplémentaire des fichiers, configurez cette règle sur **Camoufler** pour masquer les noms de fichiers sur le site Web Cloud en tant que noms GUID.

  REMARQUE :
  Si la règle est configurée d'abord sur Extension uniquement et que les utilisateurs ont des fichiers sur le site Web Cloud,puis que la règle est changée à Camoufler, les noms de fichiers préexistants sur le site Web ne seront pas camouflés. Pour camoufler les noms de fichiers préexistants, l'utilisateur doit télécharger puis charger les fichiers via l'interface de Data Guardian. Ou, si l'utilisateur modifie un fichier, il sera chargé avec un nom de fichier camouflé.

- **Documents Office protégés** : protège les documents Office (.docx, .pptx, .xlsx, .docm, .pptm, .xlsm) sur le Cloud, mais affiche l'extension de fichier et non pas une extension .xen.

  Si cette règle est activée, les documents Office (.docx, .pptx, .xlsx, .docm, .pptm, .xlsm) sur le Cloud affichent l'extension de fichier et non pas une extension .xen. Toutefois, les fichiers ne peuvent pas être ouverts sur le Cloud ou s'ils ont été téléchargés. S'ils sont ouverts, seule une page de garde s'affiche, indiquant que le document est protégé. Si vous avez installé Data Guardian sans l'authentifier, la page de garde indique également cette information.
- **Événements d'audit** : si cette option est activée, le système envoie des événements d'audit au serveur Dell.
- **Géolocalisation** : si cette option est activée, les événements d'audit qui sont envoyés au serveur Dell contiennent des données de géolocalisation (latitude et longitude).

- **Balise de rappel** : si cette option est activée, le système envoie une balise de rappel vers chaque fichier Office protégé.
- **URL de balise de rappel** : si cette option est activée, le système spécifie l'URL à utiliser lorsque la balise de rappel est insérée dans les fichiers Office protégés.
- **Fournisseurs de protection de stockage Cloud** : un nom de fournisseur s'affiche en fonction des paramètres de la règle. Les options disponibles sont **Box**/ **Dropbox**/ **Google Drive** / **OneDrive OneDrive for Business**.

  Activez ou désactivez le cryptage des fichiers chargés sur ce fournisseur de stockage Cloud. L'une des options suivantes s'affiche :

  - **Chiffrer** : les fichiers envoyés sur le Cloud sont chiffrés.
  - **Autoriser** : l'utilisateur peut accéder aux fichiers dans le Cloud, mais les fichiers envoyés sur un site Web de fournisseur de stockage Cloud ne sont pas chiffrés.
  - **Bloqué** : le fournisseur de stockage Cloud étant actuellement indisponible, le nom de ce fournisseur ne s'affiche pas dans la fenêtre principale.

GUID-74395D32-C5C3-46A5-A090-CE195AD50CC0

Sécurité et autres considérations concernant les clients de synchronisation et Data Guardian

GUID-ED3DC4CF-B650-4583-83F3-84FE0268BBC3

Google Drive

Le *chiffrement Cloud* de Data Guardian chiffre des dossiers et des fichiers sur le Cloud afin de protéger les données. Soyez conscient de ces considérations.

- La stratégie de sécurité de l'entreprise, définie sur Protéger, interdit l'utilisation de Google Docs avec Data Guardian. Si elle est définie sur Autoriser, vous pouvez modifier ces fichiers. 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. Les fichiers Google Docs que vous créez s'affichent dans vos dossiers de fournisseur de stockage Cloud Google Docs.

  Cependant, si vous ouvrez le dossier, une boîte de dialogue vous avertit que Data Guardian ne peut pas chiffrer ce document.

GUID-5454F808-40A1-4609-BED2-7D3D08391FC4

OneDrive for Business

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

GUID-A6AA7EB4-E62B-44A2-BAC2-902473A21C42

Commentaires sur ce produit

Si la règle le permet, les utilisateurs peuvent fournir des commentaires sur Dell Data Guardian. Le formulaire de commentaires est disponible à partir de la barre de menus > **Fournir des commentaires sur Dell Data Protection.**

Tâches de désinstallation de Data Guardian

Cette section présente le processus d'administrateur permettant de désinstaller Data Guardian. Si un utilisateur possède un compte administrateur local, il peut désinstaller lui-même Data Guardian pour Mac.

GUID-0AEC84CA-AADA-44B7-A403-5D8C97FFAFD5

Configuration requise

Pour effectuer la désinstallation, vous devez posséder un compte administrateur local.

GUID-C8A4F2ED-6FE8-4B26-A3FB-60795D070304

Désinstallation de Data Guardian

Procédez de l'une des manières suivantes pour supprimer Data Guardian :

Finder

1 Tout en appuyant sur la touche <option>, sélectionnez **Accéder** dans la barre de menus.
2 Ouvrez le dossier **~/Library/Application Support/Dell**.
3 Supprimez le dossier **DataGuardian**.
4 À partir de l'option **Accéder** dans la barre de menus, ouvrez le dossier Applications et supprimez l'application **Data Guardian**.

Terminal

Data Guardian peut se trouver dans les emplacements suivants.

1 Utilisez l'une de ces commandes ou les deux :
   - rm -R ~/Applications/Data\ Guardian.app
   - rm -R ~/Library/Application Support/Dell/DataGuardian
2 Supprimez le dossier **DataGuardian**.

Glossaire

Activer/activé : l'activation se produit lorsque l'ordinateur a été inscrit sur le serveur Dell et qu'il a reçu au moins un jeu de règles initial.

Serveur Dell : le serveur Dell est composé d'une collection de composants. Lorsque l'on fait référence au côté serveur du produit dans son ensemble, il est généralement appelé le serveur Dell.

Console de gestion à distance : la console de gestion à distance est une console d'administration des déploiements pour toute l'entreprise. La console de gestion à distance est un composant de Dell Enterprise Server.

Serveur d'administration de la sécurité : composant du serveur Dell gérant Dell Data Guardian. Le serveur d'administration de la sécurité assure la sécurité des données dans le Cloud, peu importe avec qui elles sont partagées. Le serveur d'administration de la sécurité protège également les périphériques internes de la transmission de données sensibles.

Utilisateurs externes- Utilisateurs à l'extérieur de l'adresse de domaine de l'entreprise.