Dell Data Guardian

Guide d'utilisation de Windows, Mac, Mobile et Web v2.5

Identifier	GUID-5B8DE7B7-879F-45A4-88E0-732155904029
Status	Translated

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.

Identifier	GUID-8935090F-D61D-41F4-ABC8-F4654D88B0FA
Status	Translation Validated

Guide d'utilisation de Windows, de Mac, Mobile et du Web

2019 - 04

Rév. A01

Table des matières

Identifier	**GUID-1E29C798-6A65-41FB-8102-6**
Status	**Translation Validated**

Introduction

Le *Guide d'utilisation de Dell Data Guardian* contient les informations nécessaires pour installer et utiliser Data Guardian sur Windows, Mac, Mobile ou un portail Web.

Identifier	**GUID-6EE59323-7410-43F4-AD47-C5B7B04044E8**
Status	**Translation Validated**

Présentation

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

- Les documents Office stockés localement, partagés avec d'autres utilisateurs de différentes façons ou stockés sur un média amovible. Les documents Office suivants peuvent être protégés : .docx, .pptx, .xlsx, .docm, .pptm, .xlsm, .pdf.
- Protection de fichiers de base pour d'autres applications et types de fichiers, par exemple Bloc-notes.
- 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.

REMARQUE :
Votre administrateur vous indiquera si votre entreprise utilise Data Guardian pour les documents Office uniquement, le stockage cloud uniquement, ou les deux. Votre administrateur vous parlera également des autres applications et types de fichiers que vous pouvez protéger.

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

- Windows
- iOS
- Android
- Mac
- Le portail Web Data Guardian, s'il est configuré par votre administrateur

REMARQUE :
Data Guardian pour Mac peut ouvrir des fichiers chiffrés par les autres plateformes. Toutefois, certains de ces fichiers seront peut-être en lecture seule. La plupart des informations utilisateur à propos de Data Guardian pour Mac se trouvent dans le logiciel en tant qu'aide en ligne.

Identifier	GUID-C9552E05-51A1-4C2D-AADE-C078B4639CD4
Status	In Translation

Options de chiffrement pour Data Guardian

En fonction du niveau de sécurité établi par votre entreprise, votre administrateur configure des stratégies pour protéger les données au repos et de données en mouvement. Votre administrateur vous indiquera les stratégies qui s'appliquent à votre entreprise.

Cette liste fournit une vue d'ensemble de certaines options de chiffrement et, pour certaines plateformes, l'emplacement des paramètres de stratégie.

Modes et documents Office

La règle peut être définie de manière à protéger les documents Office. Le comportement du chiffrement peut varier selon la plateforme et le mode. Pour Mac, voir l'aide en ligne.

Modes	Documents Office
Options de mode pour **Windows et Mac** : **Mode de protection individuelle** : vous permet de déterminer quels documents Office protéger. • **Windows** et **Mac** : un dossier **Documents sécurisés** est ajouté à la racine de votre dossier Documents. Ce dossier fournit une autre méthode pour chiffrer un fichier. **Mode de protection forcée** : votre entreprise requiert un niveau élevé de sécurité. Data Guardian effectue un balayage pour chiffrer les fichiers. • **Windows** et **Mac** : une autre stratégie peut ajouter un dossier **Documents non protégés** à la racine de votre dossier Documents. • **Mac** : protège les fichiers dans **\Utilisateurs**. Ces plates-formes ne se basent pas sur les modes : • Mobile • Portail Web	**Documents Office utilisés sous Windows, Mac, Mobile et le portail Web** • .docx • .pptx • .xlsx • .docm • .pptm • .xlsm • .pdf : si le document est protégé avec Data Guardian, ouvrez-le avec Adobe Acrobat Reader DC ou Microsoft Word et non pas à partir du réseau.

Documents Office - Windows

Votre administrateur peut configurer d'autres stratégies Data Guardian pour contrôler ou éviter des pertes de données via ces options. Le comportement du chiffrement peut varier selon le mode.

Options pour les documents Office protégés sous Windows	Description
• Enregistrer : si un document Office est protégé, vous pouvez enregistrer du nouveau contenu. (L'option **Enregistrer sous** est grisée.) • Opération Enregistrer sous protégée • Si un document Office est déjà protégé, l'option **Enregistrer sous** est grisée.	Informations supplémentaires pour Windows : • Document Office **Non protégé** : vous pouvez sélectionner **Enregistrer**, **Enregistrer sous** ou **Enregistrer sous protégée**. • Une bordure rouge s'affiche sur les documents Office et les e-mails protégés.
Copier/Coller et presse-papiers	Vous pouvez copier et coller à partir d'un document Office protégé vers un autre document Office protégé. Vous ne pouvez pas coller du contenu provenant d'un document protégé dans un document non protégé.
Impression	En fonction de la stratégie, l'impression d'un document Office protégé peut être autorisée, avoir un filigrane ou être désactivée.
Exporter (Windows et Office 2013 et version ultérieure, mobile)	En fonction de la stratégie, cela peut être autorisé, avoir un filigrane ou être désactivé. **REMARQUE :** Si le filigrane est configuré, les documents Office peuvent être exportés. Les fichiers PDF ne peuvent pas être exportés.
Écran Impression	En fonction de la stratégie, cela peut être autorisé ou bloqué.
Processus bloqués Exemple : outil Capture d'écran	En fonction de la règle définie par votre entreprise, certains processus sont bloqués lorsqu'un document Office protégé est ouvert.
Filigrane affiché à l'écran	Lorsqu'un document Office protégé est ouvert, l'écran affiche un filigrane avec le nom de l'ordinateur et le nom de l'utilisateur.
Classification TITUS (Windows avec le mode de protection individuelle)	Si une stratégie est activée, vous pouvez cliquer avec le bouton droit de la souris sur un document Office et sélectionner une classification TITUS. Les utilisateurs disposent ainsi d'une autre méthode pour protéger un document Office.
Classification des données (Windows avec le mode de protection individuelle)	Lorsqu'une stratégie est activée et configurée de façon à protéger des données sensibles, tels que des numéros de sécurité sociale ou des numéros de carte de crédit, les documents Office contenant ce type de données sont chiffrés.

Documents Office - Mac, Mobile et portail Web

Le comportement du chiffrement peut varier selon la plateforme et le mode. Votre administrateur vous informera des règles qui s'appliquent à votre entreprise.

Option de chiffrement	Description
Mac : interface Dell Data Guardian	**Mac** : télécharger un document protégé à chiffrer. Téléchargez un document protégé à déchiffrer. Une fois qu'un document protégé est modifié, il est enregistré sous le fichier d'origine, sur le cloud ou en local.
Mobile : dans l'application Data Guardian • Impression • Filigrane affiché à l'écran	**Mobile** : en fonction de la règle • Les documents Office au sein de l'application Data Guardian sont protégés.

Option de chiffrement	Description
• Filigrane masqué • Exporter	• L'impression d'un document Office protégé peut être autorisée, avoir un filigrane ou être désactivée. • Lorsqu'un document Office protégé est ouvert, l'écran affiche un filigrane avec le nom de l'ordinateur et le nom de l'utilisateur.
Portail Web • Filigrane affiché à l'écran	**Portail Web** : vous pouvez télécharger des documents protégés ou non protégés, mais tout fichier téléchargé est protégé lorsque vous cliquez sur Télécharger. Lorsqu'un document Office protégé est ouvert, l'écran affiche un filigrane avec le nom de l'ordinateur et le nom de l'utilisateur.

Options supplémentaires

Le comportement du chiffrement peut varier selon la plateforme et le mode. Votre administrateur vous informera des règles qui s'appliquent à votre entreprise.

Option	Description (modes de protection individuelle et forcée)
Protection de fichiers de base : permet la protection d'autres applications et types de fichiers. (Windows, Mac, Mobile et portail Web) • Exemples : .txt ou .png **REMARQUE :** Actuellement, aucune bordure rouge ne s'affiche pour ces types de fichiers, même lorsqu'ils sont protégés.	Votre administrateur peut configurer une stratégie pour spécifier les applications et types de fichiers à chiffrer. **Windows, Mac et Mobile** : ces fichiers sont balayés et chiffrés. • **Mac** : exige que le mode de protection forcée soit disponible. **Portail Web** : également basés sur une règle, ces fichiers peuvent être en lecture seule ou l'utilisateur peut les modifier.
Partager des documents Office protégés ou des fichiers au format .xen avec des **utilisateurs externes**. (Windows, Mac, Mobile et portail Web) Une page de garde répertorie les liens pour l'inscription et les informations pour installer Data Guardian.	• Utilisateurs externes et **Windows** : vous pouvez également ajouter une **restriction de date (un embargo)** sur des documents Office protégés et des PDF. • **Portail Web** : vous pouvez charger des fichiers partagés vers le portail Web. Vous ne pouvez pas partager un fichier à partir du portail Web, mais vous pouvez le partager une fois son téléchargement terminé.
Page de garde ou fichier altéré (Windows, Mac, Mobile et Web)	Pour les fichiers Office, Data Guardian peut analyser les documents protégés pour y détecter certaines formes d'altération.
Groupes d'accès (local) (Windows, Mac, Mobile et portail Web)	Lorsque cette option est activée par votre administrateur, seules les personnes dans votre Groupe d'accès peuvent voir vos fichiers chiffrés. Vous pouvez accorder l'accès aux utilisateurs internes et externes pour les fichiers individuels et ils peuvent demander l'accès.
Geofencing (mobile)	Seuls les utilisateurs situés dans une zone spécifiée peuvent accéder aux fichiers à partir de leurs téléphones mobiles.
Chiffrement des e-mails Outlook (Windows)	Suivant la stratégie définie, vous disposez d'un bouton *Protéger* qui vous permet de chiffrer le contenu d'un e-mail et de ses pièces jointes. Lorsqu'ils sont envoyés à des utilisateurs extérieurs, une page de garde répertorie les liens pour l'inscription et les informations pour installer Data Guardian.

Hébergé ou local

Si vous devez installer Data Guardian vous-même, votre administrateur vous confirme les options qui s'appliquent à votre entreprise.

REMARQUE :
Pour les applications mobiles, si vous Workspace ONE est installé, vous pouvez vous authentifier sur Data Guardian à l'aide de l'authentification unique.

Dell Security Center hébergé	Serveur Dell Management local
Solution SaaS (Software as a Service) hébergée permettant de gérer le logiciel Dell Data Security. Si votre entreprise est multitenant, votre administrateur vous fournira un ID d'installation. Lorsqu'une page de garde s'affiche pour un utilisateur qui n'a pas encore accès à un document protégé, celle-ci inclut des informations sur l'ID d'installation. Toutes les plates-formes : si un tenant ne s'acquitte pas du paiement pendant un délai spécifié, ses opérations peuvent être suspendues.	Serveur sur site situé dans le réseau de l'entreprise et permettant de gérer le logiciel Dell Data Security. Votre administrateur vous fournira le nom de l'URL de Dell Server.

Cryptage Cloud

Le comportement du chiffrement peut varier selon la plateforme et le mode. Votre administrateur vous informera des règles qui s'appliquent à votre entreprise.

Plate-forme	Description
Windows **REMARQUE :** Actuellement, la protection par chiffrement Cloud de Data Guardian a été désactivée sur Windows pour éviter problèmes de compatibilité avec les nouvelles fonctionnalités des prestataires de services Cloud. Pour afficher les fichiers déjà protégés par chiffrement Cloud, utilisez l'application Data GuardianMobile, le portail Web ou Data Guardian sous Mac.	Voir la section Utilisation du chiffrement Cloud de Data Guardian sous Windows.
Mobile	Voir Utilisation de la protection cloud avec Mobile.
Mac	Voir l'aide en ligne.
Portail Web	Voir l'aide en ligne.

Paramètres de stratégie

Certaines plateformes incluent une liste partielle des paramètres de stratégie pour votre périphérique.

Plate-forme	Emplacement des paramètres de stratégie
Mac	Volet *Préférences*
Mobile	Icône **Paramètres** > **À propos de**

Plate-forme	Emplacement des paramètres de stratégie
Portail Web	Icône **Paramètres** > **À propos de**

Identifier	**GUID-DEFFD392-F513-445E-A87C-2CE7250245A2**
Status	**Translation Validated**

Assistance supplémentaire

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

Identifier	**GUID-1DE0401E-4073-46BA-95E3-**
Status	**Translation Validated**

Configuration requise

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

Identifier	**GUID-7C606C28-5532-4F36-AFA3-03126F14A6EF**
Status	**Translation Validated**

Serveur Dell

Data Guardian pour Windows, Mac et appareils mobiles exige les serveurs Security Management Server ou Security Management Server Virtual v9.6 ou versions ultérieures. Le client Web Data Guardian exige les serveurs Security Management Server ou Security Management Server Virtual v9.8 ou versions ultérieures. 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 de Security Management Server Virtual).

Identifier	**GUID-198D0A89-3C37-4C12-87A4-1F801B60DB21**
Status	**In Translation**

Data Guardian pour Windows

- 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 ou la désinstallation.
- Lors de l'installation, n'apportez aucune modification à l'ordinateur, notamment, n'insérez ou ne retirez pas de lecteurs externes (USB).
- Data Guardian est pris en charge avec certaines versions de Microsoft Office 2016 ainsi que Microsoft Office 365 Business et Business Premium. Il n'est pas pris en charge avec Office 365 Business Essentials.
- Pour le cryptage cloud, l'ordinateur doit disposer d'un lecteur de disque (valeur de lettre) attribuable disponible.
- Data Guardian pour Windows est compatible avec Workspace ONE. Le programme d'installation de Data Guardian pour Workspace ONE avec une installation MSI dispose d'une extension .msi.
- Data Guardian v2.4 et les versions ultérieures sous Windows sont prises en charge dans les environnements Air Gap, mais avec certaines restrictions. Actuellement, les données de géolocalisation des événements d'audit et les fichiers Embargo ne sont pas pris en charge. Les balises Web exigent certaines configurations.
- 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 avec le cryptage Cloud, 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 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.

- Les documents Office protégés sont pris en charge avec Mozy, une solution complémentaire de Data Guardian, ainsi qu'avec les clouds, e-mails et produits de stockage NFS.
- Bien que Dell Encryption ne soit pas obligatoire, s'il est utilisé, la version du client Encryption doit être v8.12 ou une version ultérieure.
- Data Guardian ne prend pas en charge l'outil de restauration du système de Windows ou Windows Insider Preview.
- L'option Redirection de dossier de Microsoft n'est pas prise en charge avec Data Guardian.
- IPv6 n'est pas pris en charge avec le cryptage cloud.
- Consultez régulièrement le site www.dell.com/support pour obtenir la documentation la plus récente et des conseils techniques.

Pré-requis

Fichier .exe prérequis

Le programme d'installation installe le package redistribuable Microsoft Visual C++ 2017 (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.

Fichier .msi prérequis

Vous devez installer Microsoft Visual Studio C++ 2017 Redistributable Package (x86 et x64).

REMARQUE :
En outre, si vous exécutez MSI, vous devez également installer Visual Studio 2010 Tools pour Office Runtime (x86 et x64).

Éléments prérequis généraux

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 Data Guardian pour éviter tout échec d'installation/de mise à niveau. Pour vérifier la version de .Net installée, suivez ces instructions sur l'ordinateur ciblé pour l'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

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 Mo 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 décrit les systèmes d'exploitation pris en charge.

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

- Windows 7 SP1 : Entreprise, Professionnel, Ultimate
- Windows 8.1 Mise à jour 0-1 : Enterprise Edition, Pro Edition
- Windows 10 : Éducation, Entreprise, Pro Version 1703 (Creators Update/Redstone 2) jusqu'à la version 1809 (Mise à jour octobre 2018/Redstone 5)

REMARQUE :
Le client doit être sur l'un de ces systèmes d'exploitation. Dans le cas contraire, il sera bloqué. Si nécessaire, un paramètre d'une clé de Registre permet à l'administrateur de contourner le blocage.

Pour la prise en charge de Redstone 4, vous devez mettre l'agent à niveau avant d'effectuer la mise à niveau du système d'exploitation. Voir https://www.dell.com/support/article/us/en/04/sln307922.

REMARQUE :
Data Guardian n'est pas compatible avec Windows Defender Exploit Guard (WDEG) de Microsoft dans Redstone 3 et versions ultérieures ou avec Enhanced Mitigation Experience Toolkit (EMET) dans Redstone 2 et versions antérieures.

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

Data Guardian ne prend pas en charge plusieurs versions d'Office sur un ordinateur.

Fournisseurs de stockage cloud

Le tableau ci-dessous décrit les fournisseurs de stockage cloud qui fonctionnent avec Data Guardian pour Windows. Les mises à jour des fournisseurs de stockage cloud sont mises sur le marché fréquemment. Dell recommande de tester les nouvelles versions avec Data Guardian avant de les présenter à l'environnement de production.

Fournisseurs de stockage cloud

- Dropbox
- Dropbox for Business (Windows uniquement)

  REMARQUE :
  Selon la version de Serveur Dell utilisée 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 sont pas pris en charge par Data Guardian. L'utilisation de Box Tools peut entraîner la survenue d'un écran bleu.

- Google Drive

  REMARQUE :
  La sauvegarde et la synchronisation Google ne sont pas prises en charge.

- OneDrive

Fournisseurs de stockage cloud

- OneDrive for Business
- Unified OneDrive

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

Microsoft Office

Data Guardian prend en charge les versions d'Office suivantes. Cependant, une seule version d'Office doit être installée.

Microsoft Office

- Office 2013 SP1
- Office 2016
- Office 2019
- Office 365 ProPlus : versions 1705, 1708 et 1803 (canal semestriel)

Identifier	**GUID-371FFDE5-7A34-4288-AA88-617E73C0F9A4**
Status	**Translation Validated**

Data Guardian pour 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

Systèmes d'exploitation

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

Systèmes d'exploitation Mac

- macOS Sierra 10.12.6
- macOS High Sierra 10.13.5 - 10.13.6

- macOS Mojave 10.14.0 - 10.14.3

Fournisseurs de stockage cloud

Selon les paramètres de règles, les éléments suivants peuvent s'afficher dans l'interface Mac de 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

  REMARQUE :
  La sauvegarde et la synchronisation Google ne sont pas prises en charge.

- OneDrive
- OneDrive for Business

Microsoft Office

Data Guardian pour Mac prend en charge les versions d'Office suivantes.

Microsoft Office

- Office 2013 SP1
- Office 2016
- Office 2019

Identifier	**GUID-70934847-A1D7-4AD3-8822-A1E474D4ECD6**
Status	**In Translation**

Application Data Guardian pour appareils mobiles

La liste suivante répertorie les systèmes d'exploitation pris en charge avec l'application Data Guardian pour appareils mobiles.

Systèmes d'exploitation Android

- 5.0—5.1.1 Lollipop
- 6.0—6.0.1 Marshmallow

- 7.0—7.1.2 Nougat
- 8.0—8.1 Oreo
- 9.0 Pie

Systèmes d'exploitation iOS

- iOS 10.x—10.3
- iOS 11.x—11.4.1
- iOS 12.x—12.1.4

Système d'exploitation Chromebook

Microsoft Office

Data Guardian pour l'application Mobile peut ouvrir des fichiers créés avec les versions d'Office suivantes.

Microsoft Office

- Office 2013 SP1
- Office 2016
- Office 2019

Identifier	**GUID-E0E57A65-225C-46FB-9E51-60FAC92BA57A**
Status	**In Translation**

Data Guardian pour le Web

Pour activer le client Web Data Guardian, l'administrateur met en place une machine virtuelle qui héberge le client Web et communique avec Serveur Dell v9.8 ou versions ultérieures.

Les environnements virtualisés suivants peuvent être utilisés pour déployer le client Web Data Guardian.

Environnements virtualisés

- **VMware ESXi 6.0**
  - UC 64 bits x86 requise
  - Ordinateur hôte avec au moins deux cœurs
  - Au moins 8 Go de RAM recommandés
  - Un système d'exploitation n'est pas nécessaire
  - Reportez-vous à http://www.vmware.com/resources/compatibility/search.php pour obtenir une liste complète des systèmes d'exploitation hôte pris en charge
  - Le matériel doit être conforme à la configuration minimale requise par VMware
  - Au moins 4 Go de RAM pour la ressource d'image dédiée

Environnements virtualisés

- Voir http://pubs.vmware.com/vsphere-60/index.jsp pour obtenir plus d'informations

- **VMware ESXi 5.5**
  - UC 64 bits x86 requise
  - Ordinateur hôte avec au moins deux cœurs
  - Au moins 8 Go de RAM recommandés
  - Un système d'exploitation n'est pas nécessaire
  - Reportez-vous à http://www.vmware.com/resources/compatibility/search.php pour obtenir une liste complète des systèmes d'exploitation hôte pris en charge
  - Le matériel doit être conforme à la configuration minimale requise par VMware
  - Au moins 4 Go de RAM pour la ressource d'image dédiée
  - Voir http://pubs.vmware.com/vsphere-55/index.jsp pour obtenir plus d'informations

- **Microsoft Hyper-V**
  - Processeur 64 bits avec SLAT (Second Level Address Translation ou second niveau de translation d'adresse)
  - Au moins 8 Go de RAM recommandés
  - Le matériel doit être conforme à la configuration minimale requise par Hyper-V.
  - Voir https://docs.microsoft.com/en-us/virtualization/hyper-v-on-windows/reference/hyper-v-requirements pour davantage d'informations.

REMARQUE :
Ces valeurs minimales représentent vingt-cinq connexions simultanées ou moins vers un seul portail Web.

Microsoft Office

Data Guardian pour le Web peut ouvrir des fichiers créés avec les versions d'Office suivantes.

Microsoft Office

- Office 2013 SP1
- Office 2016
- Office 2019

Identifier	**GUID-F414365D-DE5B-4703-88AB-FCB73F3BD14D**
Status	**Translation Validated**

Autres conditions requises

Actuellement, l'authentification multifacteur (MFA) d'Amazon Cognito n'est prise en charge par aucune plate-forme Data Guardian.

Identifier	**GUID-E2815EA1-85AF-4049-B317-DF016FBA39EE**
Status	**Translation Validated**

Navigateurs Web

Vous pouvez utiliser Data Guardian avec Internet Explorer, Mozilla Firefox, Google Chrome et Microsoft Edge.

Pour Mac, Safari est également pris en charge.

Identifier	**GUID-582A5665-D2A2-4B98-A51D-5F14376D98BA**
Status	**Translation Validated**

Adobe Acrobat

Pour Windows et Mac, les fichiers .pdf protégés peuvent être ouverts avec Adobe Acrobat Reader DC.

REMARQUE :
Les versions suivantes ne sont pas prises en charge : Adobe Acrobat *Standard* DC, Adobe Acrobat *Pro* DC et Adobe Acrobat DC.

Identifier	GUID-36045ECC-D303-4A63-9ABA
Status	Translation Validated

Installation ou désinstallation de Data Guardian sous Windows

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

Si votre entreprise utilise le chiffrement cloud de Data Guardian, l'ordinateur doit disposer d'un caractère alphabétique libre pouvant être affecté à un lecteur de disque.

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

Identifier	GUID-D0717325-F700-400C-BC03-5FD8190A81A9
Status	Translation Validated

Présentation des tâches d'installation pour Windows

Cette vue d'ensemble résume la séquence d'installation de Data Guardian. Vous pouvez installer le produit avec ou sans chiffrement cloud.

Installation de Data Guardian sans chiffrement cloud

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.	Installations par l'utilisateur : voir Installation interactive de 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 zone de notification 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. **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.

Installation de Data Guardian avec le chiffrement cloud et les documents protégés

Tâche	Description	Pour en savoir plus
Si un client de synchronisation cloud est installé	Les dossiers et fichiers existants qui se synchronisent vers le cloud ne sont pas cryptés.	Voir Dossiers préexistants contenant des fichiers non cryptés.

Tâche	Description	Pour en savoir plus
avant Data Guardian	**REMARQUE :** Les dossiers et fichiers existants qui se synchronisent depuis le cloud sont 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.	Installations par l'utilisateur : voir Installation interactive de 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 zone de notification 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. **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.
Si des règles protègent les documents dans le cloud, installez un client de synchronisation cloud	Client de synchronisation Business ou Client de synchronisation Basic	Comptes de client de synchronisation cloud d'entreprise ou Comptes de client de synchronisation cloud de base

Options pour Windows

Tâche	Description	Pour en savoir plus
Afficher le menu zone de notification	Fournit des informations utiles concernant les fichiers, les dossiers et le dépannage.	Présentation des éléments de menu de Data Guardian dans la zone de notification

Identifier	**GUID-B54EDFCA-AFBB-4BD0-8427-515A3E052962**
Status	**Translation Validated**

Dossiers préexistants contenant des fichiers non cryptés

Lors du déploiement de Cloud Encryption de Data Guardian, il est préférable de ne pas avoir créé de compte de fournisseur de stockage cloud sur les périphériques cibles.

Si un compte de fournisseur de stockage cloud est configuré pour les dossiers qui sont synchronisés sur l'ordinateur local avant l'installation de 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

Pour que les fichiers déjà existants soient cryptés, accédez au Lecteur virtuel DDG vDisk (créé à l'installation de Data Guardian), créez un nouveau sous-dossier dans le client de synchronisation Cloud et déplacez les fichiers déjà existants dans ce dossier.

ou

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

Identifier	**GUID-7BBFA9B6-C19E-44E8-908C-F5AF181462C8**
Status	**Translated**

Installation interactive de Data Guardian sous Windows

Vous devez disposer des droits d'administrateur pour installer Data Guardian. Si ce sont les utilisateurs qui installent le produit, informez-les de l'emplacement du kit d'installation.

Avant de commencer

En fonction de l'environnement et du produit Data Guardian, déterminez l'élément dont vous avez besoin parmi les suivants :

Dell Security Center hébergé	Serveur Dell Management local	Cryptage Cloud
Si votre environnement hébergé est multitenant, vous aurez besoin d'un ID d'installation.	Assurez-vous que vous connaissez le nom du Serveur Dell.	L'ordinateur doit disposer d'une lettre disponible, pouvant être attribuée à un lecteur de disque.

Installez Data Guardian

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 et copiez-le sur l'ordinateur local. Voici des exemples de noms de programme d'installation :
   - Dell Security Center hébergé : les noms de programme d'installation ont une extension .exe
   - local : les programmes d'installation noms ont une
     - extension .exe
     - extension .msi pour Workspace One et une installation MSI
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 vous êtes invité à installer Microsoft Visual C++ 2015 Redistributable Package ou Microsoft .NET Framework 4.5.2 Client Profile, cliquez sur **OK**.
7. Dans la page d'accueil, cliquez sur **Suivant**.
8. Lisez le contrat de licence, acceptez-en les termes, 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\Data Guardian\.**

   N'installez pas Data Guardian dans les dossiers **C:\Users** ou **C:\Windows**, ou à la racine d'un lecteur.
10. Sélectionnez l'une de ces options :

Dell Security Center hébergé	Serveur Dell Management local
Solution SaaS (Software as a Service) hébergée permettant de gérer le logiciel Dell Data Security.	Serveur sur site situé dans le réseau de l'entreprise et permettant de gérer le logiciel Dell Data Security.
a Sélectionnez **Dell Security Center hébergé**. b Vous pouvez aussi, si votre entreprise est multitenant, entrez un ID d'installation. **REMARQUE :** Si votre entreprise est multitenant et que vous ne renseignez pas l'ID d'installation, l'administrateur peut l'ajouter au registre ultérieurement. c Cliquez sur **Continuer**. d Passez à l'étape 11.	a Sélectionnez **Serveur Dell Management local**. b Dans le champ *Nom du serveur de gestion Dell :*, saisissez le nom du Serveur Dell 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. **REMARQUE :** Ne décochez pas la case *Activer la vérification de confiance SSL* sauf si votre administrateur vous le demande. c Cliquez sur **Suivant**. d Dans l'écran d'information Confirmer le serveur de gestion Dell, confirmez que l'adresse URL du Serveur Dell est correcte. Le programme d'installation ajoute www ou http(s) et le port. Cliquez sur **Suivant**. e Passez à l'étape 11.

11 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.

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

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

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

15 Les utilisateurs doivent confirmer l'activation. L'icône Data Guardian dans la zone de notification affiche une coche verte  .

REMARQUE :

En fonction de la manière dont Data Guardian est déployé au sein de l'entreprise, l'activation peut ne pas être immédiate. Cependant, si l'activation n'est pas effective, l'utilisateur doit la faire manuellement.

Identifier	**GUID-AF4BEC71-F3FB-43E9-A588-FA2C2BC7E4BD**
Status	**Translation Validated**

Problèmes possibles à l'activation : cloud et Office protégé

Si vous avez installé Data Guardian, mais que l'icône Data Guardian de la zone de notification 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 :

Option Data Guardian	Problème possible
Office protégé	• 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.
Cryptage Cloud	• L'accès aux sites Web de synchronisation Cloud est bloqué • La connexion entre les applications de synchronisation Cloud et leurs services Web est bloquée

Option Data Guardian	Problème possible
	• Les dossiers de synchronisation locaux ne sont pas mis à jours pendant cette période de temps

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.

Identifier	**GUID-10DDD78A-61B2-4AE9-9DF4-0527FEE42D0D**
Status	**Translation Validated**

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 zone de notification, une icône en forme de bouclier assortie d'un point d'exclamation orange s'affiche.
2 Cliquez sur l'icône **Data Guardian** dans la zone de notification 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 zone de notification  .
4 Confirmez l'état de votre mode utilisateur. Cliquez sur l'icône de la zone de notification 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 Utilisation de Data Guardian en tant qu'utilisateur externe.

> **REMARQUE :**
> Si le mode utilisateur indique **Non enregistré**, votre Data Guardian n'est pas encore activé.

Identifier	**GUID-8882A835-A7A8-4C7B-8330-3080F871A121**
Status	**Translation Validated**

Dell Security Center hébergé et tenant suspendu

Avec Dell Security Center hébergé, si un tenant ne s'acquitte pas du paiement pendant un délai spécifié, ses opérations peuvent être suspendues. Ceci s'applique à Windows, Mac, Mobile et au portail Web.

Les utilisateurs internes et externes de Data Guardian peuvent être confrontés aux situations suivantes :

- Toutes les plates-formes : si vous essayez d'installer Data Guardian, de l'activer, ou de vous connecter, une boîte de dialogue s'affiche et vous signale que les opérations du tenant sont suspendues.

- Mac : si les opérations de votre tenant sont suspendues alors que Data Guardian est ouvert, la boîte de dialogue vous informant de cette suspension s'affiche après la fermeture de l'Explorateur et de tous les fichiers, et lorsque vous essayez ensuite d'ouvrir un fichier protégé.
- Portail Web :
  - Si vous êtes déjà connecté et que vous chargez un fichier chiffré, un message vous informe de l'échec du chargement.
  - Si un fichier chiffré ou non chiffré a été chargé, puis que les opérations du tenant sont suspendues, un message indiquant l'échec du téléchargement s'affiche.
  - Si vous vous déconnectez, puis que vous tentez de vous connecter à nouveau, une boîte de dialogue s'affiche pour indiquer que les opérations du tenant sont suspendues.

Contactez votre administrateur.

Identifier	**GUID-43BA606D-3F31-4E67-97B4-039DE9CEBC65**
Status	**Translation Validated**

Présentation des éléments de menu de Data Guardian dans la Zone de notification

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 **Fichiers** > **État des fichiers**.
- 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 avec le bouton droit de la souris sur l'icône **Data Guardian** dans la zone de notification, puis cliquez sur **Détails**.

Le coin supérieur gauche de l'écran Détails affiche les informations suivantes :

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
- **Non enregistré** : un utilisateur interne ou externe pour lequel Data Guardian n'est pas activé

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 : le serveur Serveur Dell 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 règle : version de la règle générée par le Serveur Dell.

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 droit de l'écran Détails.

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

Si une entreprise possède le chiffrement cloud de Data Guardian, la zone **Dossiers** 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

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'affiche 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*.

Identifier	**GUID-5726752F-D15C-479E-8E8E-6BBE27B23F90**
Status	**Translation Validated**

Vérifier les mises à jour de règle

Si votre administrateur modifie une règle et vous avertit de sa mise à jour, accédez à la zone de notification de Windows, cliquez sur l'icône **Dell 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.

Identifier	**GUID-62C18A73-A619-46BF-BE3A-76911412C43A**
Status	**Translation Validated**

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.

Identifier	**GUID-E67381E8-70C7-46BE-A822-9B5C48B0FFC3**
Status	**Translation Validated**

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.

Identifier	**GUID-CC8C1B76-3E85-415F-AAE0-3C20521D70A6**
Status	**Translation Validated**

Désinstaller le client de synchronisation ou Data Guardian sur Windows

Si votre administrateur a installé Data Guardian, lui seul devrait 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.

Identifier	**GUID-3BAFF359-6522-4E5B-827F-500C79875FF7**
Status	**Translation Validated**

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.

Identifier	**GUID-FB8AEF07-F76C-4E52-9920-B56A973DB1E6**
Status	**Translation Validated**

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 Guardian**, puis 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 confirmer la désinstallation de Data Guardian de Dell. Si c'est le cas, cliquez sur **Suivant**.
6 Sur l'écran Supprimer le programme, cliquez sur **Supprimer**.
Une fenêtre affiche l'avancement.
7 Si vous recevez un message d'erreur du client de synchronisation, cliquez sur **Continuer**.
8 Si une boîte de dialogue indique qu'un document Office est ouvert, cliquez sur **OK**, fermez le document Office et recommencez la désinstallation.
9 Cliquez sur **Terminer** lorsque l'écran Terminé s'affiche.
10 Cliquez sur **Oui** pour redémarrer.

La désinstallation de Data Guardian est maintenant terminée.

Identifier	**GUID-05F5667F-C3BE-4C5E-B64D-5629C60C049D**
Status	**Translation Validated**

Envoyer des commentaires à Dell

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

Pour y accéder, cliquez sur l'icône Data Guardian dans la zone de notification et sélectionnez **Envoyer des commentaires**.

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

Identifier	GUID-E68E0B8D-7519-4C11-A918-
Status	Translation Validated

Utilisation de Data Guardian sous Windows

Votre administrateur a déjà configuré des stratégies pour protéger des documents, et il vous indiquera lesquelles de ces options s'appliquent à votre entreprise.

REMARQUE :
Si votre entreprise gère également votre client de synchronisation cloud, voir Utilisation du chiffrement cloud de Data Guardian sous Windows.

Identifier	GUID-162A20CF-D1AD-4701-9A28-1000DB2FE1D4
Status	Translation Validated

Présentation des options

Cette vue d'ensemble résume les options possibles pour Data Guardian en fonction de la stratégie définie par votre administrateur. Ces documents seront protégés si vous les partagez avec d'autres utilisateurs ou si vous les enregistrez sur un média amovible.

L'option	Description	Pour en savoir plus
Documents Office et prenant en charge les macros	Cela inclut les formats .docx, .pptx, .xlsx, .pdf, .docm, .pptm, .xlsm et .pdf.	Voir Observation de l'option de menu Fichier pour déterminer le niveau de sécurité des documents Office. Vous disposerez de l'un de ces modes : • Protection individuelle • Protection forcée
Protection des fichiers de base	Pour les autres applications et types de fichiers que votre entreprise souhaite chiffrer et que votre administrateur a configurés.	Voir Protection d'autres applications et types de fichiers avec la protection de fichiers de base.
Options supplémentaires	Peut s'appliquer à des documents Office, à des fichiers de base, ou aux deux.	Voir Options supplémentaires pour Data Guardian.
Partage d'un fichier avec un utilisateur externe	Un utilisateur qui dispose d'une adresse e-mail hors domaine, qu'il s'agisse d'une personne d'une autre entreprise ou d'un utilisateur interne qui souhaite accéder aux fichiers protégés à partir d'une adresse e-mail hors domaine.	Voir Utilisation de Data Guardian en tant qu'utilisateur externe.

Travail en ligne avec des documents protégés

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

Propriétés du fichier > onglet Dell Data Guardian

Avec des documents Office protégés, vous pouvez cliquer avec le bouton droit et sélectionner **Propriétés**. Un onglet **Dell Data Guardian** s'affiche, pour indiquer des informations, comme les données concernant l'ID de clé du fichier, ou l'embargo/accès au fichier.

Icônes superposées pour Windows

Pour Data Guardian 2.2 et les versions ultérieures, des icônes superposées s'affichent sur les fichiers protégés dans l'Explorateur de fichiers. Si vous cliquez avec le bouton droit de la souris sur ce fichier protégé, un onglet Dell Data Guardian fournit des informations supplémentaires.

Filigrane masqué

En fonction des règles définies par votre administrateur, les documents Office protégés peuvent disposer d'un filigrane masqué qui identifie l'utilisateur. Si vous imprimez ou partagez le document, le filigrane demeure.

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.

Identifier	**GUID-E88C0771-29BE-4292-AD26-F913747EE0FC**
Status	**Translation Validated**

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
- .pdf

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 avez ouvert 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.

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* 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* 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.
  - Dossier **Documents > Non protégé** : si cette option est activée par la stratégie en mode de protection forcée (et non en mode de protection individuelle), un dossier Non protégé est ajouté à la racine du dossier Documents. Les documents Office de ce dossier sont déchiffrés. Si vous supprimez le dossier, celui-ci se recrée.

- 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.

Identifier	**GUID-077EC2B6-61AD-4F13-95D0-CF91EF0143AF**
Status	**Translation Validated**

Utilisation du mode de protection individuelle pour protéger des documents Office

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

- Travail avec les options du menu Fichier pour le mode de protection individuelle
- Options supplémentaires pour Data Guardian

Travail avec les options du menu Fichier pour le mode de protection individuelle

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
Ouvrez le fichier	Les fichiers s'ouvrent normalement
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 et vous devez 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 le lecteur virtuel du chiffrement Cloud, si vous cliquez avec le bouton droit de la souris pour créer un nouveau document Office, celui-ci est au format .xen. Vous devez l'enregistrer manuellement en tant que document protégé.
Enregistrer sous	Dispose des options standard (mais pas du mode protégé)
Opération Enregistrer sous protégée	La seule option dans le champ Type d'opération Enregistrer sous est Office protégé

Menu Fichier	Mode de protection individuelle et documents Office protégés
Impression	**Activé** Toutefois, pour les documents Office protégés, si un administrateur désactive l'option Impression par l'intermédiaire de la règle, vous pouvez toujours sélectionner Impression, mais un message toast s'affiche et vous signale que le document protégé ne peut pas être imprimé. Si votre administrateur autorise l'option Impression, une autre 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	Option **Activée** pour les documents Office protégés. Option **Désactivée** pour les documents non protégés.
Exporter (Office 2013 et versions ultérieures)	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. 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 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.

Classification TITUS et mode de protection individuelle

Si une stratégie est activée, votre administrateur configure certaines classifications TITUS pour chiffrer un document à l'aide de cette classification. Vous pouvez cliquer avec le bouton droit de la souris sur un document Office non protégé et sélectionner cette classification TITUS. Cela fournit une autre méthode pour protéger un document Office.

Classification de données et mode de protection individuelle

Si cette stratégie est activée, votre administrateur peut définir des classifications pour un contenu spécifique, tels que le numéro de sécurité sociale, le numéro de carte de crédit, ou d'autres données sensibles. Votre administrateur vous informera des informations qui ont été classifiées. Lorsque vous enregistrez un document qui contient des informations basées sur ces règles de classification, le document est chiffré.

Si vous utilisez des balises dans un document Office pour déclencher une classification des données utilisées dans les métadonnées de la stratégie pour les balises de fichier, la balise que vous utilisez dans le document Office est sensible à la casse et doit correspondre à la casse utilisée par votre administrateur dans la stratégie.

REMARQUE :

Si cette règle est activée, un balayage entraînera le chiffrement des fichiers qui répondent aux règles de classification. Cependant, lorsque vous créez le fichier, vous pouvez cliquer avec le bouton droit de la souris et sélectionner **Protéger le fichier**.

Dépannage du mode de protection individuelle

Si la stratégie Data Guardian a désactivé l'impression pour les documents Office protégés, vous pouvez toujours sélectionner Imprimer dans **Fichier > Info** ou cliquer avec le bouton droit de la souris sur un fichier Office protégé dans l'Explorateur Windows. 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 individuelle et souhaitez vérifier si un document est protégé ou non, ouvrez ce document : la barre de titre le désigne comme protégé.

REMARQUE :
Si vous disposez du mode de protection forcée, tous les documents Office sont protégés.

Identifier	**GUID-5E368002-F3BB-48A7-9A30-B4591019B21F**
Status	**Translation Validated**

Utilisation du mode de protection forcée pour protéger des documents Office

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

- Travail avec les options du menu Fichier pour le mode de protection forcée
- Options supplémentaires pour Data Guardian

Travail avec les options du menu Fichier pour le mode de protection forcée

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 forcée pour protégés et non protégés
Ouvrez le fichier	Les fichiers non protégés s'ouvrent en lecture seule.
Enregistrer	• 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.

Menu Fichier	Mode de protection forcée pour protégés et non protégés
	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	**Désactivée**
Opération Enregistrer sous protégée	La seule option dans le champ Type d'opération Enregistrer sous est Office protégé
Impression	**Activé** Toutefois, pour les documents Office protégés, si un administrateur désactive l'option Impression par l'intermédiaire de la règle, vous pouvez toujours sélectionner Impression, mais un message toast s'affiche et vous signale que le document protégé ne peut pas être imprimé. Si votre administrateur autorise l'option Impression, une autre 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	**Désactivée**
Exporter (Office 2013 et versions ultérieures)	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.

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.

Identifier	**GUID-669244A9-0658-46A3-A9EB-A5D349D7EDBC**
Status	**Translation Validated**

Options supplémentaires pour Data Guardian

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.

Coller

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

- Vous pouvez copier et coller des données protégées ou non dans le document protégé d'origine ou dans un PDF protégé. Cependant, un PDF non protégé ne peut pas être ouvert dans Adobe Acrobat Reader DC.
- 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.

Ouvrir et modifier un PDF protégé avec Adobe Acrobat Reader DC

Lorsque vous utilisez Acrobat Reader DC :

- Vous pouvez ajouter des annotations à un fichier .pdf protégé ou remplir un formulaire. Lorsque vous enregistrez le fichier, un nouveau fichier .pdf protégé comprenant les modifications est créé. Il s'agit d'une fonctionnalité Acrobat Reader DC.
- Pour optimiser la sécurité, lorsqu'un fichier .pdf protégé est ouvert avec Acrobat Reader DC, l'accès Internet est bloqué jusqu'à la fermeture d'Acrobat Reader DC.
- Pour optimiser la sécurité, si un .pdf protégé est ouvert, l'utilisateur ne peut pas l'envoyer par e-mail à partir de cette instance.

> **REMARQUE :**
> Vous ne pouvez pas ouvrir un fichier .pdf protégé à partir du réseau. Vous pouvez utiliser Word pour ouvrir un fichier .pdf protégé à partir du réseau.

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.

Options supplémentaires

Processus bloqués

En fonction de la règle définie par votre administrateur, certains processus comme l'outil de capture d'écran peuvent être bloqués. Votre administrateur peut vous indiquer ces processus. En outre, une boîte de dialogue vous indique que le processus est bloqué.

- **Mode de protection forcée** : si votre administrateur configure une stratégie pour bloquer le bouton *PrtScr*, cela peut également empêcher l'utilisation de l'écran tactile ou de la tablette pour imprimer des écrans.
- Windows avec RS5 dispose d'une application Croquis sur capture d'écran (anciennement l'outil Capture d'écran). Avec Data Guardian, votre administrateur peut activer une règle qui bloque cette application afin d'améliorer la sécurité.

Attachement d'un document protégé à un e-mail Outlook

Lorsque vous joignez un document 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.

Il est possible d'attacher un document Office protégé, un type de fichier protégé supplémentaire basé sur une règle, ou un fichier .xen.

Pour Windows avec Data Guardian, si vous attachez un document protégé, Data Guardian ajoute les informations d'accès au fichier chiffré au sein de cet e-mail.

- Utilisateurs internes : les informations s'affichent avec un lien pour le téléchargement d'un client.
- Utilisateurs externes : les informations s'affichent avec un lien pour l'inscription et le téléchargement d'un client.

REMARQUE :
Pour les informations ajoutées à afficher, vous devez envoyer l'e-mail à partir de Microsoft Office Outlook, pas la version Web d'Outlook.

Cryptage des e-mails Outlook avec Data Guardian

En fonction de la règle de Data Guardian v2.0.1 et version ultérieure, les utilisateurs internes ont une option *Protéger* dans le coin supérieur gauche d'Outlook pour crypter à la fois les e-mails et les pièces jointes. L'expéditeur et le destinataire doivent tous deux avoir installé et activé Data Guardian.

Le cryptage des e-mails Outlook de Data Guardian est pris en charge avec Office 2013 et les versions ultérieures, mais pas avec la messagerie Web.

Utilisation :

1. Dans le coin supérieur gauche, cliquez sur **Protéger**.
2. Pour une adresse e-mail externe, cliquez sur **Oui** pour confirmer le partage de clé ou sur **Non** si vous décidez de ne pas envoyer l'e-mail.

La meilleure pratique est d'avoir un seul e-mail ouvert à la fois. Si vous en avez plusieurs ouverts, assurez-vous de cliquer sur l'e-mail pour le mettre au point avant de cliquer sur le bouton Protéger. Le bouton Protéger doit s'afficher en gris lorsque vous ne passez pas la souris par-dessus.

Les données en mouvement sont sécurisées. Dans cette version préliminaire, une protection contre la perte de données (DLP) des données au repos est partiellement prise en charge. Les versions futures continueront d'améliorer la sécurité.

Afin de minimiser la DLP lorsqu'un e-mail chiffré est ouvert, certaines actions sont désactivées ou bloquées :

- *Étapes rapides* d'Outlook
- *Déplacer*, *Déplacer vers un dossier* et d'autres actions relatives au dossier.
- Flèches *Suivant* et *Précédent*
- *Transférer*
- Certaines options de clic droit

Afin de réduire la DLP lorsqu'un e-mail chiffré est ouvert, ces actions sont commandées :

- *Copier/Coller*
- *Imprimer* et *exporter* les données
- Certaines options de clic droit
- Dossier Brouillons et *Enregistrement automatique*

Pour les destinataires d'e-mail Outlook

Lorsque vous ouvrez e-mail Outlook chiffré, un avertissement s'affiche et indique que le document est protégé. L'utilisateur doit double-cliquer sur le fichier pour l'ouvrir. Dans l'aperçu, vous ne visualisez pas le contenu de l'e-mail, seulement une page de couverture. La page de garde répertorie le nom du serveur Serveur Dell pour l'option local ou un ID d'installation pour ce tenant spécifique si votre Dell Security Center hébergé est multitenant. La page de garde contient également des liens pour télécharger le client Data Guardian.

Rapport local pour les documents Office protégés et chiffrés à l'aide de la classification des données (mode de protection individuelle)

Pour protéger les données sensibles contenues dans les documents Office et les fichiers PDF, votre administrateur peut définir une stratégie pour ranger puis chiffrer les fichiers en fonction de la classification des données. Les données sensibles peuvent couvrir les numéros de sécurité sociale, les numéros de carte de crédit, les adresses postales, ou des données propres à l'entreprise. Votre administrateur vous informera des données sensibles pour lesquelles vos fichiers seront chiffrés.

Pour afficher un rapport local sur les fichiers chiffrés en raison de la classification des données ainsi que le motif de ce chiffrement :

1 Accédez au répertoire **C:\Users\<nom d'utilisateur>\AppData\Local\Dell\Data Guardian**.
2 Ouvrez le fichier **Classification Report.log**.

> **REMARQUE :**
> Lorsqu'un fichier est en cours de chiffrement, plusieurs lignes peuvent correspondre à l'entrée tant que le chiffrement n'est pas terminé.

Identifier	**GUID-D11E8451-72A7-4179-8693-28D0FAFF9B8B**
Status	**In Translation**

Protection d'autres applications et types de fichiers avec la protection de fichiers de base

Votre administrateur vous informera si des stratégies permettent le chiffrement d'autres applications et types de fichiers. Si une personne ouvre un fichier chiffré à l'aide de la protection de fichiers de base, mais que Data Guardian n'est pas installé sur son système, le contenu est illisible.

Vue d'ensemble de la protection de fichiers de base

Applications

Voici quelques exemples d'applications que votre administrateur voudra peut-être chiffrer :

- Bloc-notes
- Wordpad
- Visio
- MS Paint

REMARQUE :
Certaines applications ne sont que partiellement prises en charge avec Data Guardian. Si tel est le cas, votre administrateur vous en informera.

Types de fichiers

Voici quelques exemples de types de fichiers supplémentaires qui peuvent être configurés : .txt, .rtf, .csv, .odt, .vsdx, .png, .jpg, .jpeg, .jpe, .jfif, .gif, .tif, .tiff, .bmp

Windows, Mac et appareil mobile

Lorsque la stratégie de protection de fichiers de base est configurée, Data Guardian organise l'ordinateur des utilisateurs et chiffre tous les fichiers locaux portant ces extensions. Les fichiers chiffrés à l'aide de la protection de fichiers de base ne peuvent être consultés et modifiés qu'à l'aide de l'application associée à l'extension de ces fichiers.

REMARQUE :
Les fichiers contenus dans des dossiers système spécifiques ne sont pas chiffrés. Exemple : AppData. C'est également le cas pour les dossiers en relation avec des documents Office protégés, comme le dossier Documents sécurisés.

Icônes superposées pour Windows

Pour Data Guardian 2.2 et les versions ultérieures, des icônes superposées s'affichent sur les fichiers protégés dans l'Explorateur de fichiers. Si vous cliquez avec le bouton droit de la souris sur ce fichier protégé, un onglet Dell Data Guardian fournit des informations supplémentaires.

Retrait d'une extension de fichier dans Windows ou Mac

Votre administrateur peut décider de retirer une extension de fichier. Si c'est le cas, votre ordinateur est analysé pour déchiffrer ces types de fichiers.

- L'onglet *Propriétés > Dell Data Gardian* du fichier chiffré ne s'affiche plus.
- Si vous aviez des icônes en transparence, ils ne s'affichent plus.
- Le déchiffrage des fichiers peut prendre plusieurs minutes. Si un fichier avec cette extension est toujours chiffré, il a peut-être été ouvert pendant l'analyse ou stocké sur un serveur de fichiers à un autre emplacement.

Contactez votre administrateur pour demander la récupération des fichiers avec cette extension qui ne seront pas déchiffrés.

Applications Office

Vous pouvez utiliser une application Office pour ouvrir un fichier chiffré à l'aide de la protection de fichiers de base, mais son contenu sera en lecture seule.

Portail Web

Dans Paramètres > Règles, si l'option Protection de fichiers de base est définie sur Vrai, votre administrateur a ajouté des types de fichiers non Office que Data Guardian chiffrera, une fois ceux-ci téléchargés à partir du portail Web. Votre administrateur doit vous indiquer les types de fichiers.

REMARQUE :
Si vous téléchargez un type de fichiers qui n'est pas encore pris en charge, le contenu est illisible sur le portail Web.

Vous pouvez charger des types de fichiers non Office chiffrés ou non chiffrés. Cependant, lorsque vous téléchargez le fichier non Office, l'extension de fichier varie.

Fichiers non Office (tels que .txt ou .png)	Télécharger la description
Chiffré avant le chargement Exemple : fichiers non Office déjà chiffrés par Windows ou Mac.	Après avoir été téléchargé depuis le portail Web, l'extension de fichier, telle que .txt ou .png, est maintenue.
Fichiers non chiffrés	En cas de téléchargement depuis le portail Web, l'extension de fichier varie si votre administrateur a ajouté l'extension à une règle. Cependant, ils sont chiffrés. Exemples d'un fichier .txt téléchargé depuis le portail Web : • **nomfichier.txt** : votre administrateur a ajouté le type de fichier .txt à une règle. • **nomfichier.txt.xen** : le type de fichier .txt n'est pas inclus dans une règle. Le fichier est chiffré, mais il ajoute une extension .xen.

Si la règle *Modifier* est activée pour le portail Web, les utilisateurs peuvent modifier les fichiers non Office.

Identifier	**GUID-801B897D-9A0F-48C0-B46C-A3726B8BD9E4**
Status	**Translation Validated**

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.

Identifier	**GUID-7A2816C4-2882-4B5B-B2C6-A8032B1C4508**
Status	**Translation Validated**

Partage de documents Office protégés avec des utilisateurs externes

Avec Data Guardian, vous pouvez partager un document Office protégé via un e-mail, un support amovible, un partage réseau ou vous pouvez le télécharger sur le Cloud et le partager :

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

Lorsque vous joignez le document et cliquez sur *Envoyer*, une fenêtre de confirmation s'affiche et vous rappelle que la clé de ce document protégé sera partagée avec l'utilisateur externe.

Optimiser la sécurité en ajoutant des restrictions calendaires

Si vous le souhaitez, 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 protégé par un utilisateur externe.

1 Sélectionnez **Fichier > Informations > Restriction calendaire**.

2 Dans le menu déroulant, 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 entraîne 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, un message vous informe que vous ne pouvez pas ouvrir ce fichier avant cette échéance en raison de restrictions d'accès.

Identifier	GUID-33C8CA6C-96EE-45A8-A46A
Status	Translation Validated

Utilisation du chiffrement cloud de Data Guardian sous Windows

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 ne gère pas de client de synchronisation cloud, suivez la procédure décrite dans la section Utilisation de Data Guardian avec Windows.

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.

Identifier	GUID-FF091B7E-57FB-4625-8914-A87D018225D5
Status	Translated

Présentation des tâches pour Data Guardian avec un client de synchronisation cloud

Cette vue d'ensemble résume la séquence pour utiliser le chiffrement cloud.

REMARQUE :

Actuellement, la protection par chiffrement Cloud de Data Guardian a été désactivée sur Windows pour éviter problèmes de compatibilité avec les nouvelles fonctionnalités des prestataires de services Cloud. Pour afficher les fichiers déjà protégés par chiffrement Cloud, utilisez l'application Data GuardianMobile, le portail Web ou Data Guardian sous Mac.

Tâche	Description	Pour en savoir plus
Si des règles protègent les documents dans le cloud, installez un client de synchronisation cloud	Client de synchronisation Business ou Client de synchronisation Basic	Comptes de client de synchronisation cloud d'entreprise ou Comptes de client de synchronisation cloud de base
Afficher le client de synchronisation Cloud dans	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

Tâche	Description	Pour en savoir plus
l'Explorateur de fichiers.		
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 zone de notification	Fournit des informations utiles concernant les fichiers, les dossiers et le dépannage.	Présentation des éléments de menu de Data Guardian dans la zone de notification
Détermination d'options supplémentaires pour protéger des fichiers	En fonction de la stratégie, ces options peuvent être : · Documents Office · Types de fichiers de base	Présentation des options
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 Utilisation de Data Guardian en tant qu'utilisateur externe.

Identifier GUID-0F4189F6-3C5C-48C4-A0B0-EA6935288EEC

Status Translated

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.

REMARQUE :
Actuellement, la protection par chiffrement Cloud de Data Guardian a été désactivée sur Windows pour éviter problèmes de compatibilité avec les nouvelles fonctionnalités des prestataires de services Cloud. Pour afficher les fichiers déjà protégés par chiffrement Cloud, utilisez l'application Data GuardianMobile, le portail Web ou Data Guardian sous Mac.

Identifier	**GUID-2E518A2B-FE6C-49C1-A093-CB0DE9392011**
Status	**Translation Validated**

Installer un client de synchronisation Cloud sur Windows

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/

    REMARQUE :
    La sauvegarde et la synchronisation Google ne sont pas prises en charge.
  - 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 zone de notification, 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 zone de notification, 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 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, saisissez votre adresse e-mail de domaine et votre 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.

Identifier	**GUID-B115635A-294E-4CFF-9891-7A23A1003357**
Status	**Translation Validated**

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 Utilisation de Data Guardian en tant qu'utilisateur externe.
- Annuler le partage de dossiers

Identifier	**GUID-97FFFFE9-A9D1-4026-BB11-5726671FAE22**
Status	**Translation Validated**

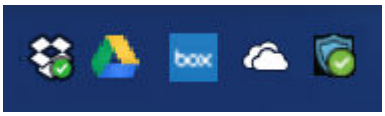
Afficher les dossiers et les fichiers sur l'ordinateur local et dans le cloud

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 zone de notification, 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.



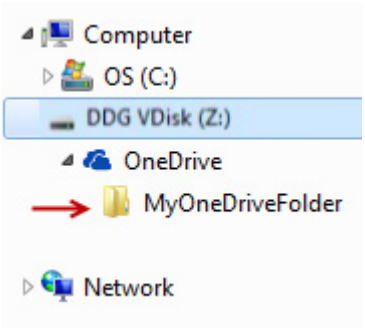
- Dans les favoris, cliquez sur l'icône Client de synchronisation.

  Lorsque vous cliquez sur l'icône Client de synchronisation dans la zone de notification ou dans Favoris, vous noterez que le Lecteur virtuel DDG vDisk s'affiche 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.



Ajout de 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 Utilisation de Data Guardian en tant qu'utilisateur externe.

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

Data Guardian chiffre 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

Pour 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.

Identifier	**GUID-C5BA22C5-E08C-424E-9431-D758B5A19D87**
Status	**Translation Validated**

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 Afficher l'accès	Lorsque la fenêtre de partage s'ouvre, assurez-vous que l'option Autoriser le téléchargement est définie sur **Oui**. 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 Afficher ou modifier l'accès	Lorsque la fenêtre d'invitation s'ouvre, vous pouvez sélectionner **Éditeur** ou **Spectateur**. Les destinataires des partages peuvent synchroniser le dossier vers leur ordinateur. Celui-ci se synchronise alors avec le Lecteur virtuel DDG vDisk.

Identifier	**GUID-398F0A82-8EBB-4931-9CB0-A63A1849DD53**
Status	**Translation Validated**

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.

Identifier	**GUID-9F26053C-CA6C-4C2D-956A-AE61838E2147**
Status	**Translation Validated**

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 .

Identifier	**GUID-1A97DE74-4DB5-445D-A0AA-6B80D2639311**
Status	**Translation Validated**

Dropbox for Business

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

Aide concernant les fournisseurs de stockage Cloud

Avant d'utiliser Data Guardian, familiarisez-vous avec le fournisseur de stockage Cloud. Voir le support 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 zone de notification, cliquez sur l'icône de Data Guardian et 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 zone de notification, 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 zone de notification 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 Zone de notification Dropbox for Business

Dans la zone de notification, 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 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 à Serveur Dell.

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.

Identifier	**GUID-E30CBE8F-03BF-4237-94D5-12962A78200E**
Status	**Translation Validated**

OneDrive Entreprise/OneDrive unifié

Data Guardian ne prend pas en charge les éléments suivants :

- Microsoft Office 365
- Partage de données dans OneDrive for Business

Aide concernant les fournisseurs 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 zone de notification, 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 Zone de notification OneDrive for Business

Dans la zone de notification :

- 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. Pour supprimer un fichier, patientez jusqu'à 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.

Identifier	**GUID-BF84B11F-886B-41AD-84C7-24614F17FD83**
Status	**Translation Validated**

Dropbox

Aide concernant les fournisseurs de stockage Cloud

Avant d'utiliser Data Guardian, familiarisez-vous avec le fournisseur de stockage Cloud. Voir le support Dropbox à l'adresse 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 zone de notification, 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 zone de notification et indique que les dossiers sont en cours de synchronisation.

Utiliser l'icône Zone de notification de Dropbox

Dans la zone de notification, 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 du 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 n'est 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 personne doit accéder au Cloud pour effacer les doublons.

Chaque utilisateur peut alors utiliser la synchronisation sélective afin de remettre le dossier dans la liste des dossiers à synchroniser.

Identifier	**GUID-2AF8CA9C-4CA7-483C-99CC-08F76D3F7744**
Status	**Translation Validated**

Box

Aide concernant les fournisseurs de stockage Cloud

Avant d'utiliser Data Guardian, familiarisez-vous avec le fournisseur de stockage Cloud. Voir l'assistance Box à l'adresse 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 zone de notification, 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 zone de notification indique que les paramètres sont appliqués. Cela peut prendre quelques minutes.

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

Utiliser l'icône de Zone de notification de Box

Dans la zone de notification, 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.

Identifier	**GUID-924AA99D-3A05-42D7-A904-4B19AA9CFB61**
Status	**Translation Validated**

Google Drive

Aide concernant les fournisseurs de stockage Cloud

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

REMARQUE :
La sauvegarde et la synchronisation Google ne sont pas prises en charge.

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 zone de notification, 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 Zone de notification

Dans la zone de notification, 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.

Identifier	**GUID-29F58BB7-31AF-43EA-9B92-23FFDA0C9709**
Status	**Translation Validated**

OneDrive

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

Aide concernant les fournisseurs de stockage Cloud

Avant d'utiliser Data Guardian, familiarisez-vous avec le fournisseur de stockage Cloud. Voir le 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 zone de notification, 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 zone de notification indique que les paramètres sont appliqués. Cela peut prendre quelques minutes.
7. Une fois l'opération terminée, accédez à **Explorateur Windows** > **OneDrive**. Les dossiers synchronisés sont affichés avec une coche.

REMARQUE :
Avec Windows 10 Falls Creator et les versions ultérieures, OneDrive utilise les fichiers d'espaces réservés. Il se peut que le lecteur virtuel DDG VDisk n'affiche pas tous vos fichiers. Dans la zone de notification, cliquez avec le bouton droit de la souris sur l'icône de OneDrive, puis sur **Paramètres**. Dans l'onglet Paramètres, cochez la case **Économiser de l'espace et télécharger les fichiers que vous souhaitez utiliser uniquement**.

Utiliser l'icône de Zone de notification de OneDrive

Dans la zone de notification :

- 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.

OneDrive et Excel pour Office 2019

Dans Excel pour Office 2019, Data Guardian bloque l'utilisation de **Fichier > Ouvrir > OneDrive** pour ouvrir les documents protégés. Un message d'erreur s'affiche pour vous le signaler. Pour ouvrir un document protégé ou pour le réenregistrer ensuite dans OneDrive, vous pouvez copier le fichier localement ou, si le *cryptage cloud* est activé dans votre entreprise, dans le lecteur virtuel *DDG VDisk*.

Identifier	**GUID-4A27A7C8-81CC-4636-8C92-14BE0EF16093**
Status	**Translation Validated**

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.

Identifier	GUID-FFED5E16-B72A-4858-A64D-
Status	Translation Validated

Installation et utilisation de Data Guardian sous Mac

Data Guardian pour Mac a intégré une aide pour les écrans spécifiques qui fournissent des informations sur les éléments suivants :

- Interface Dell Data Guardian, où les utilisateurs peuvent charger des fichiers pour les chiffrer
- Cryptage Cloud
- Utilisateurs externes et restrictions d'accès
- Altération

Dans l'interface Dell Data Guardian pour Mac, cliquez sur l'icône d'aide.

Identifier	GUID-0DB59561-F614-4FEB-9265-6F2711737741
Status	Translated

Installer le client pour Mac

Si votre administrateur vous a ajouté à la liste blanche de votre entreprise, vous pouvez vous inscrire sur : https://nomvotreserveursécurité.domaine.com:8443/cloudweb/register.

Après l'inscription, vous recevrez un e-mail vous dirigeant vers https://nomvotreserveursécurité.domaine.com:8443/cloudweb pour vous connecter et télécharger le client approprié.

Vous devez être un administrateur local.

Pour installer Data Guardian pour Mac :

1 Pour le client Data Guardian, localisez le programme d'installation dans **Dell-Data-Guardian-Mac-0.x.x.xxxx.dmg.**
2 Utilisez le fichier **.pkg** situé dans Dell-Data-Guardian-0.x.x.xxxx.dmg pour effectuer une installation ou une mise à niveau.
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 de configuration, sélectionnez l'une des actions suivantes :

Dell Security Center hébergé	Serveur Dell Management local
Solution SaaS (Software as a Service) hébergée permettant de gérer le logiciel Dell Data Security. a Sélectionnez **Dell Security Center hébergé**. b Cliquez sur **Continuer**.	Serveur sur site situé dans le réseau de l'entreprise et permettant de gérer le logiciel Dell Data Security. a Sélectionnez **Serveur Dell Management local**.

Dell Security Center hébergé	Serveur Dell Management local
c Passez à l'étape 9.	b Dans le champ *Nom du serveur de gestion Dell :*, saisissez le nom du serveur Dell 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. c Cliquez sur **Continuer**. d Passez à l'étape 9.

9 Dans la fenêtre Type d'installation, effectuez l'une des actions suivantes :

- Cliquez sur **Installer**, puis passez à l'étape 10.
- Cliquez sur **Modifier l'emplacement d'installation**.
  1 Sur la fenêtre Sélectionnez la destination, sélectionnez tous les utilisateurs. Actuellement, il s'agit de la seule option.
  2 Cliquez sur **Continuer**.
  3 Cliquez sur **Installer**, puis passez à l'étape 10.

10 Dans la boîte de dialogue, saisissez votre nom et votre mot de passe et cliquez sur **Installer le logiciel**.

11 Dans la page Résumé, cliquez sur **Fermer**.

12 Lorsque vous y êtes invité, conservez le fichier .pkg ou déplacez-le vers la *Corbeille*.

13 Effectuez l'une des opérations suivantes :

Dell Security Center hébergé	Serveur Dell Management local
La fenêtre Informations d'identification s'ouvre automatiquement une fois l'installation terminée. Si votre entreprise est multitenant, vous aurez besoin d'un ID d'installation. 1 Dans la fenêtre des informations d'identification, saisissez l'e-mail de votre compte de connexion et cliquez sur **Continuer**. 2 Effectuez l'une des opérations suivantes : • Si votre entreprise est multitenant, saisissez un ID d'installation, cliquez sur **Continuer** et poursuivez avec l'étape 3. **REMARQUE :** Si une erreur s'affiche, vérifiez vos informations d'identification. Si vous constatez une adresse électronique ou un ID d'installation erroné(e), cliquez sur **Redémarrer l'initialisation** afin de saisir de nouveau vos informations d'identification. • Pour les tenants uniques, passez à l'étape 3. 3 Dans la fenêtre Microsoft, saisissez votre mot de passe, puis cliquez sur **Connexion**. 4 Dans la fenêtre Azure, saisissez votre mot de passe. 5 Cliquez sur **Connexion**. **REMARQUE :** Si une erreur s'affiche, vérifiez vos informations d'identification. Si vous constatez une adresse électronique erronée, cliquez sur **Redémarrer l'initialisation** afin de saisir de nouveau vos informations d'identification. 6 L'interface de Dell Data Guardian s'ouvre. Voir l'application Dell Data Guardian.	1 Fermez la fenêtre .dmg pour ouvrir le Finder. 2 Reportez-vous à Activation de l'utilisateur final.

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

Identifier	**GUID-839E9A73-4125-4A28-84A6-4F5CC4D734AC**
Status	**Translated**

Activation de l'utilisateur final (local)

Activation pour Serveur Dell Management local

En mode local, lorsque vous ouvrez Dell Data Guardian pour la première fois, vous devez vous connecter pour activer :

1 Dans Finder, sélectionnez **Applications** et double-cliquez sur **Dell Data Guardian**.
2 Lorsque la fenêtre Informations d'identification s'affiche, saisissez l'adresse du Serveur Dell, par exemple : company.server.com.

REMARQUE :
Ne cochez pas la case Erreurs SSL sauf si votre administrateur vous le demande.

3 Saisissez votre adresse e-mail et votre mot de passe.
4 Cliquez sur **Connexion** pour activer Data Guardian.
5 Voir l'*application Dell Data Guardian* ci-dessous.

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

Application Dell Data Guardian

Une fois l'application Dell Data Guardian ouverte et l'activation réussie, le nom du fournisseur de stockage cloud s'affiche en gris 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'authentification pour Data Guardian est révoquée ou expire, le nom du fournisseur de stockage Cloud est également grisé.

1 Dans le volet de gauche, sélectionnez le fournisseur de stockage Cloud.
2 Une fenêtre vous demandant d'entrer vos identifiants s'affiche. Entrez vos informations d'identification.

Une fois authentifié, le nom du fournisseur de stockage cloud est activé.

Identifier	**GUID-8882A835-A7A8-4C7B-8330-3080F871A121**
Status	**Translation Validated**

Dell Security Center hébergé et tenant suspendu

Avec Dell Security Center hébergé, si un tenant ne s'acquitte pas du paiement pendant un délai spécifié, ses opérations peuvent être suspendues. Ceci s'applique à Windows, Mac, Mobile et au portail Web.

Les utilisateurs internes et externes de Data Guardian peuvent être confrontés aux situations suivantes :

- Toutes les plates-formes : si vous essayez d'installer Data Guardian, de l'activer, ou de vous connecter, une boîte de dialogue s'affiche et vous signale que les opérations du tenant sont suspendues.
- Mac : si les opérations de votre tenant sont suspendues alors que Data Guardian est ouvert, la boîte de dialogue vous informant de cette suspension s'affiche après la fermeture de l'Explorateur et de tous les fichiers, et lorsque vous essayez ensuite d'ouvrir un fichier protégé.
- Portail Web :
  - Si vous êtes déjà connecté et que vous chargez un fichier chiffré, un message vous informe de l'échec du chargement.
  - Si un fichier chiffré ou non chiffré a été chargé, puis que les opérations du tenant sont suspendues, un message indiquant l'échec du téléchargement s'affiche.
  - Si vous vous déconnectez, puis que vous tentez de vous connecter à nouveau, une boîte de dialogue s'affiche pour indiquer que les opérations du tenant sont suspendues.

Contactez votre administrateur.

Identifier	**GUID-D11E8451-72A7-4179-8693-28D0FAFF9B8B**
Status	**In Translation**

Protection d'autres applications et types de fichiers avec la protection de fichiers de base

Votre administrateur vous informera si des stratégies permettent le chiffrement d'autres applications et types de fichiers. Si une personne ouvre un fichier chiffré à l'aide de la protection de fichiers de base, mais que Data Guardian n'est pas installé sur son système, le contenu est illisible.

Vue d'ensemble de la protection de fichiers de base

Applications

Voici quelques exemples d'applications que votre administrateur voudra peut-être chiffrer :

- Bloc-notes
- Wordpad
- Visio
- MS Paint

> **REMARQUE :**
> Certaines applications ne sont que partiellement prises en charge avec Data Guardian. Si tel est le cas, votre administrateur vous en informera.

Types de fichiers

Voici quelques exemples de types de fichiers supplémentaires qui peuvent être configurés : .txt, .rtf, .csv, .odt, .vsdx, .png, .jpg, .jpeg, .jpe, .jfif, .gif, .tif, .tiff, .bmp

Windows, Mac et appareil mobile

Lorsque la stratégie de protection de fichiers de base est configurée, Data Guardian organise l'ordinateur des utilisateurs et chiffre tous les fichiers locaux portant ces extensions. Les fichiers chiffrés à l'aide de la protection de fichiers de base ne peuvent être consultés et modifiés qu'à l'aide de l'application associée à l'extension de ces fichiers.

REMARQUE :

Les fichiers contenus dans des dossiers système spécifiques ne sont pas chiffrés. Exemple : AppData. C'est également le cas pour les dossiers en relation avec des documents Office protégés, comme le dossier Documents sécurisés.

Icônes superposées pour Windows

Pour Data Guardian 2.2 et les versions ultérieures, des icônes superposées s'affichent sur les fichiers protégés dans l'Explorateur de fichiers. Si vous cliquez avec le bouton droit de la souris sur ce fichier protégé, un onglet Dell Data Guardian fournit des informations supplémentaires.

Retrait d'une extension de fichier dans Windows ou Mac

Votre administrateur peut décider de retirer une extension de fichier. Si c'est le cas, votre ordinateur est analysé pour déchiffrer ces types de fichiers.

- L'onglet *Propriétés > Dell Data Gardian* du fichier chiffré ne s'affiche plus.
- Si vous aviez des icônes en transparence, ils ne s'affichent plus.
- Le déchiffrage des fichiers peut prendre plusieurs minutes. Si un fichier avec cette extension est toujours chiffré, il a peut-être été ouvert pendant l'analyse ou stocké sur un serveur de fichiers à un autre emplacement.

Contactez votre administrateur pour demander la récupération des fichiers avec cette extension qui ne seront pas déchiffrés.

Applications Office

Vous pouvez utiliser une application Office pour ouvrir un fichier chiffré à l'aide de la protection de fichiers de base, mais son contenu sera en lecture seule.

Portail Web

Dans Paramètres > Règles, si l'option Protection de fichiers de base est définie sur Vrai, votre administrateur a ajouté des types de fichiers non Office que Data Guardian chiffrera, une fois ceux-ci téléchargés à partir du portail Web. Votre administrateur doit vous indiquer les types de fichiers.

REMARQUE :

Si vous téléchargez un type de fichiers qui n'est pas encore pris en charge, le contenu est illisible sur le portail Web.

Vous pouvez charger des types de fichiers non Office chiffrés ou non chiffrés. Cependant, lorsque vous téléchargez le fichier non Office, l'extension de fichier varie.

Fichiers non Office (tels que .txt ou .png)	Télécharger la description
Chiffré avant le chargement Exemple : fichiers non Office déjà chiffrés par Windows ou Mac.	Après avoir été téléchargé depuis le portail Web, l'extension de fichier, telle que .txt ou .png, est maintenue.
Fichiers non chiffrés	En cas de téléchargement depuis le portail Web, l'extension de fichier varie si votre administrateur a ajouté l'extension à une règle. Cependant, ils sont chiffrés. Exemples d'un fichier .txt téléchargé depuis le portail Web : • **nomfichier.txt** : votre administrateur a ajouté le type de fichier .txt à une règle. • **nomfichier.txt.xen** : le type de fichier .txt n'est pas inclus dans une règle. Le fichier est chiffré, mais il ajoute une extension .xen.

Si la règle *Modifier* est activée pour le portail Web, les utilisateurs peuvent modifier les fichiers non Office.

Identifier	GUID-FC539BCB-1939-4E0A-8A36-
Status	Translation Validated

Installation et utilisation de 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 configure une stratégie permettant d'activer Data Guardian, les fichiers sont chiffrés et sécurisés. L'application Data Guardian doit être installée sur votre périphérique mobile pour afficher les fichiers chiffrés et vous permettre de travailler avec eux.

Identifier	GUID-116F412E-15BE-4E29-A886-5A308BA693ED
Status	Translated

Conditions requises

Avant d'utiliser l'application Data Guardian, déterminez le produit qu'il vous faut en fonction de votre environnement :

Dell Security Center hébergé	Serveur Dell Management local
Si votre environnement hébergé est multitenant, vous aurez besoin d'un ID d'installation.	Assurez-vous que vous connaissez le nom du Serveur Dell, par exemple, server.domain.com. Cette information est fournie par votre administrateur.

Identifier	GUID-A802F8F9-1B8F-47DD-8525-518A4C004221
Status	Translation Validated

Mise en route de Data Guardian Mobile

Suivez la procédure suivante si vous utilisez Data Guardian Mobile.

Tâche	Description	Voir cette section
Installation de Data Guardian - déterminer une option :	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
Détermination des stratégies s'appliquant aux périphériques mobiles	Votre administrateur vous indiquera les stratégies qui s'appliquent.	Vous pouvez disposer des éléments suivants : • Documents Office protégés • Protection cloud • Options supplémentaires

Tâche	Description	Voir cette section
Parcourir le gestionnaire de fichiers	Voir les options de Data Guardian.	Parcourir le gestionnaire de fichiers
Si la stratégie de protection cloud est activée, accédez au compte de votre fournisseur de stockage cloud	Sur l'appareil, accédez à l'écran Gestionnaire de fichiers de l'application Data Guardian et cliquez sur votre fournisseur de stockage Cloud.	Voir Accès au compte de votre fournisseur de stockage cloud.

En fonction des stratégies Data Guardian, vous pouvez disposer des éléments suivants :

- Les fichiers Office protégés (.docx, .pptx, .xlsx, .docm, .pptm, .xlsm, .pdf) conservent leur extension de fichier.
- Les applications supplémentaires et les types de fichiers, par exemple .txt.
- Les fichiers non Office du cloud portent une extension .xen.

Sur les périphériques mobiles dotés de Data Guardian, vous pouvez effectuer les actions suivantes :

- Suppression de dossiers et fichiers
- Supprimer des dossiers et des fichiers
- Partage d'un document avec un utilisateur externe (si la stratégie est activée pour les observateurs externes)

Identifier	**GUID-618A6EAF-794D-4077-A675-AC9ACA624CC3**
Status	**Translated**

Installation ou désinstallation de Data Guardian sur un appareil iOS via l'App Store

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 Touchez la case à cocher pour accepter le contrat de licence.

4 Sélectionnez l'une des options suivantes :

Dell Security Center hébergé	Local
Solution SaaS (Software as a Service) hébergée permettant de gérer le logiciel Dell Data Security. a Appuyez sur **Dell Security Center hébergé.** b Saisissez votre adresse e-mail. c Cliquez sur **Envoyer**. **REMARQUE :** Si votre adresse e-mail apparaît pour plus d'un tenant, saisissez votre ID d'installation. d Dans la fenêtre Microsoft Azure, saisissez votre mot de passe. e Cliquez sur **Se connecter**.	Serveur sur site situé dans le réseau de l'entreprise et permettant de gérer le logiciel Dell Data Security. a Appuyez sur **Local**. b Dans le champ Serveur de l'écran d'ouverture de session, saisissez le nom du Serveur Dell de votre entreprise, par exemple : serveur.domaine.com. c Entrez votre nom d'utilisateur et votre mot de passe. d Cliquez sur **Se connecter**.

Votre compte est désormais activé et l'écran Gestionnaire de fichiers de Data Guardian s'affiche.

En fonction de la règle définie par votre entreprise, vous serez peut-être invité à créer un code PIN.

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**.

Identifier	**GUID-7247F5B1-D730-4DE6-97BA-7E88AD40B7E4**
Status	**Translated**

Installation ou désinstallation de Data Guardian sur un appareil iOS avec Workspace ONE

Si Workspace ONE est installé, vous pouvez vous authentifier sur Data Guardian à l'aide de l'authentification unique. Ces étapes sont identiques pour Dell Security Center hébergé ou le Serveur Dell Management local.

Votre administrateur transmet l'application Data Guardian sur votre appareil.

1 Lorsque vous êtes invité à indiquer si vous souhaitez installer l'application **Data Guardian**, cliquez sur **OK**.
2 Lancez l'application **Data Guardian**.
3 Dans le contrat de licence, cliquez sur **Accepter**.
4 Dans l'option pour sélectionner Workspace ONE ou Data Guardian, cliquez sur **Workspace ONE** pour que l'authentification unique s'affiche.
5 Saisissez le mot de passe.

Votre compte est désormais activé et l'écran Gestionnaire de fichiers de Data Guardian s'affiche.

En fonction de la règle définie par votre entreprise, vous serez peut-être invité à créer un code PIN. Si vous vous connectez à Workspace One, il vous suffit de saisir votre code PIN pour Data Guardian.

Identifier	**GUID-D045F8A7-9124-4843-BAF6-E0BB27CE1046**
Status	**Translated**

Installation ou désinstallation de Data Guardian sur un appareil Android via Google Play

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 Touchez la case à cocher pour accepter le contrat de licence.
4 Sélectionnez l'une des options suivantes :

Dell Security Center hébergé	Serveur Dell Management local
Solution SaaS (Software as a Service) hébergée permettant de gérer le logiciel Dell Data Security. a Cliquez sur **Hébergé**. b Saisissez votre adresse e-mail. c Cliquez sur **Envoyer**.	Serveur sur site situé dans le réseau de l'entreprise et permettant de gérer le logiciel Dell Data Security. a Appuyez sur **Local**. b Dans le champ Serveur de l'écran d'ouverture de session, saisissez le nom du Serveur Dell de votre entreprise, par exemple : serveur.domaine.com. c Entrez votre nom d'utilisateur et votre mot de passe. d Cliquez sur **Se connecter**.

Dell Security Center hébergé	Serveur Dell Management local

REMARQUE :
Si votre adresse e-mail apparaît pour plus d'un tenant, saisissez votre ID d'installation.

d Dans la fenêtre Microsoft Azure, saisissez votre mot de passe.

e Cliquez sur **Se connecter**.

Votre compte est désormais activé et l'écran Gestionnaire de fichiers de Data Guardian s'affiche.

En fonction de la règle définie par votre entreprise, vous serez peut-être invité à créer un code PIN.

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 longuement sur l'icône **Data Guardian**.
4 Faites glisser l'icône vers l'option Désinstaller.
5 Appuyez sur **OK**.

Identifier	**GUID-37A6FDB2-CD4D-4EB3-BDE1-EC151BC08814**
Status	**Translated**

Installation ou désinstallation de Data Guardian sur un appareil Android avec Workspace ONE

Si Workspace ONE est installé, vous pouvez vous authentifier sur Data Guardian à l'aide de l'authentification unique. Ces étapes sont identiques pour Dell Security Center hébergé ou le Serveur Dell Management local.

1 Sur votre appareil, cliquez sur **Hub**.
2 Cliquez sur **Catalogue d'applications**.
3 Dans l'application Dell Data Guardian, cliquez sur **Installer**.
4 Dans *Confirmer l'installation*, cliquez sur **Installer**.
5 Dans *Google Play Protect*, cliquez sur **Autoriser**.
6 Dans le message indiquant que l'application est installée, cliquez sur **Terminer**.
7 Cliquez sur **Ouvrir** pour lancer l'applicationData Guardian.
8 Dans l'option permettant d'authentifier à l'aide de Workspace One ou Data Guardian, cliquez sur **Workspace One** pour que l'authentification unique s'affiche.
9 Dans le contrat de licence, désactivez la case.
10 Cliquez sur **Authentification unique**.

Votre compte est désormais activé et l'écran Data Guardian de Data Guardian s'affiche.

En fonction de la règle définie par votre entreprise, vous serez peut-être invité à créer un code PIN. Si vous vous connectez à Workspace One, il vous suffit de saisir votre code PIN pour Data Guardian.

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 longuement sur l'icône **Data Guardian**.
4 Faites glisser l'icône vers l'option Désinstaller.

5 Appuyez sur **OK**.

Identifier	**GUID-5B8DFEFC-DC7C-42AE-A662-627068964BC8**
Status	**Translation Validated**

Parcourir le gestionnaire de fichiers

Dans le gestionnaire de fichiers de Data Guardian, vous pouvez utiliser le stockage local ou le cloud. Le gestionnaire de fichiers s'ouvre lorsque vous ouvrez Data Guardian.

Écran Gestionnaire de fichiers

Les dossiers par défaut pour l'écran Gestionnaire de fichiers incluent, par exemple :

- Documents
- Téléchargements
- Photos

Création d'un nouvel écran

Cliquez sur l'icône Ajouter (**+**) et l'écran *Créer* s'affiche avec les options suivantes :

- Document
- Tableur
- Présentation (PowerPoint)
- Photo
- Folder (Dossier)
- Service cloud

Options du tiroir de navigation

Cliquez sur l'icône du tiroir de navigation. Les options comprennent :

- **Navigateur**
- **Gestionnaire de fichiers**
- Icône **Paramètres** :
  - Bouton **Modifier le code PIN** (si cette fonction est activée par la stratégie)
  - **Navigateur**
  - **Gestionnaire de fichiers (Paramètres)** : utiliser ces options
    - **Intervalle d'actualisation** : fréquence à laquelle Data Guardian synchronise vos services Cloud. Dell vous recommande les options *Manuel* ou *Tous les jours*. Les autres options disponibles sont les suivantes : *Toutes les heures* ou *Toutes les semaines*.
    - **Avertissement de téléchargement 10 Mo** : activer ou désactiver. Utilisez cette option si vous n'êtes pas connecté au Wi-Fi et que la taille de téléchargement dépasse 10 Mo.
    - **Effacer le cache** : efface les fichiers temporaires.
  - **À propos** : voir la section Règles et version de Data Guardian
  - Bouton **Quitter Data Guardian**
  - **Comptes Cloud** : indique s'ils sont liés ou dissociés.
- **Navigateur**

- **Gestionnaire de fichiers** : pour revenir à l'écran Gestionnaire de fichiers.
- **Verrouillage de Data Guardian**

Options supplémentaires

- Ajouter un fichier aux favoris
  - Pour iOS, voir le menu-tiroir de navigation.
  - Pour Android, appuyez longuement sur le nom du fichier.

Identifier	**GUID-8826272C-679E-40FF-B0A9-D1C9888AF6E5**
Status	**Translation Validated**

Détermination des stratégies pour Data Guardian Mobile

Votre administrateur vous indiquera quelles sont les stratégies configurées pour votre entreprise.

Identifier	**GUID-4C1E2DAD-C0CA-4E6F-96D4-0297C01CE8B2**
Status	**Translation Validated**

Affichage des stratégies et de la version de Data Guardian

Certaines stratégies Data Guardian sont répertoriées dans **À propos de**. Pour afficher ces stratégies ou la version de Data Guardian :

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

2 Appuyez sur **Règle**.

Selon les règles définies par votre administrateur, la liste peut inclure les éléments suivants :

- Longueur de PIN
- Délai d'expiration après une période d'inactivité
- Échec de connexion
- Copier et coller : vous permet de copier depuis un document protégé vers un document protégé.

Version

3 Déterminez d'autres options de stratégie.

Celles-ci peuvent inclure :

- Documents Office protégés
- Protection cloud
- Stratégies supplémentaires

Identifier	**GUID-3613C9F0-10DE-4A67-9158-1964C8D2D77E**
Status	**Translation Validated**

Utilisation des documents Office protégés avec Mobile

Votre administrateur vous indiquera quelles sont les options activées pour votre entreprise. Lorsque vous avez installé Data Guardian et ouvert un document Office protégé, un message s'affiche et indique que le document est en cours de déchiffrement.

Options Data Guardian pour les documents Office

Ces options Data Guardian s'affichent.

- **Créer** : en fonction de la configuration de la stratégie, le document est protégé dès que vous le créez. L'en-tête de ce fichier affiche *Document protégé*.
- **Copier/Coller** : avec un document Office protégé, vous pouvez uniquement copier vers un autre document Office protégé.
- **Imprimer** : en fonction d'autres paramètres de stratégie, vous aurez peut-être un filigrane lorsque vous imprimez.
- **Exporter** : en fonction d'autres paramètres de règle, vous aurez peut-être un filigrane lorsque vous exporterez.

Lorsqu'un document Office est ouvert, cliquez sur l'icône dans le coin supérieur gauche pour ces options :

- **Enregistrer**
- **Enregistrer sous**
- **Exporter**
- **Quitter**

Options Office supplémentaires en fonction de la règle :

- **Modifier** : vous pouvez modifier les fichiers Office .docx et .ppt.

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

- **Filigranes masqués** : en fonction de la stratégie, les documents Office protégés peuvent disposer d'un filigrane masqué qui identifie l'utilisateur. Si vous imprimez ou partagez le document, le filigrane demeure.
- **Filigrane affiché à l'écran** : lorsqu'un document Office protégé est ouvert, un filigrane s'affiche sur l'écran du client.

Informations supplémentaires pour les documents Office

Documents Office protégés hors ligne

Lorsque vous créez un document Office protégé ou un document protégé prenant en charge les macros 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.

Résolution des problèmes liés aux documents Office protégés

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.

Identifier	GUID-D11E8451-72A7-4179-8693-28D0FAFF9B8B
Status	In Translation

Protection d'autres applications et types de fichiers avec la protection de fichiers de base

Votre administrateur vous informera si des stratégies permettent le chiffrement d'autres applications et types de fichiers. Si une personne ouvre un fichier chiffré à l'aide de la protection de fichiers de base, mais que Data Guardian n'est pas installé sur son système, le contenu est illisible.

Vue d'ensemble de la protection de fichiers de base

Applications

Voici quelques exemples d'applications que votre administrateur voudra peut-être chiffrer :

- Bloc-notes
- Wordpad
- Visio
- MS Paint

> **REMARQUE :**
> Certaines applications ne sont que partiellement prises en charge avec Data Guardian. Si tel est le cas, votre administrateur vous en informera.

Types de fichiers

Voici quelques exemples de types de fichiers supplémentaires qui peuvent être configurés : .txt, .rtf, .csv, .odt, .vsdx, .png, .jpg, .jpeg, .jpe, .jfif, .gif, .tif, .tiff, .bmp

Windows, Mac et appareil mobile

Lorsque la stratégie de protection de fichiers de base est configurée, Data Guardian organise l'ordinateur des utilisateurs et chiffre tous les fichiers locaux portant ces extensions. Les fichiers chiffrés à l'aide de la protection de fichiers de base ne peuvent être consultés et modifiés qu'à l'aide de l'application associée à l'extension de ces fichiers.

> **REMARQUE :**
> Les fichiers contenus dans des dossiers système spécifiques ne sont pas chiffrés. Exemple : AppData. C'est également le cas pour les dossiers en relation avec des documents Office protégés, comme le dossier Documents sécurisés.

Icônes superposées pour Windows

Pour Data Guardian 2.2 et les versions ultérieures, des icônes superposées s'affichent sur les fichiers protégés dans l'Explorateur de fichiers. Si vous cliquez avec le bouton droit de la souris sur ce fichier protégé, un onglet Dell Data Guardian fournit des informations supplémentaires.

Retrait d'une extension de fichier dans Windows ou Mac

Votre administrateur peut décider de retirer une extension de fichier. Si c'est le cas, votre ordinateur est analysé pour déchiffrer ces types de fichiers.

- L'onglet *Propriétés > Dell Data Gardian* du fichier chiffré ne s'affiche plus.
- Si vous aviez des icônes en transparence, ils ne s'affichent plus.
- Le déchiffrage des fichiers peut prendre plusieurs minutes. Si un fichier avec cette extension est toujours chiffré, il a peut-être été ouvert pendant l'analyse ou stocké sur un serveur de fichiers à un autre emplacement.

Contactez votre administrateur pour demander la récupération des fichiers avec cette extension qui ne seront pas déchiffrés.

Applications Office

Vous pouvez utiliser une application Office pour ouvrir un fichier chiffré à l'aide de la protection de fichiers de base, mais son contenu sera en lecture seule.

Portail Web

Dans Paramètres > Règles, si l'option Protection de fichiers de base est définie sur Vrai, votre administrateur a ajouté des types de fichiers non Office que Data Guardian chiffrera, une fois ceux-ci téléchargés à partir du portail Web. Votre administrateur doit vous indiquer les types de fichiers.

REMARQUE :
Si vous téléchargez un type de fichiers qui n'est pas encore pris en charge, le contenu est illisible sur le portail Web.

Vous pouvez charger des types de fichiers non Office chiffrés ou non chiffrés. Cependant, lorsque vous téléchargez le fichier non Office, l'extension de fichier varie.

Fichiers non Office (tels que .txt ou .png)	Télécharger la description
Chiffré avant le chargement Exemple : fichiers non Office déjà chiffrés par Windows ou Mac.	Après avoir été téléchargé depuis le portail Web, l'extension de fichier, telle que .txt ou .png, est maintenue.
Fichiers non chiffrés	En cas de téléchargement depuis le portail Web, l'extension de fichier varie si votre administrateur a ajouté l'extension à une règle. Cependant, ils sont chiffrés. Exemples d'un fichier .txt téléchargé depuis le portail Web : • **nomfichier.txt** : votre administrateur a ajouté le type de fichier .txt à une règle. • **nomfichier.txt.xen** : le type de fichier .txt n'est pas inclus dans une règle. Le fichier est chiffré, mais il ajoute une extension .xen.

Si la règle *Modifier* est activée pour le portail Web, les utilisateurs peuvent modifier les fichiers non Office.

Identifier	**GUID-36644E42-9324-479F-8128-F89D438E8F17**
Status	**Translation Validated**

Utilisation de la protection cloud avec Mobile

Si votre administrateur active la protection cloud, vous avez besoin des deux applications suivantes :

- Application de client de synchronisation cloud : voir l'aide en ligne au sujet de ce client de synchronisation cloud.
- L'application Data Guardian Mobile répertorie le client de synchronisation cloud utilisé par votre société et vous permet de le télécharger.

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 document 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.

Accès au compte de votre fournisseur de stockage cloud

Pour accéder au compte de votre fournisseur de stockage cloud :

1 Sur l'écran du gestionnaire de fichiers, cliquez sur l'icône Ajouter (**+**).

2 Appuyez sur **Service cloud**.

Une règle Data Guardian détermine les fournisseurs de stockage cloud à afficher. Votre administrateur peut désigner un ou plusieurs fournisseurs de stockage cloud spécifiques à utiliser au sein de l'entreprise et bloquer les autres.

3 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.

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.

Utilisation de la protection cloud

Sur les périphériques mobiles dotés de Data Guardian, vous pouvez effectuer les actions suivantes :

- 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.

- 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.

- **Fichier > Copier** : selon la règle définie par votre administrateur, vous pouvez copier un fichier d'un fournisseur cloud vers un autre fournisseur.
- Pour Android avec OneDrive ou 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 le périphérique.

Dissocier le 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 > Gestionnaire de fichiers > Service cloud**. Lorsque vous donnez accès à un fournisseur de stockage Cloud, une coche s'affiche dans la case à cocher.

2 Effectuez l'une des opérations suivantes :

Android

a Appuyez sur **Lié**.

b Appuyez sur **Oui**.

iOS

a Cliquez sur **Dissocié**.

Cette opération supprime l'accès à Data Guardian et ses fichiers. Cependant, elle n'entraîne pas la suppression des fichiers issus du Cloud.

Résolution des problèmes liés à la protection cloud

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.

Identifier	**GUID-19337C15-12E9-4E8D-B908-29416128B500**
Status	**Translation Validated**

Utilisation d'autres stratégies avec Mobile

Votre administrateur vous indiquera laquelle de ces stratégies a été configurée pour votre entreprise.

Utiliser un code PIN

Votre administrateur peut définir une règle nécessitant un code PIN et définir sa longueur.

Altération

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

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.

Identifier	**GUID-21086952-1999-4F9B-A47C-C57073C7C715**
Status	**Translation Validated**

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 Serveur Dell. 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.

REMARQUE :

La sauvegarde et la synchronisation Google ne sont pas prises en charge.

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 Microsoft. De ce fait, laissez le téléchargement des fichiers se terminer avant de procéder à l'annulation.

Identifier	**GUID-46C6144D-AF30-4559-96AC-39DB1738D2D8**
Status	**Translation Validated**

Journaux

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

Identifier	**GUID-8882A835-A7A8-4C7B-8330-3080F871A121**
Status	**Translation Validated**

Dell Security Center hébergé et tenant suspendu

Avec Dell Security Center hébergé, si un tenant ne s'acquitte pas du paiement pendant un délai spécifié, ses opérations peuvent être suspendues. Ceci s'applique à Windows, Mac, Mobile et au portail Web.

Les utilisateurs internes et externes de Data Guardian peuvent être confrontés aux situations suivantes :

- Toutes les plates-formes : si vous essayez d'installer Data Guardian, de l'activer, ou de vous connecter, une boîte de dialogue s'affiche et vous signale que les opérations du tenant sont suspendues.
- Mac : si les opérations de votre tenant sont suspendues alors que Data Guardian est ouvert, la boîte de dialogue vous informant de cette suspension s'affiche après la fermeture de l'Explorateur et de tous les fichiers, et lorsque vous essayez ensuite d'ouvrir un fichier protégé.
- Portail Web :
  - Si vous êtes déjà connecté et que vous chargez un fichier chiffré, un message vous informe de l'échec du chargement.
  - Si un fichier chiffré ou non chiffré a été chargé, puis que les opérations du tenant sont suspendues, un message indiquant l'échec du téléchargement s'affiche.
  - Si vous vous déconnectez, puis que vous tentez de vous connecter à nouveau, une boîte de dialogue s'affiche pour indiquer que les opérations du tenant sont suspendues.

Contactez votre administrateur.

Identifier	**GUID-66FB1CE0-6669-4DDD-80E8-BCBAA27D4E13**
Status	**Translation Validated**

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.

Identifier	GUID-BDAC1DD8-21C2-4ED1-B0A
Status	Translation Validated

Affichage ou modification de fichiers protégés sur un client Web

Si votre administrateur configure un portail Web pour Data Guardian, vous pouvez créer un lien vers une URL pour ce client Web et afficher des fichiers chiffrés sans avoir à installer de client Data Guardian. En fonction des règles définies, vous pouvez également modifier un fichier.

En fonction de la stratégie configurée par votre administrateur, vous pouvez également consulter les éléments suivants :

- Documents Office protégés : .docx, .pptx, .xlsx, .docm, .pptm, .xlsm, .pdf.
- Fichiers .xen : fichiers Office ou autre chiffrés par Data Guardian lorsque de leur chargement vers le cloud.
- Autres types de fichiers, par exemple Bloc-notes.

Identifier	GUID-C468D78F-0ADF-45FC-B5A2-44B933EB2497
Status	Translation Validated

Accès au portail Web pour Data Guardian

Les étapes varient légèrement selon le navigateur utilisé.

1 Procurez-vous l'adresse URL auprès de votre administrateur pour accéder au portail Web.
2 Cliquez sur l'URL.
Si vous obtenez un avertissement, cliquez sur **Continuer** ou **Poursuivre**.
3 À l'écran Contrat de licence, cliquez sur **Accepter**.
Si vous obtenez un avertissement, cliquez sur **Continuer** ou **Poursuivre**.
4 Entrez vos informations d'identification de domaine.
5 Cliquez sur **Connexion**.
6 Si le système vous invite à effectuer un suivi de votre emplacement, sélectionnez une option.
7 Pour afficher ou modifier des fichiers, voir l'aide en ligne disponible à partir du portail Web Data Guardian.

REMARQUE :
Pour Mac, vous devez configurer Safari pour autoriser l'affichage des fenêtres contextuelles.

Identifier	GUID-D11E8451-72A7-4179-8693-28D0FAFF9B8B
Status	In Translation

Protection d'autres applications et types de fichiers avec la protection de fichiers de base

Votre administrateur vous informera si des stratégies permettent le chiffrement d'autres applications et types de fichiers. Si une personne ouvre un fichier chiffré à l'aide de la protection de fichiers de base, mais que Data Guardian n'est pas installé sur son système, le contenu est illisible.

Vue d'ensemble de la protection de fichiers de base

Applications

Voici quelques exemples d'applications que votre administrateur voudra peut-être chiffrer :

- Bloc-notes
- Wordpad
- Visio
- MS Paint

> **REMARQUE :**
> Certaines applications ne sont que partiellement prises en charge avec Data Guardian. Si tel est le cas, votre administrateur vous en informera.

Types de fichiers

Voici quelques exemples de types de fichiers supplémentaires qui peuvent être configurés : .txt, .rtf, .csv, .odt, .vsdx, .png, .jpg, .jpeg, .jpe, .jfif, .gif, .tif, .tiff, .bmp

Windows, Mac et appareil mobile

Lorsque la stratégie de protection de fichiers de base est configurée, Data Guardian organise l'ordinateur des utilisateurs et chiffre tous les fichiers locaux portant ces extensions. Les fichiers chiffrés à l'aide de la protection de fichiers de base ne peuvent être consultés et modifiés qu'à l'aide de l'application associée à l'extension de ces fichiers.

> **REMARQUE :**
> Les fichiers contenus dans des dossiers système spécifiques ne sont pas chiffrés. Exemple : AppData. C'est également le cas pour les dossiers en relation avec des documents Office protégés, comme le dossier Documents sécurisés.

Icônes superposées pour Windows

Pour Data Guardian 2.2 et les versions ultérieures, des icônes superposées s'affichent sur les fichiers protégés dans l'Explorateur de fichiers. Si vous cliquez avec le bouton droit de la souris sur ce fichier protégé, un onglet Dell Data Guardian fournit des informations supplémentaires.

Retrait d'une extension de fichier dans Windows ou Mac

Votre administrateur peut décider de retirer une extension de fichier. Si c'est le cas, votre ordinateur est analysé pour déchiffrer ces types de fichiers.

- L'onglet *Propriétés > Dell Data Gardian* du fichier chiffré ne s'affiche plus.
- Si vous aviez des icônes en transparence, ils ne s'affichent plus.
- Le déchiffrage des fichiers peut prendre plusieurs minutes. Si un fichier avec cette extension est toujours chiffré, il a peut-être été ouvert pendant l'analyse ou stocké sur un serveur de fichiers à un autre emplacement.

Contactez votre administrateur pour demander la récupération des fichiers avec cette extension qui ne seront pas déchiffrés.

Applications Office

Vous pouvez utiliser une application Office pour ouvrir un fichier chiffré à l'aide de la protection de fichiers de base, mais son contenu sera en lecture seule.

Portail Web

Dans Paramètres > Règles, si l'option Protection de fichiers de base est définie sur Vrai, votre administrateur a ajouté des types de fichiers non Office que Data Guardian chiffrera, une fois ceux-ci téléchargés à partir du portail Web. Votre administrateur doit vous indiquer les types de fichiers.

REMARQUE :
Si vous téléchargez un type de fichiers qui n'est pas encore pris en charge, le contenu est illisible sur le portail Web.

Vous pouvez charger des types de fichiers non Office chiffrés ou non chiffrés. Cependant, lorsque vous téléchargez le fichier non Office, l'extension de fichier varie.

Fichiers non Office (tels que .txt ou .png)	Télécharger la description
Chiffré avant le chargement Exemple : fichiers non Office déjà chiffrés par Windows ou Mac.	Après avoir été téléchargé depuis le portail Web, l'extension de fichier, telle que .txt ou .png, est maintenue.
Fichiers non chiffrés	En cas de téléchargement depuis le portail Web, l'extension de fichier varie si votre administrateur a ajouté l'extension à une règle. Cependant, ils sont chiffrés. Exemples d'un fichier .txt téléchargé depuis le portail Web : • **nomfichier.txt** : votre administrateur a ajouté le type de fichier .txt à une règle. • **nomfichier.txt.xen** : le type de fichier .txt n'est pas inclus dans une règle. Le fichier est chiffré, mais il ajoute une extension .xen.

Si la règle *Modifier* est activée pour le portail Web, les utilisateurs peuvent modifier les fichiers non Office.

Identifier	**GUID-8882A835-A7A8-4C7B-8330-3080F871A121**
Status	**Translation Validated**

Dell Security Center hébergé et tenant suspendu

Avec Dell Security Center hébergé, si un tenant ne s'acquitte pas du paiement pendant un délai spécifié, ses opérations peuvent être suspendues. Ceci s'applique à Windows, Mac, Mobile et au portail Web.

Les utilisateurs internes et externes de Data Guardian peuvent être confrontés aux situations suivantes :

- Toutes les plates-formes : si vous essayez d'installer Data Guardian, de l'activer, ou de vous connecter, une boîte de dialogue s'affiche et vous signale que les opérations du tenant sont suspendues.
- Mac : si les opérations de votre tenant sont suspendues alors que Data Guardian est ouvert, la boîte de dialogue vous informant de cette suspension s'affiche après la fermeture de l'Explorateur et de tous les fichiers, et lorsque vous essayez ensuite d'ouvrir un fichier protégé.

- Portail Web :
  - Si vous êtes déjà connecté et que vous chargez un fichier chiffré, un message vous informe de l'échec du chargement.
  - Si un fichier chiffré ou non chiffré a été chargé, puis que les opérations du tenant sont suspendues, un message indiquant l'échec du téléchargement s'affiche.
  - Si vous vous déconnectez, puis que vous tentez de vous connecter à nouveau, une boîte de dialogue s'affiche pour indiquer que les opérations du tenant sont suspendues.

Contactez votre administrateur.

Identifier	GUID-FF3D5442-1632-454D-8787-1
Status	Translation Validated

Utilisation de 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.

Les utilisateurs externes doivent respecter la configuration requise pour le serveur. En outre, le domaine ou l'utilisateur ne doivent pas être sur la liste noire de l'entreprise.

Pour un environnement hébergé, les utilisateurs externes peuvent activer uniquement un tenant.

Les options pour les utilisateurs externes sont les suivantes :

- **Windows** : télécharger et installer un client Data Guardian. Voir les sections Tâches de l'utilisateur interne sous Windows et Tâches de l'utilisateur externe.
- **Mac** : voir la section Utilisateur externe et Mac.
- **Mobile**
- **Portail Web** : au lieu de télécharger un client Data Guardian, utilisez le portail Web de Data Guardian. Les utilisateurs externes peuvent afficher un document Office protégé au format de fichier .pdf ou .xen. Selon la règle, l'utilisateur externe peut modifier le fichier. Reportez-vous à Utilisateur externe et portail Web.

Identifier	GUID-EBDBAE23-A90F-4603-934B-6B40EE93C248
Status	Translated

Tâches de l'utilisateur interne sous Windows

Pour partager des fichiers protégés avec un utilisateur externe, vous pouvez :

- Utiliser l'option *Accès au fichier protégé* avec les documents Office protégés
- Approuver ou refuser la demande d'accès d'un utilisateur externe
- Envoyer un document Office protégé ou un fichier au format .xen via un e-mail Outlook.
- Chiffrement Cloud et fichiers non-Office au format .xen fichiers : créer un dossier à partager sur le client de synchronisation, ajouter des fichiers, puis accorder l'accès. Les étapes peuvent varier en fonction de la méthode que vous employez ou du client de synchronisation utilisé.

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 de la souris sur un fichier protégé et sélectionnez **Accès au fichier protégé**. Vous pouvez sélectionner jusqu'à 50 fichiers maximum. La fenêtre Accès partagé à un document protégé s'ouvre. Les fichiers peuvent se trouver aux emplacements suivants :
   - Dossier local ou lecteur réseau
   - E-mail
   - Média amovible
   - Partage réseau
2 Dans le champ *E-mail à partager* en haut à droite, 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 les utilisateurs externes qui ne sont pas encore inscrits de la réception d'un e-mail de votre part contenant des instructions leur permettant de s'inscrire à un Serveur Dell, de télécharger et d'activer Data Guardian et d'afficher 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.

Envoi d'un fichier protégé via un e-mail Outlook

Lorsque vous joignez un fichier protégé et cliquez sur *Envoyer*, une invite de confirmation vous rappelle que la clé du fichier protégé sera partagée.

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

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 documents 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 aux fichiers individuels de ce dossier que vous souhaitez partager.

Identifier	**GUID-967BF32F-F6F1-4C5A-BA0B-34CA9F73A438**
Status	**Translation Validated**

Tâches de l'utilisateur externe sous Windows

Un utilisateur interne peut décider de vous accorder l'accès aux fichiers protégés. Vous pouvez recevoir les éléments suivants :

- Un e-mail contenant les instructions relatives à l'inscription
- Un fichier protégé dont la page de garde contient un lien pour inscrire une adresse e-mail valide

> **REMARQUE :**
> La page de garde répertorie le nom du serveur Serveur Dell pour l'option local ou un ID d'installation pour ce tenant spécifique si votre Dell Security Center hébergé est multitenant. La page de garde contient également des liens pour télécharger le client Data Guardian.

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

- S'enregistrer dans Data Guardian
- Télécharger et 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 Effectuez l'une des opérations suivantes :
   - E-mail : cliquez sur **Accepter**.
   - Document protégé affichant un avertissement sur la page de garde : cliquez sur le lien fourni pour enregistrer une adresse e-mail valide.

2 Suivez l'ensemble d'étapes définies en fonction de l'environnement de votre entreprise :

Dell Security Center hébergé	Serveur Dell Management local
Solution SaaS (Software as a Service) hébergée permettant de gérer le logiciel Dell Data Security.	Serveur sur site situé dans le réseau de l'entreprise et permettant de gérer le logiciel Dell Data Security.
a Lorsque le portail Web Dell Data Guardian s'ouvre, saisissez votre adresse e-mail. b Faites défiler la page et cliquez sur **J'accepte**. c Dans la fenêtre Dell Security Center, faites défiler la liste jusqu'à *Besoin d'un compte ?* et cliquez sur **S'inscrire**.	**REMARQUE :** Pour local, vous pouvez installer Data Guardian avant de vous inscrire. Lorsque vous essayez d'activer, cliquez sur le lien d'**inscription** disponible. a Lorsque la fenêtre Data Guardian de Dell s'ouvre, entrez votre adresse e-mail.

Dell Security Center hébergé

d Sur la page du nouveau compte, saisissez une adresse e-mail, un prénom, un nom de famille et un mot de passe. Le mot de passe doit comporter au moins huit caractères et contenir une minuscule, une majuscule, un caractère spécial et un chiffre.

e Cliquez sur **Se connecter**.

f Accédez à l'adresse e-mail que vous avez utilisée pour vous inscrire, récupérez le code de vérification et saisissez-le.

> **REMARQUE :**
> Si vous ne voyez aucun e-mail, vérifiez le courrier indésirable.

g Cliquez sur **Confirmer le compte**. Si le compte est vérifié, le portail Web s'ouvre.

h Faites glisser les fichiers protégés dans le portail Web, puis cliquez sur **Charger maintenant**.

i Vous recevrez un e-mail de bienvenue après vous être inscrit. Cet e-mail contient un lien permettant de télécharger un client Windows.

> **REMARQUE :**
> Si votre Dell Security Center hébergé est multitenant, l'e-mail répertorie également un ID d'installation dont vous aurez besoin.

Serveur Dell Management local

b Cliquez sur **S'inscrire**.

c Sur la page S'inscrire, saisissez votre mot de passe et confirmez-le, puis cliquez sur **Se connecter**.
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. Si vous ne voyez aucun e-mail, vérifiez le courrier indésirable.

d Dans l'e-mail de vérification de compte de Serveur Dell, cliquez sur le lien hypertexte.

> **REMARQUE :**
> Si vous ne voyez aucun e-mail, vérifiez le courrier indésirable.

e Continuez vers la page Web.

f Sur la page Confirmation, cliquez sur **Poursuivre la connexion**.

g Sur la page Connexion, cliquez sur **Mot de passe oublié**.

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

h 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.

i Ouvrez l'e-mail d'activation de compte et cliquez sur le lien.
L'e-mail comporte aussi le nom de Serveur Dell à utiliser lors de l'installation de Data Guardian.

j Sur la page Se connecter, saisissez l'adresse e-mail et le mot de passe utilisés pour vous enregistrer.

k Cliquez sur **Connexion**.
Une page de téléchargement Data Guardian s'ouvre.

Télécharger et installer Data Guardian pour Windows

Une fois inscrit, vous pouvez cliquer sur un lien permettant de télécharger un client Windows. En fonction des éléments fournis par l'utilisateur interne au début, les liens peuvent être disponibles ici :

- S'il s'agit d'un Security Management Server, une page Téléchargement s'ouvre avec des options pour le client Windows.
- Dans le cas d'un serveur Security Management Server Virtual, le fait de cliquer sur Windows vous redirige vers le site dell.com/support.
- Si vous avez reçu un fichier protégé, la page de garde contient des liens pour télécharger un client.
- Il est possible que vous receviez un e-mail de bienvenue avec des liens pour le téléchargement d'un client.

Les étapes suivantes décrivent l'installation de Data Guardian sous Windows.

1 Sous Windows, cliquez sur **Télécharger (32 bits)** ou **Télécharger (64 bits)** selon le système d'exploitation de votre ordinateur.
2 Téléchargez le fichier d'installation sur un répertoire de votre ordinateur.
3 Double-cliquez sur le fichier d'installation pour lancer le programme d'installation.
4 Sélectionnez une langue, puis cliquez sur **OK**.
5 Si vous êtes invité(e) à installer Microsoft Visual C++ 2010 Redistributable Package, cliquez sur **OK**.
6 Dans la page d'accueil, cliquez sur **Suivant**.
7 Lisez le contrat de licence, acceptez-en les termes, puis cliquez sur **Suivant**.
8 À l'écran Dossier de destination, cliquez sur **Suivant** pour installer à l'emplacement par défaut suivant **C:\Program Files\Dell\Dell Data Guardian\.**

9 Sur l'écran Type de configuration, sélectionnez l'une des options suivantes :

Dell Security Center hébergé	Serveur Dell Management local
a Sélectionner Dell Security Center hébergé. b Si votre entreprise est multitenant, saisissez l'ID d'installation qui se trouve sur la page de garde ou dans l'e-mail de bienvenue. c Cliquez sur **Suivant**. d Passez à l'étape 10.	a Sélectionnez Serveur Dell Management local. b Dans le champ *Nom du serveur :*, saisissez le nom du serveur Serveur Dell avec lequel cet ordinateur va communiquer. Vous trouverez ce nom dans l'e-mail d'activation que vous avez reçu ou en haut de la page de téléchargement. c Cliquez sur **Suivant**. d Sur l'écran Confirmer le serveur d'activation, confirmez que l'adresse URL du serveur Serveur Dell est correcte. Le programme d'installation ajoute www ou http(s) et le port. Cliquez sur **Suivant**. e Passez à l'étape 10.

10 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.

11 Cliquez sur **Installer** pour démarrer l'installation.

Une fenêtre affichant l'avancée de l'installation apparaît.

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

13 Cliquez sur **Oui** pour redémarrer.

L'installation de Data Guardian est maintenant terminée.

14 Voir Activer Data Guardian.

REMARQUE :

Veillez à bien lire les notes et exceptions dans Utilisation de Data Guardian avec Windows ; par exemple, vous ne pouvez pas ouvrir un fichier .pdf protégé à partir du réseau. Vous pouvez utiliser Word pour ouvrir un fichier .pdf protégé à partir du réseau.

Identifier	**GUID-92B941BF-52D2-4302-AFA1-3D348E260E03**
Status	**Translation Validated**

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 zone de notification, une icône en forme de cloud assortie d'un point d'exclamation orange s'affiche.

2 Lorsqu'une boîte de dialogue s'affiche dans la zone de notification cliquez sur **Cliquez ici pour activer**.

Si cette boîte de dialogue ne s'affiche pas, cliquez sur l'icône **Data Guardian** dans la zone de notification et sélectionnez **Activation utilisateur**.

REMARQUE :

Pour un environnement hébergé, les utilisateurs externes peuvent uniquement activer un tenant à la fois. Si vous avez déjà activé un tenant, vous devez désinstaller Data Guardian et le réinstaller avec l'autre ID d'installation. Vous pouvez éventuellement utiliser le portail Web pour télécharger et afficher des documents protégés.

3 Saisissez l'adresse e-mail et le mot de passe utilisés pour vous enregistrer, puis cliquez sur **Activer**.

REMARQUE :

Pour local, si vous avez installé Data Guardian avant votre inscription, lorsque vous procédez à l'activation, cliquez sur le lien d'**inscription**.

Une fois l'activation terminée, une coche verte s'affiche sur l'icône Data Guardian dans la zone de notification  .

4 Confirmez l'état de votre mode utilisateur. Cliquez sur l'icône de la zone de notification 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.

Identifier	**GUID-55AD51F6-9437-4B64-9A9F-E598A3BBDC74**
Status	**Translation Validated**

Demande d'accès d'un utilisateur interne

Sous Windows, Mac et Mobile, si un utilisateur externe a installé et activé Data Guardian, il peut demander l'accès à un document Office protégé ou .pdf à partir d'un utilisateur interne. L'utilisateur externe doit faire une demande séparée pour chaque fichier.

1 Si vous ouvrez un document 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 zone de notification, 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.

Identifier	**GUID-1DB6F793-018B-4F14-AA95-63980FCDD713**
Status	**Translation Validated**

Tâches de l'utilisateur externe et Mac

Tâches de l'utilisateur interne pour Mac

Effectuez l'une des opérations suivantes :

- Documents protégés : envoyez un document protégé à l'utilisateur externe via un e-mail, un partage réseau ou un stockage amovible.
- Si le chiffrement Cloud de Data Guardian est activé : dans l'interface de Dell Data Guardian, faites glisser les fichiers protégés vers la colonne en regard de la colonne des fournisseurs de stockage Cloud.

Tâches de l'utilisateur externe pour Mac

Enregistrer Data Guardian

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

Pour enregistrer Data Guardian :

1 Lorsque vous ouvrez un document protégé qui affiche un avertissement sur la page de garde, cliquez sur le lien fourni pour enregistrer une adresse e-mail valide.

REMARQUE :
La page de garde répertorie le nom du serveur Serveur Dell pour l'option local ou un ID d'installation pour ce tenant spécifique si votre Dell Security Center hébergé est multitenant. La page de garde contient des liens pour enregistrer le client Data Guardian.

2 Effectuez l'une des actions suivantes en fonction de votre environnement :

Dell Security Center hébergé	Serveur Dell Management local
Solution SaaS (Software as a Service) hébergée permettant de gérer le logiciel Dell Data Security.	Serveur sur site situé dans le réseau de l'entreprise et permettant de gérer le logiciel Dell Data Security.
a Lorsque le portail Web Dell Data Guardian s'ouvre, saisissez votre adresse e-mail. b Faites défiler la page et cliquez sur **J'accepte**. c Dans la fenêtre Dell Security Center, faites défiler la liste jusqu'à *Besoin d'un compte ?* et cliquez sur **S'inscrire**. d Sur la page du nouveau compte, saisissez une adresse e-mail, un prénom, un nom de famille et un mot de passe. Le mot de passe doit comporter au moins huit caractères et contenir une minuscule, une majuscule, un caractère spécial et un chiffre. e Cliquez sur **Se connecter**. f Accédez à l'adresse e-mail que vous avez utilisée pour vous inscrire, récupérez le code de vérification et saisissez-le. **REMARQUE :** Si vous ne voyez aucun e-mail, vérifiez le courrier indésirable. g Cliquez sur **Confirmer le compte**. Si le compte est vérifié, le portail Web s'ouvre. h Téléchargez le fichier protégé pour l'afficher. Vous recevez un e-mail contenant des liens vous permettant de télécharger le client Mac. Vous pouvez également cliquer sur le lien situé sur la page de garde. Voir ci-dessous.	a Lorsque la fenêtre Data Guardian de Dell s'ouvre, entrez votre adresse e-mail. b Cliquez sur **S'inscrire**. c Sur la page S'inscrire, saisissez votre mot de passe et confirmez-le, puis cliquez sur **Se connecter**. 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. Si vous ne voyez aucun e-mail, vérifiez le courrier indésirable. d Ouvrez l'e-mail d'activation de compte et cliquez sur le lien. L'e-mail comporte aussi le nom de Serveur Dell à utiliser lors de l'installation de Data Guardian. e Sur la page Confirmation de l'inscription, cliquez sur **Retour à la connexion**. Vous pouvez cliquer sur le lien de la page de garde pour télécharger et installer un client. Voir ci-dessous.

Télécharger et installer un client Data Guardian (facultatif).

1 Sur la page Data Guardian de Dell, saisissez l'adresse e-mail et le mot de passe utilisés pour vous enregistrer.
2 Cliquez sur **Connexion**.
Une page de téléchargement Data Guardian s'ouvre avec des options pour Windows, iOS, Android et Mac OS X.
3 Sous Mac OS X, cliquez sur **Télécharger**.
4 Sur la page *Pilotes et téléchargements*, sélectionnez **Apple Mac OS** et cliquez sur **Télécharger**.
5 Téléchargez le fichier .dmg dans un répertoire sur votre ordinateur et exécutez le fichier .pkg.
6 Pour vous connecter/activer, effectuez l'une des actions suivantes :

Dell Security Center hébergé	Serveur Dell Management local
a Utilisez l'adresse e-mail fournie lors de l'inscription. b Les informations de connexion sont ce que vous avez utilisé pour vous connecter au fichier .dmg. c Cliquez sur **Connexion**.	a Reportez-vous à l'aide en ligne intégrée pour Data Guardian et saisissez le nom du Serveur Dell répertorié dans l'e-mail de vérification du compte. b Saisissez également votre adresse e-mail et votre mot de passe. Les informations de connexion correspondent aux éléments fournis lors de l'inscription. c Cliquez sur **Connexion**.

Identifier	**GUID-B2D2A78A-86B7-4D46-A530-C531CE3B706A**
Status	**Translation Validated**

Utilisateur externe et Mobile

Si un utilisateur interne partage dans le cloud un lien vers un fichier protégé, le fichier affiche une page de garde qui contient un lien pour l'inscription d'une adresse e-mail valide.

REMARQUE :
La page de garde répertorie le nom du serveur Serveur Dell pour l'option local ou un ID d'installation pour ce tenant spécifique si votre Dell Security Center hébergé est multitenant. La page de garde contient également des liens pour télécharger le client Data Guardian.

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

- S'enregistrer dans Data Guardian
- Télécharger et installer Data Guardian : l'utilisateur externe doit disposer des droits d'administrateur sur son ordinateur.

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'avertissement de la page de garde, cliquez sur le lien fourni pour inscrire une adresse e-mail valide.

2 Suivez l'ensemble d'étapes définies en fonction de l'environnement de votre entreprise :

Dell Security Center hébergé

Solution SaaS (Software as a Service) hébergée permettant de gérer le logiciel Dell Data Security.

a Lorsque le portail Web Dell Data Guardian s'ouvre, saisissez votre adresse e-mail.

b Faites défiler la page et cliquez sur **J'accepte**.

c Dans la fenêtre Dell Security Center, faites défiler la liste jusqu'à *Besoin d'un compte ?* et cliquez sur **S'inscrire**.

d Sur la page du nouveau compte, saisissez une adresse e-mail, un prénom, un nom de famille et un mot de passe. Le mot de passe doit comporter au moins huit caractères et contenir une minuscule, une majuscule, un caractère spécial et un chiffre.

e Cliquez sur **Se connecter**.

f Accédez à l'adresse e-mail que vous avez utilisée pour vous inscrire, récupérez le code de vérification et saisissez-le.

REMARQUE :
Si vous ne voyez aucun e-mail, vérifiez le courrier indésirable.

g Cliquez sur **Confirmer le compte**. Si le compte est vérifié, le portail Web s'ouvre.

h Faites glisser les fichiers protégés dans le portail Web, puis cliquez sur **Charger maintenant**.

i Vous recevrez un e-mail de bienvenue après vous être inscrit. Cet e-mail contient un lien permettant de télécharger un client Windows.

Serveur Dell Management local

Serveur sur site situé dans le réseau de l'entreprise et permettant de gérer le logiciel Dell Data Security.

REMARQUE :
Pour local, vous pouvez installer Data Guardian avant de vous inscrire. Lorsque vous essayez d'activer, cliquez sur le lien d'**inscription** disponible.

a Lorsque la fenêtre Data Guardian de Dell s'ouvre, entrez votre adresse e-mail.

b Cliquez sur **S'inscrire**.

c Sur la page S'inscrire, saisissez votre mot de passe et confirmez-le, puis cliquez sur **Se connecter**.

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. Si vous ne voyez aucun e-mail, vérifiez le courrier indésirable.

d Dans l'e-mail de vérification de compte de Serveur Dell, cliquez sur le lien hypertexte.

REMARQUE :
Si vous ne voyez aucun e-mail, vérifiez le courrier indésirable.

e Continuez vers la page Web.

f Sur la page Confirmation, cliquez sur **Poursuivre la connexion**.

g Sur la page Connexion, cliquez sur **Mot de passe oublié**.

Dell Security Center hébergé	Serveur Dell Management local
REMARQUE : Si votre Dell Security Center hébergé est multitenant, l'e-mail répertorie également un ID d'installation dont vous aurez besoin.	**REMARQUE :** Serveur Dell vous a attribué un mot de passe aléatoire que vous devez réinitialiser.

h 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.

i Ouvrez l'e-mail d'activation de compte et cliquez sur le lien.
L'e-mail comporte aussi le nom de Serveur Dell à utiliser lors de l'installation de Data Guardian.

j Sur la page Se connecter, saisissez l'adresse e-mail et le mot de passe utilisés pour vous enregistrer.

k Cliquez sur **Connexion**.
Une page de téléchargement Data Guardian s'ouvre.

Télécharger et installer Data Guardian pour Mobile

Effectuez l'une des opérations suivantes :

- Installation ou désinstallation de Data Guardian sur un appareil Android
- Installation ou désinstallation de Data Guardian sur un appareil iOS

Identifier	**GUID-FE0A7159-E0F3-4E21-9FE6-008C831F7D44**
Status	**Translation Validated**

Utilisateur externe et portail Web

Tâches de l'utilisateur interne

Un utilisateur interne peut effectuer l'une des opérations suivantes :

- Envoyer à l'utilisateur externe l'URL de l'entreprise pour accéder au portail Web de Data Guardian.
- Envoyer un fichier protégé à l'utilisateur externe. Lorsque l'utilisateur ouvre le fichier, une page de couverture s'affiche.

L'utilisateur externe peut uniquement afficher un document Office protégé au format de fichier .pdf ou .xen, ou modifier des fichiers selon la règle. Cependant, il n'est pas nécessaire que l'utilisateur externe télécharge un client Data Guardian.

Tâches de l'utilisateur externe pour le portail Web

Pour s'inscrire au portail Web de Data Guardian :

1 Cliquez sur l'URL du portail Web que vous avez reçue d'un utilisateur interne ou qui est présente sur la page de garde d'un fichier protégé.

2 Sur l'écran Contrat de licence, défilez vers le bas et cliquez sur **Accepter**.

3 Procédez à l'une des deux opérations suivantes selon que votre entreprise est hébergée ou en Local.

Dell Security Center hébergé	Serveur Dell Management local
Solution SaaS (Software as a Service) hébergée permettant de gérer le logiciel Dell Data Security.	Serveur sur site situé dans le réseau de l'entreprise et permettant de gérer le logiciel Dell Data Security.

Dell Security Center hébergé	Serveur Dell Management local
a Saisissez une adresse e-mail et un mot de passe. b Cliquez sur **Se connecter**. c Saisissez un e-mail, un prénom, un nom de famille et un mot de passe. Le mot de passe doit comporter au moins huit caractères et contenir une minuscule, une majuscule, un caractère spécial et un chiffre. d Cliquez sur **Se connecter**. e Accédez à l'adresse e-mail que vous avez utilisée pour vous inscrire, récupérez le code de vérification et saisissez-le. f Saisissez le code de vérification et cliquez sur **Confirmer le compte**. Le portail Web s'ouvre.	a b Cliquez sur **Vous ne possédez pas encore de compte ?** c Saisissez une adresse e-mail et cliquez sur **S'inscrire**. **REMARQUE :** Pour les utilisateurs internes qui veulent s'inscrire en tant qu'externes, il s'agit d'une adresse e-mail extérieure au domaine. d Sur la page S'inscrire, saisissez et confirmez un mot de passe, puis cliquez sur **S'inscrire**. La page de confirmation indique qu'un e-mail de confirmation a été envoyé à l'adresse e-mail que vous avez fournie. e Pour terminer l'activation du compte, ouvrez l'e-mail intitulé *Vérification du compte* et cliquez sur le lien. f Sur l'écran Confirmation de l'inscription, cliquez sur **Retour à la connexion**. g Saisissez l'adresse e-mail et le mot de passe utilisés lors de l'inscription.

Si un utilisateur interne ne partage pas la clé, vous pouvez accéder au portail Web mais ne pouvez pas ouvrir le fichier.

4 La page de téléchargement de Dell Data Guardian s'ouvre.

5 Cliquez sur **Parcourir** pour accéder au fichier et le télécharger, ou faites glisser et déposer le fichier dans le portail Web.

6 Cliquez sur **?** pour afficher l'aide en ligne de chaque page.

Pour modifier des fichiers, l'administrateur doit modifier une règle pour cet utilisateur. Si vous y avez accès une fois inscrit, vous devez vous déconnecter du portail Web, puis vous reconnecter.

Si vous le désirez, vous pouvez télécharger un client Data Guardian. La page de garde contient des liens pour enregistrer le client Data Guardian. La page de garde répertorie également le nom du serveur Serveur Dell pour l'option local ou un ID d'installation pour ce tenant spécifique si votre Dell Security Center hébergé est multitenant.

Demande d'accès d'un utilisateur interne

Si vous chargez un document Office protégé ou .pdf et qu'une boîte de dialogue *Échec du chargement* vous indique que vous n'avez pas accès, vous pouvez demander l'accès à l'auteur du fichier :

1 Sur la boîte de dialogue *Échec du chargement*, cliquez sur **Oui**.

2 Attendez un e-mail de l'utilisateur interne indiquant si l'accès a été accordé ou refusé.

REMARQUE : Si vous ne recevez pas d'e-mail de l'utilisateur interne, vous devez attendre 48 heures avant de demander l'accès à nouveau. Si vous ouvrez le fichier protégé avant que l'utilisateur interne n'approuve l'accès, un message s'affiche en indiquant que la demande est en attente.

Identifier	**GUID-01B874EC-88D4-4264-803C-472B65D1180F**
Status	**Translation Validated**

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 à 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 à Serveur Dell 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.

- Imprimer
- Exporter
- Enregistrer sous
- Partager

Identifier	**GUID-8882A835-A7A8-4C7B-8330-3080F871A121**
Status	**Translation Validated**

Dell Security Center hébergé et tenant suspendu

Avec Dell Security Center hébergé, si un tenant ne s'acquitte pas du paiement pendant un délai spécifié, ses opérations peuvent être suspendues. Ceci s'applique à Windows, Mac, Mobile et au portail Web.

Les utilisateurs internes et externes de Data Guardian peuvent être confrontés aux situations suivantes :

- Toutes les plates-formes : si vous essayez d'installer Data Guardian, de l'activer, ou de vous connecter, une boîte de dialogue s'affiche et vous signale que les opérations du tenant sont suspendues.
- Mac : si les opérations de votre tenant sont suspendues alors que Data Guardian est ouvert, la boîte de dialogue vous informant de cette suspension s'affiche après la fermeture de l'Explorateur et de tous les fichiers, et lorsque vous essayez ensuite d'ouvrir un fichier protégé.
- Portail Web :
  - Si vous êtes déjà connecté et que vous chargez un fichier chiffré, un message vous informe de l'échec du chargement.
  - Si un fichier chiffré ou non chiffré a été chargé, puis que les opérations du tenant sont suspendues, un message indiquant l'échec du téléchargement s'affiche.
  - Si vous vous déconnectez, puis que vous tentez de vous connecter à nouveau, une boîte de dialogue s'affiche pour indiquer que les opérations du tenant sont suspendues.

Contactez votre administrateur.

Identifier	GUID-EF1D5890-EB47-482E-AF29-
Status	In Translation

Optimisation de la sécurité avec les Groupes d'accès de Data Guardian (local)

Les Groupes d'accès de Data Guardian améliorent la sécurité en créant des groupes d'utilisateurs qui peuvent collaborer sur les données chiffrées. Les utilisateurs qui se trouvent en dehors d'un groupe ne peuvent pas accéder aux données ni les afficher à moins que le propriétaire du fichier ne leur en accorde l'accès. Les Groupes d'accès peuvent inclure des utilisateurs internes et externes. Vous pouvez utiliser les Groupes d'accès sur Windows, Mac, mobile et sur le portail Web.

Sélectionnez l'une de ces options en fonction de votre entreprise :

- Data Guardian est installé dans l'entreprise avec le mode de protection individuelle
- Data Guardian est installé dans l'entreprise avec le mode de protection forcée
- L'entreprise ne possède pas encore Data Guardian ni le mode de protection individuelle
- L'entreprise ne possède pas encore Data Guardian ni le mode de protection forcée

Identifier	GUID-F71ADE66-5107-4796-B57E-FC00340C788C
Status	In Translation

Data Guardian est installé dans l'entreprise avec le mode de protection individuelle

Si votre entreprise utilise des Groupes d'accès pour optimiser la sécurité des données sensibles, vous devez savoir qui se trouve dans votre Groupe d'accès. Initialement, pour faciliter la transition, votre entreprise peut fournir une brève période de traitement de n'importe quel fichier partagé et chiffré existant. Après la période transitoire, le Groupe d'accès permet aux utilisateurs d'afficher tous les fichiers partagés et chiffrés que vous créez. Vous pouvez autoriser l'accès à des individus en dehors de votre Groupe d'accès.

Identification des membres de votre Groupe d'accès

Votre administrateur vous indiquera qui se trouve dans au moins un de vos Groupes d'accès, en fonction des individus nécessitant l'accès aux fichiers spécifiques. Il peut s'agir d'utilisateurs internes et externes. Si vous travaillez sur des données sensibles avec des utilisateurs spécifiques, vous pouvez demander à votre administrateur de créer un Groupe d'accès pour ce contenu.

Utilisation d'une période transitoire pour le traitement des fichiers partagés et chiffrés

Si Data Guardian est déjà installé et que les fichiers existants sont chiffrés, nous recommandons à votre entreprise d'effectuer une courte période de transition pour traiter ces fichiers existants, et ainsi faciliter la transition. Tenez compte des points suivants si vous souhaitez continuer de partager ou de collaborer sur ces fichiers :

- Utilisateurs internes ou externes, au sein ou en dehors de votre Groupe d'accès : à l'exception de l'auteur d'origine, les utilisateurs doivent ouvrir les fichiers partagés et chiffrés pendant la période transitoire pour avoir accès à la clé. S'ils ne le font pas, ils perdent l'accès au fichier. Toutefois, ils peuvent demander l'accès au propriétaire du fichier, après la période transitoire. Le propriétaire peut également octroyer l'accès.
- Utilisateurs internes en dehors de votre Groupe d'accès : les utilisateurs doivent ouvrir les fichiers partagés pendant la période transitoire pour avoir accès à la clé. S'ils ne le font pas, ils perdent l'accès au fichier. Toutefois, ils peuvent vous demander l'accès après la période transitoire.
- Utilisateurs externes en dehors de votre Groupe d'accès : si vous avez déjà octroyé l'accès à un fichier chiffré, l'utilisateur externe conservera l'accès après la période transitoire.

Traitement des fichiers chiffrés pré-existants non ouverts pendant la période de transition

Pour Windows et Mac en mode de protection individuelle, vous devez ouvrir n'importe quel fichier pré-existant chiffré par Data Guardian. Les utilisateurs internes, qui ne sont pas propriétaires du fichier et qui n'ont pas ouvert un fichier pendant la période transitoire, ne peuvent pas visualiser le fichier, même s'ils font partie de ce Groupe d'accès. Une boîte de dialogue les invite à demander l'accès, et le propriétaire du fichier peut décider si oui ou non il l'accorde.

Collaboration sur des fichiers chiffrés après la période transitoire

Pour les nouveaux fichiers que vous créez et chiffrez après la période transitoire :

- Utilisateurs internes ou externes au sein de votre Groupe d'accès : ont accès à tous les fichiers partagés et chiffrés.
  - Toute personne retirée du Groupe d'accès perd l'accès.
  - Si le propriétaire d'un fichier est retiré du groupe, les autres utilisateurs conservent l'accès.
- Utilisateurs internes ou externes en dehors de votre Groupe d'accès : ne peuvent pas afficher un fichier chiffré.
  - Un utilisateur interne au sein du Groupe d'accès peut accorder l'accès.
  - Un utilisateur externe propriétaire d'un fichier chiffré peut accorder l'accès à une autre personne.
  - Si un utilisateur interne ou externe en dehors du groupe reçoit un fichier chiffré et tente de l'ouvrir, une boîte de dialogue l'invite à demander l'accès.

Identifier	**GUID-18DE070B-862D-4CAF-8CDE-DA86552E6C57**
Status	**In Translation**

Data Guardian est installé dans l'entreprise avec le mode de protection forcée

Si votre entreprise utilise des Groupes d'accès pour optimiser la sécurité des données sensibles, vous devez savoir qui se trouve dans votre Groupe d'accès. Initialement, pour faciliter la transition, votre entreprise peut fournir une brève période de traitement de n'importe quel fichier partagé et chiffré existant. Après la période transitoire, le Groupe d'accès permet aux utilisateurs d'afficher tous les fichiers partagés et chiffrés que vous créez. Vous pouvez autoriser l'accès à des individus en dehors de votre Groupe d'accès.

Identification des membres de votre Groupe d'accès

Votre administrateur vous indiquera qui se trouve dans au moins un de vos Groupes d'accès, en fonction des individus nécessitant l'accès aux fichiers spécifiques. Il peut s'agir d'utilisateurs internes et externes. Si vous travaillez sur des données sensibles avec des utilisateurs spécifiques, vous pouvez demander à votre administrateur de créer un Groupe d'accès pour ce contenu.

Utilisation d'une période transitoire pour le traitement des fichiers partagés et chiffrés

Si Data Guardian est déjà installé et que les fichiers existants sont chiffrés, nous recommandons à votre entreprise d'effectuer une courte période de transition pour traiter ces fichiers existants, et ainsi faciliter la transition. Tenez compte des points suivants si vous souhaitez continuer de partager ou de collaborer sur ces fichiers :

- Utilisateurs internes ou externes, au sein ou en dehors de votre Groupe d'accès : à l'exception de l'auteur d'origine, les utilisateurs doivent ouvrir les fichiers partagés et chiffrés pendant la période transitoire pour avoir accès à la clé. S'ils ne le font pas, ils perdent l'accès au fichier. Toutefois, ils peuvent demander l'accès au propriétaire du fichier, après la période transitoire. Le propriétaire peut également octroyer l'accès.
- Utilisateurs internes en dehors de votre Groupe d'accès : les utilisateurs doivent ouvrir les fichiers partagés pendant la période transitoire pour avoir accès à la clé. S'ils ne le font pas, ils perdent l'accès au fichier. Toutefois, ils peuvent vous demander l'accès après la période transitoire.
- Utilisateurs externes en dehors de votre Groupe d'accès : si vous avez déjà octroyé l'accès à un fichier chiffré, l'utilisateur externe conservera l'accès après la période transitoire.

Traitement des fichiers chiffrés pré-existants non ouverts pendant la période de transition

Pour Windows et Mac en mode de protection forcée, vous devez ouvrir n'importe quel fichier pré-existant chiffré et analysé par Data Guardian. Cela inclut les documents Office, les PDF et les fichiers chiffrés avec la protection de fichiers de base. Les utilisateurs internes, qui ne sont pas propriétaires du fichier et qui n'ont pas ouvert un fichier pendant la période transitoire, ne peuvent pas visualiser le fichier, même s'ils font partie de ce Groupe d'accès. Une boîte de dialogue les invite à demander l'accès, et le propriétaire du fichier peut décider si oui ou non il l'accorde.

Collaboration sur des fichiers nouvellement créés après la période transitoire

Pour les nouveaux fichiers que vous créez et chiffrez après la période transitoire :

- Utilisateurs internes ou externes au sein de votre Groupe d'accès : ont accès à tous les fichiers partagés et chiffrés.
  - Toute personne retirée du Groupe d'accès perd l'accès.
  - Si le propriétaire d'un fichier est retiré du groupe, les autres utilisateurs conservent l'accès.
- Utilisateurs internes ou externes en dehors de votre Groupe d'accès : ne peuvent pas afficher un fichier chiffré.
  - Un utilisateur interne au sein du Groupe d'accès peut accorder l'accès.
  - Un utilisateur externe propriétaire d'un fichier chiffré peut accorder l'accès à une autre personne.
  - Si un utilisateur interne ou externe en dehors du groupe reçoit un fichier chiffré et tente de l'ouvrir, une boîte de dialogue l'invite à demander l'accès.

Identifier	**GUID-BDD3EF46-A9A1-48C2-BB76-B9D874BC37E4**
Status	**In Translation**

L'entreprise ne possède pas encore Data Guardian ni le mode de protection individuelle

Si votre entreprise prévoit d'utiliser Data Guardian avec les Groupes d'accès pour optimiser la sécurité des données sensibles, il est recommandé d'identifier tous les fichiers que vous partagez avec les utilisateurs internes ou externes, et de voir si ces utilisateurs

appartiennent à un Groupe d'accès que votre administrateur a créé pour vous. Initialement, pour faciliter la transition, votre entreprise peut prévoir un courte période pour le traitement de n'importe quel fichier partagé existant. Après la période transitoire, le Groupe d'accès permet aux utilisateurs d'afficher tous les fichiers partagés et chiffrés que vous créez. Vous pouvez autoriser l'accès à des individus qui ne sont pas dans votre Groupe d'accès afin de pouvoir collaborer avec eux tout en bénéficiant d'une sécurité accrue.

Identification des membres de votre Groupe d'accès

Votre administrateur vous indiquera qui se trouve dans au moins un de vos Groupes d'accès, en fonction des individus nécessitant l'accès aux fichiers spécifiques. Il peut s'agir d'utilisateurs internes et externes. Si vous travaillez sur des données sensibles avec des utilisateurs spécifiques, vous pouvez demander à votre administrateur de créer un Groupe d'accès pour ce contenu.

Mise en place d'une période de transition pour traiter les fichiers partagés

Lorsque Data Guardian est installé, une analyse est lancée sur Windows ou Mac pour chiffrer les fichiers suivants, si votre administrateur a activé une règle pour ces fichiers.

- Types de fichiers supplémentaires, par exemple .txt ou .png, configurés pour la protection de fichiers de base
- Fichiers de classification des données (Windows)
- Fichiers de classification TITUS (Windows)

Si vous collaborez déjà sur des fichiers ou que vous les partagez avec des utilisateurs internes ou externes, ces utilisateurs peuvent être ou non dans votre Groupe d'accès. Pour faciliter la transition, il est recommandé de pratiquer une période transitoire pour traiter tous les fichiers chiffrés qui sont partagés avec d'autres utilisateurs. Vous devez vous connecter à votre ordinateur pendant cette période de transition.

Tenez compte des points suivants si vous souhaitez continuer de partager ou de collaborer sur ces fichiers :

- Pour les fichiers partagés, la première personne à se connecter et dont l'ordinateur est en cours d'analyse devient propriétaire des fichiers partagés.
- Si une autre personne devient propriétaire du fichier et que l'auteur d'origine ne se trouve pas dans le groupe d'accès, le propriétaire d'origine doit demander l'accès au nouveau propriétaire. Le propriétaire d'origine peut également demander à l'administrateur de changer de propriétaire.
- Les ordinateurs des utilisateurs externes ne sont pas analysés. Ainsi, toutes les copies des fichiers partagés non protégés ne sont ni analysées ni chiffrées.
- Si le chiffrement Cloud de Data Guardian est activé et que les utilisateurs partagent des dossiers ou fichiers sur un fournisseur de stockage Cloud, ces fichiers seront également analysés.

Collaboration sur des fichiers nouvellement créés après la période transitoire

Pour les nouveaux fichiers que vous créez et chiffrez après la période transitoire :

- Utilisateurs internes ou externes au sein de votre Groupe d'accès : ont accès à tous les fichiers partagés et chiffrés.
  - Toute personne retirée du Groupe d'accès perd l'accès.
  - Si le propriétaire d'un fichier est retiré du groupe, les autres utilisateurs conservent l'accès.
- Utilisateurs internes ou externes en dehors de votre Groupe d'accès : ne peuvent pas afficher un fichier chiffré.
  - Un utilisateur interne au sein du Groupe d'accès peut accorder l'accès.
  - Un utilisateur externe propriétaire d'un fichier chiffré peut accorder l'accès à une autre personne.
  - Si un utilisateur interne ou externe en dehors du groupe reçoit un fichier chiffré et tente de l'ouvrir, une boîte de dialogue l'invite à demander l'accès.

Identifier	GUID-16B7D77E-57D2-47D9-B2CC-39DB65B223E2
Status	In Translation

L'entreprise ne possède pas encore Data Guardian ni le mode de protection forcée

Si votre entreprise prévoit d'utiliser Data Guardian avec les Groupes d'accès pour optimiser la sécurité des données sensibles, il est recommandé d'identifier tous les fichiers que vous partagez avec les utilisateurs internes ou externes, et de voir si ces utilisateurs appartiennent à un Groupe d'accès que votre administrateur a créé pour vous. Initialement, pour faciliter la transition, votre entreprise peut prévoir un courte période pour le traitement de n'importe quel fichier partagé existant. Après la période transitoire, le Groupe d'accès permet aux utilisateurs d'afficher tous les fichiers partagés et chiffrés que vous créez. Vous pouvez autoriser l'accès à des individus qui ne sont pas dans votre Groupe d'accès afin de pouvoir collaborer avec eux tout en bénéficiant d'une sécurité accrue.

Identification des membres de votre Groupe d'accès

Votre administrateur vous indiquera qui se trouve dans au moins un de vos Groupes d'accès, en fonction des individus nécessitant l'accès aux fichiers spécifiques. Il peut s'agir d'utilisateurs internes et externes. Si vous travaillez sur des données sensibles avec des utilisateurs spécifiques, vous pouvez demander à votre administrateur de créer un Groupe d'accès pour ce contenu.

Mise en place d'une période de transition pour traiter les fichiers partagés

Lorsque Data Guardian est installé, une analyse est lancée sur Windows ou Mac pour chiffrer les fichiers suivants, si votre administrateur a activé une règle pour ces fichiers.

- Documents Office
- PDF
- Types de fichiers supplémentaires, par exemple .txt ou .png, configurés pour la protection de fichiers de base

Pour faciliter la transition, il est recommandé de pratiquer une période transitoire pour traiter tous les fichiers chiffrés qui sont partagés avec d'autres utilisateurs. Vous devez vous connecter à votre ordinateur pendant cette période de transition.

Tenez compte des points suivants si vous souhaitez continuer de partager ou de collaborer sur ces fichiers :

- Pour les fichiers partagés, la première personne à se connecter et dont l'ordinateur est en cours d'analyse devient propriétaire des fichiers partagés.
- Si une autre personne devient propriétaire du fichier et que l'auteur d'origine ne se trouve pas dans le groupe d'accès, le propriétaire d'origine doit demander l'accès au nouveau propriétaire. Le propriétaire d'origine peut également demander à l'administrateur de changer de propriétaire.
- Les ordinateurs des utilisateurs externes ne sont pas analysés. Ainsi, toutes les copies des fichiers partagés non protégés ne sont ni analysées ni chiffrées.
- Si le chiffrement Cloud de Data Guardian est activé et que les utilisateurs partagent des dossiers ou fichiers sur un fournisseur de stockage Cloud, ces fichiers seront également analysés.

Collaboration sur des fichiers nouvellement créés après la période transitoire

Pour les nouveaux fichiers que vous créez et chiffrez après la période transitoire :

- Utilisateurs internes ou externes au sein de votre Groupe d'accès : ont accès à tous les fichiers partagés et chiffrés.
  - Toute personne retirée du Groupe d'accès perd l'accès.
  - Si le propriétaire d'un fichier est retiré du groupe, les autres utilisateurs conservent l'accès.
- Utilisateurs internes ou externes en dehors de votre Groupe d'accès : ne peuvent pas afficher un fichier chiffré.
  - Un utilisateur interne au sein du Groupe d'accès peut accorder l'accès.
  - Un utilisateur externe propriétaire d'un fichier chiffré peut accorder l'accès à une autre personne.
  - Si un utilisateur interne ou externe en dehors du groupe reçoit un fichier chiffré et tente de l'ouvrir, une boîte de dialogue l'invite à demander l'accès.

Identifier	**GUID-2627974A-3D0D-4075-81BC-86DFD31CF90B**
Status	**In Translation**

Modification du propriétaire d'un fichier chiffré

Au cours de la période de transition des Groupes d'accès, si un autre utilisateur a été désigné comme propriétaire d'un document partagé et chiffré dont vous êtes l'auteur, vous pouvez demander que votre administrateur vous désigne comme étant le propriétaire.

Identifier	GUID-F553E0C3-FCF3-4782-8FD4-
Status	Translation Validated

Questions fréquemment posées

Identifier	GUID-D70F8E30-C205-474A-BC17-DB3867AE07AE
Status	Translation Validated

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. Ensuite, ils sont 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 Dell reconnaît uniquement le point de terminaison sur lequel vous avez effectué l'activation initiale. Si vous modifiez le nom du point de terminaison, le Serveur Dell 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 bénéficier des privilèges d'administrateur pour procéder à la désinstallation.

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.

Identifier	**GUID-36E78894-7902-4034-8BFA-6D63A1743855**
Status	**Translation Validated**

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 zone de notification est dotée d'une coche verte, indiquant 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**.