Dell Data Guardian

Guide de l'administrateur v1.2

Remarques, précautions et avertissements

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

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

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

Guide de l'administrateur Dell Data Guardian

2017 - 04

Rév. A01

Table des matières

1

Introduction

Toutes les informations relatives aux règles ainsi que leur description se trouvent dans AdminHelp.

Avant de commencer

1 Installez l'EE Server/VE Server avant de déployer les clients. Localisez le guide qui convient tel qu'illustré ci-dessous, suivez les instructions puis revenez à ce guide.

- *DDP Enterprise Server Installation and Migration Guide (Guide d'installation et de migration de DDP Enterprise Server)*
- *DDP Enterprise Server - Virtual Edition Quick Start Guide and Installation Guide (DDP Enterprise Server - Guide de démarrage rapide et Guide d'installation de Virtual Edition)*

Vérifiez que les stratégies sont définies comme vous le souhaitez. Naviguez dans AdminHelp, disponible à partir du « **?** » à l'extrême-droite de l'écran. La page AdminHelp est une aide de niveau page, conçue pour vous aider à configurer et à modifier une stratégie et à comprendre les options disponibles avec votre EE Server/VE Server.

2 Lisez attentivement le chapitre Configuration requise de ce document.

3 Déployez les clients sur les utilisateurs finaux.

Contacter Dell ProSupport

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

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

Aidez-nous à vous mettre rapidement en contact avec l'expert technique approprié en ayant votre Code de service à portée de main lors de votre appel.

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

2

Configuration requise

Serveur

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

Client Data Guardian

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

  Si les utilisateurs décident de conserver leurs comptes existants, ils doivent déplacer tout fichier devant rester *non crypté* hors 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 finaux doivent donc se familiariser avec le fonctionnement de ces applications avant de déployer Data Guardian. Pour plus d'informations, reportez-vous au support Box sur https://support.box.com/home, au support Dropbox sur https://www.dropbox.com/help, ou au support OneDrive sur http://windows.microsoft.com/en-us/onedrive/onedrive-help#onedrive=other.
- Si vous utilisez Office 2010 : si les règles de protection des documents Office et des documents prenant en charge les macros sont définies, les utilisateurs doivent disposer d'Office 2010 Service Pack 1 ou version supérieure (v14.0.6029 ou supérieure). Voir https://support.microsoft.com/en-us/kb/2121559 pour déterminer si un service pack a été appliqué à la suite Microsoft Office 2010. Sans cette mise à jour, il n'est pas possible d'accéder aux documents protégés. Les nouveaux documents Office ne sont pas protégés, quelles que soient les règles définies, sauf si la fonctionnalité de balayage est activée. Le prochain balayage effectué convertit les documents Office en fichiers protégés, mais les utilisateurs ne peuvent pas y accéder sans une version prise en charge d'Office.
- 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 Windows Restauration du système.
- Consultez régulièrement la rubrique www.dell.com/support pour obtenir la dernière documentation et conseils techniques.

Conditions préalables du client

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

REMARQUE :

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

Microsoft .Net 4.5.2 (ou version ultérieure) est requis pour Data Guardian. Tous les ordinateurs expédiés depuis l'usine Dell sont préinstallés avec .Net 4.5.2. Cependant, si vous n'effectuez pas l'installation sur du matériel Dell ou que vous procédez à une mise à niveau de Data

Guardian sur du matériel Dell plus ancien, vous devez vérifier la version de .Net installée et la mettre à jour, si nécessaire, avant d'installer Dell Data Guardian pour éviter tout échec d'installation/de mise à niveau. Pour vérifier la version .Net installée, suivez ces instructions sur l'ordinateur ciblé pour installation : http://msdn.microsoft.com/en-us/library/hh925568(v=vs.110).aspx. Pour installer Microsoft .Net Framework 4.5.2, accédez à https://www.microsoft.com/en-us/download/details.aspx?id=42643.

Matériel client Windows

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

Matériel Windows

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

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

Systèmes d'exploitation

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

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

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

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

Systèmes d'exploitation Android

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

Systèmes d'exploitation iOS

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

Clients de synchronisation Cloud

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

Clients de synchronisation Cloud

- Dropbox
- Dropbox for Business (Windows uniquement)

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

- Box

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

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

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

Navigateurs Web

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

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

Langues prises en charge

Ces clients sont compatibles avec l'interface utilisateur multilingue (MUI – Multilingual User Interface) et prennent en charge les langues suivantes.

Langues prises en charge

- EN : anglais
- ES : espagnol
- FR : français
- IT : italien
- JA : japonais
- KO : coréen
- PT-BR : portugais brésilien
- PT-PT : portugais du Portugal (ibère)

- DE : allemand

3

Paramètres de registre

- Cette section décrit en détail tous les paramètres du registre approuvé Dell ProSupport des ordinateurs **clients** locaux, quel que soit le motif des paramètres de registre. Si un paramètre de registre chevauche deux produits, il est répertorié dans chaque catégorie.
- Ces modifications de registre doivent être effectués par les administrateurs uniquement et peuvent ne pas être appropriées ou fonctionner dans tous les scénarios.

Paramètres de registre du client Data Guardian

- Les niveaux de journalisation peuvent être augmentés pour aider au dépannage. Créez ou modifiez le paramètre de registre suivant :

  [HKLM\SOFTWARE\Dell\Dell Data Protection\Data Guardian]

  "LogVerbosity"=dword:0x1f (31)

  Par défaut, le type de notifications est réglé sur 0xf (15).

  Valeurs disponibles :

  Désactivé = 0x0 (0)

  Critique = 0x1 (1)

  Erreur = 0x3 (3)

  Avertissement = 0x7 (7)

  Information = 0xf (15)

  Débogage = 0x1f (31)

- Une fois Data Guardian installé, les utilisateurs internes sont automatiquement activés. Si nécessaire, vous pouvez modifier un paramètre de registre pour remplacer l'activation automatique.
  [HKLM\SOFTWARE\Dell\Dell Data Protection\Data Guardian]

  Valeur DWORD : DisableAutomaticActivation=1

  REMARQUE :
  Vous pouvez également confirmer les alias de votre domaine sur le serveur Dell. Voir Dépanner les problèmes d'activation automatique.

Configurer le serveur pour Data Guardian

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

- Les systèmes de partage de fichiers cloud : les ordinateurs ou périphériques mobiles Windows capturent des données destinées au stockage cloud, les chiffrent, puis téléchargent les données cryptées dans le cloud.
- Les documents Office stockés localement, partagés avec d'autres utilisateurs de diverses façons, ou stockés sur un support amovible. Les documents Office suivants peuvent être protégés : .docx, .pptx, .xlsx, .docm, .pptm, .xlsm.

Informez les utilisateurs si votre entreprise utilise Data Guardian pour le stockage cloud uniquement, les documents Office uniquement, ou les deux.

Configurer VE Server pour Data Guardian

Pour configurer VE Server de sorte qu'il prenne en charge Data Guardian, accédez à la Console de gestion à distance, et réglez l'une ou les deux règles Data Guardian sur :

- *Documents Office protégés* - Niveau Entreprise uniquement
- *Cryptage Cloud* - Niveau Entreprise, Groupes finaux, ou Points de terminaison

Configurer EE Server pour Data Guardian

Pour configurer EE Server de sorte qu'il prenne en charge Data Guardian, accédez à la Console de gestion à distance, et réglez l'une ou les deux règles Data Guardian sur :

- *Documents Office protégés* - Niveau Entreprise uniquement
- *Cryptage Cloud* - Niveau Entreprise, Groupes finaux, ou Points de terminaison

Ensuite, configurez le Security Server pour autoriser les téléchargements du client Cloud.

Configurer le Security Server pour autoriser les téléchargements du client Data Guardian

Cette rubrique décrit la procédure à suivre pour permettre aux utilisateurs de télécharger le client Data Guardian Windows depuis Dell Security Server.

1 Sur le serveur EE, accédez au **<répertoire d'installation de Security Server>\webapps\root\cloudweb\brand\dell\resources** et ouvrez le fichier **messages.properties** dans un éditeur de texte.

2 Vérifiez que les entrées sont conformes aux informations suivantes :

download.deviceWin.mode=remote

download.deviceWin.local.filename.32=DataGuardian_32bit_setup.exe

download.deviceWin.local.filename.64=DataGuardian_64bit_setup.exe

3 Modifiez les entrées comme suit :

download.deviceWin.remote.link.32=https://<VOTRE URL HÔTE>:<PORT>/cloudweb/download/DataGuardian_32bit_setup.exe

download.deviceWin.remote.link.64=https://<VOTRE URL HÔTE>:<PORT>/cloudweb/download/DataGuardian_64bit_setup.exe

4 Enregistrez le fichier, puis fermez-le.

5 Rendez-vous sur <répertoire d'installation du serveur de sécurité> et créez un nouveau dossier dans cette catégorie en l'appelant Download (Serveur de sécurité\Download).

6 Dans le dossier Download, créez un autre dossier en l'appelant cloudweb (Security Server\Download\cloudweb).

7 Ajoutez les fichiers de configuration 64 bits et 32 bits de Data Guardian dans le dossier cloudweb et renommez-les, par exemple respectivement DataGuardian64.exe et DataGuardian32.exe.

Les noms de ces fichiers sont définis par l'utilisateur mais doivent correspondre aux noms de fichier figurant dans le fichier versions.xml.

8 Redémarrez Security Server pour appliquer les modifications.

Configurer l'EE Server pour des téléchargements automatiques du client Data Guardian Windows (facultatif)

Pour les téléchargements automatiques, le fichier versions.xml et les fichiers binaires doivent se trouver au même emplacement. Le client doit pouvoir y accéder. Il peut donc s'agir d'IIS ou vous pouvez utiliser le dossier **Security Server\Download\cloudweb** que vous avez créé. Si vous utilisez le dossier cloudweb, voici un exemple de configuration du serveur.

1 Accédez au dossier **Security Server\Download\cloudweb**. (Voir l'étape 6 dans Configurer le Security Server pour autoriser les téléchargements du client Data Guardian.)

2 Créez un dossier nommé MiseàjourDataGuardian.

REMARQUE :

Nous avons utilisé MiseàjourDataGuardian dans cet exemple, mais vous pouvez choisir un autre nom.

3 Placez les fichiers exécutables mis à jour dans le dossier MiseàjourDataGuardian.

4 Créez un fichier *versions.xml* dans le dossier MiseàjourDataGuardian.

5 Ouvrez *versions.xml* dans un éditeur de texte et vérifiez que le chemin d'accès du nom de fichier est correct pour votre environnement.

Exemple :

```
<?xml version="1.0"?>
<VERSIONS>
<VERSION arch="x86" product="sl" version="0.x.x.xxxx" filename="/setup32.exe"/>
<VERSION arch="x64" product="sl" version="0.x.x.xxxx" filename="/setup64.exe"/>
</VERSIONS>
```

Version : version de fichier des éléments exécutables mis à jour

Nom du fichier setup.exe : le nom de configuration des fichiers exécutables est défini par l'utilisateur, mais il doit correspondre au nom de configuration figurant dans le fichier messages.properties. (Voir l'étape 3 dans Configurer le Security Server pour autoriser les téléchargements du client Data Guardian.)

6 Enregistrez le fichier, puis fermez-le.

7 Ajoutez les fichiers binaires à ce dossier.

8 Si vous utilisez IIS, redémarrez-le.

9 Connectez-vous à la console de gestion à distance en tant qu'administrateur Dell.

10 Dans le volet de gauche, cliquez sur **Populations** > **Entreprise**. L'onglet Règles de sécurité s'affiche.

11 Dans le groupe de technologies Data Guardian, cliquez sur **Cryptage cloud**.

12 Cliquez sur **Afficher les paramètres avancés**.

13 Faites défiler jusqu'à la règle *URL du serveur de mise à jour de logiciels* et saisissez **https://<VOTRE URL D'HÔTE > / MiseàjourDataGuardian**.

REMARQUE :

MiseàjourDataGuardian est donné à titre de suggestion pour correspondre à l'exemple ci-dessus.

14 Cliquez sur **Enregistrer** pour placer la modification de la règle dans la file d'attente de validation.

15 Cliquez sur **Gestion** > **Valider**.

16 Saisissez un commentaire et cliquez sur **Valider les règles**.

Gérer les profils de fournisseur de protection du stockage Cloud

Data Guardian crypte les fichiers des utilisateurs et envoie les événements d'audit à EE Server/VE Server. Pour modifier le comportement de chaque fournisseur de stockage cloud, définissez chaque fournisseur sur l'une de ces valeurs :

Valeur	Description
Protéger	Autoriser le fournisseur/la connexion, crypter les fichiers et envoyer des événements d'audit sur l'activité des fichiers/dossiers.
Bloquer	Bloque tous les accès au fournisseur/à la connexion.
Autoriser	Autoriser le fournisseur/la connexion à transiter sans cryptage, mais faire un audit de l'activité des fichiers/dossiers.
Éviter	Éviter la protection du fournisseur/de la connexion, sans cryptage ni audit. Lorsque cette valeur est définie, le dossier du fournisseur de stockage cloud ne s'affiche pas dans l'unité virtuelle Data Guardian sur l'ordinateur client.

Pour en savoir plus, voir l'*Aide administrateur*, disponible à partir de la Console de gestion à distance.

Autoriser/Refuser les utilisateurs de la liste d'accès total/liste noire

Vous pouvez déterminer quels utilisateurs externes peuvent s'enregistrer sur l'EE Server/VE Server afin d'utiliser Data Guardian. Pour assurer une sécurité adéquate, configurez et gérez soigneusement ces listes.

- Un utilisateur interne se situe dans le domaine.
- Un utilisateur externe est un utilisateur hors domaine, c'est-à-dire soit une personne appartenant à une autre organisation avec laquelle un utilisateur interne souhaite partager des documents commercialement sensibles, soit un utilisateur interne désirant avoir accès à son ordinateur à partir d'un périphérique non membre du domaine.

Pour permettre à un utilisateur extérieur au domaine de l'organisation de s'inscrire pour utiliser Data Guardian :

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

2 Cliquez sur **Ajouter**.

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

Liste noire : bloque l'inscription d'un utilisateur ou d'un domaine. L'utilisateur n'est pas en mesure d'ouvrir un document Office protégé ou un fichier .xen.

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

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

5 Cliquez sur **Ajouter**.

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

Réinstaller une image d'un ordinateur avec Data Guardian

Si une image de l'ordinateur d'un utilisateur distant a besoin d'être réinstallée et que l'ordinateur est doté de Dell Data Guardian, demandez si l'utilisateur a travaillé hors ligne et s'il a créé des documents Office protégés pendant cette période. Si c'est le cas, des clés hors ligne ont été générées pour ces documents et celles-ci n'ont pas été mises en dépôt sur le serveur Dell.

1 Pour plus d'informations sur la récupération des clés Data Guardian créées hors ligne qui n'ont pas été mises en dépôt sur le serveur Dell, voir le *Guide de récupération*.

2 Vérifiez la présence d'un dossier de clés hors ligne avant de réinstaller l'image de l'ordinateur de l'utilisateur.

Lorsque les premières clés mises en dépôt sont créées, un dossier Data Guardian est ajouté à **C:\Program Files\Dell\Dell Data Protection**. Accédez au dossier **Data Guardian > OfflineKeys**. Si un tel dossier n'existe pas, vérifiez le dossier **Mes documents** de l'utilisateur.

5

Installer Data Guardian

Il existe deux méthodes d'installation de Data Guardian :

- Installer Data Guardian de manière interactive
- Installer Data Guardian par ligne de commande

Les utilisateurs Data Guardian doivent effectuer les tâches suivantes pour que les fichiers et dossiers de leurs clients de synchronisation Cloud soient protégés. Une fois le client Data Guardian installé, les utilisateurs doivent télécharger un fournisseur de stockage cloud :

- L'administrateur doit indiquer le fournisseur de synchronisation cloud à utiliser.

  ou

- Fournissez aux utilisateurs un lien de téléchargement et d'installation de Dropbox for Business ou OneDrive for Business/Unified OneDrive si votre entreprise utilise un de ces fournisseurs. Les utilisateurs de Dropbox for Business doivent se connecter à Dropbox for Business via Data Guardian.

Dossiers préexistants contenant des fichiers non cryptés

Lors du déploiement 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 fichiers et dossiers déjà existants qui sont synchronisés vers le cloud restent en clair
- Les fichiers que vous ajoutez aux dossiers déjà existants restent en clair
- Les fichiers qui sont synchronisés à partir du cloud sont cryptés

  Si vous souhaitez 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.

Installer Data Guardian

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

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

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

1. Pour télécharger le programme d'installation de Data Guardian, rendez-vous à l'emplacement spécifié par votre administrateur.
2. En fonction de votre système d'exploitation, sélectionnez le programme d'installation 32 bits ou 64 bits, généralement appelé **setup32.exe** ou **setup64.exe**, et copiez-le sur l'ordinateur local.
3. Double-cliquez sur le fichier pour lancer le programme d'installation.
4. Si vous recevez un avertissement de sécurité, cliquez sur **Exécuter**.
5. Sélectionnez la langue, puis cliquez sur **OK**.

6 Si un message vous invite à installer Microsoft Visual C++ 2015 Redistributable Package ou Microsoft .NET Framework 4.0 Client Profile, cliquez sur **OK**.

7 Dans la page d'accueil, cliquez sur **Suivant**.

8 Lisez le contrat de licence, acceptez les conditions, puis cliquez sur **Suivant**.

9 À l'écran Dossier de destination, cliquez sur **Suivant** pour effectuer l'installation dans l'emplacement par défaut **C:\Program Files\Dell \Dell Data Protection\Dell Data Guardian\.**

Sur **C:**, n'installez pas Data Guardian dans les dossiers Utilisateurs ou Windows, ni à la racine de n'importe quel lecteur. Vous obtiendrez un message d'erreur.

10 Dans le champ *Nom du serveur :*, saisissez le nom du serveur avec lequel cet ordinateur communiquera, par exemple server.domain.com. Il n'est pas nécessaire d'inclure www ou http(s). Cette information est fournie par votre administrateur.

Ne décochez pas la case *Activer la vérification de confiance SSL* sauf si votre administrateur vous y invite.

11 Cliquez sur **Suivant**.

12 Dans l'écran d'information Confirmer le serveur d'activation, confirmez que l'adresse URL du serveur est correcte. Le programme d'installation ajoute www ou http(s) et le port. Cliquez sur **Suivant**.

13 Dans la fenêtre Type de gestion, sélectionnez l'option suivante :

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

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

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

15 Lorsque la fenêtre Installation terminée s'affiche, cliquez sur **Terminer**.

16 Cliquez sur **Oui** pour redémarrer.

L'installation de Data Guardian est terminée.

17 L'icône Data Guardian dans la barre d'état système affiche une coche verte  après l'activation. En fonction de la manière dont Data Guardian est déployé au sein de l'entreprise, l'activation peut ne pas être immédiate.

Installer Data Guardian par ligne de commande

- Les commutateurs et les paramètres de ligne de commande sont sensibles à la casse.
- Veillez à inclure une valeur contenant un ou plusieurs caractères spéciaux, tels qu'un espace dans la ligne de commande, entre des guillemets d'échappement.
- Le tableau suivant indique les commutateurs disponibles dans le cadre de l'installation.

Commutateur	Signification
/V	Transmission des variables au fichier .msi dans l'élément setup.exe. Le contenu doit toujours être entouré de guillemets en texte brut.
/s	Mode Silencieux

Option	Signification
/QB	Boîte de dialogue de progression dotée du bouton **Annuler** : vous invite à effectuer un redémarrage
/QB!	Boîte de dialogue de progression sans bouton **Annuler** : vous invite à effectuer un redémarrage
/QN	Pas d'interface utilisateur

- Le tableau suivant indique les paramètres disponibles dans le cadre de l'installation.

Paramètres

SERVER= <nom du serveur> (le nom de domaine complet (FQDN) du serveur Dell pour l'activation)

ENTERPRISE=1 (utilisateur interne)

ENABLESSLTRUST=0 (Désactiver la validation d'approbation SSL)

REBOOT=SUPPRESS (Null permet les redémarrages automatiques, SUPPRESS désactive le redémarrage)

Exemple de ligne de commande

- L'exemple suivant installe Data Guardian en mode silencieux, pour un utilisateur interne, sans validation d'approbation SSL, les journaux étant stockés dans C:\Library\Logs\Install.log.

```
setup.exe /S /V"/QB! REBOOT=SUPPRESS ENTERPRISE=1 SERVER=server.domain.com /L*V "c:\Library
\Logs\install.log" ENABLESSLTRUST=0"
```

Utiliser Data Guardian avec Dropbox for Business

Data Guardian avec Dropbox for Business offre des fonctionnalités supplémentaires par rapport à Dropbox de base.

- Effacer à distance le compte d'un membre de l'équipe
- Vous pouvez définir des règles pour contrôler la façon dont les dossiers Dropbox professionnels et personnels sont protégés. Si votre entreprise autorise les comptes professionnels et personnels, les utilisateurs doivent comprendre le cryptage de chaque type de compte. Voir Règle pour les comptes professionnels et personnels.

Règle pour les comptes professionnels et personnels

Votre entreprise peut définir des lignes directrices sur l'utilisation de comptes professionnels et personnels par les membres de l'équipe. En outre, l'entreprise peut autoriser uniquement certains utilisateurs à avoir des comptes professionnels et personnels.

REMARQUE :
Si votre entreprise permet d'avoir des comptes professionnels et personnels, et qu'un utilisateur choisit d'utiliser les deux, celui-ci doit comprendre la gestion des dossiers pour les deux types de compte.

Le tableau suivant décrit le cryptage en fonction du paramètre de règle *Dropbox crypte les dossiers personnels*.

Cryptage	Paramètre de règle	Considérations relatives au déploiement
Crypter tous les fichiers et dossiers professionnels et personnels.	Règle > Dropbox crypte les dossiers personnels > configurée sur **Sélectionné** (par défaut)	Avant de déployer Data Guardian, les utilisateurs doivent sauvegarder les fichiers professionnels préexistants qui se trouvent dans les dossiers de synchronisation de stockage cloud en dehors des dossiers de synchronisation. Les utilisateurs dotés de fichiers personnels qui doivent rester non cryptés doivent les déplacer hors des dossiers de synchronisation professionnels ou dissocier les comptes personnels des clients de synchronisation professionnels. Une fois Data Guardian déployé, les fichiers et dossiers cloud ne peuvent être affichés que sur les ordinateurs ou périphériques exécutant Data Guardian. Si un dossier personnel est crypté de manière non intentionnelle, voir la section « Décrypter des dossiers dans un compte personnel » du Guide d'utilisation de Dell Data Guardian.
Crypter tous les fichiers et dossiers de comptes professionnels. Autoriser que les fichiers et dossiers de comptes personnels restent non cryptés.	Règle > Dropbox crypte les dossiers personnels > configurée sur **Non sélectionné**	Vous pouvez utiliser la règle facultative Message Dropbox crypte les dossiers personnels pour afficher un message personnalisé pour rappeler aux utilisateurs de **ne pas** stocker de fichiers professionnels dans les comptes personnels, puisque ces

Cryptage	Paramètre de règle	Considérations relatives au déploiement
		fichiers ne seront pas protégés. Le message s'affiche dans les cas suivants : • À chaque fois que l'utilisateur se connecte • Lorsque l'utilisateur crée ou ajoute un nouveau fichier ou dossier à un compte Dropbox personnel Si vous configurez la règle Dropbox crypte les dossiers personnels sur **Faux** pour un point final ou un groupe de points finaux, les comptes personnels de tous les utilisateurs sur ces points finaux resteront non cryptés.

Dossiers professionnels et personnels

Si votre organisation est dotée de Dropbox for Business et que vous permettez aux utilisateurs d'avoir des dossiers professionnels et personnels, vous pouvez exécuter des rapports pour s'assurer que tous les fichiers professionnels sont dotés de l'extension de fichier .xen, au cas où un utilisateur copierait un fichier non protégé sensible dans un dossier professionnel. Voir Dépannage de Data Guardian.

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

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

Configuration requise

- Avant d'effectuer un effacement à distance, vous devez sauvegarder tous les fichiers ou dossiers du compte du membre de l'équipe qui peuvent être utiles à l'entreprise ou à d'autres membres de l'équipe Dropbox for Business.
- Seul un administrateur de Dropbox for Business peut effacer à distance un compte Dropbox for Business.
- Data Guardian doit avoir été activé, et l'utilisateur final doit s'être connecté à Dropbox for Business.

S'inscrire dans la Console de gestion à distance

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

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

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

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

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

1 Dans la Console de gestion à distance, sélectionnez **Populations** > **Utilisateurs** dans le volet gauche.
2 Recherchez l'utilisateur donné.
3 Cliquez sur l'onglet **Détails et actions**.
4 Dans la colonne Commande, cliquez sur **Effacer à distance**.

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

5 Cliquez sur **Oui** en réponse au message de confirmation de l'Effacement à distance. La page Détails de l'utilisateur indique la date à laquelle l'effacement à distance est effectué.
6 Actualisez la liste de Membres de l'équipe dans la page de membres de la Console administrateurs de Dropbox for Business. L'utilisateur est supprimé de la liste. Vous pouvez sélectionner l'onglet **Membres supprimés** pour voir quels utilisateurs ont été supprimés.

Afficher les rapports

Les informations relatives à votre environnement Data Guardian sont disponibles dans la Console de gestion à distance du serveur Dell. Sélectionnez **Génération de rapports > Événements d'audit** pour les événements d'audit liés aux dossiers des clients de synchronisation sur le cloud et aux documents Office protégés.

Pour en savoir plus, voir l'*Aide administrateur*, disponible à partir de la Console de gestion à distance.

Dépannage de Data Guardian

Utiliser l'écran Détails

Vous pouvez utiliser l'écran **Détails** pour les problèmes de dépannage ou de support. Par exemple :

- si un utilisateur crée un dossier, mais qu'il ne se crypte pas, sélectionnez **Détails** > **Fichiers** > **État du dossier** pour en vérifier l'état.
- Si un utilisateur final demande une assistance, vous pouvez lui indiquer de configurer l'écran Détails optimisés et de sélectionner l'onglet **Détails** > **Règle**. Cet onglet répertorie les règles en vigueur.
- Afficher les journaux pour le dépannage.

Utiliser l'écran Détails optimisés

- Tout en appuyant sur **<Ctrl><Maj>**, cliquez sur l'icône de Data Guardian, dans la barre d'état système, puis sélectionnez **Détails**.
- Outre les fichiers et dossiers, les éléments suivants s'affichent :

  Sécurité : affiche la clé, le type de clé, et l'état. Ce volet répertorie temporairement certains fichiers Office protégés jusqu'à ce qu'ils soient envoyés au serveur. La durée d'affichage dépend de l'intervalle d'interrogation.

  Audit : affiche les modules, l'ID utilisateur et le type d'événement. Les informations sont mises en file d'attente dans ce journal d'audit, puis envoyées au EE Server/VE Server aux intervalles spécifiés. L'administrateur peut consulter les **Événements d'audit** dans le volet de gauche de la Console de gestion à distance pour effectuer un audit.

  Règle : affiche les noms et valeurs de règle.

Affichage des fichiers journaux

- Cliquer sur **Afficher le journal** dans le coin inférieur gauche de l'écran Détails.

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

  Les fichiers journaux des documents Office protégés se trouvent dans le dossier Custom.xml.

Dépanner les problèmes d'activation automatique

Si Data Guardian ne s'active pas automatiquement pour plusieurs utilisateurs, vous pouvez modifier les paramètres de registre du client Data Guardian. Il est également conseillé de vérifier les alias sur le serveur Dell :

1 Dans la console de gestion à distance, accédez à **Populations > Domaines**, puis sélectionnez un domaine et tous les sous-domaines désirés.

2 Sur la page Détails du domaine, cliquez sur l'onglet **Paramètres**.

3 Dans le champ *Alias*, vérifiez que tous les alias sont corrects.

Fournir des droits temporaires de gestion de dossiers

Vous pouvez octroyer des droits temporaires de gestion des dossiers à un administrateur ou un utilisateur. Par exemple, si les utilisateurs ont chargé des fichiers dans le cloud avant l'installation de Data Guardian, vous pouvez fournir des droits temporaires de gestion de dossiers à certains utilisateurs afin qu'ils puissent gérer le cryptage de chaque dossier au sein des dossiers des clients de synchronisation.

Pour octroyer les droits de gestion des dossiers :

1 Dans la Console de gestion à distance, cliquez sur **Populations** > **Points de terminaison**.
2 Recherchez ou cliquez sur un point de terminaison, puis cliquez sur l'onglet **Règles de sécurité**.
3 Sélectionnez **Cryptage cloud**, puis cliquez sur **Afficher les paramètres avancés**.
4 Cliquez sur la case à cocher en regard de *Gestion de dossiers activée* pour sélectionner la règle.
5 Cliquez sur **Enregistrer**.
6 Dans le volet de gauche, cliquez sur **Gestion** > **Valider**.
7 Saisissez un commentaire et cliquez sur **Valider les règles**.

REMARQUE :
Dell recommande de décocher la case à cocher *Gestion de dossiers activée* une fois les dossiers cryptés ou que le dépannage est terminé, pour désactiver la règle pour ce point de terminaison.

Pour gérer les dossiers sur le point de terminaison :

1 Créez un dossier dans le dossier du client de synchronisation et ajoutez-y des fichiers, de sorte qu'ils soient cryptés dans le cloud.
2 Cliquez sur l'icône de Data Guardian dans la barre d'état système et sélectionnez **Gérer les dossiers**.

   Pour chaque client de synchronisation, une vue hiérarchique des dossiers synchronisés sur le cloud s'affiche. Tous les dossiers sont sélectionnés par défaut. Désélectionnez les dossiers que vous ne souhaitez pas crypter. Si vous désélectionnez un dossier dans Gérer les dossiers, une analyse de décryptage déchiffre les fichiers existants dans ce dossier. Les nouveaux fichiers de ce dossier ne sont pas cryptés sur le disque local ou dans le cloud.

   REMARQUE :
   Si vous faites glisser un fichier crypté dans un dossier qui est désélectionné dans Gérer les dossiers dans le cloud ou sur l'unité virtuelle DDP|SL, le fichier reste crypté et vous ne pouvez pas en afficher le contenu. En outre, si vous partagez le dossier avec un autre utilisateur Data Guardian pour qui la règle Gérer les dossiers n'est pas activée, celui-ci ne pourra pas afficher le contenu des fichiers car ils resteront cryptés.

3 Pour crypter un dossier déjà existant, activez manuellement le cryptage pour ce dossier. Les fichiers seront cryptés lorsque les fichiers se synchronisent sur le Cloud.

Questions fréquemment posées

FAQ sur la gestion des dossiers

Question

J'ai un dossier contenant des fichiers que j'ai partagé avec un autre utilisateur. Dans la barre d'état système, j'ai utilisé l'utilitaire Data Guardian **> Gérer les dossiers** pour décrypter le contenu de ce dossier. Récemment, mes fichiers sont redevenus cryptés dans le Cloud. Ce dossier ne s'affiche plus dans l'utilitaire Gestion des dossiers ; je ne peux donc plus décrypter ces fichiers dans le cloud.

Réponse

Un ID de clé de cryptage est associé à un dossier en fonction du premier utilisateur qui ajoute un fichier à ce dossier. Si un utilisateur crée un dossier et n'ajoute pas de fichiers, sa clé n'est pas associée à ce dossier. L'utilisateur dont l'ID de clé de cryptage a été placée sur le dossier est le seul qui peut voir le dossier dans l'utilitaire Gestion des dossiers. Si l'utilisateur dont l'ID de clé de cryptage est défini sur le dossier désélectionne le dossier dans l'utilitaire Gérer les dossiers et le partage avec un autre utilisateur de Data Guardian, le Data Guardian du deuxième utilisateur crypte à nouveau le contenu.

Solution

1 Créez un nouveau dossier.

2 Déplacez tous les fichiers devant être cryptés dans le nouveau dossier.

3 Dans la barre d'état système, utilisez à nouveau l'utilitaire **Dell Data Guardian** > **Gérer les dossiers** pour décrypter ces fichiers.

REMARQUE :

Si vous décryptez le contenu d'un dossier partagé avec d'autres utilisateurs Data Guardian, le client Data Guardian des autres utilisateurs appliquera la règle de cryptage de celui-ci. La meilleure pratique consiste à utiliser l'utilitaire Gérer les dossiers pour décrypter uniquement les fichiers qui ne sont pas partagés avec d'autres utilisateurs Data Guardian.

Question

Je synchronise un dossier décrypté que j'ai désélectionné à l'aide de l'utilitaire Gérer les dossiers. Pourtant, lorsque je tente de le charger dans mon navigateur web, je peux seulement charger des fichiers cryptés.

Réponse

Data Guardian n'est pas conçu pour rechercher activement des dossiers dans le cloud. Avec les dossiers non cryptés, Data Guardian peut synchroniser via le client de synchronisation, car il ne contrôle pas cet environnement. Les fichiers chargés dans un navigateur web doivent être cryptés.

Solution

Ajoutez les fichiers au dossier de synchronisation.

Question

J'ai récemment désinstallé mon système de partage de fichiers Cloud de mon ordinateur. Pourtant, quand j'ouvre l'utilitaire Gérer les dossiers, l'un des clients de synchronisation était toujours répertorié comme option.

Réponse

Data Guardian ne contrôle pas l'installation ou la désinstallation des logiciels tiers. Ils ne disparaissent pas de la liste d'options car ils ne sont pas conçus pour supprimer vos fichiers existants au moment de leur désinstallation. Ces fichiers sont toujours protégés par Data Guardian, même si le client de synchronisation n'est plus installé.

Solution

Pour supprimer l'option du client de synchronisation désinstallé de l'utilitaire Gérer les dossiers, déplacez les fichiers ou dossiers que vous souhaitez conserver hors du dossier de synchronisation, puis supprimez le dossier. Après sa suppression, le dossier n'est plus répertorié dans l'utilitaire Gérer les dossiers.

Forum aux questions - Divers

Question

Un utilisateur utilisant Data Guardian en mode Documents Office protégés ne peut ni copier ni coller.

Réponse

Certaines fonctionnalités de Data Guardian sont gérées via la barre d'état système. Vérifiez si l'utilisateur l'a modifiée.

Solution

Les paramètres par défaut de la barre d'état système doivent être utilisés. L'utilisateur doit conserver ces paramètres.

Question

J'ai modifié la règle **Obscurcissement des noms de fichiers** en remplaçant GUID par Extension uniquement. Toutefois, les fichiers qui se trouvent dans des dossiers que j'avais synchronisés précédemment sont encore cryptés dans l'autre format, avec des noms de fichiers GUID. Pourquoi ?

Réponse

Lorsque vous modifiez une règle sur l'EE Server/VE Server, Data Guardian maintient la règle précédente pour ce dossier. Si vous créez de nouveaux dossiers, la nouvelle règle leur sera appliquée, et les fichiers de ces dossiers seront cryptés au format **Extension uniquement**.

Solution

Pour appliquer de nouveau le format **Extension uniquement** aux anciens fichiers, transférez-les par couper-coller dans un nouveau dossier auquel la nouvelle règle est appliquée.

8

Glossaire

Advanced Authentication : le produit Advanced Authentication fournit des options totalement intégrées de lecture d'empreintes digitales, de carte à puce et de carte à puce sans contact. Advanced Authentication aide à la gestion de ces nombreuses méthodes d'authentification matérielles, prend en charge la connexion aux lecteurs à encryptage automatique, SSO et gère l'utilisation des identifiants et des mots de passe. De plus, Advanced Authentication peut-être utilisé pour accéder non seulement aux ordinateurs mais à n'importe quel site Internet, SaaS ou application. Lorsque les utilisateurs enregistrent leurs identifiants, Advanced Authentication permet l'utilisation de ces identifiants pour la connexion au périphérique et pour effectuer le remplacement du mot de passe.

BitLocker Manager : Windows BitLocker est conçu pour aider à la protection des ordinateurs Windows en cryptant à la fois les données et les fichiers du système d'exploitation. Afin d'améliorer la sécurité des déploiements de BitLocker, de simplifier et de réduire le coût de propriété, Dell fournit une console de gestion centrale qui traite de nombreux problèmes relevant de la sécurité et offre une approche intégrée à la gestion du cryptage sur d'autres plateformes autres que BitLocker, quelles soient physiques, virtuelles, ou sur le cloud. BitLocker Manager prend en charge le cryptage BitLocker des systèmes d'exploitation, des lecteurs fixes et de BitLocker To Go. BitLocker Manager vous permet d'intégrer facilement BitLocker à vos besoins existants en terme de cryptage et de gérer BitLocker à moindre effort lors de la rationalisation de la conformité et de la sécurité BitLocker Manager fournit la gestion intégrée de la récupération de clé, la gestion des règles et leur application, la gestion automatisée du TPM, la conformité à FIPS et des rapports de conformité.

Désactiver : la désactivation se produit lorsque vous désactivez la gestion SED dans la Console de gestion à distance. Une fois que l'ordinateur est désactivé, la base de données d'authentification avant démarrage est supprimée et il n'y a plus aucun enregistrement des utilisateurs en mémoire cache.

EMS - External Media Shield : ce service du client Dell Encryption applique les règles aux supports amovibles et aux périphériques de stockage externes.

Code d'accès EMS : ce service de Dell Enterprise Server/VE permet d'effectuer une opération de récupération des périphériques protégés par External Media Shield lorsque l'utilisateur oublie son mot de passe et ne peut plus se connecter. Cette manipulation permet à l'utilisateur de réinitialiser le mot de passe défini sur le support amovible ou le périphérique de stockage externe.

Client Encryption : le client Encryption est un composant du périphérique qui permet d'appliquer les règles de sécurité, qu'un point final soit connecté au réseau, déconnecté du réseau, perdu ou volé. En créant un environnement de calcul de confiance pour les points finaux, le client Encryption opère à un niveau supérieur du système d'exploitation du périphérique et fournit une authentification, un cryptage et une autorisation constamment renforcés qui permettent d'optimiser la protection des informations sensibles.

Point de terminaison : ordinateur ou périphérique matériel mobile géré par Dell Enterprise Server/VE.

Balayage de cryptage : un balayage de cryptage est un processus d'analyse des dossiers à crypter sur un point de terminaison géré afin de s'assurer que les fichiers contenus se trouvent en état de cryptage adéquat. Les opérations de création de fichier et de renommage ne déclenchent pas de balayage de cryptage. Il est important de savoir à quel moment un balayage de cryptage peut avoir lieu et ce qui risque d'affecter les temps de balayage résultants et ce de la manière suivante : un balayage de cryptage se produira à la réception initiale d'une règle pour laquelle le cryptage est activé. Ceci peut se produire immédiatement après l'activation si le cryptage a été activé sur votre règle. - Si la règle Balayage de la station de travail lors de la connexion est activée, les dossiers à crypter seront balayés à chaque connexion de l'utilisateur. - Un balayage peut être déclenché à nouveau en raison de certaines modifications ultérieures apportées à des règles. Toute modification de règle en relation avec la définition des dossiers de cryptage, les algorithmes de cryptage, l'utilisation de clés de cryptage (communes par rapport à celles de l'utilisateur), déclencheront un balayage. De plus, le basculement entre l'activation et la désactivation du cryptage déclenchera un balayage de cryptage.

Mot de passe à usage unique (OTP – One-Time Password) : un mot de passe à usage unique est un mot de passe qui ne peut être utilisé qu'une seule fois et n'est valide que pendant une période limitée. OTP exige que le TPM soit présent, activé et détenu. Pour activer OTP, un terminal mobile doit être associé à l'ordinateur utilisant la Security Console et l'application Security Tools Mobile. L'application Security Tools

Mobile génère le mot de passe sur le terminal mobile utilisé pour se connecter à l'ordinateur dans l'écran de connexion Windows. En fonction de cette règle, la fonction OTP peut être utilisée pour récupérer l'accès à l'ordinateur si un mot de passe a expiré ou été oublié, si OTP n'a pas été utilisé pour se connecter à l'ordinateur. La fonction OTP peut être utilisée pour l'authentification ou pour la récupération, mais pas pour les deux. La sécurité OTP est supérieure à celle de quelques autres méthodes d'authentification car le mot de passe généré ne peut être utilisé qu'une seule fois et expire rapidement.

Gestion SED : la gestion SED fournit une plateforme permettant de gérer les disques à auto-cryptage de manière sécurisée. Les disques à auto-cryptage assurent leur propre cryptage, mais ils ont besoin d'une plate-forme pour gérer le cryptage et les règles disponibles. SED Management est un élément de gestion centrale évolutif, qui vous permet de protéger et de gérer vos données plus efficacement. SED Management vous permet d'administrer votre entreprise plus rapidement et plus facilement.