Dell Encryption Personal

Installation Guide v11.9

January 2024
Rev. A01

DELL Technologies

Remarques, précautions et avertissements

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

PRÉCAUTION : ATTENTION vous avertit d'un risque de dommage matériel ou de perte de données et vous indique comment éviter le problème.

AVERTISSEMENT : Un AVERTISSEMENT signale un risque d'endommagement du matériel, de blessure corporelle, voire de décès.

Contents

1

Présentation

Ce guide part du principe qu'Advanced Authentication est installé avec Encryption Personal.

Encryption Personal

L'objet d'Encryption Personal est de protéger les données de votre ordinateur même si vous le perdez ou s'il est volé.

Afin d'assurer la sécurité de vos données confidentielles, Encryption Personal chiffre les données sur votre ordinateur Windows. Vous pouvez toujours accéder aux données lorsque vous êtes connecté à l'ordinateur, mais des utilisateurs non autorisés n'ont pas accès à ces données protégées. Les données demeurent toujours cryptées sur le disque, mais comme le cryptage est transparent, vous n'avez pas besoin de modifier la manière dont vous travaillez avec les applications et les données.

Normalement, l'application décrypte les données lorsque vous les utilisez. Parfois, une application logicielle peut tenter d'accéder à un fichier alors que l'application est en train de le crypter ou de le décrypter. Dans ce cas, au bout de quelques secondes, une boîte de dialogue s'affiche qui donne la possibilité de patienter ou d'annuler le cryptage/décryptage. Si vous décidez de patienter, l'application libère le fichier dès qu'elle a terminé (au bout de quelques secondes, généralement).

Client Advanced Authentication

La console Data Security est l'interface qui guide les utilisateurs pendant la configuration de leurs identifiants PBA et des questions d'auto-récupération, selon la règle définie par l'administrateur local.

Voir Configurer les paramètres administrateur d'Advanced Authentication et le *Dell Data Security Console User Guide* (Guide d'utilisation de la console Dell Data Security) pour savoir comment utiliser l'authentification avancée.

Contactez Dell ProSupport for Software

Appelez le 877-459-7304, poste 4310039, afin de recevoir 24x7 une assistance téléphonique concernant votre produit Dell.

Un support en ligne pour les produits Dell 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 numéro de série ou votre code de service express à portée de main lors de votre appel.

Pour les numéros de téléphone en dehors des États-Unis, consultez l'article Numéros de téléphone internationaux Dell ProSupport for Software.

2

Configuration requise

Cette configuration requise indique tous les éléments nécessaires à l'installation d'Encryption Personal.

Chiffrement

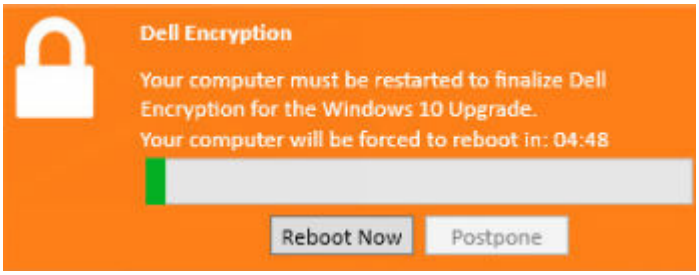
- Encryption Personal exige l'installation réussie d'un droit. Ce droit vous est attribué lors de l'achat d'Encryption Personal. En fonction du mode d'achat de votre Encryption Personal, il peut être nécessaire d'installer manuellement le droit, en suivant les instructions simples qui l'accompagnent. Vous pouvez également saisir le droit sur la ligne de commande. Si vous installez Encryption Personal à l'aide de Dell Digital Delivery, l'installation du droit est exécutée par le service Dell Digital Delivery. (Les mêmes binaires sont utilisés pour Encryption Enterprise et Encryption Personal. Le droit indique au programme d'installation la version à installer.)
- Les comptes Microsoft et Office 365 sont pris en charge lors de l'exécution de la version 11.0 d'Encryption Personal ou d'une version ultérieure sur Windows 10.
- Pour activer un compte Microsoft Live avec Encryption Personal, reportez-vous à l'article de la base de connaissances 124722.
- Un mot de passe Windows (s'il n'en existe pas déjà un) est requis pour protéger l'accès à vos données chiffrées. La création d'un mot de passe sur votre ordinateur permet de bloquer l'accès à votre compte d'utilisateur à toute personne qui ne dispose pas du mot de passe. Encryption Personal ne s'active pas si le mot de passe n'a pas été créé.
- Dell Encryption ne peut pas être mis à niveau vers v10.7.0 à partir de versions antérieures à v8.16.0. Les points de terminaison exécutant des versions antérieures à la version v8.16.0 doivent être mis à niveau vers v8.16.0 , puis vers v10.7.0.
- Dell Encryption utilise les jeux d'instructions de chiffrement d'Intel IPP (Integrated Performance Primitives). Pour plus d'informations, reportez-vous à l'article de la base de connaissances 126015.

1. Accédez au Panneau de configuration de Windows (**Démarrer** > **Panneau de configuration**).
2. Cliquez sur l'icône **Comptes utilisateur**.
3. Cliquez sur **Créer un mot de passe pour votre compte**.
4. Saisissez un nouveau mot de passe et confirmez-le.
5. Il est également possible d'ajouter un indice de mot de passe.
6. Cliquez sur **Créer un mot de passe**.
7. Redémarrez votre ordinateur.

- Les pratiques d'excellence IT 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 d'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. 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/la désinstallation/la mise à niveau.
- Lors de l'installation/la désinstallation/la mise à niveau, n'apportez aucune modification à l'ordinateur, notamment, n'insérez ou ne retirez pas de lecteurs externes (USB).
- Afin de réduire la durée du chiffrement initial (ainsi que la durée de déchiffrement lors d'une désinstallation), lancez l'Assistant Nettoyage de disque Windows qui supprimera les fichiers temporaires et toute autre donnée inutile.
- Désactivez le mode Veille lors du balayage de chiffrement initial pour prévenir la mise en veille d'un ordinateur lors des périodes d'inactivité. Le chiffrement ne peut pas être exécuté sur un ordinateur en veille (le déchiffrement non plus).
- Le client Encryption ne prend pas en charge les configurations à double démarrage dans la mesure où il est possible de chiffrer les fichiers système de l'autre système d'exploitation, ce qui perturberait son fonctionnement.
- Le programme d'installation principal ne prend pas en charge les mises à niveau des composants antérieurs à la version v8.0. Extrayez les programmes d'installation enfants du programme d'installation principal et mettez à niveau le composant individuellement. Si vous avez des questions ou des problèmes, contactez Dell ProSupport.
- Le client Encryption prend désormais en charge le mode Audit. Le mode Audit permet aux administrateurs de déployer le client Encryption dans le cadre de l'image d'entreprise, plutôt que d'utiliser un SCCM tiers ou des solutions similaires pour déployer le client Encryption. Pour obtenir des instructions relatives à l'installation du client Encryption dans une image d'entreprise, reportez-vous à l'article de la base de connaissances 129990.
- Le module TPM (Trusted Platform Module) est utilisé pour sceller la clé GPK. Par conséquent, si vous exécutez le client Encryption, supprimez le module TPM du BIOS avant d'installer un nouveau système d'exploitation sur l'ordinateur cible.

- Le client Encryption est testé avec plusieurs antivirus basés sur des signatures populaires et des solutions antivirus pilotées par l'intelligence artificielle dont McAfee Virus Scan Enterprise, McAfee Endpoint Security, Symantec Endpoint Protection, CylancePROTECT, CrowdStrike Falcon, Carbon Black Defense, etc. avec lesquels il est compatible. Les exclusions codées en dur sont incluses par défaut pour de nombreux fournisseurs d'antivirus afin d'éviter les incompatibilités entre l'analyse antivirus et le chiffrement.

  Si votre organisation utilise un fournisseur d'antivirus non répertorié ou si des problèmes de compatibilité sont observés, reportez-vous à l'article de la base de connaissances 126046 ou contactez Dell ProSupport pour obtenir de l'aide pour la validation de la configuration afin d'assurer l'interopérabilité entre vos solutions logicielles et les solutions Dell Data Security.
- La réinstallation du système d'exploitation n'est pas prise en charge. Pour réinstaller le système d'exploitation, effectuez une sauvegarde de l'ordinateur cible, effacez le contenu de l'ordinateur, installez le système d'exploitation, puis récupérez les données cryptées selon les procédures de récupération établies ci-après.
- Consultez régulièrement le site dell.com/support pour obtenir la documentation la plus récente et des conseils techniques.
- Suite à la mise à niveau des fonctionnalités de Windows 10, un redémarrage est **nécessaire** pour finaliser Dell Encryption. Le message suivant s'affiche dans la zone de notification après la mise à niveau des fonctionnalités de Windows 10 :



Conditions préalables

- Microsoft .Net Framework 4.5.2 (ou version ultérieure) est nécessaire pour les programmes d'installation principal et enfant. Le programme d'installation n'installe pas le composant Microsoft .Net Framework.

  REMARQUE : .Net Framework 4.6 (ou version ultérieure) est nécessaire pour l'exécution du mode FIPS.

- Le programme d'installation principal installe les conditions préalables suivantes si elles ne sont pas déjà installées sur l'ordinateur. **Lors de l'utilisation du programme d'installation enfant**, vous devez installer ce composant avant d'installer Encryption.

Conditions préalables
○ Visual C++ 2012 Redistributable Package (x86 ou x64) Mise à jour 4 ou ultérieure ○ Visual C++ 2017 Redistributable Package (x86 ou x64) Mise à jour 3 ou ultérieure ○ Sans ces mises à jour installées, les applications et modules d'installation signés avec des certificats SHA1 fonctionnent, mais une erreur s'affiche sur le point de terminaison lors de l'installation ou de l'exécution des applications.

Matériel

- Le tableau suivant indique la configuration matérielle minimale prise en charge.

Matériel
○ Processeur Intel Pentium ou AMD ○ 110 Mo d'espace disque disponible ○ 512 Mo de RAM **REMARQUE :** De l'espace disque libre supplémentaire est nécessaire pour chiffrer les fichiers sur le point de terminaison. Cette taille varie en fonction des stratégies et de la capacité du lecteur.

- Le tableau suivant répertorie les matériels informatiques compatibles.

Matériel intégré en option
○ TPM 1.2 ou 2.0

Systèmes d'exploitation

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

Systèmes d'exploitation Windows (32 bits et 64 bits)
○ Windows 10 : Éducation, Entreprise, Pro v1909-v22H2 (mise à jour novembre 2019/19H2 - Mise à jour novembre 2022/22H2) **Remarque :** les OEM et ODM ne sont pas livrés avec Windows 10 v2004 (mise à jour de mai 2020/20H1 et versions ultérieures) avec une architecture 32 bits. Pour plus d'informations, voir https://docs.microsoft.com/windows-hardware/design/minimum/minimum-hardware-requirements-overview. ■ Windows 10 2019 LTSC ■ Windows 10 2021 LTSC ○ Windows 11 : Entreprise, Pro v21H2 - 22H2

Systèmes d'exploitation Encryption External Media

- Le support externe doit disposer d'environ 55 Mo, ainsi que d'un espace libre sur le support égal au plus gros fichier à chiffrer, pour héberger Encryption External Media.
- La liste suivante décrit les systèmes d'exploitation pris en charge lors de l'accès à des supports sécurisés par Dell.

Systèmes d'exploitation Windows pris en charge pour accéder à un support chiffré (32 bits et 64 bits)
○ Windows 10 : Éducation, Entreprise, Pro v1909-v22H2 (mise à jour novembre 2019/19H2 - Mise à jour novembre 2022/22H2) **Remarque :** les OEM et ODM ne sont pas livrés avec Windows 10 v2004 (mise à jour de mai 2020/20H1 et versions ultérieures) avec une architecture 32 bits. Pour plus d'informations, voir https://docs.microsoft.com/windows-hardware/design/minimum/minimum-hardware-requirements-overview. ■ Windows 10 2019 LTSC ■ Windows 10 2021 LTSC ○ Windows 11 : Entreprise, Pro v21H2 - 22H2

Systèmes d'exploitation Mac pris en charge pour accéder à un support chiffré (noyaux 64 bits)
○ macOS High Sierra 10.13.5 - 10.13.6 ○ macOS Mojave 10.14.0 - 10.14.4 ○ macOS Catalina 10.15.5 - 10.15.6

Localisation

- Encryption est compatible avec l'interface utilisateur multilingue et localisé dans les langues suivantes.

Langues prises en charge	
○ EN : anglais	○ JA : japonais
○ ES : espagnol	○ KO : coréen
○ FR : français	○ PT-BR : portugais brésilien

Langues prises en charge	
○ IT : italien	○ PT-PT : portugais du Portugal (ibère)
○ DE : allemand	

SED Manager

- IPv6 n'est pas pris en charge.
- Après avoir appliqué des règles, préparez-vous à redémarrer l'ordinateur avant de pouvoir les mettre en application.
- Les ordinateurs équipés de disques auto-cryptables ne peuvent pas être utilisés avec des cartes HCA. Il existe des incompatibilités qui empêchent le provisionnement des accélérateurs HCA. Notez que Dell ne vend pas d'ordinateurs comportant des disques à auto-chiffrement prenant en charge le module HCA. Cette configuration non prise en charge est une configuration après-vente.
- Si l'ordinateur ciblé pour chiffrement est équipé d'un accélérateur d'un disque à autochiffrement, vérifiez que l'option Active Directory, *l'utilisateur doit changer de mot passe lors de la prochaine connexion*, est désactivée. L'authentification avant démarrage ne prend pas en charge cette option Active Directory.
- SED Manager n'est pas pris en charge avec les configurations à plusieurs disques.
- **REMARQUE :**

  En raison de la nature du RAID et des SED, SED Manager ne prend pas en charge le RAID. *RAID=On* avec disques SED présente un problème : le RAID exige un accès au disque pour la lecture et l'écriture des données associées au RAID dans un secteur élevé non disponible sur un SED verrouillé dès le début, et, pour lire ces données, ne peut pas attendre que l'utilisateur se connecte. Pour résoudre le problème, dans le BIOS, définissez l'opération SATA sur *AHCI* au lieu de *RAID=On*. Si les pilotes de contrôleur AHCI ne sont pas pré-installés sur le système d'exploitation, ce dernier plante lors du passage de *RAID=On* à *AHCI*.

- Le programme d'installation principal installe les conditions préalables suivantes si elles ne sont pas déjà installées sur l'ordinateur. **Lors de l'utilisation du programme d'installation enfant**, vous devez installer ce composant avant d'installer SED Manager.

Conditions préalables
○ Visual C++ 2017 Redistributable Package (x86 ou x64) Mise à jour 3 ou ultérieure
○ Sans ces mises à jour installées, les applications et modules d'installation signés avec des certificats SHA1 fonctionnent, mais une erreur s'affiche sur le point de terminaison lors de l'installation ou de l'exécution des applications.

- La configuration des disques à chiffrement automatique pour SED Manager est différente entre les disques NVMe et non NVMe (SATA).
  - Tout disque NVMe utilisé pour la fonction PBA :
    - Si l'appareil Dell a été fabriqué en 2018 ou après : RAID ON ou AHCI peut être utilisé avec les disques NVMe.
    - Le mode de démarrage du BIOS doit être défini sur UEFI (Unified Extensible Firmware Interface). Les ROM de l'opération existante doivent être désactivées.
  - Tout disque non NVMe utilisé pour la fonction PBA :
    - L'opération SATA du BIOS peut être définie sur AHCI ou RAID ON.
    - Le système d'exploitation plante lorsqu'il est transféré de RAID ON à AHCI si les disques du contrôleur AHCI ne sont pas préinstallés. Pour obtenir des instructions sur le passage de RAID à AHCI (ou vice-versa), reportez-vous à l'article de la base de connaissances 124714.

  Les lecteurs SED compatibles OPAL pris en charge exigent les pilotes Intel Rapid Storage Technology mis à jour, disponibles à l'adresse www.dell.com/support. Dell recommande la dernière version du pilote Intel Rapid Storage Technology avec des disques NVMe.

  REMARQUE : Les pilotes Intel Rapid Storage Technology dépendent de la plate-forme. Vous pouvez obtenir le pilote de votre système en suivant le lien ci-dessus, en fonction du modèle de votre ordinateur.

- Les configurations de chiffrement à plusieurs disques avec SED Manager nécessitent les conditions suivantes :

- Tous les disques du système cible doivent être des disques à auto-chiffrement (SED).
- Tous les disques du système cible doivent être configurés dans le même mode de démarrage.
- En mode de démarrage UEFI, le système d'exploitation peut être installé sur n'importe quel disque cible.
- En mode de démarrage hérité, le système d'exploitation doit être installé sur le premier disque (Disque 0). Si le système d'exploitation n'est pas installé sur le premier disque, le chiffrement sur plusieurs disques est désactivé.

- Certaines versions du BIOS peuvent activer le SID de bloc par défaut, ce qui peut désactiver SED Manager. Pour plus d'informations, reportez-vous à l'article de la base de connaissances 126083.
- Les mises à jour des fonctionnalités Direct à partir de Windows 10 v1607 (mise à jour anniversaire/Redstone 1) vers Windows 10 v1903 (mise à jour mai 2019/19H1) ne sont pas prises en charge avec Dell Encryption. Dell vous recommande de mettre à jour le système d'exploitation avec une mise à jour des fonctionnalités plus récente en cas de mise à jour vers Windows 10 v1903. Si vous tentez d'effectuer la mise à jour directement de Windows 10 v1607 à v1903, un message d'erreur s'affiche et la mise à jour est impossible.
- **REMARQUE :** Un mot de passe est requis pour l'authentification avant démarrage. Dell vous recommande de définir un mot de passe d'au moins 9 caractères.

- **REMARQUE :** Un mot de passe est requis pour tous les utilisateurs ajoutés dans le panneau *Ajouter un utilisateur*. Les utilisateurs ayant un mot de passe de longueur nulle ne pourront plus utiliser l'ordinateur suite à l'activation.
- **REMARQUE :** Les ordinateurs protégés par SED Manager doivent effectuer la mise à jour vers Windows 10 v1703 (mise à jour Creators Update/Redstone 2) ou une version ultérieure avant d'effectuer la mise à jour vers Windows 10 v1903 (mise à jour mai 2019/19H1) ou une version ultérieure. Si vous tentez cette stratégie de mise à niveau, un message d'erreur s'affiche.
- SED Manager nécessite l'utilisation du fournisseur d'informations d'identification personnalisé Dell pour synchroniser les modifications de mots de passe Windows et les clés de chiffrement des données. Si vous avez besoin d'utiliser des applications tierces qui utilisent des fournisseurs d'informations d'identification personnalisés s'exécutant sur des ordinateurs protégés par SED Manager, vous devez lancer les modifications de mots de passe Windows via la Data Security Console. Pour plus d'informations sur la modification de votre mot de passe dans la Data Security Console, voir le chapitre *Mot de passe* du Guide de l'utilisateur de Data Security Console.

Matériel

- Pour consulter la toute dernière liste de SED compatibles Opal pris en charge par SED Manager, reportez-vous à l'article de la base de connaissances 126855.
- Pour consulter la toute dernière liste des plates-formes compatibles avec SED Manager, reportez-vous à l'article de la base de connaissances 126855.
- Pour obtenir la liste des stations d'accueil et des adaptateurs compatibles avec SED Manager, reportez-vous à l'article de la base de connaissances 124241.

Claviers internationaux

Le tableau suivant répertorie les claviers internationaux pris en charge avec l'authentification avant démarrage sur les ordinateurs avec ou sans UEFI.

Clavier international pris en charge - UEFI	
DE-FR - Suisse (français)	EN-GB - Anglais (anglais britannique)
DE-CH - Suisse (allemand)	EN-CA - Anglais (anglais canadien)
EN-US - Anglais (anglais américain)	

Clavier International prise en charge : Non-UEFI	
AR - Arabe (avec lettres latines)	EN-US - Anglais (anglais américain)
DE-FR - Suisse (français)	EN-GB - Anglais (anglais britannique)
DE-CH - Suisse (allemand)	EN-CA - Anglais (anglais canadien)

Systèmes d'exploitation

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

Systèmes d'exploitation Windows (32 bits et 64 bits)
○ Windows 10 : Éducation, Entreprise, Pro v1909-v22H2 (mise à jour novembre 2019/19H2 - Mise à jour novembre 2022/22H2) **Remarque :** les OEM et ODM ne sont pas livrés avec Windows 10 v2004 (mise à jour de mai 2020/20H1 et versions ultérieures) avec une architecture 32 bits. Pour plus d'informations, voir https://docs.microsoft.com/windows-hardware/design/minimum/minimum-hardware-requirements-overview. ▪ Windows 10 2019 LTSC ▪ Windows 10 2021 LTSC ○ Windows 11 : Entreprise, Pro v21H2 - 22H2

Les fonctions d'authentification sont disponibles uniquement lorsque l'authentification avant démarrage est activée.

Localisation

SED Manager est compatible avec l'interface utilisateur multilingue et est localisée dans les langues suivantes. Le mode UEFI et l'authentification avant démarrage prennent en charge les langues suivantes :

Langues prises en charge	
• EN : anglais	• JA : japonais
• FR : français	• KO : coréen
• IT : italien	• PT-BR : portugais brésilien
• DE : allemand	• PT-PT : portugais du Portugal (ibère)
• ES : espagnol	

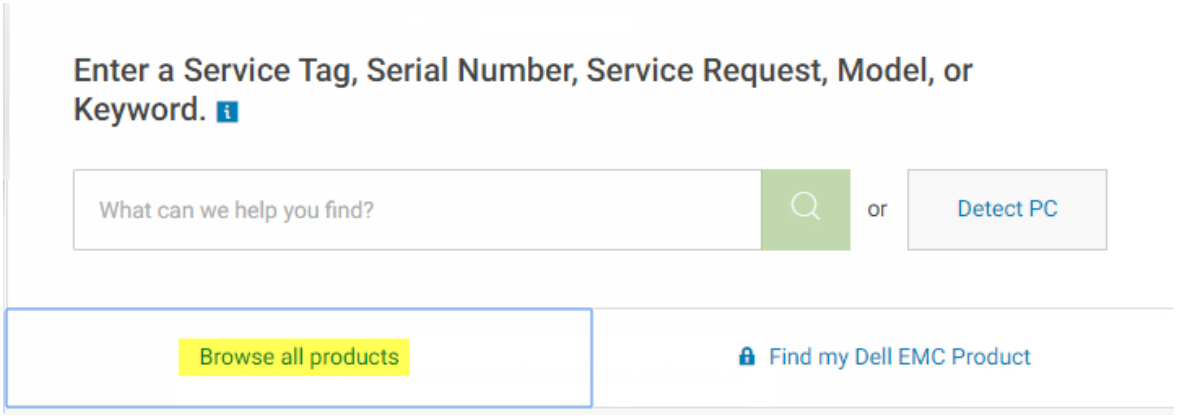
3

Téléchargement du logiciel

Cette section détaille l'obtention du logiciel depuis dell.com/support. Si vous possédez déjà le logiciel, veuillez ignorer cette section.

Rendez-vous sur dell.com/support pour commencer.

1. Sur la page Web de support Dell, sélectionnez **Parcourir tous les produits**.



2. Sélectionnez **Sécurité** dans la liste des produits.
3. Sélectionnez **Dell Data Security**.

   Le site Web se rappelle la sélection initiale.
4. Sélectionnez le produit Dell.

   Exemples :

   Dell Encryption Enterprise

   Dell Endpoint Security Suite Enterprise
5. Sélectionnez **Pilotes et téléchargements**.
6. Sélectionnez le type de système d'exploitation client souhaité.
7. Sélectionnez **Dell Encryption** dans les correspondances. Ceci n'étant qu'un exemple, elles pourront être légèrement différentes. Par exemple, il pourra ne pas exister quatre fichiers parmi lesquels choisir.
8. Sélectionnez **Téléchargement**.

   Passez à l'étape Installation d'Encryption Personal.

4

Installation

Vous pouvez installer Encryption Personal à l'aide du programme d'installation principal (recommandé) ou individuellement en extrayant les programmes d'installation enfants du programme d'installation principal. Dans les deux cas, Encryption Personal peut être installé par l'interface utilisateur, à l'aide d'une ligne de commande ou de scripts, par le biais de toute technologie Push disponible dans votre entreprise.

Les utilisateurs devraient consulter les fichiers d'aide suivants en cas de besoin au moment de l'application :

REMARQUE : Si le chiffrement basé sur des règles est installé avant Encryption Management Agent, l'ordinateur peut se bloquer. Ce problème est dû à l'échec du chargement du pilote de veille pour le chiffrement qui gère l'environnement PBA. Pour contourner ce problème, utilisez le programme d'installation principal ou vérifiez que le chiffrement basé sur des règles est installé après Encryption Management Agent.

- Pour apprendre à utiliser les fonctionnalités d'Encryption, reportez-vous à l'*Aide concernant Dell Encrypt*. Accédez à l'aide à partir de `<Install dir>\Program Files\Dell\Dell Data Protection\Encryption\Help`.
- Voir l'*Encryption External Media* pour apprendre à utiliser les fonctionalités d'Encryption External Media. Accédez à l'aide à partir de `<Install dir>\Program Files\Dell\Dell Data Protection\Encryption`.
- Pour apprendre à utiliser les fonctionnalités d'Advanced Authentication, voir l'*Encryption Personal*. Accédez à l'aide à partir de `<Install dir>\Program Files\Dell\Dell Data Protection\Security Tools\Help`.

Importation d'un droit

L'installation d'Encryption Personal nécessite une clé de registre sur l'ordinateur cible. Cette clé de registre est ajoutée via l'interface de ligne de commande au cours de l'installation ou via l'interface utilisateur avant l'installation.

Pour ajouter la clé de registre via l'interface de ligne de commande, voir Installation par ligne de commande.

Pour ajouter la clé de registre via l'interface utilisateur :

1. Ouvrez un éditeur de texte.
2. Ajoutez le texte suivant.

   ```
   [HKEY_LOCAL_MACHINE\Software\Dell\Dell Data Protection\Entitlement]

   "SaEntitlement"="1:PE:{XXXXX-XXX-XXXX-XXX-XXXX-
   XXXXXXXXXXXX}:xXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX="
   ```

3. Enregistrez le fichier texte avec l'extension `.reg`.
4. Double-cliquez sur le fichier de registre enregistré pour importer le droit Encryption Personal.

Choisir une méthode d'installation

Il existe deux méthodes pour installer le client, sélectionnez l'**une** des suivantes :

- Installation interactive - RECOMMANDÉE
- Installation par ligne de commande

Installation interactive

Pour installer Encryption Personal, le programme d'installation doit trouver le droit approprié sur l'ordinateur. Si le droit approprié est introuvable, Encryption Personal ne peut pas être installé.

- Le programme d'installation principal installe plusieurs clients. Dans le cas d'Encryption Personal, il installe Encryption et la gestion SED.

- Les fichiers journaux du Programme d'installation principal sont disponibles à l'adresse `C:\ProgramData\Dell\Dell Data Protection\Installer`.

1. Installez le droit sur l'ordinateur cible, si nécessaire. Les instructions pour l'ajout du droit à l'ordinateur sont incluses avec l'e-mail contenant les informations de licence.
2. Copiez DDSSetup.exe sur l'ordinateur local.
3. Double-cliquez sur DDSSetup.exe pour lancer le programme d'installation.
4. La boîte de dialogue qui s'affiche indique le statut de l'installation de conditions préalables. Ceci prend quelques minutes.
5. Cliquez sur **Suivant** sur l'écran de bienvenue.
6. Lisez le contrat de licence, acceptez-en les termes, puis cliquez sur **Suivant**.
7. Cliquez sur **Suivant** pour installer Encryption Personal à l'emplacement par défaut `C:\Program Files\Dell\Dell Data Protection\`.
8. Authentication est installé par défaut et ne peut pas être désélectionné. Il correspond à Security Framework dans le programme d'installation.

   Cliquez sur **Suivant**.
9. Cliquez sur **Installer** pour démarrer l'installation.

   Une fenêtre de statut s'affiche. Ceci peut prendre plusieurs minutes.
10. Sélectionnez **Oui, je souhaite redémarrer mon ordinateur maintenant**, puis cliquez sur **Terminer**.
11. Lorsque l'ordinateur redémarre, authentifiez-vous dans Windows.

L'installation d'Encryption Personal et d'Advanced Authentication est terminée.

L'Assistant de configuration d'Encryption Personal et la configuration sont traités séparément.

Une fois l'Assistant de configuration d'Encryption Personal et la configuration terminés, lancez la Console Encryption Personal Administrator.

Le reste de cette section présente des informations détaillées sur d'autres tâches d'installation et peut être ignoré. Passez aux Assistants de configuration d'Advanced Authentication et d'Encryption Personal.

Installation par ligne de commande

Pour installer Encryption Personal à l'aide de la ligne de commande, vous devez préalablement extraire les fichiers exécutables enfant du programme d'installation principal. Voir Extraire les programmes d'installation enfants du programme d'installation principal. Après avoir terminé, revenez à cette section.

- Installez le droit sur l'ordinateur cible, si nécessaire.
- **REMARQUE :** Les journaux Dell Encryption n'indiquent pas si un espace disque insuffisant a provoqué l'échec de l'installation.
- Commutateurs :

  Pour une installation par ligne de commande, les commutateurs doivent être spécifiés au préalable. Le tableau suivant indique les commutateurs disponibles dans le cadre de l'installation.

Commutateur	Signification
/s	Mode Silencieux
/z	Envoi des données à la variable système InstallScript CMDLINE

- Paramètres :

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

Paramètres
InstallPath=chemin de l'emplacement d'installation alternatif.
FEATURES=PE

Paramètres
ENTITLEMENT=1:PE:{Encryption Personal Entitlement key here} **REMARQUE :** Ce paramètre peut **uniquement** être utilisé avec Encryption Personal

- Exemple d'installation par ligne de commande

  Le redémarrage a été supprimé dans les exemples de ligne de commande. Cependant, un redémarrage éventuel est requis.

  Le chiffrement basé sur les règles ne pourra commencer que lorsque l'ordinateur aura redémarré.

  Veillez à placer une valeur contenant un ou plusieurs caractères spéciaux, tels qu'un espace, entre des guillemets d'échappement (sans programmation spéciale).

  Les lignes de commande tiennent compte de la casse.

- L'exemple suivant correspond à l'installation du Encryption client (installation silencieuse, pas de redémarrage et installation dans l'emplacement par défaut `C:\Program Files\Dell\Dell Data Protection`) en transmettant la clé de droit directement au programme d'installation.

  DDPE_XXbit_setup.exe /s /v"ENTITLEMENT=1:PE:{XXXXX-XXX-XXXX-XXX-XXXX-XXXXX-XXXXXXX}:xXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX= /l*v c:\Shieldinstall.log /qn /norestart"

- L'exemple suivant correspond à l'installation d'Encryption Personal (installation silencieuse, pas de redémarrage, installation à l'emplacement par défaut `C:\Program Files\Dell\Dell Data Protection`).

  ```
  DDSSetup.exe /s /z"\"FEATURE=PE\""
  ```

- L'exemple suivant correspond à l'installation d'Encryption Personal et d'Advanced Authentication (installation silencieuse, pas de redémarrage et installation dans l'emplacement alternatif `C:\Program Files\Dell\My_New_Folder`).

  ```
  DDSSetup.exe /s /z"\"FEATURE=PE, InstallPath=C:\Program Files\Dell\My_New_Folder\""
  ```

  Une fois l'ordinateur redémarré, authentifiez-vous dans Windows.

  L'installation d'Encryption Personal et d'Advanced Authentication est terminée.

  L'Assistant de configuration d'Encryption Personal et la configuration sont traités séparément.

  Une fois l'Assistant de configuration d'Encryption Personal et la configuration terminés, lancez la Console Encryption Personal Administrator.

  Le reste de cette section présente des informations détaillées sur d'autres tâches d'installation et peut être ignoré. Accédez aux Assistants de configuration d'Advanced Authentication et de Personal Edition.

5

Assistants de configuration d'Advanced Authentication et d'Encryption Personal

Connectez-vous avec vos nom d'utilisateur et mot de passe Windows. Vous accédez en toute transparence à Windows. L'interface peut présenter un aspect différent de celui auquel vous êtes habitué.

1. Vous pouvez être invité par UAC à exécuter l'application. Si oui, cliquez sur Oui.
2. L'Assistant Activation d'Advanced Authentication s'affiche après le redémarrage de l'installation initiale. Cliquez sur **Suivant**.
3. Saisissez et entrez de nouveau un nouveau mot de passe d'Administrateur de chiffrement (EAP). Cliquez sur **Suivant**.

   Remarque : le mot de passe de l'administrateur du chiffrement doit comporter au moins huit caractères et ne peut pas dépasser 127 caractères.
4. Pour stocker les informations de restauration, saisissez un emplacement de sauvegarde sur un lecteur réseau ou un support amovible, puis cliquez sur **Suivant**.
5. Cliquez sur **Appliquer** pour commencer l'activation d'Advanced Authentication.

   Une fois l'Assistant Activation d'Advanced Authentication terminé, passez à l'étape suivante.
6. Lancez l'Assistant d'installation d'Encryption Personal à partir de l'icône Dell Encryption dans la zone de notification (il peut se lancer automatiquement).

   Cet Assistant Configuration facilite l'utilisation du chiffrement pour protéger les informations qui figurent sur l'ordinateur. Si cet Assistant n'est pas terminé, le chiffrement ne peut pas commencer.

   Lisez l'écran de bienvenue, puis cliquez sur **Suivant**.
7. Sélectionnez un modèle de règles. Le modèle de règles établit les paramètres de règles par défaut du chiffrement

   Une fois la configuration initiale terminée, vous pouvez facilement appliquer un autre modèle de règles ou personnaliser le modèle sélectionné dans la console locale de gestion.

   Cliquez sur **Suivant**.
8. Veuillez prendre en compte l'avertissement concernant le mot de passe Windows. Pour créer un mot de passe Windows maintenant, voir Exigences.
9. Créez un caractère 8-127 Mot de passe administrateur de chiffrement (EAP) et confirmez. Le mot de passe doit comporter des caractères alphabétiques, numériques et spéciaux. Ce mot de passe peut être identique à l'EAP que vous avez défini pour Advanced Authentication, mais il n'est pas associé à celui-ci. **Enregistrez et sauvegardez ce mot de passe en lieu sûr**. Cliquez sur **Suivant**.

   Remarque : le mot de passe de l'administrateur du chiffrement doit comporter au moins huit caractères et ne peut pas dépasser 127 caractères.
10. Cliquez sur **Parcourir** pour choisir un lecteur réseau ou un périphérique amovible pour sauvegarder vos clés de chiffrement (qui sont encapsulées dans l'application LSARecovery_[hostname].exe).

    Ces clés servent à récupérer vos données, suite à certaines défaillances de l'ordinateur.

    Vous devrez parfois les sauvegarder à nouveau après certaines modifications de règles de chiffrement. Si le disque réseau ou le stockage amovible est disponible, la sauvegarde des clés de chiffrement est effectuée en arrière-plan. Toutefois, si l'emplacement n'est pas disponible (ex. : le périphérique de stockage amovible original n'est pas inséré), les modifications de règles ne prennent effet qu'après la sauvegarde manuelle des clés de chiffrement.

    REMARQUE : Pour en savoir plus sur la sauvegarde manuelle des clés de chiffrement, cliquez sur « **?** > **Aide** » dans l'angle supérieur droit de la console de gestion locale ou sur **Démarrer > Dell > Chiffrement - Aide.**

    Cliquez sur **Suivant**.

11. La liste des paramètres de chiffrement s'affiche sur l'écran Confirmer les paramètres de chiffrement Vérifiez les éléments, et si les paramètres sont corrects, cliquez sur **Confirmer**.

    La configuration de l'ordinateur démarre. Une barre d'état indique l'avancée du processus de configuration.

12. Cliquez sur **Terminer** pour terminer la configuration.

13. Un redémarrage est requis une fois l'ordinateur configuré pour le chiffrement. Cliquez sur **Redémarrer maintenant** ou vous pouvez reporter le redémarrage 5 x 20 minutes chacun.

14. Une fois l'ordinateur redémarré, ouvrez la Console de gestion locale depuis le menu Démarrer pour afficher l'état du chiffrement.

    Le chiffrement s'effectue en arrière-plan. La Console de gestion locale peut être ouverte ou fermée. Le chiffrement des fichiers n'en sera pas affecté. Vous pouvez continuer à utiliser votre système lors du chiffrement.

15. Lorsque l'analyse est terminée, l'ordinateur redémarre une fois de plus.

    Une fois tous les balayages et redémarrages terminés, vous pouvez vérifier l'état de conformité en lançant la Console de gestion locale. La mention « Conforme » s'affiche en regard du nom du lecteur.

6

Configuration des paramètres de la console

Les paramètres par défaut permettent aux administrateurs et aux utilisateurs d'utiliser l'authentification avancée immédiatement après l'activation, sans aucune configuration supplémentaire. Les utilisateurs sont ajoutés automatiquement comme utilisateurs de l'authentification avancée lorsqu'ils se connectent à l'ordinateur avec leur mot de passe Windows, mais l'authentification Windows multifacteur n'est pas activée par défaut.

Pour configurer les fonctions d'authentification avancée, vous devez être administrateur sur l'ordinateur.

Changement du mot de passe de l'administrateur et de l'emplacement de sauvegarde

Après l'activation d'Advanced Authentication, le mot de passe d'administrateur et l'emplacement de sauvegarde peuvent être changés, si nécessaire.

1. En tant qu'administrateur, lancez la console Dell Data Security à partir du raccourci sur le bureau.
2. Cliquez sur la mosaïque **Paramètres d'administrateur**.
3. Dans la boîte de dialogue Authentification, entrez le mot de passe d'administrateur qui a été configuré pendant l'activation, puis cliquez sur **OK.**
4. Cliquez sur l'onglet **Paramètres administrateur**.
5. Dans la page Modifier le mot de passe d'administrateur, pour modifier le mot de passe, entrez un nouveau mot de passe contenant 8 à 32 caractères et comprenant au moins une lettre, un chiffre et un caractère spécial.
6. Saisissez à nouveau le mot de passe pour le confirmer, puis cliquez sur **Appliquer**.
7. Pour modifier l'emplacement de stockage de la clé de récupération, dans le panneau de gauche, sélectionnez **Modifier l'emplacement de sauvegarde**.
8. Sélectionnez un nouvel emplacement pour la sauvegarde, puis cliquez sur **Appliquer**.

   Le fichier de sauvegarde doit être enregistré soit sur un lecteur réseau, soit sur un support amovible. Il contient les clés nécessaires à la récupération des données sur l'ordinateur. Dell ProSupport doit avoir accès à ce fichier pour pouvoir vous aider à récupérer les données.

   Les données de récupération sont sauvegardées automatiquement à l'emplacement défini. Si l'emplacement n'est pas disponible (par exemple, si votre clé USB de sauvegarde n'est pas insérée), Advanced Authentication vous invitera à indiquer un emplacement où sauvegarder vos données. L'accès aux données de récupération est requis pour commencer le chiffrement.

Configuration avant démarrage

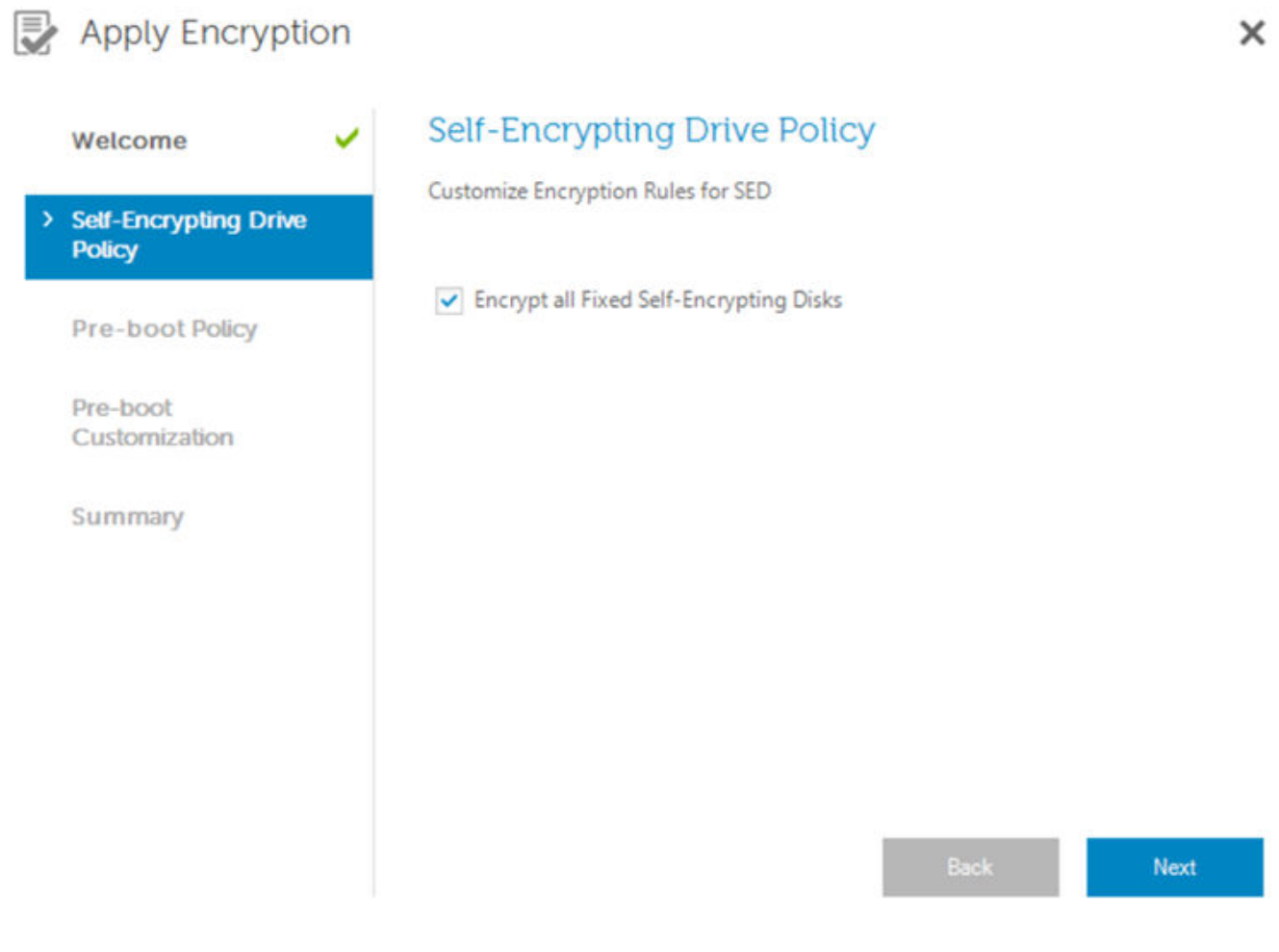
La PBA est disponible si votre ordinateur est équipé d'un SED. Elle est configurée via l'onglet Chiffrement. Lorsque SED Manager devient propriétaire du SED, la PBA est activée.

Pour activer la gestion SED :

1. Dans la console Data Security, cliquez sur la mosaïque **Paramètres d'administrateur**.
2. Vérifiez que l'emplacement de sauvegarde est accessible depuis l'ordinateur.

   Si le message *Emplacement de sauvegarde introuvable* s'affiche et que l'emplacement de sauvegarde se trouve sur un lecteur USB, le lecteur n'est pas connecté ou il est connecté dans un autre logement que celui utilisé lors de la sauvegarde. Si le message s'affiche et que l'emplacement de sauvegarde se trouve sur un lecteur réseau, le lecteur est inaccessible depuis l'ordinateur. S'il est nécessaire de changer l'emplacement de sauvegarde, dans l'onglet **Paramètres administrateur**, sélectionnez **Changer l'emplacement de sauvegarde** pour remplacer l'emplacement par le logement ou le lecteur accessible actuel. Quelques secondes après la redéfinition de l'emplacement, le processus d'activation du chiffrement peut continuer.

3. Cliquez sur l'onglet **Chiffrement**, puis sur **Chiffrer**.
4. Dans la page d'accueil, cliquez sur Suivant.
5. Sélectionnez **Chiffrer tous les disques à autochiffrement fixes** pour activer le chiffrement sur plusieurs disques.



6. Dans la page Stratégie avant démarrage, modifiez ou confirmez les valeurs suivantes, puis cliquez sur **Suivant**.

Tentatives de connexion d'un utilisateur non placé en mémoire cache	Nombre de tentatives de connexion possibles pour un utilisateur inconnu (un utilisateur qui ne s'est pas encore connecté à l'ordinateur [aucune information d'identification en cache]).
Tentatives de connexion d'un utilisateur placé en mémoire cache	Nombre de fois qu'un utilisateur connu peut tenter de se connecter.
Tentatives de réponse aux questions de récupération	Nombre de fois que l'utilisateur peut tenter d'entrer la réponse correcte.
Activer un mot de passe de suppression de chiffrement	Sélectionnez pour l'activer.
Entrez le mot de passe de suppression de chiffrement	Un mot ou un code de 100 caractères maximum, servant de mécanisme de sécurité en cas de défaillance. La saisie de ce mot ou de ce code dans le champ Nom d'utilisateur ou Mot de passe pendant l'authentification PBA déclenche un effacement cryptographique qui supprime les clés du stockage sécurisé. Une fois que ce processus est invoqué, le lecteur est irrécupérable. N'entrez rien dans ce champ si vous ne voulez pas disposer d'un mot de passe d'effacement cryptographique en cas d'urgence.

	N'entrez rien dans ce champ si vous ne voulez pas disposer d'un mot de passe d'effacement cryptographique en cas d'urgence.
Se souvenir de moi	Permet ou non aux utilisateurs de cocher « Mémoriser mes informations » sur l'écran d'ouverture de session de la fonctionnalité PBA.

7. Dans la page Personnalisation du prédémarrage, entrez le texte à afficher dans l'écran Preboot Authentication (PBA), puis cliquez sur **Suivant.**

Texte du titre de prédémarrage	Ce texte s'affiche dans l'écran PBA. Si vous n'entrez rien dans ce champ, aucun titre ne s'affiche. Le texte n'est pas renvoyé à la ligne. Si vous entrez plus de 17 caractères, le texte est tronqué.
Texte du service clientèle	Texte qui sera affiché sur l'écran d'assistance concernant la prise en charge de l'authentification avant démarrage. Personnalisez le message afin d'y inclure les instructions à suivre pour contacter le centre d'assistance technique ou l'administrateur de la sécurité. Si ce champ n'est pas renseigné, les coordonnées du support ne s'affichent pas. Le renvoi à la ligne automatique se produit au niveau du mot et non pas du caractère. Si un mot dépasse 50 caractères environ, il ne bénéficie pas de renvoi à la ligne automatique et aucune barre de défilement n'est proposée, ce qui entraîne la troncature du texte.
Avertissement légal	Ce texte s'affiche avant que l'utilisateur ne soit autorisé à se connecter au périphérique. Par exemple : « En cliquant sur OK, vous acceptez la politique d'utilisation de l'ordinateur ». Si vous n'entrez pas de texte dans ce champ, aucun texte ou bouton OK/Annuler ne s'affiche. Le renvoi à la ligne automatique se produit au niveau du mot et non pas du caractère. Ainsi, si un mot comporte plus d'une cinquantaine de caractères, il ne bénéficie pas de renvoi à la ligne automatique et aucune barre de défilement n'est proposée. Le texte sera donc tronqué.

8. Dans la page récapitulative, cliquez sur **Appliquer**.
9. Lorsque vous y êtes invité, cliquez sur **Arrêter**.

   Un arrêt complet est requis pour que le chiffrement soit lancé.

10. Après l'arrêt, redémarrez l'ordinateur.

    L'authentification est désormais gérée par Encryption Management Agent. Les utilisateurs doivent se connecter dans l'écran PBA avec leurs mots de passe Windows.

Modification des paramètres de gestion SED et de gestion PBA

Après l'activation du chiffrement et la configuration de la stratégie de prédémarrage et la personnalisation initiales, les actions suivantes sont disponibles dans l'onglet Chiffrement :

- Modifier les règles ou la personnalisation du prédémarrage : cliquez sur l'onglet **Chiffrement**, puis cliquez sur **Modifier**.
- Déchiffrer la gestion SED, par exemple, pour la désinstallation : cliquez sur **Déchiffrer**

Après l'activation de la gestion SED et la configuration de la stratégie de prédémarrage et la personnalisation initiales, les actions suivantes sont disponibles dans l'onglet Paramètres de prédémarrage :

- Modifier les règles ou la personnalisation du prédémarrage : cliquez sur l'onglet **Paramètres de prédémarrage** et sélectionnez **Stratégie pour les disques à autochiffrement**, **Stratégie de prédémarrage** ou **Personnalisation du prédémarrage**.

Gestion des utilisateurs et de leur authentification

Ajouter un utilisateur

Les utilisateurs Windows deviennent automatiquement des utilisateurs d'Encryption Personal lorsqu'ils se connectent à Windows ou enregistrent des coordonnées.

L'ordinateur doit être connecté au domaine pour ajouter un utilisateur de domaine dans l'onglet Ajouter un utilisateur de Data Security Console.

1. Dans le volet gauche de l'outil Paramètres administrateur, sélectionnez **Utilisateurs**.
2. Dans l'angle supérieur droit de la page Utilisateur, cliquez sur **Ajouter un utilisateur** pour commencer le processus d'inscription pour un utilisateur Windows existant.
3. Lorsque la boîte de dialogue Sélectionner un utilisateur s'affiche, sélectionnez **Types d'objets**.
4. Entrez le nom d'objet d'un utilisateur dans la zone de texte et cliquez sur **Vérifier les noms**.
5. Cliquez sur **OK** lorsque vous avez terminé.

Suppression d'un utilisateur

1. Dans le volet gauche de l'outil Paramètres administrateur, sélectionnez **Utilisateurs**.
2. Pour supprimer un utilisateur, localisez la colonne correspondant à l'utilisateur et cliquez sur **Supprimer**. (Défilez jusqu'au bas de la colonne de l'utilisateur pour voir l'option Supprimer.)

Supprimer tous les identifiants enregistrés d'un utilisateur

1. Cliquez sur la mosaïque **Paramètres d'administrateur** et effectuez l'authentification avec votre mot de passe.
2. Cliquez sur l'onglet **Utilisateurs** et recherchez l'utilisateur à supprimer.
3. Cliquez sur **Supprimer**. (La commande de suppression apparaît en rouge au bas des paramètres de l'utilisateur).

   Après la suppression, l'utilisateur ne pourra plus se connecter à l'ordinateur, sauf s'il s'enregistre à nouveau.

7

Désinstaller le programme d'installation principal

- Chaque composant doit être désinstallé séparément avant la désinstallation du programme d'installation principal. Les clients doit être désinstallée dans un **ordre spécifique pour éviter les échecs de désinstallation.**
- Suivez les instructions de la section Extraire les programmes d'installation enfants du programme d'installation principal pour obtenir les programmes d'installation enfants.
- Assurez-vous d'utiliser la même version du programme d'installation principal (et donc des clients) pour la désinstallation et l'installation.
- Ce chapitre vous réfère à un autre chapitre qui contient des instructions *détaillées* concernant la désinstallation des programmes d'installation enfants. Ce chapitre explique **uniquement** la dernière étape de désinstallation du programme d'installation principal.

Désinstallez les clients dans l'ordre suivant :

1. Désinstallez le client Encryption.
2. Désinstallez Encryption Management Agent.

Il n'est pas nécessaire de désinstaller le progiciel de pilote.

Accédez à Choisir une méthode de désinstallation.

Choisir une méthode de désinstallation

Il existe deux méthodes d'installation du client, sélectionnez l'**une** des suivantes :

- Désinstaller à partir de Ajout/Suppression de programmes
- Désinstaller à partir de la ligne de commande

Désinstaller de manière interactive

1. Accédez à *Désinstaller un programme* dans le Panneau de configuration Windows (dans la zone de recherche de la barre des tâches, saisissez **Panneau de configuration**, puis sélectionnez *Panneau de configuration* dans les résultats).
2. Sélectionnez le **programme d'installation Dell** et cliquez avec le bouton gauche de la souris sur **Modifier** pour lancer l'Assistant de configuration.
3. Lisez l'écran d'accueil, puis cliquez sur **Suivant**.
4. Suivez les invites pour désinstaller puis cliquez sur **Terminer**.
5. Redémarrez votre ordinateur, puis entrez vos identifiants pour accéder à Windows.

   Le programme d'installation principal est désinstallé.

Désinstaller à partir de la ligne de commande

- L'exemple suivant permet de désinstaller silencieusement le programme d'installation principal.

  ```
  "DDSSetup.exe" /s /x
  ```

  Lorsque vous avez terminé, redémarrez l'ordinateur.

  Le programme d'installation principal est désinstallé.

  Passez à Désinstallation à l'aide des programme d'installation enfants.

8

Désinstaller à l'aide des programme d'installation enfants

- Dell recommande l'utilisation du programme de désinstallation de Data Security pour supprimer Encryption Personal.
- L'utilisateur effectuant l'installation et l'activation doit être un administrateur local ou de domaine. Si vous effectuez une désinstallation à partir de la ligne de commande, vous devez saisir les références d'administrateur.
- Si vous avez installé Encryption Personal à l'aide du programme d'installation principal, vous devez extraire les fichiers exécutables enfants du programme d'installation principal avant la désinstallation, tel qu'indiqué dans Extraire les programmes d'installation enfants du programme d'installation principal.
- Assurez-vous que la version de clients utilisée pour la désinstallation est identique à celle utilisée pour l'installation.
- Dans la mesure du possible, lancez le décryptage la veille au soir.
- Désactivez le mode Veille pour empêcher la mise en veille lors des périodes d'inactivité. Le décryptage ne peut pas être exécuté sur un ordinateur en veille.
- Arrêtez tous les processus et applications afin de minimiser le risque d'échecs de décryptage dus à des fichiers verrouillés.

Désinstallation d'Encryption

- **Avant de lancer la désinstallation**, voir (Facultatif) Créer un fichier journal de Encryption Removal Agent. Ce fichier journal permet de diagnostiquer les erreurs, si vous rencontrez un problème lors de la désinstallation / du déchiffrement Si vous ne souhaitez pas déchiffrer les fichiers à la désinstallation, il n'est pas nécessaire de créer un fichier journal Encryption Removal Agent.

  REMARQUE : Avant la désinstallation, assurez-vous que tous les modèles de stratégie sont définis sur Désactivé et insérez tout support chiffré externe pour un déchiffrement approprié.

  Cette vidéo présente les modifications des modèles de stratégie dans la console de gestion locale.
- Exécutez WSScan pour vous assurer que toutes les données sont dédéchiffrée une fois la désinstallation terminée, mais avant de redémarrer l'ordinateur. Reportez-vous à Utiliser WSScan pour obtenir des instructions.
- A intervalles réguliers, Vérifiez l'état de l'agent Encryption Removal. Le déchiffrement de données est encore en cours si le service Encryption Removal Agent existe encore dans le panneau de services.
-

Choisir une méthode de désinstallation

Il existe deux méthodes de désinstallation du client Encryption, sélectionnez l'**une** des suivantes :

- Désinstaller de manière interactive
- Désinstaller à partir de la ligne de commande

Désinstaller de manière interactive

1. Accédez à *Désinstaller un programme* dans le Panneau de configuration Windows (dans la zone de recherche de la barre des tâches, saisissez **Panneau de configuration**, puis sélectionnez **Panneau de configuration** dans les résultats).
2. Sélectionnez **Dell Encryption XX-bit** et cliquez avec le bouton gauche sur **Modifier** pour lancer l'Assistant de configuration d'Encryption Personal.
3. Lisez l'écran de bienvenue, puis cliquez sur **Suivant**.
4. Lorsque la fenêtre d'installation d'Encryption Removal Agent s'ouvre, choisissez l'une des options :

REMARQUE : La deuxième option est activée par défaut. **Si vous voulez déchiffrer des fichiers, veillez à modifier la sélection selon l'option une**.

- Encryption Removal Agent - Importer des clés à partir d'un fichier

  Pour le chiffrement SDE, Utilisateur ou Commun, cette option déchiffre les fichiers et désinstalle le client Encryption. ***// s'agit de la sélection recommandée.***

- N'installez pas Encryption Removal Agent

  Cette option désinstalle le client Encryption *mais ne décrypte pas les fichiers*. Cette option ne doit être utilisée **qu'à** des fins de dépannage, comme conseillé par Dell Pro Support.

  Cliquez sur **Suivant**.

5. Dans *Fichier de sauvegarde*, saisissez le chemin d'accès au disque réseau ou à l'emplacement du support amovible du fichier de sauvegarde, ou cliquez sur **...** pour rechercher l'emplacement. Le format du fichier est LSARecovery_[hostname].exe.

   Saisissez votre mot de passe d'administrateur de chiffrement. Il s'agit du mot de passe utilisé dans l'Assistant d'installation lorsque le logiciel a été installé.

   Cliquez sur **Suivant**.

6. Dans l'écran *Connexion au Dell Decryption Agent Service en tant que*, sélectionnez **Compte du système local** et cliquez sur **Terminer**.
7. Cliquez sur **Supprimer** à l'écran Supprimer le programme.
8. Lorsque l'écran Installation terminée s'affiche, cliquez sur **Terminer**.
9. Redémarrez votre ordinateur, puis connectez-vous à Windows.

Déchiffrement en cours.

Le déchiffrement peut prendre plusieurs heures en fonction du nombre d'unités à déchiffrer et du volume de données sur les unités. Pour vérifier le processus de déchiffrement, voir Vérifier l'état de l'agent Encryption Removal.

Désinstaller à partir de la 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. Les paramètres de ligne de commande sont sensibles à la casse.
- Utilisez ces programmes d'installation pour désinstaller les clients à l'aide d'une installation avec script, de fichiers de commandes ou de toute technologie Push disponible dans votre entreprise.
- Fichiers journaux

  Windows crée les fichiers journaux de désinstallation de l'unique programme d'installation destinés à l'utilisateur connecté à %temp%, à l'adresse `C:\Users\<UserName>\AppData\Local\Temp`.

  Si vous décidez d'ajouter un fichier journal distinct lorsque vous exécutez le programme d'installation, assurez-vous que le fichier journal possède un nom unique, car les fichiers journaux de programme d'installation enfant ne s'ajoutent pas. La commande standard .msi peut être utilisée pour créer un fichier journal à l'aide de /l `C:\<any directory>\<any log file name>.log`. Dell recommande de ne pas utiliser la consignation détaillée « /l*v » dans une désinstallation avec ligne de commande, car le nom d'utilisateur/mot de passe est enregistré dans le fichier journal.

- Tous les programmes d'installation enfants utilisent les mêmes options d'affichage et commutateurs .msi de base, sauf lorsque cela est précisé, pour les désinstallations avec ligne de commande. Les commutateurs doivent être indiqués en premier. Le commutateur /v est requis et nécessite un argument. D'autres paramètres figurent dans un argument transmis au commutateur /v.

  Les options d'affichage peuvent être spécifiées en fin d'argument transmis au commutateur /v, pour obtenir le comportement voulu. N'utilisez pas /q et /qn dans la même ligne de commande. Utilisez uniquement ! et - après /qb.

Commutateur	Signification
/v	Transmission des variables au fichier .msi dans l'élément setup.exe
/s	Mode Silencieux

Commutateur	Signification
/x	Mode Désinstallation

Option	Signification
/q	Boîte de dialogue Aucune progression, se réinitialise après la fin du processus
/qb	Boîte de dialogue de progression dotée du bouton **Annuler** : vous invite à effectuer un redémarrage
/qb-	Boîte de dialogue de progression avec bouton **Annuler**: redémarre automatiquement à la fin du processus
/qb!	Boîte de dialogue de progression sans bouton **Annuler** : vous invite à effectuer un redémarrage
/qb!-	Boîte de dialogue de progression sans le bouton **Annuler**, redémarre automatiquement une fois le processus terminé
/qn	Pas d'interface utilisateur

- Après son extraction du programme d'installation principal, le programme d'installation du client Encryption est disponible sur `C:\extracted\Encryption\DDPE_XXbit_setup.exe`.
- Le tableau suivant indique les paramètres disponibles dans le cadre de la désinstallation.

Paramètre	Sélection
CMG_DECRYPT	propriété permettant de sélectionner le type d'installation d'Encryption Removal Agent : 2 : obtenir les clés à l'aide du groupe Clé d'analyse approfondie 0 : ne pas installer Encryption Removal Agent
CMGSILENTMODE	Propriété permettant d'activer la désinstallation silencieuse : 1 - Silencieux : requis lors de l'exécution avec des variables msiexec contenant /q ou /qn 0 - Non silencieux : possible uniquement lorsque les variables msiexec contenant /q ne sont pas présentes dans la syntaxe de ligne de commande
DA_KM_PW	Mot de passe du compte d'administrateur de domaine.
DA_KM_PATH	Chemin d'accès au groupe matériel de clés.

- L'exemple suivant illustre la désinstallation du client Encryption sans installer Encryption Removal Agent (Agent de suppression Encryption).

  ```
  DDPE_XXbit_setup.exe /s /x /v"CMG_DECRYPT=0 CMGSILENTMODE=1 DA_KM_PATH=C:
  \FullPathToLSA.exe DA_KM_PW=password /qn /l C:\ddpe_uninstall.txt"
  ```

- L'exemple suivant correspond à la désinstallation du client Encryption à l'aide d'un groupe de clés d'analyse approfondie. Copiez le groupe de clés d'analyse approfondie sur le disque local, puis exécutez cette commande.

  ```
  DDPE_XXbit_setup.exe /s /x /v"CMG_DECRYPT=2 CMGSILENTMODE=1 DA_KM_PATH=C:
  \FullPathToForensicKeyBundle DA_KM_PW=password /qn /l C:\ddpe_uninstall.txt"
  ```

  Lorsque vous avez terminé, redémarrez l'ordinateur.

  Le déchiffrement peut prendre plusieurs heures en fonction du nombre d'unités à déchiffrer et du volume de données sur les unités. Pour vérifier le processus de déchiffrement, voir Vérifier l'état de l'agent Encryption Removal.

Désinstallation d'Encryption Management Agent

Choisir une méthode de désinstallation

Il existe deux méthodes de désinstallation d'Encryption Management Agent, sélectionnez l'**une** des suivantes :

- Désinstaller de manière interactive
- Désinstaller à partir de la ligne de commande

Désinstaller de manière interactive

1. Accédez à *Désinstaller un programme* dans le Panneau de configuration Windows (dans la zone de recherche de la barre des tâches, saisissez **Panneau de configuration**, puis sélectionnez **Panneau de configuration** dans les résultats).
2. Sélectionnez **Dell Encryption Management Agent** et cliquez avec le bouton gauche sur **Modifier** pour lancer l'Assistant de configuration.
3. Lisez l'écran de bienvenue, puis cliquez sur **Suivant**.
4. Suivez les invites pour désinstaller puis cliquez sur **Terminer**.
5. Redémarrez votre ordinateur, puis connectez-vous à Windows.

Client Security Framework est désinstallé..

Désinstaller à partir de la ligne de commande

- Après son extraction du programme d'installation principal, le programme d'installation Encryption Management Agent est disponible sur `C:\extracted\Encryption Management Agent\EMAgent_XXbit_setup.exe`.
- L'exemple suivant correspond à la désinstallation silencieuse de la gestion SED.

  ```
  EMAgent_XXbit_setup.exe /x /s /v" /qn"
  ```

  Après avoir terminé, éteignez et redémarrez l'ordinateur.

9

Programme de désinstallation de Data Security

Désinstaller Encryption Personal

Dell fournit le programme de désintallation de Data Security comme programme de désinstallation maître. Cet utilitaire rassemble les produits actuellement installés et les supprime dans l'ordre approprié.

Le programme de désinstallation de Data Security est disponible sous : `C:\Program Files (x86)\Dell\Dell Data Protection`

Pour obtenir plus d'informations ou pour découvrir comment utiliser l'interface de ligne de commande (CLI), reportez-vous à l'article de la base de connaissances 125052.

Des journaux sont générés sous `C:\ProgramData\Dell\Dell Data Protection\` pour tous les composants qui ont été retirés.

Pour exécuter l'utilitaire, ouvrez le dossier le contenant, faites un clic droit sur **DataSecurityUninstaller.exe**, et sélectionnez **Exécuter en tant qu'administrateur**.

Cliquez sur **Suivant**.

Vous pouvez également effacer n'importe quelle application de la suppression et cliquer sur **Suivant**.

Les dépendances requises sont automatiquement sélectionnées ou effacées.

Pour supprimer des applications sans installer Encryption Removal Agent, choisissez **Ne pas installer Encryption Removal Agent** et sélectionnez **Suivant**.

Sélectionnez **Encryption Removal Agent : importer des clés depuis un fichier**, puis sélectionnez **Suivant**.

Accédez à l'emplacement des clés de récupération, saisissez la phrase de passe pour le fichier et cliquez sur **Suivant**.

Sélectionnez **Supprimer** pour lancer la désinstallation.

Cliquez sur **Terminer** pour terminer la suppression et redémarrez l'ordinateur. L'option **Redémarrer la machine après avoir cliqué sur Terminé** est sélectionnée par défaut.

La désinstallation et la suppression sont terminées.

10

Descriptions des règles et des modèles

Des infobulles s'affichent lorsque vous placez le pointeur de la souris sur une règle dans la console de gestion locale.

Stratégies

Stratégie	Protection avancée pour tous les lecteurs fixes et supports externes	Législation relative à PCI	Législation relative à la protection des données	Législation relative à HIPAA	Protection de base pour tous les lecteurs fixes et disques externes (par défaut)	Protection de base pour tous les lecteurs fixes	Protection de base pour le disque système uniquement	Protection de base pour les supports externes	Cryptage désactivé	Description
Règles relatives au stockage fixe										
Cryptage SDE activé	Vrai								Faux	Il s'agit de la « règle maîtresse » pour toutes les autres règles SDR (System Data Encryption, cryptage des données système). Si cette règle est définie sur Faux, le cryptage SDE n'a pas lieu, indépendamment des autres valeurs de la règle. Vrai = toutes les données non chiffrées par d'autres règles de cryptage basé sur des règles sont chiffrées par les règles de cryptage SDE. Toute modification apportée à cette règle nécessite un redémarrage.
Algorithme de cryptage SDE	AES256									AES-256, AES-128
Règles de cryptage SDE										Règles de cryptage à utiliser pour crypter/ne pas crypter certains disques, répertoires et dossiers.

Stratégie	Protection avancée pour tous les lecteurs fixes et supports externes	Législation relative à PCI	Législation relative à la protection des données	Législation relative à HIPAA	Protection de base pour tous les lecteurs fixes et disques externes (par défaut)	Protection de base pour tous les lecteurs fixes	Protection de base pour le disque système uniquement	Protection de base pour les supports externes	Cryptage désactivé	Description
										Contactez Dell ProSupport si vous ne savez pas comment changer les valeurs par défaut.
Règles relatives aux paramètres généraux										
Cryptage activé	Vrai							Faux		Cette règle est la « règle principale » pour toutes les règles de paramètres généraux. Une valeur Faux signifie l'absence de cryptage, indépendamment des autres valeurs des règles. Une valeur Vrai signifie que toutes les règles de cryptage sont activées. Une modification de la valeur de cette règle lance une nouvelle analyse de cryptage / décryptage.
Dossiers communs cryptés										Chaîne de caractères : 100 entrées maximum de 500 caractères chacune (2 048 caractères maximum) Liste des dossiers des lecteurs du point final à crypter/ne pas crypter disponibles pour tous les utilisateurs gérés qui ont accès au point final. Les lettres génériques sont les suivantes : # : fait référence à tous les lecteurs f# : fait référence à tous les lecteurs fixes r# : fait référence à tous les lecteurs amovibles

Stratégie	Protection avancée pour tous les lecteurs fixes et supports externes	Législation relative à PCI	Législation relative à la protection des données	Législation relative à HIPAA	Protection de base pour tous les lecteurs fixes et disques externes (par défaut)	Protection de base pour tous les lecteurs fixes	Protection de base pour le disque système uniquement	Protection de base pour les supports externes	Cryptage désactivé	Description
										Important : passer outre la protection des répertoires peut empêcher le démarrage de votre ordinateur et/ou nécessiter le reformatage de vos disques/lecteurs. Si le même dossier est concerné par cette règle et la règle Dossiers cryptés de l'utilisateur, c'est cette règle qui prévaut.
Algorithme de cryptage commun	AES256									AES-256, Rijndael 256, AES 128, Rijndael 128 Les fichiers de pagination système sont chiffrés grâce à l'algorithme AES 128 bits.
Liste des données cryptées de l'application (ADE)	winword.exe excel.exe powerpnt.exe msaccess.exe winproj.exe outlook.exe acrobat.exe visio.exe mspub.exe notepad.exe wordpad.exe winzip.exe winrar.exe onenote.exe onenotem.exe									Chaîne de caractères : 100 entrées maximum de 500 caractères chacune Dell recommande de ne pas ajouter explorer.exe ou iexplorer.exe à cette liste ADE, car cela peut entraîner des effets indésirables. Toutefois, explorer.exe est le processus utilisé pour créer un fichier de Bloc-notes sur le bureau en utilisant le menu contextuel. Le paramètre de cryptage par extension de fichier, plutôt que par liste ADE, permet de couvrir davantage de fichiers. Liste des noms de processus des applications (sans chemin d'accès) dont les nouveaux fichiers doivent être cryptés.

Stratégie	Protection avancée pour tous les lecteurs fixes et supports externes	Législation relative à PCI	Législation relative à la protection des données	Législation relative à HIPAA	Protection de base pour tous les lecteurs fixes et disques externes (par défaut)	Protection de base pour tous les lecteurs fixes	Protection de base pour le disque système uniquement	Protection de base pour les supports externes	Cryptage désactivé	Description
										Séparés par retour chariot. N'utilisez pas de caractère de remplacement. Dell recommande fortement de ne pas inclure des applications/ programmes d'installation qui génèrent des fichiers système essentiels. En effet, vous courez le risque de crypter des fichiers système importants, ce qui pourrait rendre impossible le démarrage d'un ordinateur. Noms de processus courants : outlook.exe, winword.exe, powerpnt.exe, msaccess.exe, wordpad.exe, mspaint.exe, excel.exe Ces noms de processus système et de programmes d'installation codés en dur sont ignorés si vous les spécifiez dans cette règle : hotfix.exe, update.exe, setup.exe, msiexec.exe, wuauclt.exe, wmiprvse.exe, migrate.exe, unregmp2.exe, ikernel.exe, wssetup.exe, svchost.exe
Clé de cryptage des données applicatives	Courant									Courant ou utilisateur Choisissez une clé pour indiquer qui peut avoir accès aux fichiers chiffrés par la liste des données chiffrées de l'application et où. Commun, afin que ces fichiers soient accessibles

Stratégie	Protection avancée pour tous les lecteurs fixes et supports externes	Législation relative à PCI	Législation relative à la protection des données	Législation relative à HIPAA	Protection de base pour tous les lecteurs fixes et disques externes (par défaut)	Protection de base pour tous les lecteurs fixes	Protection de base pour le disque système uniquement	Protection de base pour les supports externes	Cryptage désactivé	Description
										à tous les utilisateurs gérés sur le point de terminaison de création (même niveau d'accès que les dossiers communs chiffrés), et chiffrés à l'aide de l'algorithme de chiffrement Commun. Utilisateur, afin que ces fichiers soient accessibles uniquement à l'utilisateur qui les a créés, sur le point de terminaison de création (même niveau d'accès que les dossiers chiffrés de l'utilisateur), et chiffrés à l'aide de l'algorithme de chiffrement utilisateur. Toute modification apportée à cette règle n'affecte pas les fichiers déjà cryptés.
Crypter les dossiers personnels d'Outlook	Vrai							Faux		Vrai crypte les dossiers personnels d'Outlook.
Crypter les fichiers temporaires	Vrai							Faux		Vrai = chiffrement des chemins compris dans les variables d'environnement TEMP et TMP à l'aide de la clé de chiffrement des données utilisateur.
Crypter les fichiers temporaires Internet	Vrai	Faux								Vrai = chiffrement du chemin compris dans la variable d'environnement CSIDL_INTERNET_CACHE à l'aide de la clé de chiffrement des données utilisateur.

Stratégie	Protection avancée pour tous les lecteurs fixes et supports externes	Législation relative à PCI	Législation relative à la protection des données	Législation relative à HIPAA	Protection de base pour tous les lecteurs fixes et disques externes (par défaut)	Protection de base pour tous les lecteurs fixes	Protection de base pour le disque système uniquement	Protection de base pour les supports externes	Cryptage désactivé	Description
										Afin de réduire la durée de l'analyse de cryptage, le client efface le contenu de CSIDL_INTERNET_CACHE pour le cryptage initial, ainsi que les mises à jour de cette règle. Cette règle ne s'applique qu'à Microsoft Internet Explorer.
Crypter les documents de profil utilisateur	Vrai								Faux	Vrai = cryptage : · Le profil utilisateur (`C:\Users\jsmith`) avec la clé de chiffrement des données utilisateur · \Users\Public avec la clé de cryptage commun
Crypter le fichier de pagination Windows	Vrai								Faux	Vrai crypte le fichier de pagination Windows. Une modification apportée à cette règle nécessite un redémarrage.
Services gérés										Chaîne de caractères : 100 entrées maximum de 500 caractères chacune (2 048 caractères maximum) Lorsque cette règle gère un service, ce dernier démarre uniquement une fois l'utilisateur connecté et le client déverrouillé. Cette règle s'assure également que le service qu'elle gère est arrêté avant le verrouillage du client durant la déconnexion. Cette règle empêche aussi la déconnexion si un service ne répond pas.

Stratégie	Protection avancée pour tous les lecteurs fixes et supports externes	Législation relative à PCI	Législation relative à la protection des données	Législation relative à HIPAA	Protection de base pour tous les lecteurs fixes et disques externes (par défaut)	Protection de base pour tous les lecteurs fixes	Protection de base pour le disque système uniquement	Protection de base pour les supports externes	Cryptage désactivé	Description
										La syntaxe est un nom de service par ligne. Vous pouvez insérer des espaces dans le nom du service. Les caractères de remplacement ne sont pas autorisés. Les services gérés ne démarrent pas si un utilisateur non géré se connecte.
Sécuriser le nettoyage après cryptage	Écrasement à trois passages	Écrasement à un passage							Écrasement impossible	Écrasement impossible, Écrasement à un passage, Écrasement à trois passages, Écrasement à sept passages Une fois que les fichiers spécifiés via d'autres règles de cette catégorie ont été cryptés, cette règle détermine le traitement du résidu non crypté des fichiers originaux : · Écrasement impossible le supprime. Cette valeur génère le traitement de cryptage le plus rapide. · Écrasement à un passage écrase le fichier avec des données aléatoires. · Écrasement à trois passages écrase le fichier avec une suite standard de 1 et de 0, puis avec son complément, puis avec des données aléatoires. · Écrasement à sept passages écrase le fichier avec une suite standard de 1 et de 0, puis avec

Stratégie	Protection avancée pour tous les lecteurs fixes et supports externes	Législation relative à PCI	Législation relative à la protection des données	Législation relative à HIPAA	Protection de base pour tous les lecteurs fixes et disques externes (par défaut)	Protection de base pour tous les lecteurs fixes	Protection de base pour le disque système uniquement	Protection de base pour les supports externes	Cryptage désactivé	Description
										son complément, puis avec des données aléatoires cinq fois. Cette valeur constitue le processus de cryptage le plus sécurisé, dans la mesure où elle rend extrêmement difficile la récupération des fichiers d'origine depuis la mémoire.
Fichier de mise en veille prolongée Windows sécurisé	Vrai					Faux		Vrai	Faux	Si cette règle est activée, le fichier d'hibernation est crypté uniquement quand l'ordinateur entre en veille prolongée. Le client retire la protection lorsque l'ordinateur sort de la mise en veille prolongée, fournissant ainsi une protection sans impacter les utilisateurs ni les applications lorsque l'ordinateur est utilisé.
Empêcher la mise en mode hibernation non sécurisé	Vrai					Faux		Vrai	Faux	Lorsque cette règle est activée, le client ne permet pas la mise en veille prolongée de l'ordinateur si le client ne peut pas chiffrer les données de mise en veille prolongée.
Priorité d'analyse du poste de travail	Élevé	Normale								Maximum, Élevé, Normal, Bas, Minimum Précise le niveau de priorité Windows relative de l'analyse des dossiers cryptés.
Dossiers cryptés de l'utilisateur										Chaîne de caractères : 100 entrées maximum de 500 caractères chacune (2 048 caractères maximum)

Stratégie	Protection avancée pour tous les lecteurs fixes et supports externes	Législation relative à PCI	Législation relative à la protection des données	Législation relative à HIPAA	Protection de base pour tous les lecteurs fixes et disques externes (par défaut)	Protection de base pour tous les lecteurs fixes	Protection de base pour le disque système uniquement	Protection de base pour les supports externes	Cryptage désactivé	Description
										Une liste des dossiers du disque dur du point de terminaison à chiffrer avec la clé de chiffrement des données utilisateur, ou exclus du chiffrement. Cette règle s'applique à tous les disques que Windows classe dans la catégorie disques durs. Vous ne pouvez pas utiliser cette règle pour chiffrer des lecteurs ou des supports amovibles dont le type affiche Disque amovible. Utilisez Chiffrer le support externe EMS.
Algorithme de cryptage de l'utilisateur	AES256									AES 256, Rijndael 256, AES 128, Rijndael 128 Algorithme de cryptage des données au niveau de l'utilisateur individuel. Des valeurs différentes selon l'utilisateur sont possibles sur un point final.
Clé de cryptage des données utilisateur	Utilisateur	Courant		Utilisateur	Courant				Utilisateur	Courant ou utilisateur Choisissez une clé pour indiquer qui peut avoir accès aux fichiers chiffrés par les règles suivantes, et où : · Dossiers cryptés de l'utilisateur · Crypter les dossiers personnels d'Outlook · Crypter les fichiers temporaires (\Documents et Paramètres\nom d'utilisateur\Paramètres locaux\Temp uniquement) · Crypter les fichiers temporaires Internet

Stratégie	Protection avancée pour tous les lecteurs fixes et supports externes	Législation relative à PCI	Législation relative à la protection des données	Législation relative à HIPAA	Protection de base pour tous les lecteurs fixes et disques externes (par défaut)	Protection de base pour tous les lecteurs fixes	Protection de base pour le disque système uniquement	Protection de base pour les supports externes	Cryptage désactivé	Description
										· Crypter les documents de profil utilisateur Sélectionnez : · Commun, afin que ces fichiers/dossiers chiffrés utilisateur soient accessibles à tous les utilisateurs gérés sur le point de terminaison de création (même niveau d'accès que les dossiers communs chiffrés), et chiffrés à l'aide de l'algorithme de chiffrement Commun. · Utilisateur, afin que ces fichiers soient accessibles uniquement par l'utilisateur qui les a créés, uniquement sur le point de terminaison où ils ont été créés (même niveau d'accès que les dossiers chiffrés utilisateur), et chiffrés à l'aide de l'algorithme de chiffrement utilisateur. Si vous choisissez d'intégrer une règle de cryptage pour crypter l'ensemble des partitions de disque, il est recommandé d'utiliser la règle de cryptage SDE par défaut, plutôt que Commun ou Utilisateur. Ceci garantit que les fichiers de système d'exploitation cryptés sont accessibles durant les états où l'utilisateur géré n'est pas connecté.
Accélérateur de cryptage matériel (pris en charge uniquement avec les clients Encryption v8.3 à v8.9.1)										

Stratégie	Protection avancée pour tous les lecteurs fixes et supports externes	Législation relative à PCI	Législation relative à la protection des données	Législation relative à HIPAA	Protection de base pour tous les lecteurs fixes et disques externes (par défaut)	Protection de base pour tous les lecteurs fixes	Protection de base pour le disque système uniquement	Protection de base pour les supports externes	Cryptage désactivé	Description
HCA (Hardware Crypto Accelerator)	Faux									Cette règle est la « règle principale » pour toutes les autres règles de l'accélérateur de cryptage matériel (HCA). Si cette règle est définie sur Faux, le cryptage HCA n'a pas lieu, indépendamment des autres valeurs de la règle. Les règles HCA fonctionnent uniquement sur les ordinateurs équipés d'un accélérateur de cryptage matériel (HCA).
Volumes choisis pour cryptage	Tous les volumes fixes									Tous les volumes fixes ou uniquement le volume système Définissez le ou les volumes cibles du cryptage.
Métadonnées d'analyse détaillée disponibles sur le lecteur avec cryptage HCA	Faux									Vrai ou faux Vrai : les métadonnées d'analyse approfondie sont comprises sur le lecteur afin de faciliter l'analyse. Métadonnées comprises : ● ID (MCID) de l'ordinateur actuel ● ID de périphérique (DCID/SCID) de l'installation du Encryption client en cours Faux : les métadonnées d'analyse approfondie ne sont pas incluses sur le lecteur. Passer de Faux à Vrai engendre une nouvelle analyse, basée sur les règles pour ajouter les métadonnées d'analyse.

Stratégie	Protection avancée pour tous les lecteurs fixes et supports externes	Législation relative à PCI	Législation relative à la protection des données	Législation relative à HIPAA	Protection de base pour tous les lecteurs fixes et disques externes (par défaut)	Protection de base pour tous les lecteurs fixes	Protection de base pour le disque système uniquement	Protection de base pour les supports externes	Cryptage désactivé	Description
Autoriser l'approbation du cryptage des lecteurs secondaires	Faux									Vrai : permet aux utilisateurs de décider du cryptage des autres lecteurs.
Algorithme de cryptage	AES256									AES-256 ou AES-128
Règles - Contrôle des ports										
Système de contrôle de port	Désactivée									Activer ou désactiver toutes les règles du système de contrôle de port. Désactiver = aucune règle du système de contrôle de port ne s'applique, indépendamment des autres valeurs des règles en la matière. Les règles PCS nécessitent un redémarrage avant d'entrer en vigueur. **REMARQUE :** En raison du blocage des opérations sur les appareils, les noms des appareils ne sont pas renseignés.
Port : logement pour Express Card	Activé									Activer, désactiver ou contourner les ports exposés via le logement Express Card.
Port : eSATA	Activé									Activer, désactiver ou contourner l'accès aux ports SATA externes.

Stratégie	Protection avancée pour tous les lecteurs fixes et supports externes	Législation relative à PCI	Législation relative à la protection des données	Législation relative à HIPAA	Protection de base pour tous les lecteurs fixes et disques externes (par défaut)	Protection de base pour tous les lecteurs fixes	Protection de base pour le disque système uniquement	Protection de base pour les supports externes	Cryptage désactivé	Description
Port : PCMCIA	Activé									Activer, désactiver ou contourner l'accès aux ports PCMCIA.
Port : Firewire (1394)	Activé									Activer, désactiver ou contourner l'accès aux ports Firewire externes (1394).
Port : SD	Activé									Activer, désactiver ou contourner l'accès aux ports de carte SD.
Sous-catégorie de stockage : contrôle des lecteurs externes	Bloqué	Lecture seule			Accès illimité			Lecture seule	Accès illimité	ENFANT de catégorie : stockage. Classe : le stockage doit être défini sur Activé pour permettre l'utilisation de cette règle. Cette règle comporte des interactions avec PCS. Voir Encryption External Media et interactions PCS. Accès total : aucune restriction en lecture/écriture des données n'est appliquée au port du lecteur externe Lecture seule : permet la lecture. La fonction d'écriture est désactivée Bloqué : le port est bloqué en lecture/écriture Cette règle est basée sur le point final et ne peut pas être remplacée par la règle utilisateur.
Port : périphérique de transfert de mémoire (MTD)	Activé									Activer, désactiver ou contourner l'accès aux ports de périphériques de transfert de mémoire (MTD).

Stratégie	Protection avancée pour tous les lecteurs fixes et supports externes	Législation relative à PCI	Législation relative à la protection des données	Législation relative à HIPAA	Protection de base pour tous les lecteurs fixes et disques externes (par défaut)	Protection de base pour tous les lecteurs fixes	Protection de base pour le disque système uniquement	Protection de base pour les supports externes	Cryptage désactivé	Description
Catégorie : stockage	Activé									PARENT des trois règles suivantes. Configurez cette règle sur Activer pour utiliser les 3 prochaines règles de sous-catégories de stockage. Configurer cette règle sur Désactiver désactive les 3 règles de sous-catégories, quelle que soit leur valeur.
Sous-catégorie de stockage : contrôle des lecteurs optiques	Lecture seule	UDF uniquement				Accès illimité		UDF uniquement	Accès illimité	ENFANT de catégorie : stockage. Classe : le stockage doit être défini sur Activé pour permettre l'utilisation de cette règle. Accès total : aucune restriction de lecture/écriture de données sur le port de lecteur optique UDF uniquement : bloque toutes les écritures de données qui ne sont pas au format UDF (gravure de CD/DVD, gravure ISO). La fonction de lecture des données est activée. Lecture seule : permet la lecture. La fonction d'écriture est désactivée Bloqué : le port est bloqué en lecture/écriture Cette règle est basée sur le point final et ne peut pas être remplacée par la règle utilisateur. Universal Disk Format (UDF) est une application des normes ISO/IEC 13346 et ECMA-167 et un système de fichier ouvert sans fournisseur particulier pour le stockage des

Stratégie	Protection avancée pour tous les lecteurs fixes et supports externes	Législation relative à PCI	Législation relative à la protection des données	Législation relative à HIPAA	Protection de base pour tous les lecteurs fixes et disques externes (par défaut)	Protection de base pour tous les lecteurs fixes	Protection de base pour le disque système uniquement	Protection de base pour les supports externes	Cryptage désactivé	Description
										données informatiques sur une vaste gamme de supports. Cette règle comporte des interactions avec PCS. Voir Encryption External Media et interactions PCS.
Sous-catégorie de stockage : contrôle des lecteurs de disquettes	Bloqué	Lecture seule				Accès illimité		Lecture seule	Accès illimité	ENFANT de catégorie : stockage. Classe : le stockage doit être défini sur Activé pour permettre l'utilisation de cette règle. Accès total : aucune restriction de lecture/écriture de données n'est appliquée au port du lecteur de disquettes Lecture seule : permet la lecture. La fonction d'écriture est désactivée Bloqué : le port est bloqué en lecture/écriture Cette règle est basée sur le point final et ne peut pas être remplacée par la règle utilisateur.
Classe : périphérique portable Windows (WPD)	Activé									PARENT de la règle suivante. Définissez cette règle sur Activé pour utiliser la sous-catégorie périphérique portable Windows (WPD) : règle de stockage. Configurer cette règle sur Désactiver désactive la règle Sous-catégorie périphérique portable Windows (WPD) : stockage, quelle que soit sa valeur. Contrôle l'accès à tous les périphériques portables Windows.

Stratégie	Protection avancée pour tous les lecteurs fixes et supports externes	Législation relative à PCI	Législation relative à la protection des données	Législation relative à HIPAA	Protection de base pour tous les lecteurs fixes et disques externes (par défaut)	Protection de base pour tous les lecteurs fixes	Protection de base pour le disque système uniquement	Protection de base pour les supports externes	Cryptage désactivé	Description
Sous-catégorie périphérique portable Windows (WPD) : stockage	Activé									ENFANT de catégorie : périphérique portable Windows (WPD) Classe : périphérique portable Windows (WPD) doit être défini sur Activé pour utiliser cette règle. Accès total : aucune restriction d'accès aux données en lecture/écriture n'est appliquée au port. Lecture seule : permet la lecture. La fonction d'écriture est désactivée. Bloqué : le port est bloqué en lecture/écriture.
Classe : Human Interface Device (HID)	Activé									Contrôle l'accès à tous les périphériques d'interface utilisateur (claviers, souris). **Remarque** : le blocage au niveau du port USB et au niveau de la catégorie HID n'est assuré que si le type de châssis de l'ordinateur peut être identifié comme un ordinateur portable/notebook. L'identification du châssis dépend du BIOS de l'ordinateur.
Catégorie : autre	Activé									Contrôle l'accès à tous les disques/lecteurs non couverts par d'autres catégories.
Règles relatives aux périphériques de stockage amovibles										
Cryptage EMS des supports externes	Vrai					Faux	Vrai		Faux	Cette règle est la « règle principale » pour toutes les règles relatives aux périphériques de stockage

Stratégie	Protection avancée pour tous les lecteurs fixes et supports externes	Législation relative à PCI	Législation relative à la protection des données	Législation relative à HIPAA	Protection de base pour tous les lecteurs fixes et disques externes (par défaut)	Protection de base pour tous les lecteurs fixes	Protection de base pour le disque système uniquement	Protection de base pour les supports externes	Cryptage désactivé	Description
										amovibles. Une valeur Faux signifie l'absence de cryptage des périphériques de stockage amovibles, indépendamment des autres valeurs des règles. Une valeur Vrai signifie que toutes les règles de cryptage des périphériques de stockage amovibles sont activées. Cette règle comporte des interactions avec PCS. Voir Encryption External Media et interactions PCS.
EMS ne prend pas en charge le cryptage de CD/DVD	Faux								Vrai	La valeur Faux active le cryptage des lecteurs de CD/DVD. Cette règle comporte des interactions avec PCS. Voir Encryption External Media et interactions PCS.
Accès EMS aux supports non protégés	Bloquer		Lecture seule			Accès illimité		Lecture seule	Accès illimité	Bloquer, Lecture seule, Accès illimité Cette règle comporte des interactions avec PCS. Voir Encryption External Media et interactions PCS. Lorsque le statut de cette stratégie est Accès bloqué, vous n'avez pas accès au périphérique amovible, si celui-ci n'est pas crypté. Les valeurs Lecture seule ou Accès illimité vous permettent de choisir les périphériques de stockage amovibles que vous voulez crypter. Si vous décidez de ne pas crypter le périphérique

Stratégie	Protection avancée pour tous les lecteurs fixes et supports externes	Législation relative à PCI	Législation relative à la protection des données	Législation relative à HIPAA	Protection de base pour tous les lecteurs fixes et disques externes (par défaut)	Protection de base pour tous les lecteurs fixes	Protection de base pour le disque système uniquement	Protection de base pour les supports externes	Cryptage désactivé	Description
										de stockage amovible et que la valeur sélectionnée est Accès illimité, vous disposez de tous les droits d'écriture et de lecture pour le périphérique de stockage amovible. Si vous décidez de ne pas chiffrer le périphérique de stockage amovible et que la valeur sélectionnée est Lecture seule, vous ne pouvez pas lire ni supprimer les fichiers existants sur le périphérique de stockage amovible non chiffré, mais le client empêche la modification ou l'ajout de fichiers sur le périphérique de stockage amovible, sauf s'il est chiffré.
Algorithme de cryptage EMS	AES256									AES-256, Rijndael 256, AES-128, Rijndael 128
Analyse EMS des supports externes	Vrai	Faux								Vrai permet à un support amovible d'être analysé chaque fois qu'il est inséré. Lorsque cette règle est définie sur Faux et que la règle Chiffrer le support externe EMS est définie sur Vrai, seuls les nouveaux fichiers ou ceux qui ont été modifiés sont chiffrés. À chaque insertion, une analyse a lieu afin que chaque fichier ajouté au support amovible sans authentification puisse être repéré. Les fichiers peuvent être ajoutés au support même si vous

Stratégie	Protection avancée pour tous les lecteurs fixes et supports externes	Législation relative à PCI	Législation relative à la protection des données	Législation relative à HIPAA	Protection de base pour tous les lecteurs fixes et disques externes (par défaut)	Protection de base pour tous les lecteurs fixes	Protection de base pour le disque système uniquement	Protection de base pour les supports externes	Cryptage désactivé	Description
										refusez l'authentification, mais vous ne pouvez alors pas accéder aux données chiffrées. Les fichiers ajoutés ne seront pas chiffrés. Toutefois, lors de la prochaine authentification du support (pour utiliser les données chiffrées), tous les fichiers qui ont été ajoutés seront analysés et chiffrés.
Accès d'EMS aux données cryptées sur un périphérique non protégé	Vrai									Vrai permet à l'utilisateur d'accéder aux données cryptées sur le stockage amovible, que le point final soit crypté ou non.
Liste blanche de périphériques EMS										Cette règle permet de spécifier les périphériques de support amovibles à exclure du cryptage. Les périphériques de support amovibles qui ne sont pas sur cette liste sont protégés. Maximum de 150 périphériques avec un maximum de 500 caractères par ID de périphérique PNP. Jusqu'à 2 048 caractères autorisés. Pour rechercher l'ID de périphérique PNP d'un périphérique de stockage amovible : 1. insérez le périphérique de stockage amovible dans un ordinateur crypté. 2. Ouvrez le fichier EMSService.log dans

Stratégie	Protection avancée pour tous les lecteurs fixes et supports externes	Législation relative à PCI	Législation relative à la protection des données	Législation relative à HIPAA	Protection de base pour tous les lecteurs fixes et disques externes (par défaut)	Protection de base pour tous les lecteurs fixes	Protection de base pour le disque système uniquement	Protection de base pour les supports externes	Cryptage désactivé	Description
										C:\Programdata\Dell\Dell Data Protection\Encryption\EMS. 3. Recherchez "PNPDeviceID=" Par exemple : 14.03.18 18:50:06.834 [I] [Volume "F:\"] PnPDeviceID = USBSTOR\DISK&VEN_SEAGATE&PROD_USB&REV_0409\2HC015KJ&0 Définissez les éléments suivants dans la règle Liste blanche des périphériques EMS : VEN=fournisseur (ex : USBSTOR\DISK&VEN_SEAGATE) PROD=Nom du produit/modèle (ex : &PROD_USB) ; exclut également du cryptage EMS tous les lecteurs USB de Seagate ; une valeur VEN (ex : USBSTOR\DISK&VEN_SEAGATE) doit précéder cette valeur REV=révision du micrologiciel (ex : &REV_0409) ; exclut également le modèle spécifique en cours d'utilisation ; les valeurs VEN et PROD doivent précéder cette valeur Numéro de série (ex : \2HC015KJ&0) ; exclut seulement ce périphérique ; les valeurs

Stratégie	Protection avancée pour tous les lecteurs fixes et supports externes	Législation relative à PCI	Législation relative à la protection des données	Législation relative à HIPAA	Protection de base pour tous les lecteurs fixes et disques externes (par défaut)	Protection de base pour tous les lecteurs fixes	Protection de base pour le disque système uniquement	Protection de base pour les supports externes	Cryptage désactivé	Description
										VEN, PROD et REV doit précéder cette valeur Séparateurs autorisés : onglets, virgules, points-virgules, caractère hexadécimal 0x1E (caractère de séparation d'enregistrement)
Le mot de passe d'EMS doit comporter des caractères alphabétiques	Vrai									Avec la valeur Vrai, le mot de passe doit contenir au moins une lettre.
Le mot de passe d'EMS doit comporter des majuscules et des minuscules	Vrai	Faux								Avec la valeur Vrai, le mot de passe doit comporter au moins une majuscule et une minuscule.
Nombre de caractères EMS. Requis dans le mot de passe	8					6		8		de 1 à 40 caractères Nombre minimal de caractères que doit comporter le mot de passe.
Le mot de passe d'EMS doit comporter des	Vrai	Faux								Avec la valeur Vrai, le mot de passe doit contenir au moins un chiffre.

Stratégie	Protection avancée pour tous les lecteurs fixes et supports externes	Législation relative à PCI	Législation relative à la protection des données	Législation relative à HIPAA	Protection de base pour tous les lecteurs fixes et disques externes (par défaut)	Protection de base pour tous les lecteurs fixes	Protection de base pour le disque système uniquement	Protection de base pour les supports externes	Cryptage désactivé	Description
caractères numériques										
Tentatives de saisie de mot de passe EMS autorisées	2	3				4		3		1-10 Nombre de tentatives disponibles pour saisir correctement le mot de passe.
Le mot de passe d'EMS doit comporter des caractères spéciaux	Vrai	Faux							Vrai	Avec la valeur Vrai, le mot de passe doit contenir au moins un caractère spécial.
Temps de refroidissement d'EMS	30									0 à 5000 secondes Délai nécessaire avant un nouvel essai si le code d'accès n'a pas été saisi correctement lors des tentatives autorisées (en secondes).
Incrément du temps de refroidissement EMS	30	20				0.10	30	0.10		0 à 5000 secondes Délai à rajouter au temps de refroidissement si le code d'accès n'a pas été saisi correctement lors des tentatives autorisées.
Règles de cryptage EMS										Règles de cryptage à utiliser pour crypter/ne pas crypter certains disques, répertoires et dossiers. Total de 2 048 caractères autorisés. Les caractères « Espace » et « Entrée » utilisés pour ajouter des lignes entre les lignes sont

Stratégie	Protection avancée pour tous les lecteurs fixes et supports externes	Législation relative à PCI	Législation relative à la protection des données	Législation relative à HIPAA	Protection de base pour tous les lecteurs fixes et disques externes (par défaut)	Protection de base pour tous les lecteurs fixes	Protection de base pour le disque système uniquement	Protection de base pour les supports externes	Cryptage désactivé	Description
										comptabilisés. Toutes les règles dépassant la limite des 2 048 caractères sont ignorées. Les périphériques de stockage qui comprennent des connexions à interface multiple, comme Firewire, USB, eSATA, etc. peuvent nécessiter à la fois Encryption External Media et les règles de cryptage pour pouvoir crypter le périphérique. Cela est dû aux différences de gestion par le système d'exploitation Windows des périphériques de stockage amovibles en fonction du type d'interface. Voir Comment crypter un iPod avec Encryption External Media.
Accès bloqué d'EMS aux supports non protégeables	Vrai								Faux	Bloquez l'accès aux supports amovibles de moins de 55 Mo n'ayant donc pas la capacité de stockage suffisante pour héberger Encryption External Media (disquette de 1,44 Mo, par exemple). Si la valeur choisie à la fois pour EMS et cette règle est Vrai, l'accès est bloqué. Si la règle Chiffrer le support externe EMS a la valeur Vrai et que cette règle a la valeur Faux, les données peuvent être lues depuis le support non chiffrable, mais l'écriture sur le support est bloquée. Si la valeur est Faux, cette règle n'a aucun

Stratégie	Protection avancée pour tous les lecteurs fixes et supports externes	Législation relative à PCI	Législation relative à la protection des données	Législation relative à HIPAA	Protection de base pour tous les lecteurs fixes et disques externes (par défaut)	Protection de base pour tous les lecteurs fixes	Protection de base pour le disque système uniquement	Protection de base pour les supports externes	Cryptage désactivé	Description
										effet et l'accès au support non chiffrable n'est pas impacté.
Règles du contrôle d'expérience utilisateur										
Forcer le redémarrage lors de la mise à jour	Vrai								Faux	Si vous configurez cette valeur sur Vrai, l'ordinateur redémarre immédiatement pour permettre le traitement du cryptage ou des mises à jour relatives à la règle basée sur le périphérique, tel que Cryptage des données système (SDE).
Durée de chaque report de redémarrage	+5	0.10				20		15		Le nombre de minutes de retard lorsque l'utilisateur choisit de retarder le redémarrage de la règle basée sur le périphérique.
Nombre de reports de redémarrage autorisés	1					+5		3		Le nombre de fois que l'utilisateur est autorisé à retarder le redémarrage de la règle basée sur le périphérique.
Supprimer la notification de conflit de fichiers	Faux									Cette règle contrôle l'affichage des notifications à l'attention de l'utilisateur lorsqu'une application tente d'accéder à un fichier en cours de traitement par le client.
Afficher le contrôle de traitement du cryptage local	Faux		Vrai					Faux		Si vous configurez cette valeur sur Vrai, l'utilisateur voit une option de menu dans l'icône de la zone de notification qui lui permet de suspendre/relancer le cryptage/décryptage (selon l'opération exécutée par Encryption).

Stratégie	Protection avancée pour tous les lecteurs fixes et supports externes	Législation relative à PCI	Législation relative à la protection des données	Législation relative à HIPAA	Protection de base pour tous les lecteurs fixes et disques externes (par défaut)	Protection de base pour tous les lecteurs fixes	Protection de base pour le disque système uniquement	Protection de base pour les supports externes	Cryptage désactivé	Description
										Autoriser un utilisateur à suspendre le cryptage peut lui permettre d'empêcher le Encryption client de crypter ou décrypter les données en fonction de la règle.
Autoriser le cryptage uniquement lorsque l'écran est verrouillé	Faux		Utilisateur facultatif					Faux		Vrai, Faux, Utilisateur facultatif Lorsque la valeur est Vrai, il n'y a aucun chiffrement ou déchiffrement de données pendant que l'utilisateur travaille activement. Le client traite les données uniquement lorsque l'écran est verrouillé. Utilisateur facultatif ajoute une option dans l'icône de la zone de notification permettant à l'utilisateur d'activer ou de désactiver cette fonction. Lorsque la valeur est Faux, le processus de cryptage est autorisé même lorsque l'utilisateur travaille. L'activation de cette option rallonge sensiblement le processus de chiffrement ou de déchiffrement.

Description des modèles

Protection avancée pour tous les lecteurs fixes et supports externes

Ce modèle de règles a été conçu pour les entreprises dont l'objectif principal consiste à mettre en place une sécurité rigoureuse ainsi qu'une stratégie vouée à limiter les risques au sein de leur structure. Il s'adresse donc plus particulièrement aux entreprises pour lesquelles la sécurité est un aspect considérablement plus important que la convivialité et où il existe un besoin minimal d'exceptions aux règles (fournissant un niveau de sécurité inférieur) pour des utilisateurs, groupes ou périphériques spécifiques.

Ce modèle de règles comprend :

- une configuration hautement restrictive, pour une protection optimisée ;
- la protection du disque système et de tous les lecteurs fixes ;
- le chiffrement de toutes les données sur les périphériques de support amovibles et l'impossibilité d'utiliser des périphériques amovibles non chiffrés ;
- le contrôle du lecteur optique en lecture seule.

Norme PCI DSS

La norme PCI DSS (Payment Card Industry Data Security Standard) est une norme de sécurité exhaustive qui comprend des exigences en matière de gestion de la sécurité, de règles, de procédures, de structure réseau et de développement logiciel, ainsi que d'autres mesures de protection essentielles. Cette norme détaillée vise à formuler des directives pour les entreprises, dans le souci de protéger proactivement les données de comptes clients.

Ce modèle de règles comprend :

- la protection du disque système et de tous les lecteurs fixes ;
- une invitation à chiffrer les périphériques de support amovibles ;
- l'écriture de CD/DVD UDF uniquement. La configuration du contrôle de port permet un accès en lecture à tous les lecteurs optiques.

Législation relative à la protection des données

La loi Sarbanes-Oxley requiert des contrôles adéquats quant aux informations financières. Ces informations étant pour beaucoup sous format électronique, le cryptage s'avère un point de contrôle crucial lors de leur stockage ou transfert. Les directives du « Gramm-Leach-Bliley (GLB) Act » (ou « Financial Services Modernization Act ») ne requièrent aucun cryptage. Le FFIEC (Federal Financial Institutions Examination Council) recommande cependant que les institutions financières recourent au cryptage pour limiter les risques de publication ou d'altération des informations sensibles stockées et en transit. Le « California Senate Bill 1386 » (California's Database Security Breach Notification Act) vise à protéger les Californiens contre les usurpations d'identité en obligeant les sociétés victimes de failles de sécurité informatique à notifier tous les individus concernés. Le seul moyen pour une société d'éviter d'informer ses clients consiste à prouver que toutes les informations personnelles étaient cryptées avant la faille.

Ce modèle de règles comprend :

- la protection du disque système et de tous les lecteurs fixes ;
- une invitation à chiffrer les périphériques de support amovibles ;
- l'écriture de CD/DVD UDF uniquement. La configuration du contrôle de port permet un accès en lecture à tous les lecteurs optiques.

Législation relative à l'HIPAA

Aux termes de l'HIPAA (Health Insurance Portability and Accountability Act), les sociétés spécialisées dans le domaine de la santé doivent mettre en place un certain nombre de mesures techniques visant à protéger la confidentialité et l'intégrité de toutes les informations de santé identifiables individuellement.

Ce modèle de règles comprend :

- la protection du disque système et de tous les lecteurs fixes ;

- une invitation à chiffrer les périphériques de support amovibles ;
- l'écriture de CD/DVD UDF uniquement. La configuration du contrôle de port permet un accès en lecture à tous les lecteurs optiques.

Protection de base pour tous les lecteurs fixes et supports externes (par défaut)

Ce modèle de règles fournit la configuration recommandée, ce qui garantit un niveau de protection renforcé, sans que la convivialité système n'en pâtisse.

Ce modèle de règles comprend :

- la protection du disque système et de tous les lecteurs fixes ;
- une invitation à chiffrer les périphériques de support amovibles ;
- l'écriture de CD/DVD UDF uniquement. La configuration du contrôle de port permet un accès en lecture à tous les lecteurs optiques.

Protection de base pour tous les lecteurs fixes

Ce modèle de règles comprend :

- la protection du disque système et de tous les lecteurs fixes ;
- la possibilité d'écrire des CD/DVD sur tout format pris en charge. La configuration du contrôle de port permet un accès en lecture à tous les lecteurs optiques.

  Ce modèle de règles ne comprend pas :

- le chiffrement des périphériques de support amovibles.

Protection de base pour le disque système uniquement

Ce modèle de règles comprend :

- la protection du disque système, généralement le disque C:, qui contient votre système d'exploitation ;
- la possibilité d'écrire des CD/DVD sur tout format pris en charge. La configuration du contrôle de port permet un accès en lecture à tous les lecteurs optiques.

  Ce modèle de règles ne comprend pas :

- le chiffrement des périphériques de support amovibles.

Protection de base pour les supports externes

Ce modèle de règles comprend :

- la protection des périphériques de support amovibles ;
- l'écriture de CD/DVD UDF uniquement. La configuration du contrôle de port permet un accès en lecture à tous les lecteurs optiques.

  Ce modèle de règles ne comprend pas :

- la protection du disque système (généralement le disque C:, qui contient votre système d'exploitation) ou d'autres lecteurs fixes.

Cryptage désactivé

Ce modèle de règles n'offre pas de protection par cryptage. Lorsque vous utilisez ce modèle, vous devez prendre des mesures supplémentaires pour protéger les périphériques de toute perte et de tout vol.

Ce modèle est utile pour les entreprises qui préfèrent commencer leur transition sécuritaire sans cryptage actif. Dès que l'entreprise gère plus sereinement son déploiement, elle peut choisir d'activer progressivement le cryptage en ajustant certaines règles individuelles ou en appliquant des modèles renforcés au sein d'une partie ou de l'ensemble de la structure.

11

Extraire les programmes d'installation enfant

- Pour installer chaque client individuellement, vous devez d'abord extraire les fichiers exécutables du programme d'installation.
- Si le programme d'installation principal a été utilisé pour l'installation, les clients doivent être désinstallés individuellement. Utilisez ce processus pour extraire les clients du programme d'installation principal afin de pouvoir les utiliser pour la désinstallation.

1. À partir du support d'installation Dell, copiez le fichier `DDSSetup.exe` sur l'ordinateur local.
2. Ouvrez une invite de commande dans le même emplacement que le fichier `DDSSetup.exe` et saisissez :

   ```
   DDSSetup.exe /s /z"\"EXTRACT_INSTALLERS=C:\Extracted""
   ```

   Le chemin d'extraction ne peut pas comporter plus de 63 caractères.

   Avant de commencer, vérifiez que toutes les conditions préalables ont été remplies et que tous les logiciels requis ont été installés pour chaque programme d'installation enfant que vous envisagez d'installer. Reportez-vous à Exigences pour plus de détails.

   Les programmes d'installation enfants extraits se trouvent à l'emplacement `C:\extracted\.`

Accédez à la section Dépannage.

12

Dépannage

Mise à niveau à l'aide des mises à jour de fonctionnalités Windows 10 ou Windows 11

Pour effectuer la mise à niveau de Windows 10 ou Windows 11 à l'aide des mises à jour de fonctionnalités, suivez les instructions figurant dans l'article de la base de connaissances 125419.

Dépannage de Dell Encryption

Création d'un fichier journal Encryption Removal Agent (facultatif)

- Avant de lancer la désinstallation, vous pouvez, si vous le souhaitez, créer un fichier journal Encryption Removal Agent. Ce fichier journal permet de diagnostiquer les erreurs, si vous rencontrez un problème lors de la désinstallation / du décryptage. Si vous ne souhaitez pas décrypter les fichiers à la désinstallation, il n'est pas nécessaire de créer ce fichier journal.
- Le fichier log d'Encryption Removal Agent n'est créé qu'après l'exécution du service Encryption Removal Agent, après le redémarrage de l'ordinateur. Une fois la désinstallation du client et le décryptage de l'ordinateur terminés, le fichier est définitivement supprimé.
- Le chemin du fichier journal est `C:\ProgramData\Dell\Dell Data Protection\Encryption.`
- Créez l'entrée de registre suivante sur l'ordinateur cible pour le décryptage.

  [HKLM\Software\Credant\DecryptionAgent].

  "LogVerbosity"=DWORD:2

  0: aucune consignation

  1 : erreurs bloquant l'exécution du service

  2 : consigne les erreurs qui bloquent le décryptage complet des données (niveau recommandé)

  3 : consigne des informations sur tous les volumes et fichiers à décrypter

  5 : consigne des informations de débogage

Trouver la version de TSS

- La TSS est un composant qui fait interface au TPM (Trusted Platform Module). Pour identifier la version de la TSS, rendez-vous à l'emplacement par défaut : `C:\Program Files\Dell\Dell Data Protection\Drivers\TSS\bin > tcsd_win32.exe`. Cliquez avec le bouton droit de la souris sur le fichier, puis sélectionnez **Propriétés**. Vérifiez la version du fichier sur l'onglet **Détails** .

Encryption External Media et interactions PCS

Pour veiller à ce que le support ne soit pas en lecture seule et que le port ne soit pas bloqué

La règle d'accès EMS aux supports non blindés interagit avec le système de contrôle des ports - Catégorie : stockage > Sous-catégorie de stockage : règle de contrôle des lecteurs externes. Si vous avez l'intention de définir la règle d'accès EMS aux supports non blindés sur *Accès complet*, assurez-vous que la règle de contrôle du stockage de sous-catégorie : lecteur externe est également définie sur *Accès complet* pour vous assurer que le support n'est pas en lecture seule et que le port n'est pas bloqué.

Pour chiffrer les données écrites sur CD/DVD, procédez comme suit :

- Configurez Windows Media Encryption = Activé.
- Définissez EMS Exclude CD/DVD Encryption (EMS ne prend pas en charge le cryptage de CD/DVD) = non sélectionné.
- Définissez la sous-classe Stockage : Optical Drive Control = UDF Only (Contrôle des lecteurs optiques = UDF uniquement).

Utiliser WSScan

- WSScan vous permet de vous assurer que toutes les données sont décryptées lorsque vous désinstallez Encryption, d'afficher l'état de cryptage et d'identifier les fichiers non cryptés qui devraient être décryptés.
- Des privilèges d'administrateur sont requis pour exécuter cet utilitaire.

  REMARQUE : WSScan doit être exécuté en mode système avec l'outil PsExec si le compte système est propriétaire d'un fichier cible.

Exécutez l'

1. À partir du support d'installation Dell, copiez le fichier WSScan.exe sur l'ordinateur à analyser.
2. Lancez une ligne de commande à l'emplacement spécifié ci-dessus et entrez **wsscan.exe** à l'invite de commande. WSScan démarre.
3. Cliquez sur **Avancé**.
4. Sélectionnez le type du lecteur à rechercher : *Tous les lecteurs, Lecteurs fixes*, *Lecteurs amovibles*, ou *CD-ROM/DVD-ROM*.
5. Sélectionnez le type de rapport de chiffrement : *Fichiers cryptés*, *Fichiers non cryptés*, *Tous les fichiers*, ou *Fichiers non cryptés en violation* :
   - *Fichiers cryptés* : pour vérifier que toutes les données sont décryptées lors de la désinstallation d'Encryption. Suivez votre processus actuel de décryptage des données, par exemple l'envoi d'une mise à jour de règle de décryptage. Une fois les données décryptées mais avant de redémarrer l'ordinateur en préparation de la désinstallation, exécutez WSScan afin de vous assurer que toutes les données sont décryptées.
   - *Fichiers non cryptés* : pour identifier les fichiers qui ne sont pas cryptés, avec une mention indiquant si les fichiers doivent être cryptés (Y/N).
   - *Tous les fichiers* : pour répertorier tous les fichiers cryptés et non cryptés, avec une mention indiquant si les fichiers doivent être cryptés (Y/N).
   - *Fichiers non cryptés en violation* : pour identifier les fichiers qui ne sont pas cryptés, mais qui devraient l'être.
6. Cliquez sur **Rechercher**.

OU

1. Cliquez sur **Avancé** pour basculer la vue vers **Simple** afin d'analyser un dossier particulier.
2. Accédez à Paramètres d'analyse, puis saisissez le chemin du dossier dans le champ *Rechercher un chemin d'accès*. Si vous utilisez ce champ, la sélection dans le menu est ignorée.
3. Si vous ne voulez pas écrire la sortie WSScan dans un fichier, décochez la case **Sortie vers un fichier**.
4. Si vous le souhaitez, changez le chemin et le nom de fichier par défaut à partir du champ *Chemin*.
5. Sélectionnez **Ajouter au fichier existant** si vous ne souhaitez remplacer aucun des fichiers WSScan de sortie existants.
6. Choisissez le format de sortie :
   - Sélectionnez l'option Format du rapport, si vous souhaitez que les résultats de l'analyse apparaissent sous forme de liste de rapport. Il s'agit du format par défaut.
   - Sélectionnez Fichier à valeur délimitée pour que les résultats puissent être exportés dans un tableur. Le séparateur par défaut est « | », mais il peut être remplacé par un maximum de 9 caractères alphanumériques, espaces ou symboles de ponctuation.
   - Sélectionnez Valeurs désignées pour mettre chaque valeur entre doubles guillemets.
   - Sélectionnez Fichier à largeur fixe si vous souhaitez un fichier cible non délimité contenant une ligne continue d'informations à longueur fixe sur chaque fichier crypté.
7. Cliquez sur **Rechercher**.

   Cliquez sur **Arrêter la recherche** pour arrêter votre recherche. Cliquez sur **Effacer** pour effacer les messages affichés.

Fichier cible WSScan

Les données WSScan relatives aux fichiers cryptés contiennent les informations suivantes.

Exemple :

[2015-07-28 07:52:33] SysData.7vdlxrsb._SDENCR_: "c:\temp\Dell - test.log" is still AES256 encrypted

Sortie	Signification
Date/heure	Date et heure d'analyse du fichier.
Type de cryptage	Type de cryptage utilisé pour le fichier. **SysData** : clé SDE. **Utilisateur :** clé de chiffrement utilisateur. **Commun** : clé de chiffrement commun. Le rapport de cryptage ne prend pas en compte les fichiers cryptés avec l'option Encrypt for Sharing.
KCID	Identification de l'ordinateur principal. Dans l'exemple ci-dessus : « **7vdlxrsb** » Si vous analysez un disque réseau mappé, le rapport d'analyse ne comporte pas de KCID.
UCID	ID d'utilisateur. Comme dans l'exemple ci-dessus , « **_SDENCR_** » Tous les utilisateurs de l'ordinateur partagent le même UCID.
Fichier	Chemin d'accès du fichier crypté. Comme dans l'exemple ci-dessus, « **c:\temp\Dell - test.log** »
Algorithme	Algorithme utilisé pour crypter le fichier. Dans l'exemple ci-dessus, « **cryptage AES 256 toujours en place** » RIJNDAEL 128 RIJNDAEL 256 AES-128 AES-256 3DES

Vérification de l'état d'Encryption Removal Agent.

L'état de l'agent Encryption Removal s'affiche dans la zone de description du panneau des services (Démarrer > Exécuter > services.msc > OK) comme suit. Actualisez régulièrement le service (mettez-le en surbrillance > clic droit de la souris > Actualiser) pour mettre à jour son statut.

- **Attente de la désactivation SDE** - Encryption est toujours installé, toujours configuré ou les deux. Le décryptage ne démarrera pas tant qu'Encryption ne sera pas désinstallé.
- **Balayage initial** - Le service procède à un premier balayage en calculant le nombre de fichiers chiffrés et les octets. L'analyse initiale n'a lieu qu'une seule fois.
- **Balayage de décryptage** - Le service déchiffre les fichiers et demande éventuellement à déchiffrer des fichiers verrouillés.
- **Decrypter au redémarrage (partiel)** - Le balayage de décryptage est terminé et certains fichiers verrouillés (mais pas tous) devront être décryptés au prochain redémarrage.
- **Décrypter au redémarrage** - Le balayage de décryptage est terminé et tous les fichiers verrouillés devront être décryptés au prochain redémarrage.
- **Tous les fichiers n'ont pas pu être décryptés** - Le balayage de décryptage est terminé, mais tous les fichiers n'ont pas pu être décryptés. Cet état signifie que l'une des situations suivantes s'applique :
  - Les fichiers verrouillés n'ont pas pu être programmés pour être décryptés, en raison d'une taille trop importante ou du fait qu'une erreur s'est produite lors de la requête de déverrouillage.
  - Une erreur au niveau de la source / de la cible s'est produite lors du décryptage des fichiers.
  - Les fichiers n'ont pas pu être décryptés par la règle.
  - Les fichiers ont le statut « devraient être cryptés ».

- Une erreur s'est produite lors de l'analyse de décryptage.
- Dans tous les cas, un fichier de consignation est créé (si vous avez configuré la consignation) si la valeur LogVerbosity est supérieure ou égale à 2. Pour résoudre le problème, choisissez la valeur de verbosité de consignation 2, puis relancez le service Encryption Removal Agent pour forcer l'exécution d'un nouveau balayage de déchiffrement.

- **Terminé** : l'analyse de déchiffrage est terminée. Le service, le fichier exécutable, le pilote et le fichier exécutable du pilote seront supprimés au prochain redémarrage.

Comment Crypter un iPod avec Encryption External Media

Ces règles activent ou désactivent le cryptage pour ces dossiers et ces types de fichiers sur tous les périphériques de stockage amovibles (pas uniquement les iPod). Faites plus particulièrement attention lors de la définition de règles.

- En raison d'éventuels problèmes, Dell déconseille l'utilisation de l'iPod Shuffle.
- Dans la mesure où les iPods changent, ces informations sont aussi sujettes à modification. Nous vous conseillons donc de procéder avec précaution lorsque vous autorisez l'usage d'iPods sur des ordinateurs où Encryption External Media est activé.
- Étant donné que les noms de fichier sur les iPod dépendent du modèle, il est recommandé de créer une règle d'exclusion qui couvre tous les noms de fichiers pour tous les modèles d'iPod.
- Afin de vous assurer que le cryptage via Encryption External Media d'un iPod ne le rendra pas inutilisable, saisissez les règles suivantes dans la règle de cryptage Encryption External Media :

  -R#:\Calendars

  -R#:\Contacts

  -R#:\iPod_Control

  -R#:\Notes

  -R#:\Photos

- Vous pouvez également forcer le cryptage de types de fichiers spécifiques dans les répertoires ci-dessus. Les règles suivantes permettent le chiffrement de tous les fichiers aux formats PPT, PPTX, DOC, DOCX, XLS et XLSX des répertoires *exclus* du chiffrement via les règles précédentes :

  ^R#:\Calendars;ppt.doc.xls.pptx.docx.xlsx

  ^R#:\Contacts;ppt.doc.xls.pptx.docx.xlsx

  ^R#:\iPod_Control;ppt.doc.xls.pptx.docx.xlsx

  ^R#:\Notes;ppt.doc.xls.pptx.docx.xlsx

  ^R#:\Photos;ppt.doc.xls.pptx.docx.xlsx

- Si vous remplacez ces cinq règles par la règle suivante, le cryptage des fichiers aux formats PPT, PPTX, DOC, DOCX, XLS et XLSX de tous les répertoires de l'iPod, y compris Calendriers, Contacts, iPod_Control, Notes et Photos sera forcé.

  ^R#:\;ppt.doc.xls.pptx.docx.xlsx

- Ces règles ont été testées avec les iPod suivants :

  iPod Video 30 Go de cinquième génération

  iPod Nano 2 Go de deuxième génération

  iPod Mini 4 Go de deuxième génération

Pilotes Dell ControlVault

Mettre à jour les pilotes et le firmware Dell ControlVault

- Les pilotes et le firmware Dell ControlVault installés en usine sur les ordinateurs Dell sont obsolètes et doivent être mis à jour à l'aide de la procédure suivante dans l'ordre indiqué.
- Si, pendant l'installation du client, un message d'erreur vous invite à quitter le programme d'installation afin de mettre à jour les pilotes Dell ControlVault, vous pouvez ignorer ce message en toute sécurité et poursuivre l'installation du client. Les pilotes (et le firmware) Dell ControlVault peuvent être mis à jour une fois l'installation du client terminée.

Télécharger les derniers pilotes

1. Rendez-vous sur dell.com/support.
2. Sélectionnez le modèle de votre ordinateur.
3. Sélectionnez **Pilotes et téléchargements**.
4. Sélectionnez le **système d'exploitation** de l'ordinateur cible.
5. Sélectionnez la catégorie **Sécurité**.
6. Téléchargez, puis enregistrez les pilotes Dell ControlVault.
7. Téléchargez, puis enregistrez le firmware Dell ControlVault.
8. Copiez les pilotes et le firmware sur les ordinateurs cibles, le cas échéant.

Installation du pilote Dell ControlVault

1. Accédez au dossier dans lequel vous avez téléchargé le fichier d'installation du pilote.
2. Double-cliquez sur le pilote Dell ControlVault pour lancer le fichier exécutable à extraction automatique.

   REMARQUE :

   Assurez-vous d'installer le pilote en premier. Le nom de fichier du pilote *au moment de la création de ce document* est ControlVault_Setup_2MYJC_A37_ZPE.exe.

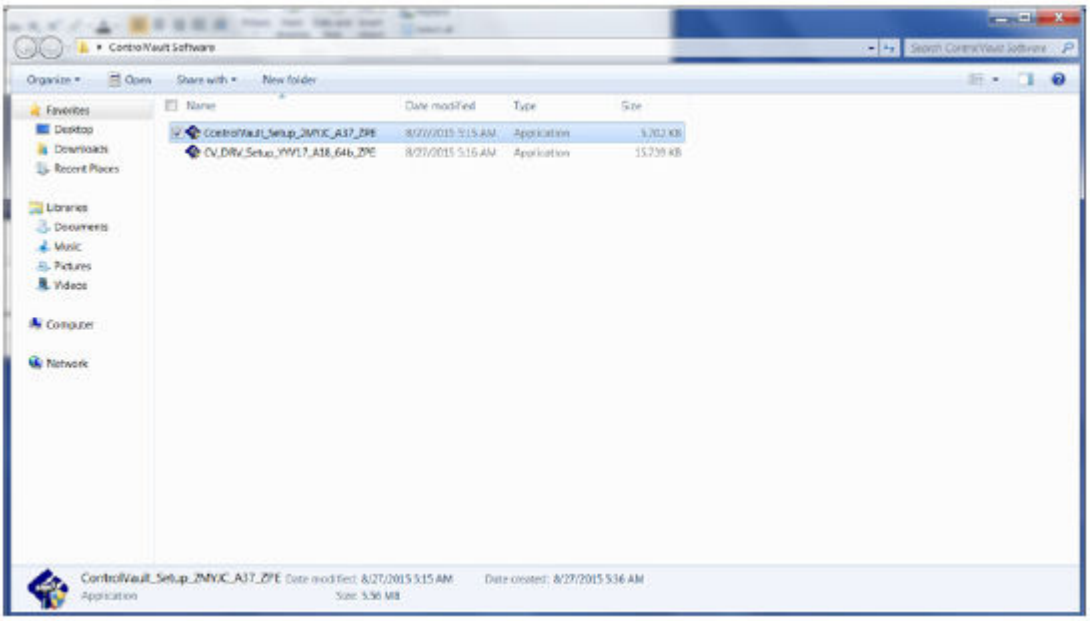
3. Cliquez sur **Continuer** pour commencer.
4. Cliquez sur **Ok** pour décompresser les fichiers de pilote dans l'emplacement par défaut `C:\Dell\Drivers\<New Folder>`.
5. Cliquez sur **Oui** pour permettre la création d'un nouveau dossier.
6. Cliquez sur **OK** lorsque le message décompression réussie s'affiche.
7. Le dossier contenant les fichiers s'affiche après l'extraction. Sinon, naviguez vers le dossier dans lequel vous avez extrait les fichiers. Dans ce cas, le dossier est **JW22F**.
8. Double-cliquez sur **CVHCI64.MSI** pour lancer le programme d'installation du pilote. [**CVHCI64.MSI** dans cet exemple, (CVHCI pour un ordinateur 32 bits)].
9. Cliquez sur **Suivant** sur l'écran de bienvenue.
10. Cliquez sur **Suivant** pour installer les pilotes à l'emplacement par défaut `C:\Program Files\Broadcom Corporation\Broadcom USH Host Components\.`
11. Sélectionnez l'option **Terminer**, puis cliquez sur **Suivant**.
12. Cliquez sur **Installer** pour démarrer l'installation des pilotes.
13. Facultativement, cochez la case permettant d'afficher le fichier journal du programme d'installation. Cliquez sur **Terminer** pour fermer l'Assistant.

Vérifiez l'installation du pilote.

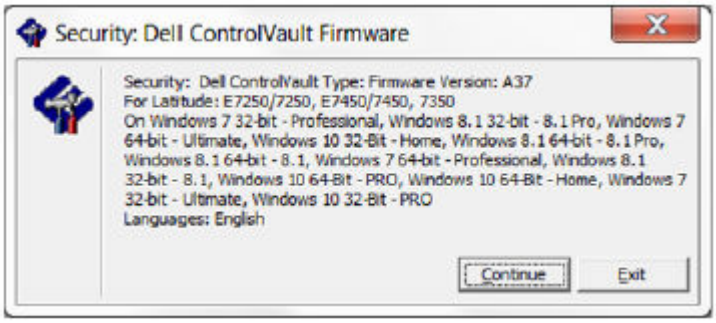
- Le Gestionnaire de périphérique disposera d'un périphérique Dell ControlVault (et d'autres périphériques) en fonction du système d'exploitation et de la configuration matérielle.

Installer le firmware Dell ControlVault

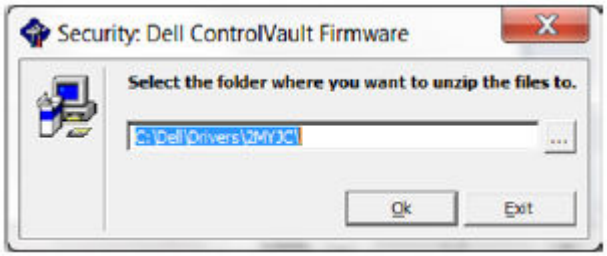
1. Accédez au dossier dans lequel vous avez téléchargé le fichier d'installation du firmware.



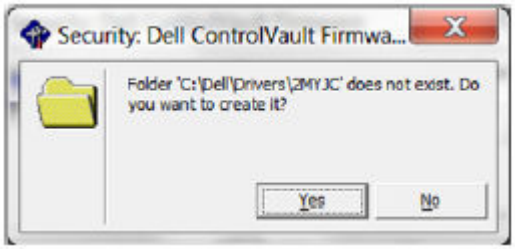
2. Double-cliquez sur le firmware Dell ControlVault pour lancer le fichier exécutable à extraction automatique.
3. Cliquez sur **Continuer** pour commencer.



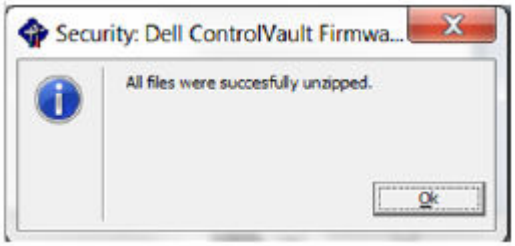
4. Cliquez sur **Ok** pour décompresser les fichiers de pilote dans l'emplacement par défaut `C:\Dell\Drivers\<New Folder>`.



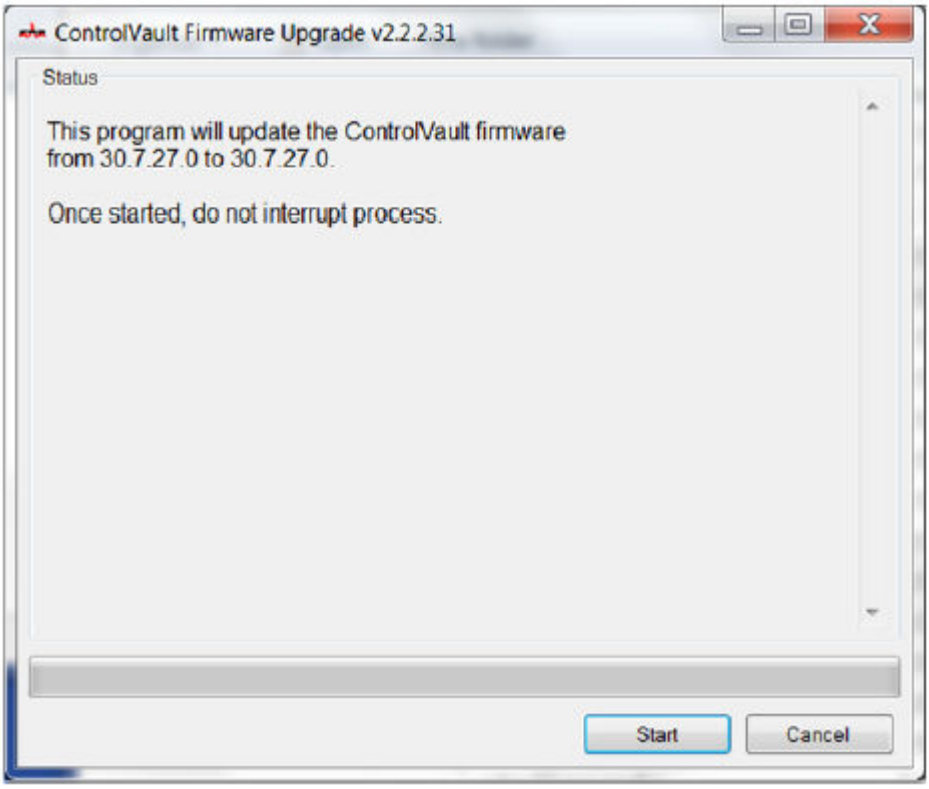
5. Cliquez sur **Oui** pour permettre la création d'un nouveau dossier.



6. Cliquez sur **OK** lorsque le message décompression réussie s'affiche.



7. Le dossier contenant les fichiers s'affiche après l'extraction. Sinon, naviguez vers le dossier dans lequel vous avez extrait les fichiers. Sélectionnez le dossier **firmware**.
8. Double-cliquez sur **ushupgrade.exe** pour lancer le programme d'installation du firmware.
9. Cliquez sur **Démarrer** pour commencer la mise à niveau du firmware.



REMARQUE :

Vous devrez peut-être saisir le mot de passe d'administrateur lors d'une mise à niveau à partir d'une version antérieure du firmware. Entrez `Broadcom` en tant que le mot de passe et cliquez sur **Entrée** en présence de cette boîte de dialogue.

Plusieurs messages d'état s'affichent.

10. Cliquez sur **Redémarrer** pour terminer la mise à niveau du firmware.

    La mise à jour des pilotes et du firmware Dell ControlVault est terminée.

Paramètres de registre

Cette section présente des informations détaillées sur les paramètres de registre Dell ProSupport des ordinateurs clients locaux.

Chiffrement

Création d'un fichier journal Encryption Removal Agent (facultatif)

- Avant de lancer la désinstallation, vous pouvez, si vous le souhaitez, créer un fichier journal Encryption Removal Agent. Ce fichier journal permet de diagnostiquer les erreurs, si vous rencontrez un problème lors de la désinstallation / du déchiffrement Si vous ne souhaitez pas décrypter les fichiers à la désinstallation, il n'est pas nécessaire de créer ce fichier journal.
- Le fichier log d'Encryption Removal Agent n'est créé qu'après l'exécution du service Encryption Removal Agent, après le redémarrage de l'ordinateur. Une fois la désinstallation du client et le déchiffrement de l'ordinateur terminés, le fichier est définitivement supprimé.
- Le chemin du fichier journal est `C:\ProgramData\Dell\Dell Data Protection\Encryption.`
- Créez l'entrée de registre suivante sur l'ordinateur cible pour le déchiffrement.

  [HKLM\Software\Credant\DecryptionAgent].

  "LogVerbosity"=DWORD:2

  0: aucune journalisation

  1 : consigne les erreurs bloquant l'exécution du service

  2 : consigne les erreurs qui bloquent le déchiffrement complet des données (niveau recommandé)

  3 : consigne des informations sur tous les volumes et fichiers à décrypter

  5 : consigne des informations de débogage

Utiliser des cartes à puce avec connexion Windows

- Pour déterminer si une carte à puce est présente et active, vérifiez que la valeur suivante est définie :

  HKLM\SOFTWARE\Dell\Dell Data Protection\

  "SmartcardEnabled"=DWORD:1

  Si le paramètre SmartcardEnabled est manquant ou si sa valeur est égale à zéro, le fournisseur d'informations d'identification affiche uniquement le mot de passe pour l'authentification.

  Si SmartcardEnabled a une valeur différente de zéro, le fournisseur d'informations d'identification affiche les options d'authentification par mot de passe et par carte à puce.

- La valeur de registre suivante indique si Winlogon doit générer une notification pour les événements de connexion par carte à puce.

  HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify

  "SmartCardLogonNotify"=DWORD:1

  0 = Désactivé

  1 = Activé

Conserver les fichiers temporaires au cours de l'installation

- Par défaut, tous les fichiers temporaires qui figurent dans le répertoire c:\windows\temp sont automatiquement supprimés au cours de l'installation. La suppression des fichiers temporaires accélère le chiffrement initial et se produit avant le balayage de chiffrement initial.

  Cependant, si votre organisation utilise une application tierce qui nécessite de conserver la structure de fichiers dans le répertoire \temp, empêchez cette suppression.

  Pour désactiver la suppression des fichiers temporaires, créez ou modifiez le paramètre de registre de la façon suivante :

  [HKLM\SOFTWARE\CREDANT\CMGShield]

  "DeleteTempFiles"=REG_DWORD:0

  Ne pas supprimer les fichiers temporaires augmente le temps de chiffrement initial.

Modifier le comportement par défaut de l'invite utilisateur pour lancer ou différer le chiffrement

- Le client de chiffrement affiche l'invite *`length of each policy update delay`* pendant cinq minutes à chaque fois. Si l'utilisateur ne répond pas à l'invite, le report suivant démarre. La dernière invite de report contient un compte à rebours et une barre d'avancement, et elle s'affiche jusqu'à ce que l'utilisateur réponde ou que le dernier report expire et que la déconnexion/le redémarrage ait lieu.

  Vous pouvez changer le comportement de l'invite utilisateur pour commencer le chiffrement ou le reporter pour empêcher le traitement du chiffrement si l'utilisateur ne répond pas à l'invite. Pour ce faire, définissez le registre sur la valeur de registre suivante :

[HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield]

"SnoozeBeforeSweep"=DWORD:1

Une valeur différente de zéro remplace le comportement par défaut par une alerte (snooze). Sans interaction de l'utilisateur, le traitement du chiffrement est reporté pendant le nombre définissable de reports autorisés. Le traitement de chiffrement démarre au bout du délai final.

Calculez le nombre de reports maximum possible comme suit (un nombre maximum de reports implique que l'utilisateur ne répond jamais à l'invite de report qui s'affiche chaque fois pendant 5 minutes) :

(Nombre de reports de mise à jour de règle autorisés x Durée de chaque report de mise à jour de règle) + (5 minutes x [Nombre de reports de mise à jour de règle autorisés - 1])

Modifier l'option Utilisation par défaut de la clé SDUser

- Le chiffrement de données système (SDE) est appliqué en fonction de la valeur de la règle « Règles du chiffrement SDE ». Les répertoires supplémentaires sont protégés par défaut lorsque la règle « Activer le chiffrement SDE » est sélectionnée. Pour plus d'informations, rechercher « Règles du chiffrement SDE » dans AdminHelp. Lorsque Encryption est en train de traiter une mise à jour de règle qui contient une règle SDE active, le répertoire du profil de l'utilisateur actuel est chiffré par défaut avec la clé SDUser (une clé utilisateur) plutôt qu'avec la clé SDE (une clé de périphérique). La clé SDUser est également utilisée pour crypter les fichiers ou les dossiers qui sont copiés (non déplacé) dans un répertoire utilisateur qui n'est pas un crypté avec SDE.

  Pour désactiver la clé SDUser et l'utiliser pour crypter ces répertoires utilisateurs, créez l'entrée de registre suivante sur l'ordinateur :

  [HKEY_LOCAL_MACHINE\SOFTWARE\Credant\CMGShield]

  "EnableSDUserKeyUsage"=DWORD:00000000

  Si cette clé de registre est absente ou est définie sur autre chose que 0, la clé SDUser est utilisée pour chiffrer ces répertoires utilisateurs.

Activation/désactivation d'Encrypt for Sharing dans le menu contextuel (clic droit)

- Pour désactiver ou activer l'option *Encrypt for Sharing* dans le menu contextuel (clic droit), utilisez la clé de registre suivante.

  HKEY_LOCAL_MACHINE\SOFTWARE\Dell\Dell Data Protection\Encryption

  "DisplaySharing"=DWORD

  0 = désactiver l'option Encrypt for Sharing dans le menu contextuel (clic droit)

  1 = activer l'option Encrypt for Sharing dans le menu contextuel (clic droit)

Activation/désactivation de la notification pour l'activation d'Encryption Personal

- HKCU\Software\Dell\Dell Data Protection\Encryption

  "HidePasswordPrompt"=DWORD

  1 = désactive l'invite de mot de passe pour l'activation d'Encryption Personal

  0 = active l'invite de mot de passe pour l'activation d'Encryption Personal

Activation/désactivation de l'invite de redémarrage lorsqu'Encryption Removal Agent atteint l'étape finale de déchiffrement

- Pour que l'utilisateur ne soit pas invité à redémarrer son ordinateur lorsqu'Encryption Removal Agent atteint son état final dans le processus de déchiffrement, modifiez la valeur de registre suivante.

  HKLM\Software\Dell\Dell Data Protection

  "ShowDecryptAgentRebootPrompt"=DWORD

  Par défaut = activé

  1 = activé (affiche l'invite)

  0 = désactivé (masque l'invite)

Client Advanced Authentication

Désactiver la carte à puce et les services biométriques (en option)

Si vous ne voulez pas qu'Advanced Authentication modifie les services associés aux cartes à puce et dispositifs biométriques selon un type de démarrage « automatique », vous pouvez désactiver la fonction de démarrage du service.

Dans ce cas, Authentication ne tente pas de démarrer ces trois services :

- SCardSvr : gère l'accès aux cartes à puce lues par l'ordinateur. Si ce service est arrêté, cet ordinateur ne peut pas lire les cartes à puce. Si ce service est désactivé, tout service qui en dépend explicitement ne peut pas démarrer.
- SCPolicySvc : permet de configurer le système de sorte à verrouiller le bureau de l'utilisateur sur retrait d'une carte à puce.
- WbioSrvc : le service de biométrie Windows donne aux applications client la possibilité de capturer, comparer, manipuler et stocker des données biométriques sans accéder directement à n'importe quel matériel ou application d'évaluation biométrique. Ce service est hébergé au sein d'un processus SVCHOST privilégié.

  La désactivation de cette fonction supprime également les avertissements associés aux services requis non exécutés.

- Par défaut, si la clé de registre n'existe pas ou si la valeur est définie sur 0, cette fonction est activée.

  [HKEY_LOCAL_MACHINE\SOFTWARE\DELL\Dell Data Protection]

  SmartCardServiceCheck=REG_DWORD:0

  Définissez la valeur sur 0 pour activer.

  Définissez la valeur sur 1 pour désactiver.

Utiliser des cartes à puce avec connexion Windows

- Pour déterminer si l'authentification avant démarrage est activée, assurez-vous que la valeur suivante est définie :

  [HKLM\System\CurrentControlSet\Services\DellMgmtAgent\Parameters]

  "PBAIsActivated"=DWORD (32-bit):1

  La valeur 1 signifie que l'authentification avant démarrage est activée. La valeur 0 signifie que l'authentification avant démarrage n'est pas activée.

  REMARQUE : Supprimer manuellement cette clé peut donner lieu à des résultats indésirables pour les utilisateurs se synchronisant avec la PBA entraînant un besoin de récupération manuelle.

- Pour déterminer si une carte à puce est présente et active, vérifiez que la valeur suivante est définie :

  HKLM\SOFTWARE\Dell\Dell Data Protection\

  "SmartcardEnabled"=DWORD:1

  Si le paramètre SmartcardEnabled est manquant ou si sa valeur est égale à zéro, le fournisseur d'informations d'identification affiche uniquement le mot de passe pour l'authentification.

  Si SmartcardEnabled a une valeur différente de zéro, le fournisseur d'informations d'identification affiche les options d'authentification par mot de passe et par carte à puce.

- La valeur de registre suivante indique si Winlogon doit générer une notification pour les événements de connexion par carte à puce.

  HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify

  "SmartCardLogonNotify"=DWORD:1

  0 = Désactivé

  1 = Activé

  Accédez au Glossaire.

- Pour empêcher la gestion SED de désactiver les fournisseurs d'informations d'identification tiers, créez la clé de registre suivante :

  HKLM\SOFTWARE\Dell\Dell Data Protection\

  "AllowOtherCredProviders" = DWORD:1

  0 = Désactivé (valeur par défaut)

1 = Activé

- Encryption Management Agent ne génère plus de stratégies par défaut. Pour générer de futures stratégies consommées, créez la clé de registre suivante :

  HKLM\Software\Dell\Dell Data Protection\

  DWORD: DumpPolicies

  Value=1

  Remarque : un redémarrage est nécessaire pour que cette modification soit prise en compte.

- Pour supprimer toutes les notifications Toaster de Encryption Management Agent, la valeur de registre suivante doit être définie sur l'ordinateur client.

  [HKEY_LOCAL_MACHINE\SOFTWARE\Dell\Dell Data Protection]

  "PbaToastersAllowClose" =DWORD:1

  0 = Activé (par défaut)

  1 = Désactivé

13

Glossaire

Advanced Authentication : ce produit fournit des options de lecteur de carte à puce. Advanced Authentication aide à la gestion de ces nombreuses méthodes d'authentification, prend en charge la connexion aux lecteurs à chiffrement automatique et SSO, et gère les informations d'identification de l'utilisateur et les mots de passe.

Mot de passe administrateur de cryptage : le mot de passe administrateur de cryptage est un mot de passe d'administration propre à chaque ordinateur. Vous aurez besoin de ce mot de passe pour la majorité des modifications de configuration dans la console locale de gestion. Il s'agit également du mot de passe qui sera demandé pour exécuter le programme LSARecovery_[hostname].exe en vue de récupérer les données. Enregistrez et conservez-le en lieu sûr.

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.

Clés de cryptage : dans la plupart des cas, Encryption utilise la clé de cryptage de l'utilisateur et deux clés de cryptage supplémentaires. Cependant, il y a des exceptions : toutes les règles SDE et la règle Identifiants Windows sécurisés utilisent la clé SDE. La règle Crypter le fichier de pagination Windows et la règle Fichier de mise en veille prolongée Windows utilisent leur propre clé, la clé General Purpose Key (GPK). La clé de cryptage commun rend les fichiers accessibles à tous les utilisateurs gérés sur leur périphérique de création. La clé de cryptage de l'utilisateur rend les fichiers accessibles uniquement à l'utilisateur qui les a créés, uniquement sur le périphérique où ils ont été créés. La clé de cryptage « Utilisateur itinérant » rend les fichiers accessibles uniquement à l'utilisateur qui les a créés sur le périphérique Windows ou Mac protégé.

Balayage de cryptage : le processus d'analyse des dossiers à crypter 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 une analyse de chiffrement peut avoir lieu et ce qui risque d'affecter les temps d'analyse résultants et ce, de la manière suivante : une analyse de chiffrement se produira à la réception initiale d'une règle pour laquelle le chiffrement est activé. Ceci peut se produire immédiatement après l'activation si le cryptage a été activé sur votre règle. - Si la règle *Analyser la station de travail lors de la connexion* est activée, les dossiers à crypter seront analysés 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 chiffrement, les algorithmes de chiffrement, l'utilisation de clés de chiffrement (commun par rapport à utilisateur), déclenchera une analyse. De plus, le basculement entre l'activation et la désactivation du chiffrement déclenche une analyse de chiffrement.

Authentification avant démarrage : l'authentification avant démarrage (PBA – Preboot Authentication) joue le rôle d'extension du BIOS ou du micrologiciel de démarrage et garantit un environnement sécurisé inviolable extérieur au système d'exploitation sous forme de couche d'authentification fiable. L'authentification avant démarrage empêche toute lecture sur le disque dur, par exemple du système d'exploitation, tant que l'utilisateur n'a pas confirmé les identifiants corrects.

Authentification unique (SSO – Single Sign-On) : cette méthode simplifie le processus de connexion lorsque le service Multi-Factor Authentication est activé à la fois avant démarrage et pour la connexion Windows. Si elle est activée, l'authentification est uniquement requise avant le démarrage et les utilisateurs sont automatiquement connectés à Windows. Si cette option n'est pas activée, l'authentification peut être requise plusieurs fois.

Cryptage des données système (SDE) : SDE est conçu pour crypter le système d'exploitation et les fichiers programmes. Pour ce faire, SDE doit pouvoir ouvrir sa clé lorsque le système d'exploitation démarre sans que l'utilisateur n'ait à saisir de mot de passe. Ceci a pour but d'empêcher les altérations ou les attaques hors ligne du système d'exploitation. SDE n'est pas conçu pour être utilisé pour les données utilisateur. Les clés de chiffrement commun et utilisateur sont destinées aux données utilisateur sensibles, car elles exigent l'utilisation d'un mot de passe pour déverrouiller les clés de chiffrement. Les règles SDE ne cryptent pas les fichiers nécessaires au démarrage du système d'exploitation. Elles ne nécessitent pas d'authentification avant démarrage et n'affectent en rien l'enregistrement de démarrage principal. Au démarrage de l'ordinateur, les fichiers cryptés sont disponibles avant l'identification de l'utilisateur (pour permettre la gestion des correctifs, les SMS et l'utilisation des outils de sauvegarde et de récupération). La désactivation de SDE déclenche le décryptage automatique de tous les fichiers et répertoires SDE cryptés pour les utilisateurs pertinents, quelles que soient les autres règles SDE, par exemple les règles de cryptage SDE.

TPM (Trusted Platform Module) : TPM est une puce de sécurité assurant trois fonctions majeures : stockage sécurisé, mesure et attestation. Le client Encryption utilise TPM pour assurer sa fonction de stockage sécurisé. Le TPM peut également fournir les conteneurs cryptés pour le coffre de logiciels.