

Dell Data Security

Guide d'installation d'Encryption Personal v8.17.1



Remarques, précautions et avertissements

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

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

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

© 2018 Dell Inc. Tous droits réservés. Dell, EMC et d'autres marques sont des marques de Dell Inc. ou de ses filiales. Les autres marques peuvent être des marques de leurs propriétaires respectifs.

Marques déposées et marques commerciales utilisées dans Dell Encryption, Endpoint Security Suite Pro, Endpoint Security Suite Enterprise et dans la suite de documents Data Guardian : Dell™ et le logo Dell, Dell Precision™, OptiPlex™, ControlVault™, Latitude™, XPS® et KACE™ sont des marques commerciales de Dell Inc. Cylance®, CylancePROTECT et le logo Cylance sont des marques déposées de Cylance, Inc. aux États-Unis et dans d'autres pays. McAfee® et le logo McAfee sont des marques ou des marques déposées de McAfee, Inc. aux États-Unis et dans d'autres pays. Intel®, Pentium®, Intel Core Inside Duo®, Itanium® et Xeon® sont des marques déposées d'Intel Corporation aux États-Unis et dans d'autres pays. Adobe®, Acrobat®, et Flash® sont des marques déposées d'Adobe Systems Incorporated. Authen Tec® et Eikon® sont des marques déposées d'Authen Tec. AMD® est une marque déposée d'Advanced Micro Devices, Inc. Microsoft®, Windows®, et Windows Server®, Internet Explorer®, MS-DOS®, Windows Vista®, MSN®, ActiveX®, Active Directory®, Access®, ActiveSync®, BitLocker®, BitLocker To Go®, Excel®, Hyper-V®, Silverlight®, Outlook®, PowerPoint®, OneDrive®, SQL Server®, et Visual C++® sont des marques commerciales ou des marques déposées de Microsoft Corporation aux États-Unis et/ou dans d'autres pays. VMware® est une marque déposée ou une marque commerciale de VMware, Inc. aux États-Unis ou dans d'autres pays. Box® est une marque déposée de Box. DropboxSM est une marque de service de Dropbox, Inc. Google™, Android™, Google™ Chrome™, Gmail™, YouTube®, et Google™ Play sont des marques commerciales ou des marques déposées de Google Inc. aux États-Unis et dans d'autres pays. Apple®, Aperture®, App StoreSM, Apple Remote Desktop™, Apple TV®, Boot Camp™, FileVault™, iCloud®SM, iPad®, iPhone®, iPhoto®, iTunes Music Store®, Macintosh®, Safari® et Siri® sont des marques de service, des marques commerciales ou des marques déposées d'Apple, Inc. aux États-Unis et/ou dans d'autres pays. GO ID®, RSA®, et SecurID® sont des marques déposées de Dell EMC. EnCase™ et Guidance Software® sont des marques commerciales ou des marques déposées de Guidance Software. Entrust® est une marque déposée d'Entrust®, Inc. aux États-Unis et dans d'autres pays. InstallShield® est une marque déposée de Flexera Software aux États-Unis, en Chine, dans l'Union européenne, à Hong Kong, au Japon, à Taïwan et au Royaume-Uni. Micron® et RealSSD® sont des marques déposées de Micron Technology, Inc. aux États-Unis et dans d'autres pays. Mozilla® Firefox® est une marque déposée de Mozilla Foundation aux États-Unis et/ou dans d'autres pays. IOS® est une marque commerciale ou une marque déposée de Cisco Systems, Inc. aux États-Unis et dans certains autres pays et elle est utilisée sous licence. Oracle® et Java® sont des marques déposées d'Oracle et/ou de ses sociétés affiliées. Les autres noms peuvent être des marques de leurs propriétaires respectifs. SAMSUNG™ est une marque commerciale de SAMSUNG aux États-Unis ou dans d'autres pays. Seagate® est une marque déposée de Seagate Technology LLC aux États-Unis et/ou dans d'autres pays. Travelstar® est une marque déposée de HGST, Inc. aux États-Unis et dans d'autres pays. UNIX® est une marque déposée de The Open Group. VALIDITY™ est une marque commerciale de Validity Sensors, Inc. aux États-Unis et dans d'autres pays. VeriSign® et d'autres marques connexes sont des marques commerciales ou des marques déposées de VeriSign, Inc. ou de ses filiales ou sociétés affiliées aux États-Unis et dans d'autres pays et dont la licence est octroyée à Symantec Corporation. KVM on IP® est une marque déposée de Video Products. Yahoo!® est une marque déposée de Yahoo! Inc. Ce produit utilise des parties du programme 7-Zip. Le code source est disponible à l'adresse 7-zip.org. L'octroi de licence est soumis à la licence GNU LGPL + aux restrictions unRAR (7-zip.org/license.txt).

Guide d'installation d'Encryption Personal

2018 - 01

Rév. A01

Table des matières

| | |
|--|-----------|
| 1 Présentation d'Encryption Personal..... | 6 |
| Encryption Personal..... | 6 |
| Client Advanced Authentication..... | 6 |
| Contacter Dell ProSupport..... | 6 |
| 2 Configuration requise pour Encryption Personal..... | 7 |
| Client Encryption..... | 7 |
| Configuration requise du client Encryption..... | 8 |
| Matériel du client Encryption..... | 8 |
| Systèmes d'exploitation du client Encryption..... | 8 |
| Systèmes d'exploitation pour Encryption External Media..... | 9 |
| Emplacement du client Encryption..... | 9 |
| Client Advanced Authentication..... | 10 |
| Prérequis du client Advanced Authentication..... | 10 |
| Matériel du client Advanced Authentication..... | 10 |
| Systèmes d'exploitation du client Advanced Authentication..... | 11 |
| Localisation du client Advanced Authentication..... | 11 |
| Client SED..... | 12 |
| Pilotes OPAL..... | 13 |
| Matériel du client SED..... | 13 |
| Claviers internationaux pour le client SED | |
| Emplacement du client SED | |
| Systèmes d'exploitation du client SED..... | 14 |
| 3 Télécharger le logiciel..... | 16 |
| 4 Installation d'Encryption Personal..... | 18 |
| Choisir une méthode d'installation..... | 18 |
| Installation d'Encryption Personal en utilisant le programme d'installation principal - RECOMMANDÉ..... | 18 |
| Installation d'Encryption Personal individuellement à l'aide de programmes d'installation enfant..... | 20 |
| 5 Assistants de configuration d'Advanced Authentication et d'Encryption Personal..... | 23 |
| 6 Configurer les paramètres de Dell Encryption Management Agent..... | 25 |
| Changement du mot de passe de l'administrateur et de l'emplacement de sauvegarde..... | 25 |
| Configuration de l'outil de cryptage (Encryption) et de l'authentification avant démarrage (Preboot Authentication)..... | 25 |
| Modifier les paramètres de cryptage et d'authentification avant démarrage..... | 27 |
| Définition des options d'authentification..... | 27 |
| Configuration des options de connexion..... | 27 |
| Configuration des questions de récupération..... | 29 |
| Configuration de l'authentification par lecture d'empreinte digitale..... | 29 |
| Configuration de l'enregistrement d'une carte à puce..... | 29 |
| Configuration des droits avancés..... | 30 |



| | |
|---|-----------|
| Gestion de l'authentification des utilisateurs..... | 30 |
| Ajouter de nouveaux utilisateurs..... | 31 |
| Inscrire ou modifier les références de l'utilisateur..... | 31 |
| Suppression d'un identifiant enregistré..... | 31 |
| Supprimer tous les identifiants enregistrés d'un utilisateur..... | 32 |
| 7 Désinstaller à l'aide du programme d'installation principal..... | 33 |
| Choisir une méthode de désinstallation..... | 33 |
| Désinstaller à partir de Ajout/Suppression de programmes..... | 33 |
| Désinstaller à partir de la ligne de commande..... | 33 |
| 8 Désinstaller à l'aide des programme d'installation enfants..... | 35 |
| Désinstaller le client Encryption..... | 35 |
| Choisir une méthode de désinstallation..... | 35 |
| Désinstaller Advanced Authentication..... | 38 |
| Choisir une méthode de désinstallation..... | 38 |
| Désinstallation d'Encryption Management/Agent..... | 38 |
| Choisir une méthode de désinstallation..... | 38 |
| 9 Désinstallation à l'aide du programme de désinstallation de Dell Data Security..... | 40 |
| Désinstaller | 40 |
| 10 Descriptions des règles et des modèles..... | 41 |
| Stratégies..... | 41 |
| Description des modèles..... | 61 |
| Protection avancée pour tous les lecteurs fixes et supports externes..... | 61 |
| Norme PCI DSS..... | 61 |
| Législation relative à la protection des données..... | 62 |
| Législation relative à l'HIPAA..... | 62 |
| Protection de base pour tous les lecteurs fixes et supports externes (par défaut)..... | 62 |
| Protection de base pour tous les lecteurs fixes..... | 63 |
| Protection de base pour le disque système uniquement..... | 63 |
| Protection de base pour les supports externes..... | 63 |
| Cryptage désactivé..... | 63 |
| 11 Extraire les programmes d'installation enfants du programme d'installation principal..... | 64 |
| 12 Dépannage..... | 65 |
| Dépannage du client Encryption et | 65 |
| Mise à niveau vers Windows 10 Creators Update..... | 65 |
| Création d'un fichier journal Encryption Removal Agent (facultatif)..... | 65 |
| Trouver la version de TSS..... | 66 |
| Encryption External Media et interactions PCS..... | 66 |
| Utiliser WSScan..... | 66 |
| Vérification de l'état d'Encryption Removal Agent..... | 68 |
| Comment Crypter un iPod avec Encryption External Media..... | 68 |
| Pilotes Dell ControlVault..... | 69 |
| Mettre à jour les pilotes et le micrologiciel Dell ControlVault..... | 69 |

| | |
|-------------------------------------|-----------|
| Paramètres de registre..... | 71 |
| Client Encryption..... | 71 |
| Client Advanced Authentication..... | 72 |
| 13 Glossaire..... | 74 |



Présentation d'Encryption Personal

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

Encryption Personal

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

Client Advanced Authentication

L'objectif d'Advanced Authentication consiste à offrir une solution de sécurité de bout en bout pour la prise en charge d'Advanced Authentication.

Advanced Authentication fournit un support multifacteur pour l'authentification Windows par mots de passe, par lecteurs d'empreintes digitales, par cartes à puce « à contact » et « sans contact », ainsi que pour l'auto-enregistrement et la [connexion en une étape \(SSO\)](#).

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

L'outil Administrator Settings est disponible aux utilisateurs disposant de privilèges d'administrateur et sert à configurer les règles d'authentification et les options de récupération, à gérer les utilisateurs et à configurer des paramètres avancés ainsi que les paramètres spécifiques aux identifiants pris en charge pour la connexion Windows.

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 les applications Advanced Authentication.

Contacter Dell ProSupport

Appelez le 877-459-7304, poste 4310039, afin de recevoir 24h/24, 7j/7 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 service 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 [Numéros de téléphone internationaux Dell ProSupport](#).

Configuration requise pour Encryption Personal

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

Client Encryption

- 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.)
- Dell vous recommande vivement de créer un mot de passe Windows (s'il n'en existe pas déjà un) pour protéger l'accès à vos données cryptées. La création d'un mot de passe sur votre ordinateur permet de bloquer l'accès à votre compte utilisateur à toute personne qui ne dispose pas du mot de passe.
 - a Accédez au Panneau de configuration de Windows (**Démarrer > Panneau de configuration**).
 - b Cliquez sur l'icône **Comptes utilisateur**.
 - c Cliquez sur **Créer un mot de passe pour votre compte**.
 - d Saisissez un nouveau mot de passe et confirmez-le.
 - e Il est également possible d'ajouter un indice de mot de passe.
 - f Cliquez sur **Créer un mot de passe**.
 - g Redémarrez votre ordinateur.
- Les meilleures pratiques informatiques doivent être suivies pendant le déploiement. Ceci inclut, sans s'y limiter, les environnements de test contrôlés pour les premiers tests et les déploiements échelonnés pour les utilisateurs.
- Le compte utilisateur servant à l'installation/la mise à jour/la désinstallation doit correspondre à un administrateur local ou de domaine, qui peut être affecté temporairement par un outil de déploiement tel que Microsoft SMS ou Dell KACE. Les utilisateurs non-administrateurs et disposant de privilèges particuliers ne sont pas pris en charge.
- Sauvegardez toutes les données importantes avant de démarrer l'installation/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 cryptage initial (ainsi que la durée de décryptage 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 cryptage initial pour prévenir la mise en veille d'un ordinateur lors des périodes d'inactivité. Le cryptage ne peut pas être exécuté sur un ordinateur en veille (le décryptage non plus).
- Le client Encryption ne prend pas en charge les configurations à double démarrage dans la mesure où il est possible de crypter 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, voir <http://www.dell.com/support/article/us/en/19/SLN304039>.
- Le module TPM (Trusted Platform Module) permet de 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 client.
- Le client Encryption a été testé et est compatible avec McAfee, le client Symantec, Kaspersky et MalwareBytes. Les exclusions codées en dur sont en place afin que ces fournisseurs d'antivirus puissent prévenir les incompatibilités entre le balayage et le cryptage des antivirus. Le client Encryption a aussi été testé avec Microsoft Enhanced Mitigation Experience Toolkit.



Si votre entreprise utilise un anti-virus fournisseur qui n'est pas répertorié, reportez-vous à l'article de la base de connaissances [SLN298707](#) ou [Contactez l'assistance Dell ProSupport](#)

- 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 la rubrique www.dell.com/support pour obtenir la dernière documentation et conseils techniques.

Configuration requise du client Encryption

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

① REMARQUE : .Net Framework 4.6 (ou version ultérieure) est nécessaire pour l'exécution du mode FIPS.

Pour vérifier la version de Microsoft .Net installée, suivez ces instructions sur l'ordinateur ciblé pour installation : [http://msdn.microsoft.com/en-us/library/hh925568\(v=vs.110\).aspx](http://msdn.microsoft.com/en-us/library/hh925568(v=vs.110).aspx). Pour installer Microsoft .Net Framework 4.5.2, accédez à <https://www.microsoft.com/en-us/download/details.aspx?id=42643>.

- Le programme d'installation principal installe les conditions 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 le client Encryption.

Conditions requises

- Visual C++ 2012 Redistributable Package (x86 et x64) Mise à jour 4 ou ultérieure
- Visual C++ 2015 Redistributable Package (x86 et x64) Mise à jour 3 ou ultérieure

Visual C++ 2015 nécessite Windows Update [KB2999226](#) s'il est installé sous Windows 7.

Matériel du client Encryption

- Le tableau suivant répertorie les matériels informatiques compatibles.

Matériel

- Processeur Intel Pentium ou AMD
- 110 Mo d'espace disque disponible
- 512 Mo de RAM

① REMARQUE : De l'espace disque libre supplémentaire est nécessaire pour crypter les fichiers sur le point de terminaison. Cette taille varie en fonction des stratégies et de la taille du lecteur.

- Le tableau suivant répertorie les matériels informatiques compatibles.

Matériel intégré en option

- TPM 1.2 ou 2.0

Systèmes d'exploitation du client Encryption

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

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

- Windows 7 SP0-SP1 : Enterprise, Professional, Ultimate

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

- Windows Embedded Standard 7 doté du modèle Compatibilité de l'application (le matériel de cryptage n'est pas pris en charge)
- Windows 8 : Enterprise, Pro
- Windows 8.1 Mise à jour 0-1 : Enterprise Edition, Pro Edition
- Windows Embedded 8.1 Industry Enterprise (le matériel de cryptage n'est pas pris en charge)
- Windows 10 : Édition Familiale Basique, Familiale Premium, Éducation, Entreprise, Professionnel version 1607 (Anniversary Update/Redstone 1) jusqu'à la version 1709 (Mise à jour Fall Creators Update/Redstone 3)
- VMWare Workstation 5.5 et version supérieure

REMARQUE : Le mode UEFI n'est pas pris en charge sur Windows 7, Windows Embedded Standard 7 ou Windows Embedded 8.1 Industry Enterprise.

Systèmes d'exploitation pour Encryption External Media

- Le tableau suivant répertorie les systèmes d'exploitation pris en charge lors de l'accès aux supports protégés par Encryption External Media.

REMARQUE : Le support externe doit disposer d'environ 55 Mo, ainsi que d'un espace libre sur le support égal au plus gros fichier à crypter, pour héberger Encryption External Media.

Systèmes d'exploitation Windows pris en charge pour accéder à un support protégé par Encryption External Media (32 bits et 64 bits)

- Windows 7 SP0-SP1 : Édition Familiale Basique, Familiale Premium, Enterprise, Professionnel, Ultimate
- Windows Embedded Standard 7 doté du modèle Compatibilité de l'application (le matériel de cryptage n'est pas pris en charge)
- Windows 8 : Édition Familiale Basique, Familiale Premium, Entreprise, Pro
- Windows 8.1 Mise à jour 0-1 : Enterprise Edition, Pro Edition
- Windows Embedded 8.1 Industry Enterprise (le matériel de cryptage n'est pas pris en charge)
- Windows 10 : Édition Familiale Basique, Familiale Premium, Éducation, Entreprise, Professionnel version 1607 (Anniversary Update/Redstone 1) jusqu'à la version 1709 (Mise à jour Fall Creators Update/Redstone 3)

Systèmes d'exploitation Mac pris en charge pour accéder à un support protégé par Encryption External Media (noyaux 64 bits)

- Mac OS X El Capitan 10.11.6
- macOS Sierra 10.12.6
- macOS High Sierra 10.13.0 et 10.13.2

Emplacement du client Encryption

- Le client Encryption est compatible avec l'interface utilisateur multilingue (MUI) et localisé dans les langues suivantes.

Langues prises en charge

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



Client Advanced Authentication

- Les fonctions d'Advanced Authentication sont disponibles uniquement lorsque l'authentification avant démarrage est activée. Lors de l'utilisation d'Advanced Authentication, vous sécuriserez l'accès à cet ordinateur à l'aide des identifiants Advanced Authentication gérés et enregistrés grâce à Advanced Authentication. Advanced Authentication est désormais le principal gestionnaire des identifiants d'authentification pour la connexion Windows, y compris le mot de passe, les empreintes digitales et les cartes à puce Windows. Les identifiants de type mot de passe image, code PIN et empreintes enregistrés à l'aide du système d'exploitation Microsoft ne seront pas reconnus lors de la connexion à Windows.

Pour continuer à utiliser le système d'exploitation Microsoft pour gérer vos identifiants, désinstallez Advanced Authentication ou ne l'installez pas.

① **REMARQUE :** Les méthodes d'authentification PBA ne peuvent pas être modifiées entre mot de passe et carte à puce lorsque le compte utilisateur existe au sein de la PBA.

Prérequis du client Advanced Authentication

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

① **REMARQUE :** .Net Framework 4.6 (ou version ultérieure) est nécessaire pour l'exécution du mode FIPS.

Pour vérifier la version de Microsoft .Net installée, suivez ces instructions sur l'ordinateur ciblé pour installation : [http://msdn.microsoft.com/en-us/library/hh925568\(v=vs.110\).aspx](http://msdn.microsoft.com/en-us/library/hh925568(v=vs.110).aspx). Pour installer Microsoft .Net Framework 4.5.2, accédez à <https://www.microsoft.com/en-us/download/details.aspx?id=42643>.

- Le programme d'installation principal installe les conditions 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 le client Encryption.

Conditions requises

- Visual C++ 2012 Redistributable Package (x86 et x64) Mise à jour 4 ou ultérieure
- Visual C++ 2015 Redistributable Package (x86 et x64) Mise à jour 3 ou ultérieure

Visual C++ 2015 nécessite Windows Update [KB2999226](#) s'il est installé sous Windows 7.

Matériel du client Advanced Authentication

- Le tableau suivant répertorie les matériels d'authentification compatibles.

Lecteurs de cartes à puces et d'empreintes digitales

- Validity VFS495 en mode sécurisé
- Lecteur à fente Dell ControlVault
- Lecteur sécurisé UPEK TCS1 FIPS 201 1.6.3.379
- Lecteurs USB Authentec Eikon et Eikon To Go

Cartes sans contact

- Cartes sans contact utilisant des lecteurs de carte sans contact intégrés dans des ordinateurs portables Dell spécifiques

Cartes à puce

- Cartes à puce PKCS #11 utilisant le client [ActivIdentity](#)

REMARQUE : Le client ActivIdentity n'est pas pré-chargé et doit être installé séparément.

- Cartes CSP
 - Cartes CAC (Common Access Cards)
 - Cartes réseau de catégorie B/SIPR
- Les pilotes et micrologiciel de Dell ControlVault, les lecteurs d'empreintes et les cartes à puce (répertoriés ci-dessous) ne sont pas inclus dans le programme d'installation principal ou dans les fichiers exécutables de programme d'installation enfant. Le pilotes et le micrologiciel doivent être conservés à jour et peuvent être téléchargés à partir de <http://www.dell.com/support> en sélectionnant votre modèle d'ordinateur. Téléchargez les pilotes et le logiciel appropriés en fonction de votre matériel d'authentification.
- Dell ControlVault
 - NEXT Biometrics Fingerprint Driver
 - Pilote Validity FingerPrint Reader 495
 - Pilote de carte à puce O2Micro

Si vous installez du matériel autre que Dell, téléchargez les pilotes et le logiciel mis à jour depuis le site internet du fournisseur. Vous trouverez les instructions d'installation des pilotes Dell ControlVault drivers dans [Dell ControlVault Drivers](#).

- Le tableau suivant contient des informations détaillées sur les modèles d'ordinateurs Dell pris en charge avec les cartes réseau SIPR.

Modèles d'ordinateurs Dell - Prise en charge de carte réseau de classe B/SIPR

- | | | |
|------------------|-------------------|------------------------------|
| • Latitude E6440 | • Precision M2800 | • Latitude 14 Rugged Extreme |
| • Latitude E6540 | • Precision M4800 | • Latitude 12 Rugged Extreme |
| | • Precision M6800 | • Latitude 14 Rugged |

Systèmes d'exploitation du client Advanced Authentication

Systèmes d'exploitation Windows

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

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

- Windows 7 SP0-SP1 : Enterprise, Professional, Ultimate
- Windows 8 : Enterprise, Pro
- Windows 8.1 Mise à jour 0-1 : Enterprise Edition, Pro Edition
- Windows 10 : Éducation, Entreprise, Pro Version 1607 Anniversary Update/Redstone 1) jusqu'à la version 1709 ((Mise à jour Fall Creators Update/Redstone 3)

REMARQUE : Le mode UEFI n'est pas pris en charge sur Windows 7.

Localisation du client Advanced Authentication

- Le client Advanced Authentication est compatible avec l'interface utilisateur multilingue (MUI) et est localisé dans les langues suivantes. Le mode UEFI et l'authentification avant démarrage prennent en charge les langues suivantes (**à l'exception** du russe, du chinois traditionnel et du chinois simplifié).



Langues prises en charge

- EN : anglais
- FR : français
- IT : italien
- DE : allemand
- ES : espagnol
- JA : japonais
- KO : coréen
- ZH-CN : chinois simplifié
- ZH-TW : chinois traditionnel/de Taïwan
- PT-BR : portugais brésilien
- PT-PT : portugais du Portugal (ibère)
- RU : russe

Accédez à [Obtenir le logiciel](#).

Client SED

- Pour que l'installation de SED réussisse, l'ordinateur doit disposer d'une connectivité à un réseau filaire.
- 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-cryptage prenant en charge le module HCA. Cette configuration non prise en charge est une configuration après-vente.
- Si l'ordinateur ciblé pour cryptage est équipé d'un accélérateur d'un lecteur à cryptage automatique, 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.
- Dell vous déconseille de changer de méthode d'authentification après avoir activé la règle PBA. Si vous devez changer de méthode d'authentification, vous devez :
 - Supprimez tous les utilisateurs de la PBA.
 - ou
 - Désactivez la PBA, changez de méthode d'authentification, puis ré-activez la PBA.

❗ IMPORTANT:

En raison de la nature du RAID et des SED, la gestion des SED 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 affichera un écran bleu lors du passage de *RAID=On* à *AHCI*.

- La configuration des disques à cryptage automatique pour SED management de Dell est différente entre les disques NVMe et non NVMe (SATA).
 - Tout disque NVMe utilisé en tant que SED : l'opération SATA du BIOS doit être définie sur RAID ON, car SED Management de Dell ne prend pas en charge AHCI sur les disques NVMe.
 - Tout disque NVMe utilisé en tant que SED : le mode de démarrage du BIOS doit être UEFI et les ROM de l'option Hérité doivent être désactivés.
 - Tout disque non NVMe utilisé en tant que SED : l'opération SATA du BIOS doit être définie sur AHCI, car SED Management de Dell ne prend pas en charge RAID avec les disques non NVMe.
 - RAID ON n'est pas pris en charge, car l'accès à la lecture et l'écriture des données RAID (sur un secteur non disponible sur un lecteur non NVMe verrouillé) n'est pas disponible au démarrage et ne peut attendre de lire ces données après la connexion de l'utilisateur.
 - 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 transfert de RAID à AHCI (ou vice-versa), voir <http://www.dell.com/support/article/us/en/19/SLN306460>.

Les lecteurs SED compatibles Opal pris en charge exigent les pilotes Intel Rapid Storage Technology mis à jour, disponibles à l'adresse <http://www.dell.com/support/home/us/en/04/product-support/product/dell-data-protection-encryption/drivers> Dell recommande Intel Rapid Storage Technology Driver version 15.2.0.0 ou ultérieure avec les disques NVMe.

Pilotes OPAL

- Les lecteurs SED compatibles Opal pris en charge exigent les pilotes Intel Rapid Storage Technology mis à jour, situés sur <http://www.dell.com/support>.

Matériel du client SED

- Pour consulter la toute dernière liste de SED compatibles Opal pris en charge avec la gestion des SED, reportez-vous à l'article suivant de la base de connaissances : <http://www.dell.com/support/article/us/en/19/SLN296720>.

Modèles informatiques Dell pris en charge avec UEFI

- Le tableau suivant répertorie les modèles d'ordinateurs Dell pris en charge avec UEFI.

Modèles d'ordinateur Dell - Prise en charge d'UEFI

| | | | |
|--|---------------------------------|---|----------------------------------|
| Latitude 5280 | Precision M3510 | Optiplex 3040 micro, Mini-tour et compact | Venue Pro 11 (Modèles 5175/5179) |
| Latitude 5480 | Precision M3520 | Optiplex 3046 | Venue Pro 11 (Modèle 7139) |
| Latitude 5580 | Precision M4800 | OptiPlex 3050 All-In-One | |
| Latitude 7370 | Precision M5510 | Tour OptiPlex 3050, petit facteur de forme, micro | |
| Latitude 7380 | Precision M5520 | Optiplex 5040 Mini-tour et compact | |
| Latitude E5250 | Precision M6800 | Tour OptiPlex 5050, petit facteur de forme, micro | |
| Latitude E5270 | Precision M7510 | OptiPlex 7020 | |
| Latitude E5285 | Precision M7520 | Optiplex 7040 micro, Mini-tour et compact | |
| Latitude E5289 2-en-1 | Precision M7710 | Tour OptiPlex 7050, petit facteur de forme, micro | |
| Latitude E5450 | Precision M7720 | Optiplex 3240 All-In-One | |
| Latitude E5470 | Precision D5720 tout All-in-One | Optiplex 5055 Ryzen CPU | |
| Latitude E5550 | Precision T1700 | OptiPlex 5250 All-In-One | |
| Latitude E5570 | Precision T3420 | Precision 5820 tour | |
| Latitude E6440 | Precision T3620 | Optiplex 7010 | |
| Latitude E6540 | Precision T5810 | Optiplex 7440 All-In-One | |
| Latitude E7240 | Precision T7810 | OptiPlex 7450 All-In-One | |
| Latitude E7250 | Precision T7910 | Precision 7820 tour | |
| Latitude E7270 | XPS 13 9333 | Precision 7920 Rack | |
| Latitude E7280 | XPS 13 9350 | Optiplex 9010 | |
| Latitude E7350 | XPS 15 9550 | Optiplex 9020 micro, mini-tour et compact | |
| Latitude 7389 2-en-1 | XPS 15 9560 | Optiplex 9020 All-In-One | |
| Latitude E740 | | Optiplex 9030 All-In-One | |
| Latitude E7450 | | Optiplex XE2 | |
| Latitude E7470 | | | |
| Latitude E7480 | | | |
| Latitude 12 Rugged Extreme (modèle 7414) | | | |
| Latitude 12 Rugged Tablet (modèle 7202) | | | |
| Latitude 7212 Rugged Extreme Tablet | | | |
| Latitude 14 Rugged Extreme (modèle 7414) | | | |



Modèles d'ordinateur Dell - Prise en charge d'UEFI

- Latitude 14 Rugged (modèle 5414)

REMARQUE :

Les fonctions d'authentification sont prises en charge avec le mode UEFI sur ces ordinateurs exécutant Windows 8, Windows 8.1 et Windows 10 avec des disques qualifiés SED compatibles OPAL. Les autres ordinateurs exécutant Windows 7, Windows 8, Windows 8.1 et Windows 10 prennent en charge le mode d'Amorçage hérité.

- Pour obtenir la liste des stations d'accueil et des adaptateurs pris en charge avec le client SED, voir la page <http://www.dell.com/support/article/us/en/19/sln296720/>.

Claviers internationaux pour le client SED

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

Clavier international pris en charge - UEFI

- DE-CH : suisse allemand
- DE-FR : suisse français

Clavier International prise en charge : Non-UEFI

- AR - Arabe (avec lettres latines)
- DE-CH : suisse allemand
- DE-FR : suisse français

Emplacement du client SED

Les clients SED et Advanced Authentication sont compatibles avec l'interface utilisateur multilingue (MUI) et localisés dans les langues suivantes. Le mode UEFI et l'authentification avant démarrage prennent en charge les langues suivantes (**à l'exception** du russe, du chinois traditionnel et du chinois simplifié).

Langues prises en charge

- | | |
|-----------------|--|
| • EN : anglais | • KO : coréen |
| • FR : français | • ZH-CN : chinois simplifié |
| • IT : italien | • ZH-TW : chinois traditionnel/de Taïwan |
| • DE : allemand | • PT-BR : portugais brésilien |
| • ES : espagnol | • PT-PT : portugais du Portugal (ibère) |
| • JA : japonais | • RU : russe |

Systèmes d'exploitation du client SED

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

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

- Windows 7 SP0-SP1 : Enterprise, Professionnel (pris en charge par mode Legacy Boot, mais pas par UEFI)

REMARQUE :

Le mode Legacy Boot est pris en charge sur Windows 7. UEFI n'est pas pris en charge sur Windows 7.

Les disques à cryptage automatique NVMe ne sont pas pris en charge avec Windows 7.

- Windows 8 : Enterprise, Pro
- Windows 8.1 : Enterprise Edition, Pro Edition
- Windows 10 : Éducation, Entreprise, Pro Version 1607 Anniversary Update/Redstone 1) jusqu'à la version 1709 ((Mise à jour Fall Creators Update/Redstone 3)

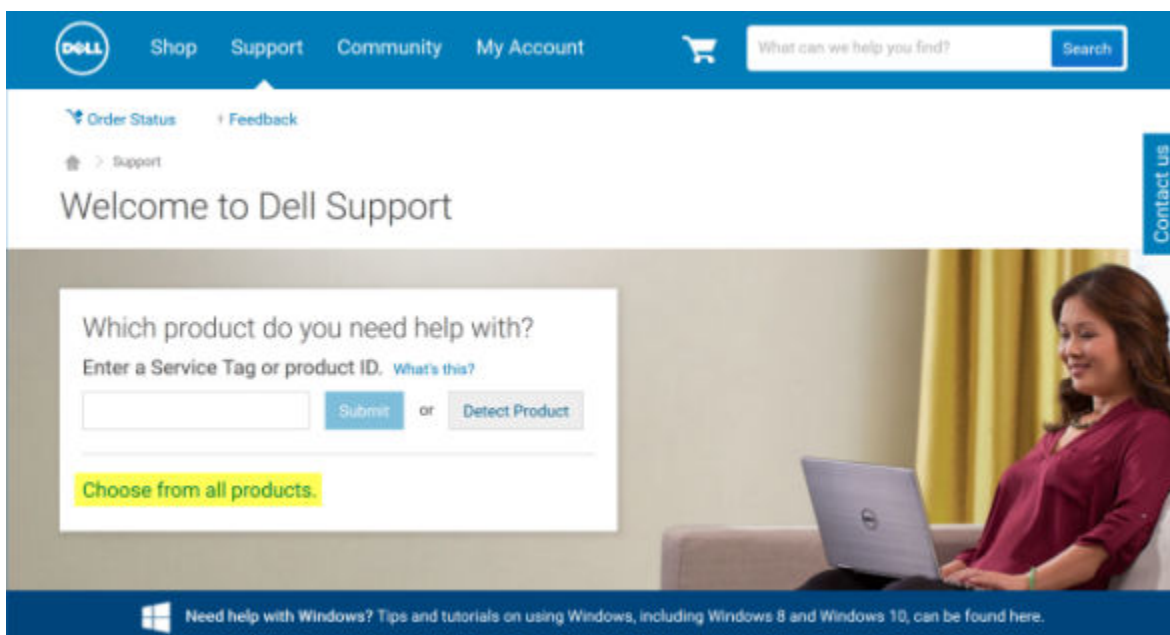


Télécharger le logiciel

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 **Choisir parmi tous les produits**.



- 2 Sélectionnez **Logiciel et sécurité** dans la liste des produits.
- 3 Sélectionnez **Solutions de sécurité des points finaux** dans la section *Logiciel et sécurité*.
Le site Web se rappellera la sélection initiale.
- 4 Sélectionnez le produit Dell.

Exemples :

Dell Encryption Enterprise

Dell Endpoint Security Suite Pro

Dell Endpoint Security Suite Enterprise

Dell Data Guardian

- 5 Sélectionnez **Pilotes et téléchargements**.
- 6 Sélectionnez le type de système d'exploitation client souhaité.
- 7 Sélectionnez **Dell Data Security (4 fichiers)** parmi les options correspondantes. Ceci n'étant qu'un exemple, elles pourront être légèrement différentes. Par exemple, il pourra ne pas exister 4 fichiers parmi lesquels choisir.

Support > Product Support

Support for Dell Data Protection | Encryption [Change product](#)

[Support topics & articles](#)
[Drivers & downloads](#)
[Manuals](#)

Optimize your system with drivers and updates. [1](#)

View all available updates for Windows 10, 64-bit. [Change OS](#)

- Apple Mac OS
- VMware ESXi 5.1
- VMware ESXi 5.5
- VMware ESXi 6.0
- Windows 10, 32-bit
- Windows 10, 64-bit**
- Windows 7, 32-bit
- Windows 7, 64-bit
- Windows 8, 32-bit
- Windows 8, 64-bit
- Windows 8.1, 32-bit
- Windows 8.1, 64-bit
- Windows Server 2003
- Windows Server 2003 x64
- Windows Server 2008 R2
- Windows Server 2008 x64
- Windows Server 2008 x86
- Windows Server 2012 R2

Looking for a different OS? [View the list of Dell supported operating systems](#)

Refine your results:

Category Importance

- 8 Sélectionnez **Télécharger le fichier** ou **Ajouter à ma liste de téléchargements #XX**.
Passez à l'étape [Installation d'Encryption Personal](#).



Installation d'Encryption Personal

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 :

- Pour apprendre à utiliser les fonctions du client Encryption, voir *Aide concernant Dell Encrypt*. Accédez à l'aide depuis **<Install dir>:\Program Files\Dell\Dell Data Protection\Encryption\Help**.
- Pour apprendre à utiliser les fonctions d'*Encryption External Media*, voir l'Aide concernant Encryption External Media. Accédez à l'aide depuis **<Install dir>:\Program Files\Dell\Dell Data Protection\Encryption\EMS**.
- Pour apprendre à utiliser les fonctions d'Advanced Authentication, voir l'Aide d'*Encryption Personal*. Accédez à l'aide depuis **<Install dir>:\Program Files\Dell\Dell Data Protection\Authentication\Help**.

Choisir une méthode d'installation

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

- [Installation d'Encryption Personal en utilisant le programme d'installation principal - RECOMMANDÉ](#)
- [Installation d'Encryption Personal individuellement à l'aide de programmes d'installation enfant](#)

Installation d'Encryption Personal en utilisant le programme d'installation principal - RECOMMANDÉ

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 Dell est généralement dénommé Programme d'installation principal, car il installe plusieurs clients. Dans le cas d'Encryption Personal, il installe le client Encryption et le client Advanced Authentication.

Si vous effectuez l'installation à l'aide de l'interface utilisateur du programme d'installation principal, Encryption Personal peut être installé sur un seul ordinateur à la fois.

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

Sélectionnez une méthode :

[Installation à l'aide de l'interface utilisateur](#)

[Installation à l'aide de la ligne de commande](#)

Installation à l'aide de l'interface utilisateur

Installez le droit sur l'ordinateur cible, si nécessaire.

Copiez DDSSetup.exe sur l'ordinateur local.

Double-cliquez sur DDSSetup.exe pour lancer le programme d'installation.

La boîte de dialogue qui s'affiche indique le statut de l'installation des prérequis. Ceci prend quelques minutes.

Cliquez sur **Suivant** sur l'écran d'accueil.

Lisez le contrat de licence, acceptez-en les termes, puis cliquez sur **Suivant**.

Cliquez sur **Suivant** pour installer Encryption Personal à l'emplacement par défaut C:\Program Files\Dell\Dell Data Protection.

Advanced Authentication est installé par défaut et ne peut pas être désélectionné. Il correspond à Security Framework dans le programme d'installation.

Cliquez sur **Suivant**.

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

Une fenêtre de statut s'affiche. Ceci peut prendre plusieurs minutes.

Sélectionnez **Oui, je souhaite redémarrer mon ordinateur maintenant**, puis cliquez sur **Terminer**.

Lorsque l'ordinateur redémarre, authentifiez-vous dans Windows.

L'installation d'Encryption Personal + 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 à l'aide de la ligne de commande

Installez le droit sur l'ordinateur cible, si nécessaire.

Commutateurs :

Pour une installation avec 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 |
|-------------|---|
| -y -gm2 | Envoi des données à l'auto-extracteur |
| /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

ENTITLEMENT=clé de droit d'Encryption Personal



: Ce paramètre peut uniquement être utilisé avec Encryption Personal

Exemple d'installation par ligne de commande

Bien que le redémarrage soit supprimé dans ces exemples, il peut être nécessaire de redémarrer l'ordinateur. Le cryptage 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 d'Client Encryption (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:
{47de1ae3-40dc-47f4-8112-86149d9d642d}:qTT0VPKdMzihsKCQddXTD3cAtX5PRCyLTa5ZOHkSPpl= /! *v c:\Shieldinstall.log /qn /
norestart"
```

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

```
DDSSetup.exe -y -gm2 /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 -y -gm2 /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 + 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](#).

Installation d'Encryption Personal individuellement à l'aide de programmes d'installation enfant

Pour installer Encryption Personal à l'aide de programmes d'installation enfant, 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.

Installation par ligne de commande

Les commutateurs et les paramètres de ligne de commande sont sensibles à la casse.

Veillez à inclure une valeur contenant un ou plusieurs caractères spéciaux, tels qu'un espace dans la ligne de commande, entre des guillemets d'échappement.

Utilisez ces programmes d'installation pour installer les clients à l'aide d'une installation avec script, de fichiers séquentiels ou de toute autre technologie Push disponible dans votre entreprise.

Le redémarrage a été supprimé dans les exemples de ligne de commande. Cependant, un redémarrage éventuel est requis. Le cryptage ne pourra commencer que lorsque l'ordinateur aura redémarré.

Fichiers journaux : Windows crée des fichiers journaux d'installation uniques pour l'utilisateur connecté à %Temp%, accessibles dans **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 .msi standard peut être utilisée pour créer un fichier journal en utilisant **/! *v C:\<any directory>\<any log file name>.log**.

Tous les programmes d'installation enfants utilisent les mêmes options d'affichage et commutateurs .msi de base, sauf lorsque cela est précisé, pour les installations 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 le fichier .exe |
| /s | Mode Silencieux |
| /i | Mode d'installation |

| Option | Signification |
|--------|--|
| /q | Boîte de dialogue Aucune progression, se réinitialise après la fin du processus |
| /qb | Boîte de dialogue de progression contenant le bouton Annuler invite à redémarrer |
| /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 |

Installer les pilotes

Les pilotes et micrologiciel de Dell ControlVault, les lecteurs d'empreintes digitales et les cartes à puce ne sont **pas** inclus au programme d'installation principal ou aux fichiers exécutables de programme d'installation enfant. Les pilotes et le micrologiciel doivent être conservés à jour et peuvent être téléchargés à partir de <http://www.dell.com/support> en sélectionnant votre modèle d'ordinateur. Téléchargez les pilotes et le logiciel appropriés en fonction de votre matériel d'authentification.

Dell ControlVault
 NEXT Biometrics Fingerprint Driver
 Pilote Validity FingerPrint Reader 495
 Pilote de carte à puce O2Micro

Si vous installez du matériel autre que Dell, téléchargez les pilotes et le logiciel mis à jour depuis le site internet du fournisseur.
 Puis :

Installez les clients Advanced Authentication

Les utilisateurs se connectent par l'intermédiaire de l'authentification avant démarrage au moyen de leur mot de passe Windows. Localisez le fichier dans **C:\extracted\Encryption Management Agent** et **C:\extracted\Advanced Authentication\<x64/x86>**.

Exemple d'installation par ligne de commande

\Encryption Management Agent

L'exemple suivant correspond à l'installation de Security Framework (installation silencieuse, pas de redémarrage et est installé dans l'emplacement par défaut suivant : **C:\Program Files\Dell\Dell Data Protection**).

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



:
 Ce client est nécessaire à l'authentification avancée dans la version 8.x.



Puis :

\Advanced Authentication\x64

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

```
setup.exe /s /v"/norestart /qn"
```

Puis :

Installer le client Encryption

Passez en revue les exigences du [Client Encryption](#) si votre organisation utilise un certificat signé par une autorité racine telle qu'EnTrust or Verisign. Une modification de paramètre de registre est nécessaire sur l'ordinateur client pour activer la validation du certificat.

Localisez le fichier sur **C:\extracted\Encryption**.

Exemple d'installation par ligne de commande

L'exemple suivant correspond à l'installation d'Encryption Personal, Encrypt for Sharing, avec masquage des icônes de recouvrement, aucune boîte de dialogue, aucune barre de progression et sans redémarrage.

```
DDPE_XXbit_setup.exe /s /v"HIDEOVERLAYICONS=1 REBOOT=ReallySuppress /qn"
```

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

L'installation d'Encryption Personal + Advanced Authentication est terminée. L'Assistant de configuration d'Encryption Personal et la configuration sont traités séparément.

Passez aux [Assistants de configuration d'Advanced Authentication et d'Encryption Personal](#).



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 cryptage (EAP). Cliquez sur **Suivant**.
- 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 de configuration d'Encryption Personal à partir de l'icône Dell Data Security dans la barre d'état système (il peut se lancer automatiquement).
Cet Assistant Configuration facilite l'utilisation du cryptage pour protéger les informations qui figurent sur l'ordinateur. Si cet Assistant n'est pas terminé, le cryptage ne peut pas commencer.

Lisez l'écran d'accueil, puis cliquez sur **Suivant**.

- 7 Sélectionnez un modèle de règles. Le modèle de règles établit les paramètres de règles par défaut du cryptage.
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 cryptage (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**.
- 10 Cliquez sur **Parcourir** pour choisir un lecteur réseau ou un périphérique amovible pour sauvegarder vos clés de cryptage (qui sont encapsulées dans l'application LSAReccovery_[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 cryptage. Si le disque réseau ou le périphérique amovible est disponible, la sauvegarde des clés de cryptage est effectuée en arrière-plan. Toutefois, si l'emplacement n'est pas disponible (ex. : le périphérique amovible original n'est pas inséré), les modifications de règles ne prennent effet qu'après la sauvegarde manuelle des clés.

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

Cliquez sur **Suivant**.

- 11 La liste des paramètres de cryptage s'affiche sur l'écran Confirmer les paramètres de cryptage. Vérifiez les éléments, et si les paramètres sont corrects, cliquez sur **Confirmer**.
La configuration de l'ordinateur démarre. Une barre de statut 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 cryptage. 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 cryptage. Le cryptage s'effectue en arrière-plan. La Console de gestion locale peut être ouverte ou fermée. Le cryptage des fichiers n'en sera pas affecté. Vous pouvez continuer à utiliser votre système lors du cryptage.
- 15 Lorsque le balayage est terminé, 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 disque.



Configurer les paramètres de Dell Encryption Management Agent

Les paramètres par défaut d'Advanced Authentication permettent aux administrateurs et aux utilisateurs d'utiliser Advanced Authentication immédiatement après l'activation, sans aucune configuration supplémentaire. Les utilisateurs sont ajoutés automatiquement comme utilisateurs Advanced Authentication 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'Advanced Authentication, 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 de l'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 administrateur, si vous souhaitez 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 cryptage.

Configuration de l'outil de cryptage (Encryption) et de l'authentification avant démarrage (Preboot Authentication)

Le cryptage et l'authentification avant démarrage (Preboot Authentication, PBA) sont disponibles si votre ordinateur est équipé d'un lecteur à auto-cryptage (SED). Les deux fonctions sont configurées via l'onglet Cryptage visible uniquement si l'ordinateur est doté d'un lecteur à autocryptage (SED). Lorsque vous activez l'une ou l'autre des fonctions de cryptage ou de PBA, l'autre fonction est également activée.



Avant l'activation du cryptage et PBA, Dell recommande de vous enregistrer et d'activer les questions de récupération afin de pouvoir récupérer le mot de passe si vous l'avez perdu. Pour en savoir plus, voir [Configurer les Options de connexion](#).

Configuration du cryptage et de l'authentification PBA (Preboot Authentication) :

- 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.

REMARQUE : Si, lors de l'activation du cryptage, 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 cryptage peut continuer.

- 3 Cliquez sur l'onglet **Cryptage**, puis sur **Crypter**.
- 4 Dans la page d'accueil, cliquez sur **Suivant**.
- 5 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 | MCW7 |
| 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 cryptage | Sélectionnez pour l'activer. |
| Entrez le mot de passe de suppression de cryptage | Un mot ou un code de 100 caractères maximum, servant de mécanisme de sécurité en cas de défaillance. Si vous entrez ce mot ou code dans le champ du nom d'utilisateur ou du mot de passe pendant l'authentification PBA, vous supprimez les jetons d'authentification de tous les utilisateurs et vous verrouillez le SED. Ensuite, seul l'administrateur peut forcer le déverrouillage du périphérique. N'entrez rien dans ce champ si vous ne voulez pas disposer d'un mot de passe d'effacement cryptographique en cas d'urgence. |

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

| | |
|---------------------------------|---|
| Texte du titre de pré démarrage | 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 | Ce texte s'affiche sur la page des informations de support de PBA. Dell recommande de personnaliser ce message afin d'y inclure les instructions à suivre pour contacter votre service d'assistance ou administrateur de sécurité. Si ce champ n'est pas renseigné, aucune information concernant les coordonnées du service d'assistance ne s'affichera. 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 bénéficiera pas de renvoi à la ligne automatique et aucune barre de défilement ne sera proposée. Le texte sera donc tronqué. |
| 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 bénéficiera pas de renvoi à la ligne automatique et aucune barre de défilement ne sera proposée. Le texte sera donc tronqué.

- 7 Dans la page récapitulative, cliquez sur **Appliquer**.
- 8 Lorsque vous y êtes invité, cliquez sur **Arrêter**.
Un arrêt complet est requis pour que le cryptage soit lancé.
- 9 Après l'arrêt, redémarrez l'ordinateur.
L'authentification est maintenant gérée par Security Tools. Les utilisateurs doivent se connecter dans l'écran d'authentification avant démarrage (PBA) avec leurs mots de passe Windows.

Modifier les paramètres de cryptage et d'authentification avant démarrage

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

Modifier la politique ou la personnalisation avant démarrage - Cliquez sur l'onglet **Cryptage**, puis cliquez sur **Modifier**.

Décrypter le lecteur à autocryptage, par exemple, pour la désinstallation : cliquez sur **Décrypter**.

Après l'activation du cryptage 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 démarrage** et sélectionnez **Personnalisation du prédémarrage** ou **Règles de connexion avant démarrage**.

Définition des options d'authentification

Les commandes dans l'onglet Authentification des paramètres de l'administrateur vous permettent de définir les options d'ouverture de session de l'utilisateur et de personnaliser les paramètres de chacune.

Configuration des options de connexion

Dans la page des options de connexion, vous pouvez définir des stratégies de connexion. Par défaut, toutes les données d'identification sont répertoriées dans les options disponibles.


Pour configurer les options de connexion :

Dans le volet gauche, sous Authentification, sélectionnez **Options de connexion**.

Pour choisir le rôle à configurer, sélectionnez le rôle dans la liste **Appliquer les options de connexion à : Utilisateurs** ou **Administrateurs**. Toutes les modifications que vous effectuez sur cette page ne s'appliqueront qu'au rôle que vous sélectionnez.

Définir les options disponibles pour l'authentification.

Par défaut, chaque méthode d'authentification est configurée pour être utilisée individuellement, pas en combinaison avec d'autres méthodes d'authentification. Vous pouvez modifier les méthodes par défaut des manières suivantes :

Pour définir une combinaison d'options d'authentification, sous Options disponibles, cliquez sur  pour sélectionner la première méthode d'authentification. Dans la boîte de dialogue Options disponibles, sélectionnez la seconde méthode d'authentification, puis cliquez sur **OK**.

Vous pouvez, par exemple, demander une empreinte digitale et un mot de passe comme identifiants de connexion. Dans la boîte de dialogue, sélectionnez le deuxième mode d'authentification à utiliser avec l'authentification par empreinte digitale.

Pour permettre l'utilisation individuelle de chaque méthode d'authentification, dans la boîte de dialogue Options disponibles, laissez la deuxième méthode d'authentification définie sur **Aucune**, puis cliquez sur **OK**.



Pour supprimer une option de connexion, sous Options disponibles dans la page Options de connexion, cliquez sur **X** pour supprimer la méthode.

Pour ajouter une nouvelle combinaison de modes d'authentification, cliquez sur **Ajouter une option**.

Définissez les options de récupération des utilisateurs pour leur permettre d'accéder de nouveau à leur ordinateur.

Pour permettre aux utilisateurs de définir un ensemble de questions et réponses à utiliser pour pouvoir accéder à nouveau à leur ordinateur, sélectionnez **Questions de récupération**.

Pour empêcher l'utilisation de questions de récupération, désélectionnez l'option.

Pour définir la durée de la période pendant laquelle les utilisateurs peuvent enregistrer leurs identifiants d'authentification, sélectionnez **Période de grâce**.

La fonction Période de grâce vous permet de définir la date à laquelle une option d'ouverture de session configurée commencera à entrer en vigueur. Vous pouvez configurer une option d'ouverture de session avant la date à laquelle elle entrera en vigueur et définir une durée permettant aux utilisateurs de s'enregistrer. Par défaut, la règle entre immédiatement en vigueur.

Pour modifier la date d'Entrée en vigueur de l'option d'ouverture de session *Immédiatement*, dans la boîte de dialogue Période de grâce, cliquez sur le menu déroulant et sélectionnez **Date spécifiée**. Cliquez sur la flèche vers le bas sur la partie droite du champ Date pour afficher un calendrier, puis sélectionnez une date dans le calendrier. La règle entre en vigueur à 12 h 01 environ, à la date sélectionnée.

Les utilisateurs peuvent être informés d'enregistrer leurs identifiants requis lors de leur prochaine connexion Windows (par défaut), ou vous pouvez définir des notifications à intervalles réguliers. Sélectionnez l'intervalle de rappel dans la liste déroulante *Rappel à l'utilisateur*.



La notification qui s'affiche est légèrement différente selon l'endroit où l'utilisateur se trouve dans l'écran de connexion Windows ou dans une session Windows lorsque la notification est déclenchée. Les notifications n'apparaissent pas sur les écrans de connexion Authentification avant démarrage.

Fonctionnalité pendant la période de grâce

Durant une période de grâce spécifiée, après chaque connexion, la notification Identifiants supplémentaire s'affiche lorsque l'utilisateur n'a pas encore enregistré les identifiants requis pour satisfaire une option d'ouverture de session modifiée. Le message est : *Des identifiants supplémentaires sont disponibles à l'enregistrement*.

Lorsque des identifiants supplémentaires sont disponibles mais non exigés, le message ne s'affiche qu'une fois après la modification de la règle.

Selon le contexte, un clic sur la notification entraîne ce qui suit :

Si aucun identifiant n'a été enregistré, l'Assistant Configuration s'affiche, permettant aux utilisateurs administratifs de configurer les paramètres associés à l'ordinateur et d'offrir aux utilisateurs la possibilité d'enregistrer les identifiants les plus communs.

Après l'enregistrement initial des identifiants, il suffit de cliquer sur la notification pour afficher l'Assistant de configuration dans la console Dell Data Security Console.

Fonctionnalité après l'expiration de la période de grâce

Dans tous les cas, une fois la période de grâce expirée, les utilisateurs ne peuvent pas se connecter sans avoir enregistré les identifiants requis par l'option d'ouverture de session. Si un utilisateur tente de se connecter à l'aide d'un identifiant ou d'une combinaison d'identifiants ne correspondant pas à l'option Ouverture de session, l'Assistant Configuration s'affiche en haut de l'écran de connexion Windows.

Si l'utilisateur enregistre les identifiants requis, il peut se connecter à Windows.

Si l'utilisateur ne réussit pas à enregistrer les identifiants requis ou s'il annule l'assistant, il est ramené à l'écran de connexion Windows.

Pour enregistrer les paramètres du rôle sélectionné, cliquez sur **Appliquer**.

Configuration des questions de récupération

Dans la page Questions de récupération, vous pouvez sélectionner les questions à présenter aux utilisateurs lorsqu'ils définissent des questions et des réponses personnelles de récupération. Les questions de récupération permettent aux utilisateurs d'accéder de nouveau à leur ordinateur lorsqu'ils ont perdu ou oublié leur mot de passe.

Pour définir des questions de récupération :

Dans le volet gauche, sous Authentification, sélectionnez **Questions de récupération**.

Dans la page Questions de récupération, sélectionnez au moins trois questions de récupération prédéfinies.

Vous pouvez éventuellement ajouter entre une et trois questions personnalisées à la liste de sélection destinée à l'utilisateur.

Pour enregistrer les questions de récupération, cliquez sur **Appliquer**.

Configuration de l'authentification par lecture d'empreinte digitale

Pour configurer l'authentification par lecture d'empreinte digitale :

Dans le volet gauche, sous Authentification, sélectionnez **Empreintes digitales**.

Dans Inscriptions, définissez le nombre minimum et le nombre maximum de doigts qu'un utilisateur peut inscrire.

Définissez la sensibilité de numérisation de l'empreinte digitale.

Une sensibilité inférieure augmente l'écart acceptable et la probabilité d'accepter une numérisation erronée. À la sensibilité la plus élevée, il est possible que le système rejette des empreintes authentiques. Le réglage de sensibilité Plus réduit le taux d'acceptation erronée à 1 sur 10 000 numérisations.

Pour supprimer toutes les numérisations d'empreintes digitales et inscriptions d'identifiants dans le tampon du lecteur, cliquez sur **Purger le lecteur**. Cette opération supprime uniquement les données que vous ajoutez. Elle ne supprime pas les lectures et les enregistrements stockés dans les sessions antérieures.

Pour enregistrer les paramètres, cliquez sur **Appliquer**.

Configuration de l'enregistrement d'une carte à puce

Dell Advanced Authentication prend en charge deux types de cartes à puce : avec contact et sans contact.

Les cartes à contact nécessitent un lecteur de carte dans lequel la carte est insérée. Ces cartes sont compatibles uniquement avec les ordinateurs de domaine. Les cartes CAC et SIPRNet sont des cartes à contact. Du fait de la nature de ces cartes, l'utilisateur doit choisir un certificat après avoir inséré sa carte pour se connecter.

Les cartes sans contact sont prises en charge par des ordinateurs extérieurs au domaine et par les ordinateurs configurés avec les spécifications du domaine.

Les utilisateurs peuvent enregistrer une carte à puce à contact par compte ou plusieurs cartes à puce sans contact par compte.

Les cartes à puce ne sont pas prises en charge avec l'authentification de prédémarrage.



Lorsque vous supprimez l'enregistrement d'une carte à puce d'un compte avec plusieurs cartes enregistrées, toutes les cartes sont désenregistrées simultanément.

Pour configurer l'enregistrement de carte à puce :

Dans l'onglet Authentification de l'outil Paramètres de l'administrateur, sélectionnez **Carte à puce**.



Configuration des droits avancés

Cliquez sur **Avancé** pour modifier les options utilisateur final avancées. Sous *Avancé*, vous avez l'option d'autoriser les utilisateurs à enregistrer eux-mêmes des informations d'identification, à modifier leurs informations d'identification enregistrées et à activer la connexion en une étape.

Cochez ou décochez les cases suivantes :

Autoriser les utilisateurs à enregistrer des identifiants : cette case est cochée par défaut. Les utilisateurs sont autorisés à enregistrer des identifiants sans intervention par un administrateur. Si vous décochez la case, les identifiants doivent être enregistrés par l'administrateur.

Autoriser les utilisateurs à modifier des identifiants inscrits : cette case est cochée par défaut. Lorsqu'elle est cochée, les utilisateurs sont autorisés à modifier ou à supprimer leurs identifiants enregistrés sans intervention d'un administrateur. Si vous décochez cette case, les identifiants ne peuvent pas être modifiés ou supprimés par un utilisateur ordinaire, mais doivent l'être par l'administrateur.



: Pour inscrire les identifiants d'un utilisateur, rendez-vous sur la page *Utilisateurs* de l'outil Paramètres administrateur, sélectionnez un utilisateur et cliquez sur Enregistrer.

Autoriser la connexion en une étape : la connexion en une étape correspond à l'authentification unique (SSO – Single Sign-on). Par défaut, cette case est cochée. Dans ce cas, les utilisateurs doivent entrer leurs données d'identification uniquement dans l'écran d'authentification au démarrage. Les utilisateurs sont connectés automatiquement à Windows. Si vous désélectionnez cette case, l'utilisateur devra peut-être se connecter plusieurs fois.



: Cette option ne peut être sélectionnée que si le paramètre Autoriser les utilisateurs à enregistrer les données d'identification est sélectionné.

Cliquez sur **Appliquer** lorsque vous avez terminé.

Gestion de l'authentification des utilisateurs

Les commandes de l'onglet Authentification de Paramètres de l'administrateur vous permettent de définir les options de connexion de l'utilisateur et de personnaliser les paramètres de chacune.

Pour gérer l'authentification utilisateur :

- 1 en tant qu'administrateur, cliquez sur la mosaïque **Paramètres administrateur**.
- 2 cliquez sur l'onglet **Utilisateurs** pour gérer les utilisateurs et afficher leur statut d'enregistrement. Dans cet onglet, vous pouvez :
 - Enregistrer de nouveaux utilisateurs
 - Ajouter ou modifier des identifiants
 - Supprimer les identifiants d'un utilisateur



REMARQUE :

Ouverture de session et **Session** indiquent l'état de l'inscription d'un utilisateur.

Si l'un de ces statuts est **Non**, l'utilisateur doit terminer les enregistrements supplémentaires. Pour déterminer les enregistrements encore nécessaires, sélectionnez l'outil **Paramètres administrateur** et ouvrez l'onglet **Utilisateurs**. Les cases à cocher en gris représentent des enregistrements incomplets. Vous pouvez aussi cliquer sur la mosaïque **Enregistrements** et consulter la colonne **Règle** de l'onglet **Statut**, où les enregistrements requis sont répertoriés.

La mosaïque **Enregistrements** ne s'affichera que si la fonctionnalité PBA est active.

Ajouter de nouveaux utilisateurs



Les nouveaux utilisateurs Windows sont ajoutés automatiquement lorsqu'ils se connectent à Windows ou enregistrent leurs identifiants d'enregistrement.

Cliquez sur **Ajouter un utilisateur** pour commencer le processus d'enregistrement pour un utilisateur Windows existant.

Lorsque la boîte de dialogue *Sélectionner un utilisateur* s'affiche, sélectionnez **Types d'objets**.

Entrez le nom d'objet d'un utilisateur dans la zone de texte et cliquez sur **Vérifier les noms**.

Cliquez sur **OK** lorsque vous avez terminé.

L'Assistant Enregistrement s'ouvre.

Accédez à [Inscrire ou modifier les références de l'utilisateur](#) pour obtenir des instructions.

Inscrire ou modifier les références de l'utilisateur

L'administrateur peut enregistrer ou modifier les identifiants d'un utilisateur à sa place, mais quelques activités d'enregistrement nécessitent la présence de l'utilisateur, par exemple pour répondre aux questions de récupération et pour numériser les empreintes digitales de l'utilisateur.

Pour enregistrer ou modifier les identifiants de l'utilisateur :

Dans Paramètres de l'administrateur, cliquez sur l'onglet **Utilisateurs**.

Dans la page Utilisateurs, cliquez sur **Inscrire**.

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

Dans la boîte de dialogue Authentification requise, connectez-vous à l'aide du mot de passe Windows de l'utilisateur, puis cliquez sur **OK**.

Dans la page Mot de passe, pour modifier le mot de passe Windows de l'utilisateur, entrez et confirmez un nouveau mot de passe, puis cliquez sur **Suivant**.

Si vous ne souhaitez pas modifier le mot de passe, cliquez sur **Ignorer**. L'Assistant vous permet d'ignorer un identifiant si vous ne voulez pas l'inscrire. Pour retourner à une page, cliquez sur **Retour**.

Suivez les instructions de chaque page, puis cliquez sur le bouton approprié : **Suivant**, **Ignorer** ou **Retour**.

Dans la page Résumé, confirmez les identifiants enregistrés, puis, une fois l'enregistrement terminé, cliquez sur **Appliquer**.

Pour revenir à la page d'enregistrement des identifiants afin d'apporter une modification, cliquez sur **Précédent** jusqu'à ce que vous parveniez à la page à modifier.


Pour des informations plus détaillées sur l'inscription d'un identifiant, ou pour modifier un identifiant, voir le *Dell Data Security Console User Guide* (Guide d'utilisation de la console Dell Data Security).

Suppression d'un identifiant enregistré

Cliquez sur la mosaïque **Paramètres d'administrateur**.

Cliquez sur l'onglet **Utilisateurs** et recherchez l'utilisateur à modifier.

Survolez la coche verte de l'identifiant que vous voulez supprimer. Elle devient .

Cliquez sur le symbole  puis cliquez sur **Oui** pour confirmer la suppression.





: Un identifiant ne peut être supprimé de cette manière s'il s'agit du seul identifiant enregistré de l'utilisateur. En outre, le mot de passe ne peut pas être supprimé avec cette méthode. Utilisez la commande Supprimer pour supprimer complètement l'accès d'un utilisateur à l'ordinateur.

Supprimer tous les identifiants enregistrés d'un utilisateur

Cliquez sur la mosaïque **Paramètres d'administrateur**.

Cliquez sur l'onglet **Utilisateurs** et recherchez l'utilisateur à supprimer.

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.

Désinstaller à l'aide du programme d'installation principal

- Chaque composant doit être désinstallé séparément avant la désinstallation du programme d'installation principal. Les clients doivent être désinstallés 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.](#)
- 3 [Désinstallez Advanced Authentication.](#)

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 à partir de Ajout/Suppression de programmes

Accédez à Désinstaller un programme dans le Panneau de configuration de Windows (**Démarrer** > **Panneau de configuration** > **Programmes et fonctionnalités** > **Désinstaller un programme**).

Sélectionnez le **programme d'installation Dell** et cliquez avec le bouton gauche de la souris sur **Modifier** pour lancer l'Assistant de configuration.

Lisez l'écran d'accueil, puis cliquez sur **Suivant**.

Suivez les invites pour désinstaller puis cliquez sur **Terminer**.

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.

```
"DDSetup.exe" -y -gm2 /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](#).

Désinstaller à l'aide des programme d'installation enfants

- 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.

Désinstaller le client 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 décryptage. Si vous ne souhaitez pas décrypter les fichiers à la désinstallation, il n'est pas nécessaire de créer un fichier journal Encryption Removal Agent.
- Exécutez WSScan pour vous assurer que toutes les données sont décryptées 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 décryptage de données est encore en cours si le service Encryption Removal Agent existe encore dans le volet Services.

Choisir une méthode de désinstallation

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

[Désinstaller à l'aide de l'interface utilisateur](#)

[Désinstaller à partir de la ligne de commande](#)

Désinstaller à l'aide de l'interface utilisateur

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).

Sélectionnez **Dell Encryption XX-bit** et cliquez avec le bouton gauche sur **Modifier** pour lancer l'Assistant de configuration d'Encryption Personal.

Lisez l'écran d'accueil, puis cliquez sur **Suivant**.

Lorsque la fenêtre d'installation d'Encryption Removal Agent s'ouvre, choisissez l'une des options :



: La deuxième option est activée par défaut. Si vous voulez décrypter des fichiers, veuillez à modifier la sélection selon l'option une.

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

Pour le cryptage SDE, Utilisateur ou Commun, cette option décrypte les fichiers et désinstalle le client Encryption. **Il 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**.

Dans la zone de texte *Fichier de sauvegarde*, entrez 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.

Entrez votre Mot de passe d'Administrateur de cryptage dans la zone de texte Mot de passe. Il s'agit du mot de passe que vous avez défini dans l'Assistant Configuration lorsque vous avez installé le logiciel.

Cliquez sur **Suivant**.

L'écran *Connexion au Dell Decryption Agent Service en tant que* contient deux options. Sélectionnez **Compte du système local**.

Cliquez sur **Terminer**.

Cliquez sur **Supprimer** à l'écran Supprimer le programme.

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

Redémarrez votre ordinateur, puis connectez-vous à Windows.

Décryptage en cours.

Le décryptage peut prendre plusieurs heures en fonction du nombre d'unités à décrypter et du volume de données sur les unités. Pour vérifier le processus de décryptage, 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 **/I C:\<tout répertoire>\<tout nom de fichier journal>.log**. Dell recommande de ne pas utiliser la consignation détaillée « /I*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 |
| /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 bouton Annuler : redémarre automatiquement à la fin du processus |
| /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 : silencieuse 0 : pas silencieuse |
| 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 décryptage peut prendre plusieurs heures en fonction du nombre d'unités à décrypter et du volume de données sur les unités. Pour vérifier le processus de décryptage, voir [Vérifier l'état de l'agent Encryption Removal](#).



Désinstaller Advanced Authentication

Choisir une méthode de désinstallation

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

[Désinstaller à l'aide de l'interface utilisateur](#)

[Désinstaller à partir de la ligne de commande](#)

Désinstaller à l'aide de l'interface utilisateur

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).

Sélectionnez **Dell Advanced Authentication** et cliquez avec le bouton gauche de la souris sur **Modifier** pour lancer l'Assistant de configuration.

Lisez l'écran d'accueil, puis cliquez sur **Suivant**.

Entrez le mot de passe administrateur.

Suivez les invites pour désinstaller puis cliquez sur **Terminer**.

Redémarrez votre ordinateur, puis entrez vos identifiants pour accéder à Windows.

Advanced Authentication est désinstallé.

Désinstaller à partir de la ligne de commande

Après son extraction du programme d'installation principal, le programme d'installation du client Advanced Authentication est disponible sur `C:\extracted\Advanced Authentication\<x64/x86>\setup.exe`.

L'exemple suivant correspond à la désinstallation silencieuse du client Advanced Authentication.

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

Après avoir terminé, éteignez et redémarrez l'ordinateur.

Accédez à [Stratégies et descriptions de modèle](#).

Désinstallation d'Encryption Management/Agent

Choisir une méthode de désinstallation

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

[Désinstaller à l'aide de l'interface utilisateur](#)

[Désinstaller à partir de la ligne de commande](#)

Désinstaller à l'aide de l'interface utilisateur

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).

Sélectionnez **Dell Encryption Management Agent** et cliquez avec le bouton gauche sur **Modifier** pour lancer l'Assistant de configuration.

Lisez l'écran d'accueil, puis cliquez sur **Suivant**.

Suivez les invites pour désinstaller puis cliquez sur **Terminer**.

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 du client Encryption Management/Agent est disponible sur **C:\extracted\Encryption Management Agent\EMAgent_XXbit_setup.exe**.

L'exemple suivant correspond à la désinstallation silencieuse du client SED.

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

Après avoir terminé, éteignez et redémarrez l'ordinateur.



Désinstallation à l'aide du programme de désinstallation de Dell Data Security

Désinstaller

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

Ce programme de désinstallation de Data Security est disponible à l'emplacement suivant : **C:\Program Files (x86)\Dell\Dell Data Protection**

Pour plus d'informations ou pour utiliser l'interface de ligne de commande (CLI), voir <http://www.dell.com/support/article/us/en/19/sln307791>.

Les journaux sont générés dans **C:\ProgramData\Dell\Dell Data Protection** pour tous les composants supprimés.

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

Cliquez sur **Suivant**.

Si vous le souhaitez, désélectionnez n'importe quelle application de la suppression, puis sélectionnez **Suivant**.

 **REMARQUE : Les dépendances requises seront automatiquement cochées ou décochées.**

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.

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 | <p>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.</p> <p>Vrai = toutes les données non cryptées par d'autres règles Intelligent Encryption seront cryptées par les règles de cryptage SDE.</p> <p>Toute modification apportée à cette règle nécessite un redémarrage.</p> |
| Algorithme de cryptage SDE | AES256 | | | | | | | | | AES 256, AES 128, 3DES |
| Règles de cryptage SDE | | | | | | | | | | <p>Règles de cryptage à utiliser pour crypter/ne pas crypter certains disques, répertoires et dossiers.</p> <p>Contactez Dell ProSupport si vous ne savez pas comment changer les valeurs par défaut.</p> |

Règles relatives aux paramètres généraux



| 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 |
|--------------------------|--|----------------------------|--|------------------------------|--|---|--|---|--------------------|--|
| Cryptage activé | Vrai | | | | | | | Faux | | <p>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.</p> <p>Une valeur Vrai signifie que toutes les règles de cryptage sont activées.</p> <p>Une modification de la valeur de cette règle lance une nouvelle analyse de cryptage / décryptage.</p> |
| Dossiers communs cryptés | | | | | | | | | | <p>Chaîne de caractères : 100 entrées maximum de 500 caractères chacune (2 048 caractères maximum)</p> <p>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.</p> <p>Les lettres génériques sont les suivantes :</p> <p># : fait référence à tous les lecteurs</p> <p>f# : fait référence à tous les lecteurs fixes</p> <p>r# : fait référence à tous les lecteurs amovibles</p> <p>Important : passer outre la protection des répertoires peut empêcher le démarrage de votre ordinateur et/ou nécessiter le reformatage de vos disques/lecteurs.</p> <p>Si le même dossier est concerné par cette règle et la règle Dossiers cryptés de l'utilisateur, c'est cette règle qui prévaut.</p> |

| 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 |
|---|---|----------------------------|--|------------------------------|--|---|--|---|--------------------|---|
| Algorithme de cryptage commun | AES256 | | | | | | | | | <p>AES 256, Rijndael 256, AES 128, Rijndael 128, 3DES</p> <p>Les fichiers de pagination système sont cryptés grâce à l'algorithme AES 128 bits.</p> |
| Liste des données cryptées de l'application (ADE) | <p>winword.exe</p> <p>excel.exe</p> <p>powerpnt.exe</p> <p>msaccess.exe</p> <p>winproj.exe</p> <p>outlook.exe</p> <p>acrobat.exe</p> <p>visio.exe</p> <p>mspub.exe</p> <p>notepad.exe</p> <p>wordpad.exe</p> <p>winzip.exe</p> <p>winrar.exe</p> <p>onenote.exe</p> <p>onenotem.exe</p> | | | | | | | | | <p>Chaîne de caractères : 100 entrées maximum de 500 caractères chacune</p> <p>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.</p> <p>Liste des noms de processus des applications (sans chemin d'accès) dont les nouveaux fichiers doivent être cryptés. Séparés par retour chariot. N'utilisez pas de caractère de remplacement.</p> <p>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.</p> <p>Noms de processus courants :</p> <p>outlook.exe, winword.exe, frontpg.exe, powerpnt.exe, msaccess.exe, wordpad.exe, mspaint.exe, excel.exe</p> <p>Ces noms de processus système et de programmes d'installation codés en dur sont</p> |



| 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 |
|---|--|----------------------------|--|------------------------------|--|---|--|---|--------------------|--|
| | | | | | | | | | | <p>ignorés si vous les spécifiez dans cette règle :</p> <p>hotfix.exe, update.exe, setup.exe, msixec.exe, wuauclt.exe, wmiprvse.exe, migrate.exe, unregmp2.exe, ikernel.exe, wssetup.exe, svchost.exe</p> |
| Clé de cryptage des données applicatives | Courant | | | | | | | | | <p>Courant ou utilisateur</p> <p>Choisissez une clé pour indiquer qui devrait avoir accès aux fichiers cryptés par la liste des données cryptées de l'application et où.</p> <p>Courant, si vous voulez que ces fichiers soient accessibles à tous les utilisateurs gérés sur le point final de création (même niveau d'accès que les dossiers communs cryptés), et cryptés à l'aide de l'algorithme de cryptage Courant.</p> <p>Utilisateur, si vous voulez que ces fichiers soient accessibles uniquement à l'utilisateur qui les a créés, sur le point final de création (même niveau d'accès que les dossiers cryptés de l'utilisateur), et cryptés à l'aide de l'algorithme de cryptage de l'utilisateur.</p> <p>Toute modification apportée à cette règle n'affecte pas les fichiers déjà cryptés.</p> |
| Crypter les dossiers personnels d'Outlook | Vrai | | | | | | | Faux | | Vrai crypte les dossiers personnels d'Outlook. |
| Crypter les fichiers temporaires | Vrai | | | | | | | Faux | | Vrai = cryptage des chemins compris dans les variables d'environnement TEMP et TMP à l'aide de la clé de cryptage 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 |
|---|--|----------------------------|--|------------------------------|--|---|--|---|--------------------|---|
| Crypter les fichiers temporaires Internet | Vrai | Faux | | | | | | | | <p>Vrai = cryptage du chemin compris dans la variable d'environnement CSIDL_INTERNET_CACHE à l'aide de la clé de cryptage des données utilisateur.</p> <p>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.</p> <p>Cette règle ne s'applique qu'à Microsoft Internet Explorer.</p> |
| Crypter les documents de profil utilisateur | Vrai | | | | | | | | Faux | <p>Vrai = cryptage :</p> <ul style="list-style-type: none"> Le profil utilisateur (C:\Users\jsmith) avec la clé de cryptage des données utilisateur \Users\Public avec la clé de cryptage commun |
| Crypter le fichier de pagination Windows | Vrai | | | | | | | | Faux | <p>Vrai crypte le fichier de pagination Windows. Une modification apportée à cette règle nécessite un redémarrage.</p> |
| Services gérés | | | | | | | | | | <p>Chaîne de caractères : 100 entrées maximum de 500 caractères chacune (2 048 caractères maximum)</p> <p>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.</p> <p>La syntaxe est un nom de service par ligne. Vous pouvez</p> |



| 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 |
|--|--|----------------------------|--|------------------------------|--|---|--|---|-----------------------|---|
| | | | | | | | | | | 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 | <p>Écrasement impossible, Écrasement à un passage, Écrasement à trois passages, Écrasement à sept passages</p> <p>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 :</p> <ul style="list-style-type: none"> · 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 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. |
| Sécuriser le fichier d'hibernation Windows | Vrai | | | | Faux | | Vrai | Faux | | Si cette règle est activée, le fichier d'hibernation sera crypté uniquement quand l'ordinateur entre en veille |

| 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 |
|---|--|----------------------------|--|------------------------------|--|---|--|---|--------------------|--|
| | | | | | | | | | | 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 crypter 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) Une liste des dossiers du disque dur du point de terminaison à crypter avec la clé de cryptage des données utilisateur, ou exclus du cryptage. Cette règle s'applique à tous les disques que Windows classe dans la catégorie disques durs. Vous ne pouvez pas utiliser cette règle pour crypter des lecteurs ou des supports externes dont le type affiche Disque amovible. Utilisez Crypter le support externe EMS. |
| Algorithme de cryptage de l'utilisateur | AES256 | | | | | | | | | AES 256, Rijndael 256, AES 128, Rijndael 128, 3DES Algorithme de cryptage des données au niveau de l'utilisateur individuel. Des valeurs différentes selon |



| 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 |
|---|--|----------------------------|--|------------------------------|--|---|--|---|--------------------|---|
| | | | | | | | | | | l'utilisateur sont possibles sur un point final. |
| Clé de cryptage des données utilisateur | Utilisateur | Courant | | Utilisateur | Courant | | | | Utilisateur | <p>Courant ou utilisateur</p> <p>Choisissez une clé pour indiquer qui devrait avoir accès aux fichiers cryptés par les règles suivantes, et où :</p> <ul style="list-style-type: none"> • 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 • Crypter les documents de profil utilisateur <p>Sélectionnez :</p> <ul style="list-style-type: none"> • Courant, si vous voulez que ces fichiers/dossiers cryptés utilisateur soient accessibles à tous les utilisateurs gérés sur le point final de création (même niveau d'accès que les dossiers communs cryptés), et cryptés à l'aide de l'algorithme de cryptage Courant. • Utilisateur, si vous voulez que ces fichiers soient accessibles uniquement par l'utilisateur qui les a créés, uniquement sur le point final où ils ont été créés (même niveau d'accès que les dossiers cryptés utilisateur), et cryptés à l'aide de l'algorithme de cryptage utilisateur. <p>Si vous choisissez d'intégrer une règle de cryptage pour crypter l'ensemble des partitions de disque, il est recommandé d'utiliser la règle</p> |

| 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 supports 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 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) | | | | | | | | | | |
| Accélérateur de cryptage matériel (HCA) | Faux | | | | | | | | | <p>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.</p> <p>Les règles HCA fonctionnent uniquement sur les ordinateurs équipés d'un accélérateur de cryptage matériel (HCA).</p> |
| Volumes choisis pour cryptage | Tous les volumes fixes | | | | | | | | | <p>Tous les volumes fixes ou uniquement le volume système</p> <p>Définissez le ou les volumes cible du cryptage.</p> |
| Métadonnées d'analyse détaillée disponibles sur le lecteur avec cryptage HCA | Faux | | | | | | | | | <p>Vrai ou faux</p> <p>Vrai : les métadonnées d'analyse approfondie sont comprises sur le lecteur afin de faciliter l'analyse. Métadonnées comprises :</p> <ul style="list-style-type: none"> ID (MCID) de l'ordinateur actuel ID de périphérique (DCID/SCID) de l'installation du Client Encryption en cours <p>Faux : les métadonnées d'analyse approfondie ne sont pas incluses sur le lecteur.</p> <p>Passer de Faux à Vrai engendre une nouvelle analyse, basée sur les règles HCA pour ajouter les métadonnées d'analyse.</p> |



| 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 | | | | | | | | | <p>Activer ou désactiver toutes les règles du système de contrôle de port.</p> <p>Désactiver = aucune règle du système de contrôle de port ne s'applique, indépendamment des autres règles en la matière.</p> <p>Remarque : les règles PCS nécessitent un redémarrage avant d'entrer en vigueur.</p> |
| 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. |
| 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 | 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. |

| 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 supports 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 |
|---|--|----------------------------|--|------------------------------|---|---|--|---|--------------------|---|
| des lecteurs externes | | | | | | | | | | <p>Cette règle comporte des interactions avec PCS. Voir Encryption External Media et interactions PCS.</p> <p>Accès total : aucune restriction en lecture/écriture des données n'est appliquée au port du lecteur externe</p> <p>Lecture seule : permet la lecture. La fonction d'écriture est désactivée</p> <p>Bloqué : le port est bloqué en lecture/écriture</p> <p>Cette règle est basée sur le point final et ne peut pas être remplacée par la règle utilisateur.</p> <p>Activer, désactiver ou contourner l'accès aux ports de périphériques de transfert de mémoire (MTD).</p> |
| Port : périphérique de transfert de mémoire (MTD) | Activé | | | | | | | | | <p>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.</p> |
| Catégorie : stockage | Activé | | | | | | | | | |
| Sous-catégorie de stockage : contrôle des lecteurs optiques | Lecture seule | UDF uniquement | | | | Accès illimité | | UDF uniquement | Accès illimité | <p>ENFANT de catégorie : stockage. Classe : le stockage doit être défini sur Activer pour permettre l'utilisation de cette règle.</p> <p>Accès total : aucune restriction de lecture/écriture de données sur le port de lecteur optique</p> <p>UDF uniquement : bloque toutes les écritures de données qui ne sont pas au format UDF (gravure de CD/DVD, gravure ISO). La fonction</p> |



| 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 |
|--|--|----------------------------|--|------------------------------|--|---|--|---|--------------------|---|
| | | | | | | | | | | <p>de lecture des données est activée.</p> <p>Lecture seule : permet la lecture. La fonction d'écriture est désactivée</p> <p>Bloqué : le port est bloqué en lecture/écriture</p> <p>Cette règle est basée sur le point final et ne peut pas être remplacée par la règle utilisateur.</p> <p>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 données informatiques sur une vaste gamme de supports.</p> <p>Cette règle comporte des interactions avec PCS. Voir Encryption External Media et interactions PCS.</p> |
| Sous-catégorie de stockage : contrôle des lecteurs de disquettes | Bloqué | Lecture seule | | | | Accès illimité | | Lecture seule | Accès illimité | <p>ENFANT de catégorie : stockage. Classe : le stockage doit être défini sur Activé pour permettre l'utilisation de cette règle.</p> <p>Accès total : aucune restriction de lecture/écriture de données n'est appliquée au port du lecteur de disquettes</p> <p>Lecture seule : permet la lecture. La fonction d'écriture est désactivée</p> <p>Bloqué : le port est bloqué en lecture/écriture</p> <p>Cette règle est basée sur le point final et ne peut pas être remplacée par la règle utilisateur.</p> |
| Classe : périphérique portable | | Activé | | | | | | | | <p>PARENT de la règle suivante. Définissez cette règle sur Activé pour utiliser la sous-</p> |

| 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 |
|---|--|----------------------------|--|------------------------------|--|---|--|---|--------------------|---|
| Windows (WPD) | | | | | | | | | | 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. |
| Sous-catégorie périphérique portable Windows (WPD) : stockage | Activé | | | | | | | | | <p>Contrôle l'accès à tous les périphériques portables Windows.</p> <p>ENFANT de catégorie : périphérique portable Windows (WPD)</p> <p>Classe : périphérique portable Windows (WPD) doit être défini sur Activé pour utiliser cette règle.</p> <p>Accès total : aucune restriction d'accès aux données en lecture/écriture n'est appliquée au port.</p> <p>Lecture seule : permet la lecture. La fonction d'écriture est désactivée.</p> <p>Bloqué : le port est bloqué en lecture/écriture.</p> |
| Classe : Human Interface Device (HID) | Activé | | | | | | | | | <p>Contrôle l'accès à tous les périphériques d'interface utilisateur (claviers, souris).</p> <p>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.</p> |
| Catégorie : autre | Activé | | | | | | | | | Contrôle l'accès à tous les disques/lecteurs non couverts par d'autres catégories. |



| 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 aux périphériques de stockage amovibles | | | | | | | | | | |
| Cryptage EMS des supports externes | Vrai | | | | | Faux | | Vrai | Faux | <p>Cette règle est la « règle principale » pour toutes les règles relatives aux périphériques de stockage amovibles. Une valeur Faux signifie l'absence de cryptage des périphériques de stockage amovibles, indépendamment des autres valeurs des règles.</p> <p>Une valeur Vrai signifie que toutes les règles de cryptage des périphériques de stockage amovibles sont activées.</p> <p>Cette règle comporte des interactions avec PCS. Voir Encryption External Media et interactions PCS.</p> |
| EMS ne prend pas en charge le cryptage de CD/DVD | Faux | | | | | | | | Vrai | <p>La valeur Faux active le cryptage des lecteurs de CD/DVD.</p> <p>Cette règle comporte des interactions avec PCS. Voir Encryption External Media et interactions PCS.</p> |
| Accès EMS aux supports non protégés | Bloquer | | Lecture seule | | | Accès illimité | | Lecture seule | Accès illimité | <p>Bloquer, Lecture seule, Accès illimité</p> <p>Cette règle comporte des interactions avec PCS. Voir Encryption External Media et interactions PCS.</p> <p>Lorsque le statut de cette stratégie est Accès bloqué, vous n'avez pas accès au périphérique amovible, si celui-ci n'est pas crypté.</p> <p>Les valeurs Lecture seule ou Accès illimité vous permettent de choisir les périphériques de stockage amovibles que vous voulez crypter.</p> <p>Si vous décidez de ne pas crypter le périphérique de stockage amovible et que la valeur sélectionnée est Accès</p> |

| 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 |
|-----------------------------------|--|----------------------------|--|------------------------------|--|---|--|---|--------------------|--|
| | | | | | | | | | | illimité, vous disposez de tous les droits d'écriture et de lecture pour le périphérique de stockage amovible. |
| | | | | | | | | | | Si vous décidez de ne pas crypter 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 crypté, mais le client empêche la modification ou l'ajout de fichiers sur le périphérique de stockage amovible, sauf s'il est crypté. |
| Algorithme de cryptage EMS | AES256 | | | | | | | | | AES 256, Rijndael 256, AES 128, Rijndael 128, 3DES |
| Analyse EMS des supports externes | Vrai | Faux | | | | | | | | La valeur Vrai permet l'analyse par Encryption External Media des périphériques de stockage amovibles à chaque insertion de ceux-ci. |
| | | | | | | | | | | Lorsque cette règle est définie sur Faux et que la règle Cryptage EMS des supports externes est définie sur Vrai, Encryption External Media ne crypte que les nouveaux fichiers ou ceux qui ont été modifiés. |
| | | | | | | | | | | À chaque insertion, une analyse a lieu afin de permettre à Encryption External Media de repérer les fichiers ajoutés au périphérique amovible sans authentification. Vous pouvez ajouter des fichiers aux périphériques de stockage amovibles si vous refusez l'authentification, mais vous ne pouvez pas accéder aux données cryptées. Les fichiers ajoutés ne seront pas cryptés. Toutefois, lors de la prochaine authentification du support amovible afin de pouvoir accéder aux données |



| 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 |
|--|--|----------------------------|--|------------------------------|--|---|--|---|--------------------|--|
| | | | | | | | | | | cryptées, Encryption External Media procédera à l'analyse puis au cryptage de tout fichier ajouté non crypté. |
| 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 | | | | | | | | | | <p>Cette règle permet de spécifier les périphériques de support externes à exclure d'Encryption External Media. Les périphériques de support externes qui ne sont pas sur cette liste seront protégés. Maximum de 150 périphériques avec un maximum de 500 caractères par ID de périphérique PNP. Jusqu'à 2 048 caractères autorisés.</p> <p>Pour rechercher l'ID de périphérique PNP d'un périphérique de stockage amovible :</p> <ol style="list-style-type: none"> 1 insérez le périphérique de stockage amovible dans un ordinateur crypté. 2 Ouvrez le fichier EMSService.log dans C:\Programdata\Dell\Dell Data Protection\Encryption\EMS. 3 Recherchez "PNPDeviceID=" <p>Par exemple : 14.03.18 18:50:06.834 [I] [Volume "F:\"] PnPDeviceID = USBSTOR \DISK&VEN_SEAGATE&PROD_USB&REV_0409\2HC015KJ&0</p> <p>Définissez les éléments suivants dans la règle Liste</p> |

| 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 |
|---|--|----------------------------|--|------------------------------|--|---|--|---|--------------------|---|
| | | | | | | | | | | <p>blanche des périphériques EMS :</p> <p>VEN=fournisseur (ex : USBSTOR \DISK&VEN_SEAGATE)</p> <p>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</p> <p>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</p> <p>Numéro de série (ex : \2HC015KJ&0) ; exclut seulement ce périphérique ; les valeurs VEN, PROD et REV doit précéder cette valeur</p> <p>Séparateurs autorisés : onglets, virgules, points-virgules, caractère hexadécimal 0x1E (caractère de séparation d'enregistrement)</p> |
| 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. |




| 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 |
|--|--|----------------------------|--|------------------------------|--|---|--|---|--------------------|---|
| 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 caractères numériques | Vrai | Faux | | | | | | | | Avec la valeur Vrai, le mot de passe doit contenir au moins un chiffre. |
| 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 | | | 10 | 30 | 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 |

| 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 |
|--|--|----------------------------|--|------------------------------|--|---|--|---|--------------------|--|
| | | | | | | | | | | <p>entre les lignes sont comptabilisés. Toutes les règles dépassant la limite des 2 048 caractères sont ignorées.</p> <p>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.</p> |
| Accès bloqué d'EMS aux supports non protégés | Vrai | | | | | | | | Faux | <p>Bloquez l'accès aux périphériques de stockage amovibles de moins de 17 Mo n'ayant donc pas la capacité de stockage suffisante pour héberger un Encryption External Media (disquette de 1,44 Mo, par exemple).</p> <p>Si la valeur choisie à la fois pour Crypter le média externe et cette règle est Vrai, l'accès est bloqué. Si la règle Crypter le support externe EMS a la valeur Vrai et que cette règle a la valeur Faux, les données peuvent être lues depuis le périphérique de stockage amovible non cryptable, mais l'écriture sur le support est bloquée.</p> <p>Si la valeur est Faux, cette règle n'a aucun effet et l'accès au périphérique de stockage amovible non cryptable n'est pas impacté.</p> |

Règles du contrôle d'expérience 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 supports 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 |
|---|--|----------------------------|--|------------------------------|---|---|--|---|--------------------|---|
| 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 | 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 sera 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 la barre d'état système qui lui permet de suspendre/relancer le cryptage/décryptage (selon l'opération exécutée par le Client Encryption). |
| <div>  REMARQUE : Autoriser un utilisateur à suspendre le cryptage peut lui permettre d'empêcher le Client Encryption de crypter ou décrypter les données en fonction de la règle. </div> | | | | | | | | | | |
| 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 cryptage ou décryptage de données pendant que l'utilisateur travaille activement. Le client traitera les données |

| 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 |
|-----------|--|----------------------------|--|------------------------------|--|---|--|---|--------------------|--|
| | | | | | | | | | | uniquement lorsque l'écran sera verrouillé. |
| | | | | | | | | | | Utilisateur facultatif ajoute une option dans l'icône de la barre d'état système 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 cryptage ou de décryptage. |

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 cryptage de toutes les données sur les périphériques amovibles et l'impossibilité d'utiliser des périphériques non cryptés ;
- 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 crypter les périphériques 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 crypter les périphériques 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 crypter les périphériques 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 ;
- Invitation à crypter les périphériques 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 cryptage des périphériques de stockage 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 cryptage des périphériques de stockage amovibles.

Protection de base pour les supports externes

Ce modèle de règles comprend :

- la protection des périphériques de stockage 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.



Extraire les programmes d'installation enfants du programme d'installation principal

- 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 /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](#).

Dépannage

Mise à niveau de la mise à jour vers Windows 10 Creators

Les ordinateurs installés avec Encryption doivent utiliser un package de mise à niveau vers Windows 10 spécialement configuré pour effectuer la mise à niveau de la mise à jour vers Windows 10 Creators. La version configurée du package de mise à niveau garantit que Dell Encryption peut gérer l'accès à vos fichiers cryptés pour les protéger contre tout préjudice au cours du processus de mise à niveau.

Pour effectuer la mise à niveau de la mise à jour vers Windows 10 Creators, suivez les instructions figurant dans l'article suivant :

<http://www.dell.com/support/article/us/en/19/SLN298382>

Dépannage du client Encryption et

Mise à niveau vers Windows 10 Creators Update

Pour effectuer la mise à niveau vers la version Windows 10 Fall Creators Update, suivez les instructions figurant dans l'article suivant :

<http://www.dell.com/support/article/us/en/19/SLN298382>.

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 de consignation 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 : consigne les erreurs qui bloquent 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 Encryption External Media aux supports non protégés interagit avec la règle Système de contrôle des ports - Classe de stockage : contrôle des lecteurs externes. Si vous avez l'intention de définir la règle d'accès Encryption External Media aux supports non protégés sur *Accès complet*, vérifiez que la règle Classe de stockage : contrôle des lecteurs externes 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 le client Encryption, d'afficher l'état de chiffrement et d'identifier les fichiers non cryptés qui devraient être décryptés.
- Des privilèges d'administrateur sont requis pour exécuter cet utilitaire.

Exécutez l'

- À partir du support d'installation Dell, copiez le fichier WSScan.exe sur l'ordinateur à analyser.
- Lancez une ligne de commande à l'emplacement spécifié ci-dessus et entrez **wsscan.exe** à l'invite de commande. WSScan démarre.
- Cliquez sur **Avancé**.
- Sélectionnez le type du lecteur à rechercher dans le menu déroulant : *Tous les lecteurs, Lecteurs fixes, Lecteurs amovibles, ou CD-ROM/ DVDROM*.
- Sélectionnez le Type de rapport de chiffrement dans le menu déroulant : *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 du client 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.
- Cliquez sur **Rechercher**.

OU

- Cliquez sur **Avancé** pour basculer la vue vers **Simple** afin d'analyser un dossier particulier.
- 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 la liste déroulante 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 de cryptage SDE. Utilisateur : clé de chiffrement de l'utilisateur. Commun : clé de cryptage commune. 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 |



| Sortie | Signification |
|--------|---------------|
| | RIJNDAEL 256 |
| | AES 128 |
| | AES 256 |
| | 3DES |

Vérification de l'état d'Encryption Removal Agent.

Le statut de l'agent Encryption Removal s'affiche dans la zone de description du volet 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** - Le client Encryption est toujours installé, toujours configuré ou les deux. Le déchiffrement ne démarrera pas tant que le client Encryption ne sera pas désinstallé.
- **Balayage initial** - Le service procède à un premier balayage en calculant le nombre de fichiers cryptés et les octets. L'analyse initiale n'a lieu qu'une seule fois.
- **Balayage de décryptage** - Le service décrypte les fichiers et demande peut-être à décrypter des fichiers verrouillés.
- **Décrypter 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 décryptage.
- **Terminé** : l'analyse de déchiffrement est terminée. Le service, le fichier exécutable, le pilote et l'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, nous vous déconseillons 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 micrologiciel Dell ControlVault

Les pilotes et le micrologiciel 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 micrologiciel) Dell ControlVault peuvent être mis à jour une fois l'installation du client terminée.

Télécharger les derniers pilotes

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



Installation du pilote Dell ControlVault

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

Double-cliquez sur le pilote Dell ControlVault pour lancer le fichier exécutable à extraction automatique.



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.

Cliquez sur **Continuer** pour commencer.

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

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

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

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**.

Double-cliquez sur **CVHCI64.MSI** pour lancer le programme d'installation du pilote. [**CVHCI64.MSI** dans cet exemple, (CVHCI pour un ordinateur 32 bits)].

Cliquez sur **Suivant** sur l'écran d'accueil.

Cliquez sur **Suivant** pour installer les pilotes dans l'emplacement par défaut de C:\Program Files\Broadcom Corporation\Broadcom USH Host Components\.

Sélectionnez l'option **Terminer**, puis cliquez sur **Suivant**.

Cliquez sur **Installer** pour démarrer l'installation des pilotes.

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 micrologiciel Dell ControlVault

- 1 Accédez au dossier dans lequel vous avez téléchargé le fichier d'installation du micrologiciel.
- 2 Double-cliquez sur le micrologiciel 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 de 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 **micrologiciel**.
- 8 Double-cliquez sur **ushupgrade.exe** pour lancer le programme d'installation du micrologiciel.
- 9 Cliquez sur **Démarrer** pour commencer la mise à niveau du micrologiciel.



Vous devrez peut-être saisir le mot de passe admin lors d'une mise à niveau à partir d'une version antérieure du micrologiciel. 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 micrologiciel.

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

Paramètres de registre

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

Client Encryption

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

Avant de lancer la désinstallation, vous pouvez créer éventuellement un fichier journal pour 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 au cours de la désinstallation, il n'est pas nécessaire de créer ce fichier journal.

Le fichier de consignation 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: consigne les erreurs qui bloquent 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

Utiliser des cartes à puce avec connexion Windows

Pour utiliser des cartes à puce avec Windows Authentication, vous devez définir la valeur de registre suivante sur l'ordinateur client :

[HKLM\SOFTWARE\DigitalPersona\Policies\Default\SmartCards]

"MSSmartcardSupport"=DWORD:1

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 cryptage initial et se produit avant le balayage de cryptage 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 cryptage initial.



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

Le client de chiffrement affiche l'invite *longueur de chaque report de mise à jour de règle* 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 cryptage ou le reporter pour empêcher le traitement du cryptage 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 cryptage est reporté pendant le nombre définissable de reports autorisés. Le traitement de cryptage 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) :

$(\text{NOMBRE DE REPORTS DE MISE A JOUR DE REGLE AUTORISES}) \times (\text{LONGUEUR DE CHAQUE REPORT DE REGLE}) + (5 \text{ MINUTES} \times [\text{NOMBRE DE REPORTS DE MISE A JOUR DE REGLES AUTORISE} - 1])$.

Modifier l'option Utilisation par défaut de la clé SDUser

Le cryptage des données système (SDE) est appliqué en fonction de la valeur des Règles de cryptage SDE. Les répertoires supplémentaires sont protégés par défaut lorsque la règle « Cryptage SDE activé » est sélectionnée. Pour plus d'informations, rechercher « Règles de cryptage SDE » dans AdminHelp. Lorsque le client Encryption est en train de traiter une mise à jour de règle qui contient une règle SDE active, le répertoire du profil utilisateur actuel est crypté 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 déplacés) 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 n'est présente ou est définie sur toute autre option que 0, la clé SDUser sera utilisée pour crypter ces répertoires utilisateurs.

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, Advanced 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 pourra pas lire les cartes à puce. Si ce service est désactivé, tout service qui en dépend explicitement ne pourra pas démarrer.

SCPolicySvc : permet de configurer le système de sorte à verrouiller le bureau de l'utilisateur sur retrait d'une carte à puce.

WbioSrv : 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 utiliser des cartes à puce avec Windows Authentication, vous devez définir la valeur de registre suivante sur l'ordinateur client :

[HKLM\SOFTWARE\DigitalPersona\Policies\Default\SmartCards]

"MSSmartcardSupport"=DWORD:1

Accédez au [Glossaire](#).



Glossaire

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

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 vous sera demandé si vous devez exécuter le programme LSARecovery_[hostname].exe en vue de récupérer vos 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, le client Encryption utilise la clé 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).
Cryptage commun : la clé « Commun » rend les fichiers accessibles à tous les utilisateurs gérés sur leur périphérique de création. La clé « Utilisateur » rend les fichiers accessibles uniquement à l'utilisateur qui les a créés, uniquement sur le périphérique où ils ont été créés. La clé « Utilisateur itinérant » rend les fichiers accessibles uniquement à l'utilisateur qui les a créés sur le périphérique Windows (ou Mac) crypté Dell.

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

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 cryptage commun et utilisateur sont destinées aux données utilisateur sensibles, car elles exigent l'utilisation d'un mot de passe pour déverrouiller les clés de cryptage. 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 du cryptage 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.

