Dell Endpoint Security Suite Enterprise

Advanced Installation Guide v3.9

January 2024
Rev. A01

DELL Technologies

Remarques, précautions et avertissements

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

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

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

Contents

Chapter 1: Introduction 6
Avant de commencer 6
Utilisation de ce Guide 6
Contactez Dell ProSupport for Software 7

Chapter 2: Configuration requise 8
Tous les clients 8
Chiffrement 9
Chiffrement complet du disque 11
Encryption sur système d'exploitation serveur 13
Advanced Threat Prevention 16
Compatibilité 18
Pare-feu client et protection Web 20
SED Manager 21
BitLocker Manager 25

Chapter 3: Paramètres de registre 27
Chiffrement 27
Chiffrement complet du disque 31
Advanced Threat Prevention 33
SED Manager 34
BitLocker Manager 36

Chapter 4: Installation à l'aide du programme d'installation principal 37
Installation interactive à l'aide du programme d'installation principal 37
Installation par la ligne de commande à l'aide du programme d'installation principal 38

Chapter 5: Désinstaller le programme d'installation principal 41
Désinstallation du programme d'installation principal d'Endpoint Security Suite Enterprise 41

Chapter 6: Installation à l'aide des programmes d'installation enfants 42
Installer les pilotes 43
Installation d'Encryption 43
Installer le chiffrement complet du disque 47
Installer Encryption sur un système d'exploitation de serveur 48
Installation interactive 49
Installation à l'aide de la ligne de commande 50
Activer 52
Installer le client Advanced Threat Prevention 54
Installation des clients du pare-feu client et de la protection Web 55
Installation de SED Manager et PBA Advanced Authentication 57
Installer BitLocker Manager 58

Chapter 7: Désinstaller à l'aide des programme d'installation enfants 60

Désinstallation de Web Protection et Firewall....61
Désinstallation d'Advanced Threat Prevention....61
Installez le chiffrement complet du disque....61
Désinstallation de SED Manager....62
Désinstaller Encryption et Encryption sur système d'exploitation de serveur....63
Désinstaller BitLocker Manager....66

Chapter 8: Programme de désinstallation de Data Security....67

Chapter 9: Scénarios couramment utilisés....68
Client Encryption et Advanced Threat Prevention....69
SED Manager et Encryption External Media....70
BitLocker Manager et Encryption External Media....70
BitLocker Manager et Advanced Threat Prevention....71

Chapter 10: Provision a Tenant....72
Provisionner un service partagé....72

Chapter 11: Configuration de la mise à jour automatique de l'agent Advanced Threat Prevention....73

Chapter 12: Configuration préalable à l'installation pour SED UEFI, et BitLocker Manager....74
Initialiser le module TPM....74
Configuration de la pré-Installation avant démarrage sur les ordinateurs UEFI....74
Configuration préalable à l'installation d'une partition d'authentification avant démarrage BitLocker....75

Chapter 13: Définir le Dell Server par le biais du registre....76

Chapter 14: Extraire les programmes d'installation enfant....77

Chapter 15: Configurer Key Server....78
Écran des services - Ajouter un utilisateur du compte de domaine....78
Fichier de configuration de Key Server - Ajouter un utilisateur pour la communication avec le Security Management Server....78
Écran des services - Redémarrage du service Key Server....79
Console de gestion - Ajouter un administrateur d'analyse approfondie....80

Chapter 16: Utiliser l'utilitaire Administrative Download (CMGAd)....81
Utilisation du mode Analyse approfondie....81
Utilisation du mode Admin....81

Chapter 17: Configuration d'Encryption sur un système d'exploitation de serveur....83

Chapter 18: Configuration de l'activation différée....86
Personnalisation de l'activation différée....86
Préparation de l'ordinateur pour l'installation....86
Installer Encryption avec activation différée....87
Activer Encryption avec activation différée....87

Résolution des problèmes d'activation différée....88

Chapter 19: Dépannage....90
Tous les clients - Dépannage.... 90
Tous les clients - État de la protection....90
Dépannage de Dell Encryption (client et serveur) 90
Dépannage d'Advanced Threat Prevention....98
Dépannage SED....101
Pilotes Dell ControlVault....103
Mettre à jour les pilotes et le firmware Dell ControlVault....103
UEFI Computers....106
TPM et BitLocker....106

Chapter 20: Glossaire.... 136

1

Introduction

Ce guide présente l'installation et la configuration d'Advanced Threat Prevention, de d'Encryption, de la gestion SED, du chiffrement complet de disque, de la protection Web, du pare-feu client et de BitLocker Manager.

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

Avant de commencer

1. Installez le Dell Server avant de déployer les clients. Localisez le guide qui convient tel qu'illustré ci-dessous, suivez les instructions puis revenez à ce guide.
   - *Security Management Server Installation and Migration Guide (Guide d'installation et de migration de Security Management Server)*
   - *Security Management Server Virtual Quick Start Guide and Installation Guide (Guide de démarrage rapide et Guide d'installation de Security Management Server Virtual)*
   - Vérifiez que les stratégies sont définies comme vous le souhaitez. Naviguez dans AdminHelp, disponible à partir du « **?** » en haut à droite de l'écran. AdminHelp est une aide au niveau de la page, conçue pour vous aider à configurer et à modifier une règle et à comprendre les options disponibles avec votre Dell Server.
2. Configuration d'un locataire pour Advanced Threat Prevention Un locataire doit être provisionné dans Dell Server pour que l'application des stratégies Advanced Threat Prevention devienne active.
3. Lisez attentivement le chapitre Configuration requise de ce document.
4. Déployez les clients sur les utilisateurs.

Utilisation de ce Guide

Utilisez le présent guide dans l'ordre suivant :

- Voir Configuration requise pour connaître les prérequis du client, des informations sur le matériel et le logiciel de l'ordinateur, les limites et les modifications spéciales du registre nécessaires aux fonctions.
- Si nécessaire, voir la section Configuration avant installation pour SED UEFI et BitLocker.
- Si vos clients doivent être autorisés à utiliser Dell Digital Delivery, reportez-vous à Définir GPO sur un contrôleur de domaine pour activer les droits.
- Si vous souhaitez installer les clients à l'aide du programme d'installation principal d'Endpoint Security Suite Enterprise , reportez-vous à :
  - Installation interactive à l'aide du programme d'installation principal

    ou
  - Installation par la ligne de commande à l'aide du programme d'installation principal
- Si vous installez des clients à l'aide des programmes d'installation enfants, vous devez extraire les fichiers exécutables des programmes d'installation enfants du programme d'installation principal. Reportez-vous à Extraire les programmes d'installation enfants du programme d'installation principal, puis revenez ici.
  - Installer des programmes d'installation enfants par ligne de commande :
    - Installation d'Encryption : ces instructions permettent d'installer Encryption, un composant qui applique les règles de sécurité, qu'un ordinateur soit connecté au réseau, déconnecté du réseau, perdu ou volé.
    - Installation du client de chiffrement complet du disque : ces instructions permettent d'installer le chiffrement complet du disque, un composant qui applique les règles de sécurité, qu'un ordinateur soit connecté au réseau, déconnecté du réseau, perdu ou volé.
    - Installation d'Advanced Threat Prevention : ces instructions permettent d'installer Advanced Threat Prevention, une protection antivirus de nouvelle génération qui utilise la science des algorithmes et l'apprentissage machine pour identifier, classifier et prévenir les cybermenaces connues ou inconnues et les empêcher de s'exécuter ou d'endommager les points de terminaison.

- Installation de Web Protection et Firewall ces instructions permettent d'installer les fonctionnalités *facultatives* : protection Web et pare-feu. Client Firewall est un pare-feu avec état qui permet de vérifier tout le trafic entrant et sortant par rapport à sa liste de règles. La protection du navigateur Web et des téléchargements pour identifier des menaces et exécuter un ensemble d'actions par règle lorsqu'une menace est détectée, en fonction des évaluations des sites Web.
- Installation de SED Manager : utilisez ces instructions pour installer un logiciel de chiffrement pour les SED. Les disques à auto-cryptage assurent leur propre cryptage, mais ils ont besoin d'une plate-forme pour gérer le cryptage et les règles. Avec SED Manager, toutes les règles, le stockage et la récupération des clés de cryptage sont disponibles à partir d'une même console, ce qui réduit le risque de manque de protection des ordinateurs en cas de perte d'accès ou d'accès non autorisé.
- Installation de BitLocker Manager : ces instructions permettent d'installer BitLocker Manager, conçu pour renforcer la sécurité des déploiements BitLocker et pour simplifier et réduire le coût de possession.

  REMARQUE :

  La plupart des programmes d'installation enfants peuvent être installés de façon interactive, mais ils ne sont pas décrits dans ce guide. Cependant, les programmes d'installation enfants Advanced Threat Prevention et le chiffrement complet du disque ne peuvent être installés que via la ligne de commande.

- Reportez-vous à Scénarios couramment utilisés pour consulter les scripts de nos scénarios les plus couramment utilisés.

Contactez Dell ProSupport for Software

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

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

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

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

2

Configuration requise

Tous les clients

Ces exigences s'appliquent à tous les clients. Les exigences répertoriées dans d'autres sections s'appliquent à des clients particuliers.

- Les meilleures pratiques IT doivent être suivies pendant le déploiement. Ceci inclut, sans s'y limiter, les environnements de test contrôlés pour les premiers tests et les déploiements échelonnés pour les utilisateurs.
- Le compte d'utilisateur servant à l'installation/la mise à niveau/la désinstallation doit correspondre à un administrateur local ou de domaine, qui peut être affecté temporairement par un outil de déploiement tel que Microsoft SCCM. Les utilisateurs non-administrateurs et disposant de privilèges particuliers ne sont pas pris en charge.
- Sauvegardez toutes les données importantes avant de démarrer l'installation ou la désinstallation.
- Lors de l'installation, n'apportez aucune modification à l'ordinateur, notamment, n'insérez ou ne retirez pas de lecteurs externes (USB).
- Les administrateurs doivent s'assurer que tous les ports nécessaires sont disponibles.
- Consultez régulièrement le site dell.com/support pour obtenir la documentation la plus récente et des conseils techniques.
- La ligne de produits Dell Data Security ne prend pas en charge les versions de Windows Insider Preview.

Conditions préalables

- Microsoft .Net Framework 4.5.2 (ou version ultérieure) est nécessaire pour les clients des programmes d'installation principal et enfant Endpoint Security Suite Enterprise . Le programme d'installation *n'installe pas* les composants Microsoft .Net Framework.
- Pour vérifier la version de Microsoft .Net installée, suivez ces instructions sur l'ordinateur ciblé pour l'installation. Reportez-vous à ces instructions pour installer Microsoft .Net Framework 4.5.2.
- Si vous choisissez d'installer Encryption en mode FIPS, Microsoft .Net Framework 4.6 est requis.

Matériel

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

Matériel
○ Processeur Intel Pentium ou AMD ○ 500 Mo d'espace disque disponible ○ 2 Go de RAM **REMARQUE :** De l'espace disque libre supplémentaire est nécessaire pour chiffrer les fichiers sur le point de terminaison. La taille varie en fonction des règles activées et de la capacité de disque.

Localisation

- Dell Encryption, SED Manager, PBA Advanced Authentication, Advanced Threat Prevention et BitLocker Manager sont compatibles avec l'interface utilisateur multilingue et sont localisés dans les langues suivantes. Les données Advanced Threat Prevention présentées sur la console de gestion sont disponibles en anglais uniquement.

Langues prises en charge		
EN : anglais	IT : italien	KO : coréen

Langues prises en charge		
ES : espagnol	DE : allemand	PT-BR : portugais brésilien
FR : français	JA : japonais	PT-PT : portugais du Portugal (ibère)

Chiffrement

- L'ordinateur client doit posséder une connectivité réseau pour être activé.
- Pour réduire la durée du chiffrement initial, lancez l'Assistant Nettoyage de disque Windows qui supprimera les fichiers temporaires et toute autre donnée inutile.
- La prise en charge de Windows Hello for Business nécessite Endpoint Security Suite Enterprise v3.0 ou une version ultérieure exécutée sur Windows 10.
- La prise en charge de Windows Hello for Business nécessite une activation sur un serveur Dell exécutant la version 11.0 ou une version ultérieure.
- Désactivez le mode Veille lors du balayage de chiffrement initial pour prévenir la mise en veille d'un ordinateur lors des périodes d'inactivité. Le chiffrement ne peut pas être exécuté sur un ordinateur en veille (le déchiffrement non plus).
- Encryption ne prend pas en charge les configurations à double amorçage, car il est possible de chiffrer les fichiers système de l'autre système d'exploitation, ce qui perturberait son fonctionnement.
- Dell Encryption ne peut pas être mis à niveau vers v2.7 à partir de versions antérieures à v1.6.0. Les points de terminaison exécutant des versions antérieures à la version v1.6.0 doivent être mis à niveau vers v1.6.0 , puis vers v2.7.
- Encryption prend désormais en charge le mode Audit. Le mode Audit permet aux administrateurs de déployer Encryption dans le cadre de l'image d'entreprise, plutôt que d'utiliser un SCCM tiers ou une solution similaire. Pour obtenir des instructions relatives à l'installation d'Encryption dans une image d'entreprise, reportez-vous à l'article de la base de connaissances 129990.
- Le client Encryption est testé avec plusieurs antivirus basés sur des signatures populaires et des solutions antivirus pilotées par l'intelligence artificielle dont McAfee Virus Scan Enterprise, McAfee Endpoint Security, Symantec Endpoint Protection, CylancePROTECT, CrowdStrike Falcon, Carbon Black Defense, etc. avec lesquels il est compatible. Les exclusions codées en dur sont incluses par défaut pour de nombreux fournisseurs d'antivirus afin d'éviter les incompatibilités entre l'analyse antivirus et le chiffrement.

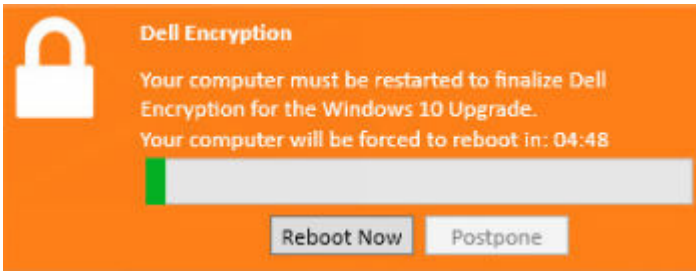
  Si votre organisation utilise un fournisseur d'antivirus non répertorié ou si des problèmes de compatibilité sont observés, reportez-vous à l'article de la base de connaissances 126046 ou contactez Dell ProSupport pour obtenir de l'aide pour la validation de la configuration afin d'assurer l'interopérabilité entre vos solutions logicielles et les solutions Dell Data Security.
- Dell Encryption utilise les jeux d'instructions de chiffrement d'Intel IPP (Integrated Performance Primitives). Pour plus d'informations, reportez-vous à l'article de la base de connaissances 126015.
- Le module TPM (Trusted Platform Module) est utilisé pour sceller la clé GPK. Par conséquent, si vous exécutez Encryption, supprimez le module TPM du BIOS avant d'installer un nouveau système d'exploitation sur l'ordinateur cible.
- La réinstallation du système d'exploitation sur place 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.
- Le programme d'installation principal installe ces composants s'ils ne sont pas déjà présents sur l'ordinateur cible. **Lors de l'utilisation du programme d'installation enfants**, vous devez installer ces composants avant d'installer les clients.

  Conditions préalables

  - Visual C++ 2012 Redistributable Package (x86 ou x64) Mise à jour 4 ou ultérieure
  - Visual C++ 2017 Redistributable Package (x86 ou x64) ou ultérieur
  - Depuis janvier 2020, les certificats de signature SHA1 ne sont plus valides et ne peuvent pas être renouvelés. Vous devez installer les mises à jour https://support.microsoft.com/help/4474419 et https://support.microsoft.com/help/4490628 de la Base de connaissances Microsoft sur les appareils exécutant Windows Server 2008 R2 pour valider les certificats de signature SHA256 dans les applications et les modules d'installation.

    Sans ces mises à jour installées, les applications et modules d'installation signés avec des certificats SHA1 fonctionnent, mais une erreur s'affiche sur le point de terminaison lors de l'installation ou de l'exécution des applications.
- Les règles *Fichier de mise en veille prolongée Windows sécurisé* et *Empêcher la mise en veille prolongée non sécurisée* ne sont pas prises en charge en mode UEFI.

- L'activation différée permet au compte d'utilisateur Active Directory utilisé lors de l'activation d'être indépendant du compte utilisé pour se connecter au point de terminaison. Au lieu que le fournisseur de réseau capture les informations d'authentification, l'utilisateur spécifie manuellement le compte basé sur Active Directory lorsqu'il y est invité. Une fois que les informations d'identification ont été saisies, les informations d'authentification sont envoyées de manière sécurisée au Dell Server qui les valide par rapport aux domaines Active Directory configurés. Pour plus d'informations, reportez-vous à l'article de la base de connaissances 124736.
- Suite à la mise à niveau des fonctionnalités de Windows 10, un redémarrage est **nécessaire** pour finaliser Dell Encryption. Le message suivant s'affiche dans la zone de notification après la mise à niveau des fonctionnalités de Windows 10 :



Matériel

- Le tableau suivant répertorie en détail le matériel compatible.

Matériel intégré en option
○ TPM 1.2 ou 2.0

Systèmes d'exploitation

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

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

Encryption External Media

Systèmes d'exploitation

- Le support externe doit disposer d'environ 55 Mo, ainsi que d'un espace libre sur le support égal au plus gros fichier à chiffrer, pour héberger Encryption External Media.
- Le tableau suivant répertorie les systèmes d'exploitation pris en charge lors de l'accès aux supports protégés par Encryption External Media :

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

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

Chiffrement complet du disque

- Le chiffrement complet du disque exige une activation sur un serveur Dell exécutant v9.8.2 ou une version ultérieure.
- Le chiffrement complet du disque n'est actuellement pas pris en charge dans les ordinateurs hôtes virtualisés.
- Le chiffrement complet du disque nécessite un module TPM matériel séparé. Les modules PTT et TPM basés sur firmware ne sont pas pris en charge à l'heure actuelle.
- Les fournisseurs d'informations d'identification tiers ne fonctionneront pas avec les fonctionnalités FDE installées et tous les fournisseurs d'informations d'identification tiers seront désactivés si la PBA est activée.
- L'ordinateur client doit posséder une connectivité réseau ou un code d'accès pour être activé.
- L'ordinateur doit disposer d'une connexion réseau filaire pour permettre aux utilisateurs de carte à puce de se connecter dans l'écran d'authentification avant démarrage à la première connexion.
- La mise à jour des fonctionnalités du système d'exploitation n'est pas prise en charge avec le chiffrement complet du disque.
- Une connexion filaire est nécessaire pour que la PBA communique avec le serveur Dell.
- Un SED ne peut pas être présent sur l'ordinateur cible.
- Le chiffrement complet du disque n'est pas pris en charge avec BitLocker ou BitLocker Manager. N'installez pas le chiffrement complet du disque sur un ordinateur sur lequel le BitLocker ou BitLocker Manager est installé.
- Dell recommande la dernière version du pilote Intel Rapid Storage Technology avec des disques NVMe.
- Tout disque NVMe utilisé pour la fonction PBA :
  - Si l'appareil Dell a été fabriqué en 2018 ou après : RAID ON ou AHCI peut être utilisé avec les disques NVMe.
  - Le mode de démarrage du BIOS doit être défini sur UEFI (Unified Extensible Firmware Interface). Les ROM de l'opération existante doivent être désactivées.
- Tout disque non NVMe utilisé pour la fonction PBA :
  - L'opération SATA du BIOS peut être définie sur AHCI ou RAID ON.
  - Le système d'exploitation plante lors du passage de RAID ON à AHCI si les disques du contrôleur AHCI ne sont pas préinstallés. Pour obtenir des instructions sur le passage de RAID à AHCI (et inversement), reportez-vous à l'article de la base de connaissances 124714.
- La gestion du chiffrement complet de disque ne prend pas en charge les configurations à double démarrage dans la mesure où il est possible de chiffrer les fichiers système de l'autre système d'exploitation, ce qui perturberait son fonctionnement.
- La réinstallation du système d'exploitation sur place 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.
- Les mises à jour des fonctions Direct à partir de Windows 10 v1607 (mise à jour anniversaire/Redstone 1) vers Windows 10 v1903 (mise à jour mai 2019/19H1) ne sont pas prises en charge avec FDE. Dell vous recommande de mettre à jour le système d'exploitation avec une mise à jour des fonctionnalités plus récente en cas de mise à jour vers Windows 10 v1903. Si vous tentez d'effectuer la mise à jour directement de Windows 10 v1607 à v1903, un message d'erreur s'affiche et la mise à jour est impossible.
- Tous les disques doivent être initialisés et formatés avant d'activer le chiffrement complet du disque.

- Les configurations de chiffrement à plusieurs disques avec chiffrement complet du disque nécessitent les conditions suivantes :
  - Tous les disques du système cible doivent respecter la configuration suivante :
    - Il doit s'agir de disques non-SED.
    - Ils doivent être configurés dans le même mode de démarrage.
    - Ils doivent être initialisés comme GPT (tableau de partition GUID).
    - Les disques doivent être des partitions principales.
    - Une lettre de lecteur doit être attribuée aux disques.
  - Un redémarrage est nécessaire pour chiffrer les nouveaux disques après la configuration initiale.
  - Il est possible de chiffrer au maximum 16 disques.
  - En mode de démarrage UEFI, le système d'exploitation peut être installé sur n'importe quel disque cible.
  - En mode de démarrage hérité, le système d'exploitation doit être installé sur le premier disque (Disque 0). Si le système d'exploitation n'est pas installé sur le premier disque, le chiffrement sur plusieurs disques est désactivé.

    Activez le chiffrement sur plusieurs disques dans la console de gestion. Reportez-vous aux Paramètres de Registre pour afficher les valeurs du Registre Windows pour le chiffrement de plusieurs disques et le multi-balayage.

  - Le chiffrement complet du disque nécessite l'utilisation du fournisseur d'informations d'identification personnalisé Dell pour synchroniser les modifications de mots de passe Windows et les clés de chiffrement des données. Si vous avez besoin d'utiliser des applications tierces qui utilisent des fournisseurs d'informations d'identification personnalisés s'exécutant sur des ordinateurs protégés par le chiffrement complet du disque, vous devez lancer les modifications de mots de passe Windows via la Data Security Console. Pour plus d'informations sur la modification de votre mot de passe dans la Data Security Console, voir le chapitre *Mot de passe* du Guide de l'utilisateur de Data Security Console.
- Le programme d'installation principal installe ces composants s'ils ne sont pas déjà présents sur l'ordinateur cible. **Lors de l'utilisation du programme d'installation enfants**, vous devez installer ces composants avant d'installer les clients.

Conditions préalables
○ Visual C++ 2017 Redistributable Package (x86 ou x64) ou ultérieur ○ Depuis janvier 2020, les certificats de signature SHA1 ne sont plus valides et ne peuvent pas être renouvelés. Vous devez installer les mises à jour https://support.microsoft.com/help/4474419 et https://support.microsoft.com/help/4490628 de la Base de connaissances Microsoft sur les appareils exécutant Windows Server 2008 R2 pour valider les certificats de signature SHA256 dans les applications et les modules d'installation. Sans ces mises à jour installées, les applications et modules d'installation signés avec des certificats SHA1 fonctionnent, mais une erreur s'affiche sur le point de terminaison lors de l'installation ou de l'exécution des applications.

- **REMARQUE :** Un mot de passe est requis pour l'authentification avant démarrage. Dell recommande d'utiliser des paramètres de mot de passe au moins conformes aux stratégies de sécurité internes.
- **REMARQUE :** Lorsque PBA est utilisé, la règle de synchronisation de tous les utilisateurs doit être activée si un ordinateur a plusieurs utilisateurs. De plus, tous les utilisateurs doivent disposer de mots de passe. Les utilisateurs ayant un mot de passe de longueur nulle ne pourront plus utiliser l'ordinateur suite à l'activation.
- **REMARQUE :** Les ordinateurs protégés par chiffrement complet du disque doivent effectuer la mise à jour vers Windows 10 v1703 (mise à jour Creators Update/Redstone 2) ou une version ultérieure avant d'effectuer la mise à jour vers Windows 10 v1903 (mise à jour mai 2019/19H1) ou une version ultérieure. Si vous tentez cette stratégie de mise à niveau, un message d'erreur s'affiche.

REMARQUE : Le chiffrement complet du disque doit être configuré avec des algorithmes de chiffrement définis sur AES-256 et le mode de chiffrement défini sur CBC.

Matériel

- Le tableau suivant répertorie en détail le matériel compatible.

Matériel intégré en option
○ TPM 1.2 ou 2.0

Options d'authentification pour les clients avec chiffrement complet du disque

- L'utilisation des cartes à puce et l'authentification sur des ordinateurs UEFI nécessitent du matériel spécifique. La configuration est nécessaire pour utiliser les cartes à puce avec l'authentification avant démarrage. Les tableaux suivants montrent les options d'authentification disponibles par système d'exploitation, lorsque les conditions en terme de configuration et de matériel sont remplies.

UEFI				
	PBA - sur les ordinateurs Dell pris en charge			
	Mot de passe	**Empr. digit.**	**Carte à puce à contact**	**Carte SIPR**
Windows 10	X[1]		X[1]	
Windows 11	X[1]		X[1]	
1. Disponible pour les ordinateurs UEFI pris en charge.				

Modèles d'ordinateur Dell pris en charge avec le mode de démarrage UEFI

- Pour consulter la toute dernière liste des plates-formes compatibles avec le chiffrement complet du disque, reportez-vous à l'article de la base de connaissances 126855.
- Pour obtenir la liste des stations d'accueil et des adaptateurs compatibles avec le chiffrement complet du disque, reportez-vous à l'article de la base de connaissances 124241.

Systèmes d'exploitation

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

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

Encryption sur système d'exploitation serveur

Encryption sur systèmes d'exploitation de serveur est conçu pour une utilisation sur des ordinateurs fonctionnant en mode Serveur, en particulier les serveurs de fichiers.

- Encryption sur systèmes d'exploitation de serveur est compatible uniquement avec Encryption Enterprise et Endpoint Security Suite Enterprise.
- Encryption sur systèmes d'exploitation de serveur fournit :
  - Le chiffrement logiciel est
  - Removable Media Encryption
  - Contrôle de port

REMARQUE :

Le serveur doit prendre en charge les contrôles de port.

Les règles du système de contrôle de port affectent le support amovible des serveurs protégés, en contrôlant par exemple l'accès et l'utilisation des ports USB du serveur par des périphériques USB. La règle du port USB s'applique aux ports USB externes. La fonction du port USB interne n'est pas affectée par la règle du port USB. Si la règle du port USB est désactivée, le clavier et la souris USB du client ne fonctionnent pas et l'utilisateur n'est pas en mesure d'utiliser l'ordinateur à moins que la connexion du bureau à distance soit définie avant l'application de la règle.

- Le programme d'installation principal installe ces composants s'ils ne sont pas déjà présents sur l'ordinateur cible. **Lors de l'utilisation du programme d'installation enfants**, vous devez installer ces composants avant d'installer les clients.

Conditions préalables
○ Visual C++ 2012 Redistributable Package (x86 ou x64) Mise à jour 4 ou ultérieure ○ Visual C++ 2017 Redistributable Package (x86 ou x64) ou ultérieur ○ Depuis janvier 2020, les certificats de signature SHA1 ne sont plus valides et ne peuvent pas être renouvelés. Vous devez installer les mises à jour https://support.microsoft.com/help/4474419 et https://support.microsoft.com/help/4490628 de la Base de connaissances Microsoft sur les appareils exécutant Windows Server 2008 R2 pour valider les certificats de signature SHA256 dans les applications et les modules d'installation. Sans ces mises à jour installées, les applications et modules d'installation signés avec des certificats SHA1 fonctionnent, mais une erreur s'affiche sur le point de terminaison lors de l'installation ou de l'exécution des applications.

Encryption sur systèmes d'exploitation de serveur peut être utilisé avec :

- les serveurs de fichier sur disque locaux
- les invités de la machine virtuelle (VM) s'exécutant sous un système d'exploitation de serveur ou autre que serveur en tant que simple serveur de fichiers
- Configurations prises en charge :
  - les serveurs équipés de disques RAID 5 ou 10 ; RAID 0 (agrégation par bandes) et RAID 1 (mise en miroir) sont pris en charge indépendamment l'un de l'autre.
  - les serveurs équipés de lecteurs RAID de plusieurs To
  - les serveurs équipés de lecteurs pouvant être remplacé sans avoir a mettre l'ordinateur hors tension.
  - Le chiffrement du serveur est validé par les principaux fournisseurs d'antivirus du marché. Les exclusions codées en dur sont en place afin que ces fournisseurs d'antivirus puissent empêcher les incompatibilités entre l'analyse et le chiffrement des antivirus. Si votre organisation utilise un fournisseur d'antivirus qui n'est pas répertorié, reportez-vous à l'article de la base de connaissances 126046 ou contactez Dell ProSupport pour obtenir de l'aide.

Encryption sur systèmes d'exploitation de serveur ne peut pas être utilisé avec :

- Security Management Servers/Security Management Server Virtuals ou les serveurs exécutant des bases de données pour Security Management Servers/Security Management Server Virtual.
- Encryption Personal.
- SED Manager, PBA Advanced Authentication ou BitLocker Manager.
- Les serveurs qui font partie de DFS (distributed file systems).
- La migration vers ou depuis Encryption sur un système d'exploitation de serveur. La mise à niveau depuis External Media Edition vers Encryption sur systèmes d'exploitation de serveur exige que le produit précédent soit entièrement désinstallé avant l'installation d'Encryption sur systèmes d'exploitation de serveur.
- les hôtes de machine virtuelle (un hôte de machine virtuelle contient généralement plusieurs invités de machine virtuelle.)
- Contrôleurs de domaine.
- Serveurs Exchange
- Serveurs hébergeant des bases de données (SQL, Sybase, SharePoint, Oracle, MySQL, Exchange etc.)
- Serveurs utilisant l'une des technologies suivantes :
  - Systèmes de fichiers résistants
  - Systèmes de fichiers fluides
  - Espace de stockage Microsoft
  - Solutions de stockage réseau SAN/NAS
  - Périphériques connectés iSCSI

- Logiciel de déduplication
- Matériel de déduplication
- RAID fractionnés (plusieurs volumes sur un RAID unique)
- Lecteurs SED (RAID et NON RAID)
- Microsoft Storage Server 2012

- Encryption sur un système d'exploitation de serveur ne prend pas en charge les configurations à double amorçage, car il est possible de chiffrer les fichiers système de l'autre système d'exploitation, ce qui perturberait son fonctionnement.
- La réinstallation du système d'exploitation sur place 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 suivantes. Pour plus d'informations sur la récupération des données cryptées, reportez-vous au *Guide de récupération*.

Systèmes d'exploitation

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

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

Systèmes d'exploitation de serveur pris en charge
• Windows Server 2008 R2 SP1 : Édition Standard, Édition Datacenter, Édition Enterprise, Édition Webserver • Windows Server 2012 : Édition Standard, Édition Essentials, Édition Datacenter (Server Core n'est pas pris en charge) • Windows Server 2012 R2 : Édition Standard, Édition Essentials, Édition Datacenter (Server Core n'est pas pris en charge) • Windows Server 2016 : Édition Standard, Édition Essentials, Édition Datacenter (Server Core n'est pas pris en charge) • Windows Server 2019 - Standard, Datacenter Edition • Windows Server 2022 : Standard Edition, Datacenter Edition

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

REMARQUE :

Sur un ordinateur UEFI pris en charge, après que vous sélectionnez **Redémarrer** dans le menu principal, l'ordinateur redémarre, puis affiche l'un des deux écrans de connexion possibles. L'écran de connexion affiché est déterminé par les différences d'architecture de plateforme de l'ordinateur.

Encryption External Media

Systèmes d'exploitation

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

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

Systèmes d'exploitation de serveur pris en charge
• Windows Server 2012 R2

Systèmes d'exploitation Mac pris en charge pour accéder à un support chiffré (noyaux 64 bits)
• macOS High Sierra 10.13.5 - 10.13.6 • macOS Mojave 10.14.0 - 10.14.4 • macOS Catalina 10.15.1 - 10.15.4

Advanced Threat Prevention

- Pour terminer l'installation d'Advanced Threat Prevention lorsque le Dell Server qui gère le client est exécuté en mode Connecté (par défaut), l'ordinateur doit disposer d'une connectivité réseau. Cependant, la connectivité réseau n'est ***pas*** requise pour l'installation d'Advanced Threat Prevention lorsque le Dell Server de gestion est exécuté en mode Déconnecté.
- Pour configurer un client pour Advanced Threat Prevention, le Dell Server doit disposer d'une connectivité Internet.
- Vous ne devez ***pas*** installer les fonctions facultatives Pare-feu client et Protection Web sur des ordinateurs clients gérés par Dell Server exécuté en mode Déconnecté.
- Les applications antivirus, anti-programmes malveillants et anti-espions des autres fournisseurs peuvent entrer en conflit avec le client Advanced Threat Prevention. Si possible, désinstallez ces applications. Les logiciels en conflit ne comprennent pas Windows Defender. Les applications de pare-feu sont autorisées.

  Si la désinstallation d'autres applications antivirus, anti-programmes malveillants et anti-espions est impossible, vous devez ajouter des exceptions à Advanced Threat Prevention dans le Dell Server ainsi qu'aux autres applications. Pour obtenir des instructions sur l'ajout d'exclusions à Advanced Threat Prevention dans le Dell Server, reportez-vous à l'article de la base de connaissances 126745. Pour obtenir la liste des exclusions à ajouter à d'autres applications anti-virus, reportez-vous à l'article de la base de connaissances 126118.

Systèmes d'exploitation

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

Systèmes d'exploitation Windows (32 bits et 64 bits)
○ Depuis janvier 2020, les certificats de signature SHA1 ne sont plus valides et ne peuvent pas être renouvelés. Vous devez installer les mises à jour https://support.microsoft.com/help/4474419 et https://support.microsoft.com/help/4490628 de la Base de connaissances Microsoft sur les appareils exécutant Windows Server 2008 R2 pour valider les certificats de signature SHA256 dans les applications et les modules d'installation. Sans ces mises à jour installées, les applications et modules d'installation signés avec des certificats SHA1 fonctionnent, mais une erreur s'affiche sur le point de terminaison lors de l'installation ou de l'exécution des applications.
○ Windows 10 : Éducation, Entreprise, Pro v1909-v22H2 (mise à jour novembre 2019/19H2 - Mise à jour novembre 2022/22H2) **Remarque :** les OEM et ODM ne sont pas livrés avec Windows 10 v2004 (mise à jour de mai 2020/20H1 et versions ultérieures) avec une architecture 32 bits. Pour plus d'informations, voir https://docs.microsoft.com/windows-hardware/design/minimum/minimum-hardware-requirements-overview. ■ Windows 10 2019 LTSC ■ Windows 10 2021 LTSC
○ Windows 11 : Entreprise, Pro v21H2 - 22H2
○ Windows Server 2008 R2 SP1 : Édition Standard, Édition Datacenter, Édition Enterprise, Édition Webserver
○ Windows Server 2012 R2 : éditions Standard, Essentials et Datacenter
○ Windows Server 2016 : éditions Standard, Essentials et Datacenter
○ Windows Server 2019 - Standard, Datacenter Edition

Ports

- Les agents Advanced Threat Prevention sont gérés par la plateforme SaaS de la console de gestion, sur laquelle ils envoient leurs rapports. Le port 443 (https) est utilisé pour la communication et doit être ouvert sur le pare-feu pour que les agents puissent communiquer avec la console. La console est hébergée par Amazon Web Services et ne dispose pas d'adresse IP fixe. Si le port 443 est bloqué pour une raison quelconque, les mises à jour ne pourront pas être téléchargées et les ordinateurs ne pourront pas bénéficier de la protection la plus récente. Assurez-vous que les ordinateurs clients peuvent accéder aux URL comme suit.

Utilisation	Protocole d'application	Protocole de transport :	Numéro de port	Destination	Direction
Toutes les communications	HTTPS	TCP	443	Autoriser tout le trafic https vers *.cylance.com	Sortant

Pour obtenir des informations détaillées concernant les URL en cours d'utilisation, reportez-vous à l'article de la base de connaissances 127053.

Vérification de l'intégrité de l'image BIOS

Si la règle *Activer l'assurance BIOS* est sélectionnée dans la console de gestion, le client Cylance vérifie une valeur de hachage BIOS sur les ordinateurs de point de terminaison afin de garantir que le BIOS n'a pas été modifié par rapport à la version d'usine Dell, ce qui est un vecteur d'attaque possible. Si une menace est détectée, une notification est transmise à Dell Server et l'administrateur informatique est averti dans la console de gestion. Pour consulter la présentation de ce processus, voir la section « Processus de vérification de l'intégrité de l'image BIOS ».

REMARQUE : Une image usine personnalisée ne peut pas être utilisée avec cette fonction, car le BIOS a été modifié.

Modèles d'ordinateur Dell pris en charge avec la vérification de l'intégrité de l'image BIOS	
● Latitude 3470 ● Latitude 3570 ● Latitude 7275	● OptiPlex 5040 ● OptiPlex 7040 ● OptiPlex 7440

Modèles d'ordinateur Dell pris en charge avec la vérification de l'intégrité de l'image BIOS		
• Latitude 7370 • Latitude E5270 • Latitude E5470 • Latitude E5570 • Latitude E7270 • Latitude E7470 • Latitude Rugged 5414 • Latitude Rugged 7214 Extrême • Latitude Rugged 7414 • OptiPlex 3040 • OptiPlex 3240	• Station de travail mobile Precision 3510 • Station de travail mobile Precision 5510 • Precision Workstation 3620 • Precision Workstation 7510 • Precision Workstation 7710 • Precision Workstation T3420 • Venue 10 Pro 5056 • Venue Pro 5855 • Venue XPS 12 9250 • XPS 13 9350 • XPS 9550	

Compatibilité

Le tableau suivant indique la compatibilité avec Windows, Mac et Linux.

n/a - Cette technologie ne s'applique pas à cette plate-forme.

Champ vide - Cette stratégie n'est pas prise en charge avec Endpoint Security Suite Enterprise.

Fonctionnalités	Stratégies	Windows	macOS	Linux
Actions de fichier				
	Quarantaine automatique (Dangereux)	x	x	x
	Quarantaine automatique (Anormal)	x	x	x
	Téléchargement auto	x	x	x
	Liste de confiance de la stratégie	x	x	x
Actions de mémoire				
	Protection de la mémoire	x	x	x
Exploitation				
	Zone dynamique d'empilement	x	x	x
	Protection de l'empilement	x	x	x
	Écraser le code	x	Sans objet	
	Collecte de données stockées en RAM	x	Sans objet	
	Charge malveillante	x		
Injection de processus				
	Attribution à distance de mémoire	x	x	Sans objet
	Adressage à distance de mémoire	x	x	Sans objet
	Écriture à distance dans la mémoire	x	x	Sans objet
	Écriture à distance de PE dans la mémoire	x	Sans objet	Sans objet
	Écraser le code à distance	x	Sans objet	
	Suppression de l'adressage de la mémoire à distance	x	Sans objet	

Fonctionnalités	Stratégies	Windows	macOS	Linux
	Création de thread à distance	x	x	
	Planification APC à distance	x	Sans objet	Sans objet
	Injection de DYLD		x	x
Escalade				
	Lecture LSASS	x	Sans objet	Sans objet
	Attribution nulle	x	x	
Paramètres de protection				
	Contrôle de l'exécution	x	x	x
	Interdire l'arrêt du service depuis le périphérique	x	x	
	Arrêter les processus et sous-processus dangereux en cours d'exécution	x	x	x
	Détection de menace d'arrière plan	x	x	x
	recherche de nouveaux fichiers	x	x	x
	Taille de fichier d'archive maximale à analyser	x	x	x
	Exclure des dossiers spécifiques	x	x	x
	Copier les fichiers exemples	x		
Contrôle des applications				
	Fenêtre de modification	x		x
	Exclusion de dossiers	x		
Paramètres de l'agent				
	Activer le téléchargement automatique des fichiers journaux	x	x	x
	Activer les notifications sur le bureau	x		
Contrôle des scripts				
	Script actif	x		
	Powershell	x		
	Macros Office	x		Sans objet
	Bloquer l'utilisation de la console Powershell	x		
	Approuver les scripts dans ces dossiers (et leurs sous-dossiers)	x		
	Niveau de journalisation	x		
	Niveau d'auto-protection	x		
	Mise à jour automatique	x		
	Exécuter une détection (à partir de l'interface utilisateur de l'agent)	x		
	Supprimer les éléments mis en quarantaine (interface utilisateur de	x		

Fonctionnalités	Stratégies	Windows	macOS	Linux
	l'agent et interface utilisateur de la console)			
	Mode Déconnecté	x		x
	Données de menace détaillées	x		
	Liste de confiance des certificats	x	x	Sans objet
	Copier les échantillons de logiciel malveillant	x	x	x
	Paramètres de proxy	x	x	x
	Vérification manuelle des stratégies (interface utilisateur de l'agent)	x	x	

Pare-feu client et protection Web

- L'installation du pare-feu client et des clients de protection Web exige une connectivité réseau de l'ordinateur.
- Désinstallez les applications antivirus, anti-logiciels malveillants, anti-logiciels espions et pare-feu des autres fournisseurs avant d'installer le pare-feu client et les clients de protection Web, afin d'éviter tout échec d'installation. Windows Defender et Endpoint Security Suite Enterprise ne font pas partie des logiciels conflictuels.
- Le programme d'installation principal installe ces composants s'ils ne sont pas déjà présents sur l'ordinateur cible. **Si vous utilisez le programme d'installation enfant**, vous devez installer ces composants avant d'installer le pare-feu client et la protection Web.

Conditions préalables
○ Package redistribuable Visual C++ 2012 (x86 et x64), mise à jour 4 ○ Package redistribuable Visual C++ 2015 (x86 ou x64) ou version ultérieure

- La fonction Web Protection est prise en charge par les navigateurs suivants :

Navigateur	Prise en charge de Web Protection	Version
Google Chrome	Oui	Toutes les versions modernes
Microsoft Edge	Oui	Microsoft Edge est pris en charge avec Endpoint Security Suite Enterprise v10.1 et versions ultérieures
Microsoft Internet Explorer 11	Oui	Toutes les versions modernes
Mozilla Firefox	Oui	○ Firefox 56 et versions ultérieures est pris en charge avec Endpoint Security Suite Enterprise v10.0 et versions ultérieures ○ Firefox 51 est pris en charge avec Endpoint Security Suite Enterprise v1.8 et versions ultérieures

Ports

- Pour garantir que le pare-feu client et Web Protection reçoivent les dernières mises à jour, les ports 443 et 80 doivent être disponibles afin que le client puisse communiquer avec les différents serveurs de destination. Si les ports sont bloqués pour une raison quelconque, les mises à jour de signature antivirus (fichiers DAT) ne pourront pas être téléchargées et les ordinateurs ne pourront pas bénéficier de la protection la plus récente. Assurez-vous que les ordinateurs clients peuvent accéder aux URL comme suit.

Utilisation	Protocole d'application	Protocole de transport :	Numéro de port	Destination	Direction
Service de réputation	SSL	TCP	443	tunnel.web.trustedsource.org	Sortant
Commentaires relatif au service de réputation	SSL	TCP	443	gtifeedback.trustedsource.org	Sortant
Mise à jour de la base de données de la réputation des URL	HTTP	TCP	80	list.smartfilter.com	Sortant
Recherche de réputation des URL	SSL	TCP	443	tunnel.web.trustedsource.org	Sortant

Systèmes d'exploitation

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

Systèmes d'exploitation Windows (32 bits et 64 bits)
○ Depuis janvier 2020, les certificats de signature SHA1 ne sont plus valides et ne peuvent pas être renouvelés. Vous devez installer les mises à jour https://support.microsoft.com/help/4474419 et https://support.microsoft.com/help/4490628 de la Base de connaissances Microsoft sur les appareils exécutant Windows Server 2008 R2 pour valider les certificats de signature SHA256 dans les applications et les modules d'installation. Sans ces mises à jour installées, les applications et modules d'installation signés avec des certificats SHA1 fonctionnent, mais une erreur s'affiche sur le point de terminaison lors de l'installation ou de l'exécution des applications.
○ Windows 10 : Éducation, Entreprise, Pro v1909-v22H2 (mise à jour novembre 2019/19H2 - Mise à jour novembre 2022/22H2) **Remarque :** les OEM et ODM ne sont pas livrés avec Windows 10 v2004 (mise à jour de mai 2020/20H1 et versions ultérieures) avec une architecture 32 bits. Pour plus d'informations, voir https://docs.microsoft.com/windows-hardware/design/minimum/minimum-hardware-requirements-overview. ▪ Windows 10 2019 LTSC ▪ Windows 10 2021 LTSC
○ Windows 11 : Entreprise, Pro v21H2 - 22H2

SED Manager

- Pour que l'installation de SED Manager réussisse, l'ordinateur doit disposer d'une connexion réseau filaire.
- L'ordinateur doit disposer d'une connexion réseau filaire pour permettre aux utilisateurs de carte à puce de se connecter dans l'écran d'authentification avant démarrage à la première connexion.
- Les fournisseurs d'informations d'identification tiers ne fonctionneront pas avec SED Manager installé et tous les fournisseurs d'informations d'identification tiers seront désactivés si la PBA est activée.
- IPv6 n'est pas pris en charge.
- SED Manager n'est actuellement pas pris en charge dans les ordinateurs hôtes virtualisés.
- Après avoir appliqué des règles, préparez-vous à redémarrer l'ordinateur avant de pouvoir les mettre en application.
- Les ordinateurs équipés de disques auto-cryptables ne peuvent pas être utilisés avec des cartes HCA. Il existe des incompatibilités qui empêchent le provisionnement des accélérateurs HCA. Notez que Dell ne vend pas d'ordinateurs comportant des disques à auto-chiffrement prenant en charge le module HCA. Cette configuration non prise en charge est une configuration après-vente.

- Si l'ordinateur ciblé pour chiffrement est équipé d'un accélérateur d'un disque à autochiffrement, vérifiez que l'option Active Directory, *l'utilisateur doit changer de mot passe lors de la prochaine connexion*, est désactivée. L'authentification avant démarrage ne prend pas en charge cette option Active Directory.
- 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.
- La configuration des disques à chiffrement automatique pour SED Manager est différente entre les disques NVMe et non NVMe (SATA).
  - Tout disque NVMe utilisé pour la fonction PBA :
    - Si l'appareil Dell a été fabriqué en 2018 ou après : RAID ON ou AHCI peut être utilisé avec les disques NVMe.
    - Le mode de démarrage du BIOS doit être défini sur UEFI (Unified Extensible Firmware Interface). Les ROM de l'opération existante doivent être désactivées.
  - Tout disque non NVMe utilisé pour la fonction PBA :
    - L'opération SATA du BIOS peut être définie sur AHCI ou RAID ON.
    - Le système d'exploitation plante lorsqu'il est transféré de RAID ON à AHCI si les disques du contrôleur AHCI ne sont pas préinstallés. Pour obtenir des instructions sur le passage de RAID à AHCI (ou vice-versa), reportez-vous à l'article de la base de connaissances 124714.

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

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

- SED Manager nécessite l'utilisation du fournisseur d'informations d'identification personnalisé Dell pour synchroniser les modifications de mots de passe Windows et les clés de chiffrement des données. Si vous avez besoin d'utiliser des applications tierces qui utilisent des fournisseurs d'informations d'identification personnalisés s'exécutant sur des ordinateurs protégés par SED Manager, vous devez lancer les modifications de mots de passe Windows via la Data Security Console. Pour plus d'informations sur la modification de votre mot de passe dans la Data Security Console, voir le chapitre *Mot de passe* du Guide de l'utilisateur de Data Security Console.
- Le programme d'installation principal installe ces composants s'ils ne sont pas déjà présents sur l'ordinateur cible. **Lors de l'utilisation du programme d'installation enfants**, vous devez installer ces composants avant d'installer les clients.

Conditions préalables
○ Visual C++ 2017 Redistributable Package (x86 ou x64) ou ultérieur ○ Depuis janvier 2020, les certificats de signature SHA1 ne sont plus valides et ne peuvent pas être renouvelés. Vous devez installer les mises à jour https://support.microsoft.com/help/4474419 et https://support.microsoft.com/help/4490628 de la Base de connaissances Microsoft sur les appareils exécutant Windows Server 2008 R2 pour valider les certificats de signature SHA256 dans les applications et les modules d'installation. Sans ces mises à jour installées, les applications et modules d'installation signés avec des certificats SHA1 fonctionnent, mais une erreur s'affiche sur le point de terminaison lors de l'installation ou de l'exécution des applications.

- SED Manager n'est pas prise en charge avec Encryption sur des systèmes d'exploitation de serveur ou Advanced Threat Prevention sur un système d'exploitation de serveur.
- Les configurations de chiffrement à plusieurs disques avec SED Manager nécessitent les conditions suivantes :
  - Tous les disques du système cible doivent respecter la configuration suivante :
    - Il doit s'agir de disques SED.
    - Une lettre de lecteur doit être attribuée aux disques.
  - En mode de démarrage UEFI, le système d'exploitation peut être installé sur n'importe quel disque cible.
  - En mode de démarrage hérité, le système d'exploitation doit être installé sur le premier disque (Disque 0). Si le système d'exploitation n'est pas installé sur le premier disque, le chiffrement sur plusieurs disques est désactivé.

    Activez le chiffrement sur plusieurs disques dans la console de gestion. Reportez-vous aux Paramètres de Registre pour afficher les valeurs du Registre Windows pour le chiffrement de plusieurs disques et le multi-balayage.

- **REMARQUE :** Un mot de passe est requis pour l'authentification avant démarrage. Dell recommande d'utiliser des paramètres de mot de passe au moins conformes aux stratégies de sécurité internes.
- **REMARQUE :** Lorsque PBA est utilisé, la règle de synchronisation de tous les utilisateurs doit être activée si un ordinateur a plusieurs utilisateurs. De plus, tous les utilisateurs doivent disposer de mots de passe. Les utilisateurs ayant un mot de passe de longueur nulle ne pourront plus utiliser l'ordinateur suite à l'activation.
- **REMARQUE :** Les ordinateurs protégés par SED Manager doivent effectuer la mise à jour vers Windows 10 v1703 (mise à jour Creators Update/Redstone 2) ou une version ultérieure avant d'effectuer la mise à jour vers Windows 10 v1903 (mise à jour mai 2019/19H1) ou une version ultérieure. Si vous tentez cette stratégie de mise à niveau, un message d'erreur s'affiche.
-

Matériel

Lecteurs SED compatibles Opal

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

Options d'authentification avant démarrage avec SED Manager

- L'utilisation des cartes à puce et l'authentification sur des ordinateurs UEFI nécessitent du matériel spécifique. La configuration est nécessaire pour utiliser les cartes à puce avec l'authentification avant démarrage. Les tableaux suivants montrent les options d'authentification disponibles par système d'exploitation, lorsque les conditions en terme de configuration et de matériel sont remplies.

Non UEFI				
	PBA			
	Mot de passe	**Empr. digit.**	**Carte à puce à contact**	**Carte SIPR**
Windows 10	X[1]		X[1 2]	
Windows 11	X[1]		X[1 2]	
1. Disponible lorsque les pilotes d'authentification sont téléchargés depuis dell.com/support 2. Disponible avec un SED Opal pris en charge				

UEFI				
	PBA - sur les ordinateurs Dell pris en charge			
	Mot de passe	**Empr. digit.**	**Carte à puce à contact**	**Carte SIPR**
Windows 10	X[1]		X[1]	
Windows 11	X[1]		X[1]	
1. Disponible avec un SED OPAL pris en charge sur les ordinateurs UEFI pris en charge				

Claviers internationaux

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

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

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

Systèmes d'exploitation

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

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

Localisation

SED Manager est compatible avec l'interface utilisateur multilingue et est localisée dans les langues suivantes. Le mode UEFI et PBA Advanced Authentication sont pris en charge dans les langues suivantes :

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

BitLocker Manager

- Envisagez de revoir la Configuration requise de Microsoft BitLocker si BitLocker n'est pas encore déployé dans votre environnement,
- Assurez-vous que la partition d'authentification avant démarrage est déjà configurée. Si vous installez BitLocker Manager avant de configurer la partition PBA, vous ne pourrez pas activer BitLocker et BitLocker Manager ne sera pas opérationnel. Voir Configuration préalable à l'installation d'une partition d'authentification avant démarrage BitLocker.
- Un Dell Server est nécessaire pour utiliser BitLocker Manager.
- Assurez-vous qu'un certificat de signature est disponible dans la base de données. Pour plus d'informations, reportez-vous à l'article de la base de connaissances 124931.
- Le clavier, la souris et les composants vidéo doivent être directement connectés à l'ordinateur. N'utilisez pas de commutateur KVM pour gérer les périphériques, car il risquerait de réduire la capacité de l'ordinateur à identifier le matériel.
- Lancez le TPM et activez-le. Le gestionnaire BitLocker Manager s'approprie le TPM sans nécessiter de redémarrage. Toutefois, si le TPM est déjà propriétaire, BitLocker Manager lance le processus de configuration du chiffrement (aucun redémarrage n'est nécessaire). Ce qui compte, c'est que le TPM soit propriétaire et activé.
- BitLocker Manager utilise les algorithmes validés AES FIPS si le mode FIPS est activé pour le paramètre de sécurité GPO « cryptographie système : utiliser les algorithmes compatibles FIPS pour le chiffrement, le hachage et la signature » sur le périphérique et si vous gérez ce périphérique avec notre produit. BitLocker Manager ne force pas ce mode en tant que mode par défaut pour les clients cryptés par BitLocker, car Microsoft suggère désormais à ses clients de ne pas utiliser leur chiffrement validé par FIPS en raison de nombreux problèmes de compatibilité des applications, de récupération et de chiffrement des supports : http://blogs.technet.com.
- BitLocker Manager n'est pas pris en charge avec Encryption sur des systèmes d'exploitation de serveur ou Advanced Threat Prevention sur un système d'exploitation de serveur.
- Lorsque vous utilisez une connexion de bureau à distance avec un point de terminaison exploitant BitLocker Manager, Dell recommande d'exécuter toutes les sessions de bureau à distance en mode console afin d'éviter tout problème d'interaction dans l'interface utilisateur avec la session utilisateur existante via la commande suivante :

  ```
  mstsc /admin /v:<target_ip_address>
  ```

- Le programme d'installation principal installe ces composants s'ils ne sont pas déjà présents sur l'ordinateur cible. **Lors de l'utilisation du programme d'installation enfants**, vous devez installer ces composants avant d'installer les clients.

Conditions préalables
○ Visual C++ 2017 Redistributable Package (x86 ou x64) ou ultérieur ○ Depuis janvier 2020, les certificats de signature SHA1 ne sont plus valides et ne peuvent pas être renouvelés. Vous devez installer les mises à jour https://support.microsoft.com/help/4474419 et https://support.microsoft.com/help/4490628 de la Base de connaissances Microsoft sur les appareils exécutant Windows Server 2008 R2 pour valider les certificats de signature SHA256 dans les applications et les modules d'installation. Sans ces mises à jour installées, les applications et modules d'installation signés avec des certificats SHA1 fonctionnent, mais une erreur s'affiche sur le point de terminaison lors de l'installation ou de l'exécution des applications.

- **REMARQUE :** Les ordinateurs protégés par Bitlocker Manager doivent effectuer la mise à jour vers Windows 10 v1703 (mise à jour Creators Update/Redstone 2) ou une version ultérieure avant d'effectuer la mise à jour vers Windows 10 v1903 (mise à jour mai 2019/19H1) ou une version ultérieure. Si vous tentez cette stratégie de mise à niveau, un message d'erreur s'affiche.
- **REMARQUE :** Les mises à niveau du système d'exploitation sur place vers une version plus récente (telle que Windows 10) pour Windows 11 ne sont pas prises en charge.

Matériel

- Le tableau suivant répertorie en détail le matériel compatible.

Matériel intégré en option
○ TPM 1.2 ou 2.0

Systèmes d'exploitation

- Les tableaux suivants décrivent les systèmes d'exploitation pris en charge.

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

Systèmes d'exploitation Windows Server
○ Windows Server 2008 R2 : Standard Edition, Enterprise Edition (64 bits) ○ Windows Server 2012 R2 : Standard Edition, Enterprise Edition (64 bits) ○ Windows Server 2016 : Standard Edition, Datacenter Edition (64 bits) ○ Windows Server 2019 : Standard Edition, Datacenter Edition (64 bits) ○ Windows Server 2022 : Standard Edition, Datacenter Edition

3

Paramètres de registre

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

Chiffrement

- Si un certificat auto-signé est utilisé sur Dell Server. Pour Windows, la validation d'approbation de certificat doit rester inactive sur l'ordinateur client (la validation d'approbation est *désactivée* par défaut avec le Dell Server). Les conditions suivantes doivent être remplies avant l'*activation* de la validation d'approbation sur l'ordinateur client :
  - Un certificat signé par une autorité racine comme EnTrust ou Verisign, doit être importé dans Dell Server.
  - La chaîne d'approbation complète du certificat doit être stockée dans le magasin de clés Microsoft de l'ordinateur client.
  - Pour *activer* la validation d'approbation pour Encryption, définissez la valeur d'entrée de registre suivante sur 0 sur l'ordinateur cible.

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

    "IgnoreCertErrors"=DWORD:00000000

    0 = Échec si une erreur de certificat est rencontrée

    1= Ignorer les erreurs

- Pour créer un fichier journal Encryption Removal Agent, créez l'entrée de registre suivante sur l'ordinateur ciblé pour le déchiffrement. Voir Créer un fichier journal Encryption Removal Agent (facultatif).

  [HKLM\Software\Credant\DecryptionAgent].

  "LogVerbosity"=DWORD:2

  0: aucune journalisation

  1 : consigne les erreurs bloquant l'exécution du service

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

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

  5 : consigne des informations de débogage

- Pour que l'utilisateur ne soit pas invité à redémarrer son ordinateur lorsqu'Encryption Removal Agent atteint son état final dans le processus de déchiffrement, modifiez la valeur de registre suivante ou modifiez la règle *Forcer le redémarrage lors de la mise à jour* dans la console de gestion.

  [HKLM\Software\Dell\Dell Data Protection]

  "ShowDecryptAgentRebootPrompt"=DWORD

  1 = activé (affiche l'invite)

  0 = désactivé (masque l'invite)

- Par défaut, l'icône de zone de notification s'affiche au cours de l'installation. Utilisez le paramètre de registre suivant pour masquer l'icône de zone de notification pour tous les utilisateurs gérés sur un ordinateur après l'installation d'origine. Créez ou modifiez le paramètre de répertoire :

  [HKLM\Software\CREDANT\CMGShield]

  "HIDESYSTRAYICON"=DWORD:1

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

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

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

  [HKLM\SOFTWARE\CREDANT\CMGShield]

  "DeleteTempFiles"=REG_DWORD:0

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

- Encryption affiche la *durée de chaque invite de délai 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 modifier le comportement de l'invite utilisateur pour commencer le chiffrement ou le reporter pour empêcher le traitement du chiffrement si l'utilisateur ne répond pas à l'invite. Pour ce faire, définissez la valeur suivante :

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

  "SnoozeBeforeSweep"=DWORD:1

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

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

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

- Utilisez le paramètre de registre pour faire interroger le Dell Server par Encryption à la recherche d'une mise à jour forcée de règle. Créez ou modifiez le paramètre de répertoire :

  [HKLM\SOFTWARE\Credant\CMGShield\Notify]

  "PingProxy"=DWORD value:1

  Le paramètre de registre disparaît automatiquement une fois la tâche terminée.

- Utilisez les paramètres de registre pour autoriser Encryption à envoyer un inventaire optimisé, complet (utilisateurs activés et désactivés) ou complet (utilisateurs activés uniquement) au Dell Server.
  - Envoyez un inventaire optimisé au Dell Server :

    Créez ou modifiez le paramètre de répertoire :

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

    "OnlySendInvChanges"=REG_DWORD:1

    En l'absence d'une entrée, l'inventaire optimisé est envoyé au Dell Server.

  - Envoyez un inventaire complet au Dell Server :

    Créez ou modifiez le paramètre de répertoire :

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

    "OnlySendInvChanges"=REG_DWORD:0

    En l'absence d'une entrée, l'inventaire optimisé est envoyé au Dell Server.

  - Envoyer l'inventaire complet de tous les utilisateurs activés

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

    "RefreshInventory"=REG_DWORD:1

    Cette entrée est supprimée du registre dès qu'elle est traitée. Comme la valeur est enregistrée dans le coffre, même si l'ordinateur est redémarré avant le chargement de l'inventaire, Encryption répond à cette demande lors du prochain téléchargement réussi de l'inventaire.

Cette entrée a précédence sur la valeur de registre OnlySendInvChanges.

- L'activation par laps de temps est une fonction qui vous permet de répartir les activations des clients sur une période de temps donnée afin d'alléger la charge de Dell Server au cours d'un déploiement en masse. Les activations sont retardées selon les laps de temps générés pour fournir une distribution sans heurt des temps d'activation.

  Dans le cas des utilisateurs exigeant une activation par l'intermédiaire d'un VPN, une configuration d'activation du client par laps de temps peut être requise, afin de retarder l'activation initiale assez longtemps pour réserver du temps nécessaire au client VPN pour établir une connexion réseau.

  Pour que les mises à jour de ces entrées de registre entrent en vigueur, l'ordinateur doit être redémarré.

  - **Activation par laps de temps**

    Pour activer ou désactiver cette fonction, créez un DWORD avec le nom **SlottedActivation** sous la clé parent suivante :

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

  - **Laps de temps d'activation**

    Pour activer ou désactiver cette fonction, créez une sous-clé avec le nom **ActivationSlot** sous la clé parent suivante :

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

    Laps de temps d'activation : chaîne qui définit la période pendant laquelle Encryption tente de s'activer avec le Dell Server. Ces valeurs sont définies en secondes et la syntaxe est définie par <lowervalue>,<uppervalue>. Par exemple : 120,300. Encryption tente de s'activer après une période aléatoire allant de 2 à 5 minutes après la connexion de l'utilisateur.

    - **Répéter le calendrier**

      Pour activer ou désactiver cette fonction, créez une sous-clé avec le nom **CalRepeat** sous la clé parent suivante :

      [HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield\ActivationSlot]

      CalRepeat : DWORD qui définit la période de temps en secondes au bout de laquelle un intervalle de laps d'activation se produit. Utilisez ce paramètre pour remplacer la période de temps en secondes au bout de laquelle un intervalle de laps d'activation se produit. 25 200 secondes sont disponibles pour les activations de laps de temps au cours d'une période de sept heures. Le paramètre par défaut est de 86 400 secondes, ce qui représente une répétition quotidienne. La valeur décimale suggérée est de 600, soit 10 minutes.

    - **Intervalle de laps de temps**

      Pour activer ou désactiver cette fonction, créez une sous-clé avec le nom **SlotInterval** sous la clé parent suivante :

      [HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield\ActivationSlot]

      Intervalle de laps de temps : chaîne qui définit les intervalles entre les laps de temps d'activation. Le paramètre suggéré est 45,120. Ce paramètre correspond à la période d'activation attribuée de manière aléatoire entre 45 et 120 secondes.

    - **Seuil manqué**

      Pour activer ou désactiver cette fonction, créez une sous-clé avec le nom **MissThreshold** sous la clé parent suivante :

      [HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield\ActivationSlot]

      Seuil manqué : valeur DWORD qui contient un nombre entier positif définissant le nombre de tentatives d'activation avant la déconnexion. Si le seuil manqué est atteint, les tentatives d'activation de l'utilisateur inactif sont interrompues jusqu'à la prochaine connexion. La valeur du seuil manqué est toujours réinitialisée à la déconnexion.

      Les clés de registre suivantes collectent les données utilisateur pour l'activation par laps de temps :

      [HKCU/Software/CREDANT/ActivationSlot] (par données utilisateur)

      Délai attribué pour une tentative d'activation par laps de temps. Ce délai est défini lorsque l'utilisateur se connecte au réseau pour la première fois après l'activation de l'activation par laps de temps. Le laps de temps d'activation est recalculé pour chaque tentative d'activation.

      [HKCU/Software/CREDANT/SlotAttemptCount] (par données utilisateur)

      Nombre de tentatives qui ont échoué ou ont été manquées, à l'occurrence d'un laps de temps et lorsqu'une tentative d'activation est effectuée mais échoue. Lorsque ce nombre atteint la valeur définie dans ACTIVATION_SLOT_MISSTHRESHOLD, l'ordinateur tente une activation immédiate au moment de sa connexion au réseau.

- Pour détecter les utilisateurs non gérés sur l'ordinateur client, définissez la valeur de registre sur l'ordinateur client :

[HKLM\SOFTWARE\Credant\CMGShield\ManagedUsers\]

"UnmanagedUserDetected"=DWORD value:1

Détecter les utilisateurs non gérés sur cet ordinateur=1

Ne pas détecter les utilisateurs non gérés sur cet ordinateur=0

- Pour la réactivation automatique silencieuse dans les rares cas où un utilisateur est désactivé, la valeur de registre suivante doit être définie sur l'ordinateur client.

  [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CMGShield]

  "AutoReactivation"=DWORD:00000001

  0 = Désactivé (valeur par défaut)

  1 = Activé

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

  Pour désactiver la clé SDUser et utiliser la clé SDE pour crypter ces répertoires utilisateurs, créez le registre suivant sur l'ordinateur :

  [HKEY_LOCAL_MACHINE\SOFTWARE\Credant\CMGShield]

  "EnableSDUserKeyUsage"=DWORD:00000000

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

  Pour plus d'informations sur la clé SDUser, reportez-vous à l'article de la base de connaissances 131035.

- Définition de l'entrée de registre, EnableNGMetadata, si des problèmes se produisent en lien avec les mises à jour Microsoft sur des ordinateurs comportant des données chiffrées par clé commune ou en lien avec le chiffrement, le déchiffrement ou la décompression d'un grand nombre de fichiers au sein d'un même dossier.

  Définissez l'entrée de registre EnableNGMetadata dans l'emplacement suivant :

  [HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\CmgShieldFFE]

  "EnableNGMetadata" = dword:1

  0 = Désactivé (valeur par défaut)

  1 = Activé

- La fonction d'activation hors domaine peut être activée en demandant les instructions à Dell ProSupport.
- Encryption Management Agent ne génère plus de stratégies par défaut. Pour générer de futures stratégies consommées, créez la clé de registre suivante :

  HKLM\Software\Dell\Dell Data Protection\

  "DumpPolicies" = DWORD

  Value=1

  Remarque : les journaux sont écrits sur C:\ProgramData\Dell\Dell Data Protection\Policy.

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

  HKEY_LOCAL_MACHINE\SOFTWARE\Dell\Dell Data Protection\Encryption

  "DisplaySharing"=DWORD

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

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

Chiffrement complet du disque

- Cette section décrit en détail tous les paramètres du registre approuvé Dell ProSupport des ordinateurs locaux, quel que soit le motif des paramètres de registre. Si un paramètre de registre chevauche deux produits, il est répertorié dans chaque catégorie.
- Ces modifications de registre doivent être effectuées par les administrateurs uniquement et peuvent ne pas être appropriées ou fonctionner dans tous les cas de figure.
- Pour définir l'intervalle entre les tentatives lorsque le Dell Server n'est pas en mesure de communiquer avec le chiffrement complet du disque, ajoutez la valeur de registre suivante.

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

  "CommErrorSleepSecs"=DWORD:300

  Cette valeur correspond au nombre de secondes pendant lesquelles le chiffrement complet du disque tente de contacter le Dell Server si celui-ci est indisponible pour communiquer avec le chiffrement complet du disque. La valeur par défaut est de 300 secondes (5 minutes).

- Si un certificat auto-signé est utilisé sur le Dell Server pour le chiffrement complet du disque, la validation d'approbation SSL/TLS doit rester désactivée sur l'ordinateur client (la validation d'approbation SSL/TLS est *désactivée* par défaut avec le chiffrement complet du disque). Avant l'*activation* de la validation d'approbation SSL/TLS sur l'ordinateur client, les conditions suivantes doivent être remplies :
  - Un certificat signé par une autorité racine comme EnTrust ou Verisign, doit être importé dans Dell Server.
  - La chaîne d'approbation complète du certificat doit être stockée dans le magasin de clés Microsoft de l'ordinateur client.
  - Pour *activer* la validation d'approbation SSL/TLS pour Dell Encryption Management, remplacez la valeur d'entrée de registre suivante par 0 sur l'ordinateur client.

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

    "DisableSSLCertTrust"=DWORD:0

    0 = Activé

    1 = Désactivé

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

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

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

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

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

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

  HKLM\SOFTWARE\Dell\Dell Data Protection\

  "SmartcardEnabled"=DWORD:1

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

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

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

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

  "SmartCardLogonNotify"=DWORD:1

  0 = Désactivé

  1 = Activé

- L'hôte Security Server peut être modifié pour qu'il soit différent de l'emplacement d'installation d'origine, au besoin. Les informations de l'hôte sont lues par l'ordinateur client à chaque fois qu'une interrogation de règles se produit. Modifiez la valeur de registre suivante sur l'ordinateur client :

HKLM\SYSTEM\CurrentControlSet\services\DellMgmtAgent

"ServerHost"=REG_SZ:<newname>.<organization>.com

- Le port du Security Server peut être modifié pour qu'il soit différent de l'emplacement d'installation d'origine, le cas échéant. Cette valeur est lue par l'ordinateur client à chaque fois qu'une interrogation de règles se produit. Modifiez la valeur de registre suivante sur l'ordinateur client :

  HKLM\SYSTEM\CurrentControlSet\services\DellMgmtAgent

  ServerPort=REG_SZ:8888

- (Avec l'authentification avant démarrage uniquement) Si vous **ne souhaitez pas** que PBA Advanced Authentication modifie les services associés aux cartes à puce et dispositifs biométriques selon un type de démarrage « automatique », désactivez la fonctionnalité de démarrage du service. La désactivation de cette fonction supprime également les avertissements associés aux services requis non exécutés.

  En cas de **désactivation**, PBA Advanced Authentication ne tente pas de démarrer ces services :

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

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

    [HKLM\SOFTWARE\DELL\Dell Data Protection]

    SmartCardServiceCheck=REG_DWORD:0

    0 = Activé

    1 = Désactivé

- Pour empêcher le chiffrement complet du disque de désactiver les fournisseurs d'informations d'identification tiers, créez la clé de registre suivante :

  HKLM\SOFTWARE\Dell\Dell Data Protection\

  "AllowOtherCredProviders" = DWORD:1

  0 = Désactivé (valeur par défaut)

  1 = Activé

  Remarque : cette valeur peut empêcher le fournisseur d'informations d'identification Dell de synchroniser correctement les informations d'identification à la suite de la désactivation des fournisseurs d'informations d'identification tiers. Assurez-vous que les appareils qui utilisent cette clé de registre peuvent communiquer correctement avec le serveur Dell.

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

  [HKEY_LOCAL_MACHINE\SOFTWARE\Dell\Dell Data Protection]

  "PbaToastersAllowClose" =DWORD:1

  0 = Activé (par défaut)

  1 = Désactivé

- Afin de permettre l'installation du chiffrement complet du disque avec le chiffrement basé sur les règles, la valeur de registre suivante doit être définie sur l'ordinateur client.

  [HKEY_LOCAL_MACHINE\SOFTWARE\Dell\Dell Data Protection]

  "EnableFDE" = DWORD: 1

  0 = Désactivé (valeur par défaut)

  1 = Activé

Advanced Threat Prevention

- Pour que le plug-in Advanced Threat Prevention surveille HKLM\SOFTWARE\Dell\Dell Data Protection pour détecter les modifications de la valeur LogVerbosity et mette à jour le niveau de journalisation client en conséquence, définissez la valeur suivante.

  [HKLM\Software\Dell\Dell Data Protection]

  "LogVerbosity"=DWORD:<see below>

  Dump: 0

  Fatal: 1

  Erreur 3

  Warning 5

  Info 10

  Verbose 12

  Trace 14

  Debug 15

  La valeur de registre est vérifiée lorsque le service Advanced Threat Prevention démarre ou à chaque fois que la valeur change. Si la valeur de registre n'existe pas, il n'y a pas de modification du niveau de journalisation.

  Utilisez ce paramètre de registre uniquement pour les tests/le débogage, car ce paramètre de registre contrôle la verbosité du log pour les autres composants, y compris Encryption et Encryption Management Agent.

- Le mode de compatibilité permet aux applications de s'exécuter sur l'ordinateur client alors que les règles « Protection de la mémoire » ou « Protection de la mémoire et contrôle des scripts » sont activées. L'activation du mode de compatibilité nécessite l'ajout d'une valeur de registre sur l'ordinateur client.

  Pour activer le mode de compatibilité, procédez comme suit :

  1. Dans la console de gestion, désactivez la règle *Protection de la mémoire activée*. Si la règle *Contrôle des scripts* est activée, désactivez-la.
  2. Ajoutez la valeur de registre CompatibilityMode.
     a. Dans l'Éditeur de registre de l'ordinateur client, accédez à `HKEY_LOCAL_MACHINE\SOFTWARE\Cylance\Desktop`.
     b. Effectuez un clic droit sur **Desktop**, cliquez sur **Permissions**, puis désignez-vous comme propriétaire et attribuez-vous le droit Contrôle total.
     c. Cliquer avec le bouton droit sur **Bureau**, puis choisissez **NouvelleValeur binaire**.
     d. Pour le nom, saisissez `CompatibilityMode`.
     e. Ouvrez le paramètre de registre et changez la valeur en `01`.
     f. Cliquez sur **OK**, puis fermez l'Éditeur de registre.

     Pour ajouter la valeur de registre à l'aide d'une commande, vous pouvez exécuter l'une des options de ligne de commande suivantes sur l'ordinateur client :

     - (Pour un seul ordinateur) Psexec :

       ```
       psexec -s reg add HKEY_LOCAL_MACHINE\SOFTWARE\Cylance\Desktop /v
       CompatibilityMode /t REG_BINARY /d 01
       ```

     - (Pour plusieurs ordinateurs) Commande Invoke-Command :

       ```
       $servers = "testComp1","testComp2","textComp3"

       $credential = Get-Credential -Credential {UserName}\administrator

       Invoke-Command -ComputerName $servers -Credential $credential -ScriptBlock {New-Item
       -Path HKCU:\Software\Cylance\Desktop -Name CompatibilityMode -Type REG_BINARY -Value
       01}
       ```

  3. Dans la console de gestion, réactivez la règle *Protection de la mémoire activée*. Si la règle *Contrôle des scripts* était précédemment activée, réactivez-la.

SED Manager

- Pour définir l'intervalle entre les tentatives lorsque le Dell Server n'est pas en mesure de communiquer avec SED Manager, ajoutez la valeur de registre suivante.

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

  "CommErrorSleepSecs"=DWORD:300

  Cette valeur correspond au nombre de secondes pendant lesquelles SED Manager tente de contacter le Dell Server si celui-ci est indisponible pour communiquer. La valeur par défaut est de 300 secondes (5 minutes).

- Si un certificat auto-signé est utilisé sur le Dell Server pour SED Manager, la validation d'approbation SSL/TLS doit rester désactivée sur l'ordinateur client (la validation d'approbation SSL/TLS est *désactivée* par défaut avec SED Manager). Avant l'*activation* de la validation d'approbation SSL/TLS sur l'ordinateur client, les conditions suivantes doivent être remplies :
  - Un certificat signé par une autorité racine comme EnTrust ou Verisign, doit être importé dans Dell Server.
  - La chaîne d'approbation complète du certificat doit être stockée dans le magasin de clés Microsoft de l'ordinateur client.
  - Pour *activer* la validation d'approbation SSL/TLS pour SED Manager, modifiez la valeur d'entrée de registre suivante sur 0 sur l'ordinateur client :

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

    "DisableSSLCertTrust"=DWORD:0

    0 = Activé

    1 = Désactivé

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

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

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

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

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

  HKLM\SOFTWARE\Dell\Dell Data Protection\

  "SmartcardEnabled"=DWORD:1

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

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

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

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

  "SmartCardLogonNotify"=DWORD:1

  0 = Désactivé

  1 = Activé

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

  HKLM\SOFTWARE\Dell\Dell Data Protection\

  "AllowOtherCredProviders" = DWORD:1

  0 = Désactivé (valeur par défaut)

  1 = Activé

  Remarque : cette valeur peut empêcher le fournisseur d'informations d'identification Dell de synchroniser correctement les informations d'identification à la suite de la désactivation des fournisseurs d'informations d'identification tiers. Assurez-vous que les appareils qui utilisent cette clé de registre peuvent communiquer correctement avec le serveur Dell.

- Pour définir l'intervalle selon lequel SED Manager tente de contacter le Dell Server lorsqu'il ne peut pas communiquer, définissez la valeur suivante sur l'ordinateur cible :

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

  "CommErrorSleepSecs"=DWORD Value:300

  Cette valeur correspond au nombre de secondes pendant lesquelles SED Manager tente de contacter le Dell Server si celui-ci est indisponible pour communiquer. La valeur par défaut est de 300 secondes (5 minutes).

- L'hôte Security Server peut être modifié pour qu'il soit différent de l'emplacement d'installation d'origine, au besoin. Les informations de l'hôte sont lues chaque fois qu'une interrogation de règles se produit. Modifiez la valeur de registre suivante sur l'ordinateur client :

  HKLM\SYSTEM\CurrentControlSet\services\DellMgmtAgent

  "ServerHost"=REG_SZ:<newname>.<organization>.com

- Le port du Security Server peut être modifié pour qu'il soit différent de l'emplacement d'installation d'origine, le cas échéant. Cette valeur est lue chaque fois qu'une interrogation de règles se produit. Modifiez la valeur de registre suivante sur l'ordinateur client :

  HKLM\SYSTEM\CurrentControlSet\services\DellMgmtAgent

  ServerPort=REG_SZ:8888

- L'URL du Security Server peut être modifiée pour qu'elle soit différente de l'emplacement d'installation d'origine, le cas échéant. Cette valeur est lue par l'ordinateur client à chaque fois qu'une interrogation de règles se produit. Modifiez la valeur de registre suivante sur l'ordinateur client :

  HKLM\SYSTEM\CurrentControlSet\services\DellMgmtAgent

  "ServerUrl"=REG_SZ:https://<newname>.<organization>.com:8888/agent

- (Avec l'authentification avant démarrage uniquement) Si vous **ne souhaitez pas** que PBA Advanced Authentication modifie les services associés aux cartes à puce et dispositifs biométriques selon un type de démarrage « automatique », désactivez la fonctionnalité de démarrage du service. La désactivation de cette fonction supprime également les avertissements associés aux services requis non exécutés.

  En cas de **désactivation**, PBA Advanced Authentication ne tente pas de démarrer ces services :

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

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

    [HKLM\SOFTWARE\DELL\Dell Data Protection]

    SmartCardServiceCheck=REG_DWORD:0

    0 = Activé

    1 = Désactivé

- Pour utiliser des cartes à puce avec l'authentification PBA SED, vous devez définir la valeur de registre suivante sur l'ordinateur client équipé d'un SED.

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

  "MSSmartcardSupport"=DWORD:1

  Définissez la règle Méthode d'authentification sur Carte à puce dans la console de gestion, puis validez la modification.

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

  [HKEY_LOCAL_MACHINE\SOFTWARE\Dell\Dell Data Protection]

  "PbaToastersAllowClose" =DWORD:1

  0 = Activé (par défaut)

1 = Désactivé

BitLocker Manager

- Si un certificat auto-signé est utilisé sur le Dell Server pour BitLocker Manager, la validation d'approbation SSL/TLS doit rester désactivée sur l'ordinateur client (la validation d'approbation SSL/TLS est *désactivée* par défaut avec BitLocker Manager). Avant l'*activation* de la validation d'approbation SSL/TLS sur l'ordinateur client, les conditions suivantes doivent être remplies :
  - Un certificat signé par une autorité racine comme EnTrust ou Verisign, doit être importé dans Dell Server.
  - La chaîne d'approbation complète du certificat doit être stockée dans le magasin de clés Microsoft de l'ordinateur client.
  - Pour *activer* la validation d'approbation SSL/TLS pour BitLocker Manager, définissez la valeur d'entrée de registre suivante sur 0 sur l'ordinateur client.

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

    "DisableSSLCertTrust"=DWORD:0

    0 = Activé

    1 = Désactivé
  - Pour empêcher BitLocker Manager de détecter les disques amovibles en tant que disques fixes, ajoutez la clé de registre suivante :

    HKLM\Software\Dell\Dell Data Protection\

    "UseEncryptableVolumeType" = DWORD:1

    0 = Désactivé (valeur par défaut)

    1 = Activé

4

Installation à l'aide du programme d'installation principal

- Les commutateurs et les paramètres de ligne de commande sont sensibles à la casse.
- Pour procéder à une installation de ports autres que ceux par défaut, utilisez les programmes d'installation enfants au lieu du programme d'installation principal.
- Les fichiers journaux du programme d'installation principal d'Endpoint Security Suite Enterprise se trouvent sur `C:\ProgramData\Dell\Dell Data Protection\Installer`.

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

- Dirigez les utilisateurs vers les documents suivants et les fichiers d'aide en cas de besoin au moment de l'application :
  - Pour apprendre à utiliser les fonctionnalités d'Encryption, reportez-vous à l' *Aide concernant Dell Encrypt*. Accédez à l'aide à partir de `<Install dir>\Program Files\Dell\Dell Data Protection\Encryption\Help`.
  - Voir l'*Encryption External Media* pour apprendre à utiliser les fonctionnalités d'Encryption External Media. Accédez à l'aide à partir de `<Install dir>\Program Files\Dell\Dell Data Protection\Encryption\EMS`.
  - Voir l'Aide d'*Endpoint Security Suite Enterprise* pour savoir comment utiliser les fonctions de et d'Advanced Threat Prevention. Accédez à l'aide à partir de `<Install dir>\Program Files\Dell\Dell Data Protection\Client Security Framework\Help`.
- Après l'installation, l'utilisateur doit mettre à jour ses règles en faisant un clic droit sur l'icône Dell Encryption située dans la zone de notification et en sélectionnant **Rechercher les mises à jour des règles**.
- Le programme d'installation principal installe la totalité de la suite de produits. Il existe deux méthodes d'installation à l'aide du programme d'installation principal. Choisissez l'une des options suivantes :
  - Installation interactive à l'aide du programme d'installation principal

  ou

  - Installation par la ligne de commande à l'aide du programme d'installation principal

Installation interactive à l'aide du programme d'installation principal

- Le programme d'installation principal d'Endpoint Security Suite Enterprise est disponible à l'emplacement suivant :
  - **À partir de votre compte FTP de Dell :** localisez le lot d'installation Endpoint-Security-Suite-Ent-1.x.x.xxx.zip.
- Ces instructions permettent d'installer ou de mettre à jour de manière interactive Dell Endpoint Security Suite Enterprise à l'aide du programme d'installation principal d'Endpoint Security Suite Enterprise. Cette méthode peut être utilisée pour installer la suite de produits sur un ordinateur à la fois.

1. Localisez **DDSSuite.exe** sur le support d'installation Dell. Copiez-le sur l'ordinateur local.
2. Double-cliquez sur **DDSSuite.exe** pour lancer le programme d'installation. Cela peut prendre quelques minutes.
3. Cliquez sur **Suivant** sur l'écran Bienvenue.
4. Lisez le contrat de licence, acceptez-en les termes, puis cliquez sur **Suivant**.
5. Dans le champ *Nom du serveur Dell local*, saisissez le nom d'hôte complet du serveur Dell pour gérer l'utilisateur cible.

   Saisissez les valeurs de port dans *Port du serveur principal* et *Port du serveur de sécurité* si votre organisation n'utilise pas des ports standards.

   Cliquez sur **Suivant.**

6. Cliquez sur **Suivant** pour installer le produit à l'emplacement par défaut `C:\Program Files\Dell\Dell Data Protection\. Dell recommends installing in the default location only`. Dell recommande de procéder à l'installation uniquement à l'emplacement par défaut pour éviter les problèmes qu'une installation dans un autre emplacement pourrait provoquer.
7. Sélectionnez les composants à installer.

   Security Framework installe le cadre de sécurité sous-jacent.

   BitLocker Manager permet d'installer le client BitLocker Manager, conçu pour optimiser la sécurité des déploiements BitLocker Manager en simplifiant et réduisant le coût de possession grâce à une gestion centralisée des règles de chiffrement de BitLocker.

   Encryption permet d'installer le client Encryption, un composant qui applique les règles de sécurité, qu'un ordinateur soit connecté au réseau, déconnecté du réseau, perdu ou volé.

   Advanced Threat Prevention permet d'installer le client Advanced Threat Prevention, une protection antivirus de nouvelle génération qui utilise la science des algorithmes et l'apprentissage automatique pour identifier, classifier et prévenir les cybermenaces connues ou inconnues et les empêcher d'exécuter ou d'endommager les points de terminaison.

   Web Protection et Firewall installe la protection Web et le pare-feu. Client Firewall vérifie tout le trafic entrant et sortant par rapport à sa liste de règles. La protection du navigateur Web et des téléchargements pour identifier des menaces et exécuter un ensemble d'actions par règle lorsqu'une menace est détectée, en fonction des évaluations des sites Web.

   Encryption External Media installe le composant qui applique Encryption External Media.

   Chiffrement complet du disque installe le composant qui applique le chiffrement complet du disque.

   Cliquez sur **Suivant** lorsque vos sélections sont terminées.
8. Cliquez sur **Installer** pour démarrer l'installation. L'installation peut prendre plusieurs minutes.
9. Sélectionnez **Oui, je souhaite redémarrer mon ordinateur maintenant**, puis cliquez sur **Terminer**.

   L'installation est terminée.

Installation par la ligne de commande à l'aide du programme d'installation principal

- Les commutateurs doivent d'abord être spécifiés dans une installation par ligne de commande. D'autres paramètres figurent dans un argument transmis au commutateur `/v`.

Commutateurs

- Le tableau suivant décrit les commutateurs qui peuvent être utilisés avec le programme d'installation principal d'Endpoint Security Suite Enterprise.

  REMARQUE : Si votre entreprise nécessite l'utilisation de fournisseurs d'informations d'identification tiers, Encryption Management Agent doit être installé ou mis à niveau en utilisant le paramètre FEATURE=BLM ou FEATURE=BASIC.

Commutateur	Description
`/s`	Installation silencieuse
`/z`	Transmission des variables au fichier .msi dans DDSSuite.exe

Paramètres

- Le tableau suivant décrit les paramètres qui peuvent être utilisés avec le programme d'installation principal d'Endpoint Security Suite Enterprise. Le programme d'installation principal d'Endpoint Security Suite Enterprise ne peut pas exclure des composants individuels, mais peut recevoir des commandes permettant de spécifier quels composants doivent être installés.

Paramètre	Description
SUPPRESSREBOOT	Supprime le redémarrage automatique une fois l'installation terminée. Peut être utilisé en mode SILENCIEUX.
SERVEUR	Spécifie l'URL du Dell Server.
InstallPath	Spécifie le chemin de l'installation. Peut être utilisé en mode SILENCIEUX.
FONCTIONS	Spécifie les composants qui peuvent être installés en mode SILENCIEUX : ATP = Advanced Threat Prevention *uniquement* DE-ATP = Advanced Threat Prevention et Encryption. Il s'agit de l'installation par défaut si le paramètre FONCTIONNALITÉS n'est pas spécifié DE = Client Drive Encryption uniquement BLM = BitLocker Manager SED = SED Manager (Encryption Management Agent/Manager, pilotes PBA/GPE)(disponible uniquement lorsqu'il est installé sur le système d'exploitation d'une station de travail) ATP-WEBFIREWALL = Advanced Threat Prevention avec pare-feu client et protection Web DE-ATP-WEBFIREWALL = Encryption et Advanced Threat Prevention avec pare-feu client et protection Web **REMARQUE :** Les mises à niveau d'Encryption Enterprise ou à partir des versions antérieures à v1.4 Endpoint Security Suite Enterprise, ATP-WEBFIREWALL ou DE-ATP-WEBFIREWALL ***doivent*** être définis pour pouvoir installer le pare-feu client et la protection Web. Ne spécifiez pas ATP-WEBFIREWALL ou DE-ATP-WEBFIREWALL lors de l'installation d'un client que Dell Server doit gérer en mode Déconnecté.
BLM_ONLY=1	Doit être utilisé lorsque vous utilisez FEATURES=BLM dans la ligne de commande pour exclure le plug-in de SED Manager.

Exemples de ligne de commande

- Les paramètres de ligne de commande sont sensibles à la casse.
- (Sur le système d'exploitation d'une station de travail) Cet exemple correspond à l'installation de tous les composants en utilisant le programme d'installation principal d'Endpoint Security Suite Enterprise sur les ports standard, de façon silencieuse, à l'emplacement par défaut C:\Program Files\Dell\Dell Data Protection\ avec la configuration requise pour utiliser le Dell Server spécifié.

  ```
  "DDSSuite.exe" /s /z"\"SERVER=server.organization.com\""
  ```
- (Sur le système d'exploitation d'une station de travail) Cet exemple correspond à l'installation d'Advanced Threat Prevention et d'Encryption ***uniquement*** avec le programme d'installation principal d'Endpoint Security Suite Enterprise, sur des ports standard, de manière silencieuse, à l'emplacement par défaut C:\Program Files\Dell\Dell Data Protection\ et avec la configuration pour utiliser le Dell Server spécifié.

  ```
  "DDSSuite.exe" /s /z"\"SERVER=server.organization.com, FEATURES=DE-ATP\""
  ```
- (Sur le système d'exploitation d'une station de travail) Cet exemple correspond à l'installation d'Advanced Threat Prevention, d'Encryption et de SED Manager avec le programme d'installation principal d'Endpoint Security Suite Enterprise, sur des ports standard, de manière silencieuse, en supprimant le redémarrage, à l'emplacement par défaut C:\Program Files\Dell\Dell Data Protection\ et avec la configuration pour utiliser le Dell Server spécifié.

  ```
  "DDSSuite.exe" /s /z"\"SERVER=server.organization.com, FEATURES=ATP-SED,
  SUPPRESSREBOOT=1\""
  ```
- (Sur le système d'exploitation d'une station de travail) Cet exemple correspond à l'installation d'Advanced Threat Prevention, d'Encryption, de Web Protection et de Client Firewall avec le programme d'installation principal d'Endpoint Security Suite Enterprise, sur des ports standard, de manière silencieuse, à l'emplacement par défaut C:\Program Files\Dell\Dell Data Protection\ et avec la configuration pour utiliser le Dell Server spécifié.

  ```
  "DDSSuite.exe" /s /z"\"SERVER=server.organization.com, FEATURES=ATP-WEBFIREWALL\""
  ```
- (Sur le système d'exploitation d'un serveur) Cet exemple correspond à l'installation d'Advanced Threat Prevention et d'Encryption ***uniquement*** avec le programme d'installation principal d'Endpoint Security Suite Enterprise, sur des ports

standard, de manière silencieuse, à l'emplacement par défaut C:\Program Files\Dell\Dell Data Protection\ et avec la configuration pour utiliser le Dell Server spécifié.

```
"DDSSuite.exe" /s /z"\"SERVER=server.organization.com, FEATURES=DE-ATP\""
```

- (Sur le système d'exploitation d'un serveur) Cet exemple correspond à l'installation d'Advanced Threat Prevention, d'Encryption, de Web Protection et de Client Firewall avec le programme d'installation principal d'Endpoint Security Suite Enterprise, sur des ports standard, de manière silencieuse et à l'emplacement suivant par défaut `C:\Program Files\Dell\Dell Data Protection\`

```
"DDSSuite.exe" /s /z"\"SERVER=server.organization.com, FEATURES=DE-ATP-WEBFIREWALL\""
```

- (Sur le système d'exploitation d'un serveur) Cet exemple correspond à l'installation d'Advanced Threat Prevention ***uniquement*** avec le programme d'installation principal d'Endpoint Security Suite Enterprise, sur des ports standard, de manière silencieuse, à l'emplacement par défaut C:\Program Files\Dell\Dell Data Protection\ et avec la configuration pour utiliser le Dell Server spécifié.

```
"DDSSuite.exe" /s /z"\"SERVER=server.organization.com, FEATURES=ATP\""
```

- (Sur le système d'exploitation d'une station de travail) Cet exemple correspond à l'installation d'Advanced Threat Prevention, de BitLocker Manager et de la protection Web avec le programme d'installation principal d'Endpoint Security Suite Enterprise, sur des ports standard, de manière silencieuse, en supprimant le redémarrage, à l'emplacement par défaut `C:\Program Files\Dell\Dell Data Protection\` et avec la configuration pour utiliser le Dell Server spécifié.

```
"DDSSuite.exe" -y -gm2 /S /z"\"SERVER=server.domain.com, FEATURES=BLM-ATP-WEBFIREWALL, SUPPRESSREBOOT=1, BLM_ONLY=1\""
```

- (Sur le système d'exploitation d'un serveur) Cet exemple correspond à l'installation d'Encryption ***uniquement*** avec le programme d'installation principal d'Endpoint Security Suite Enterprise, sur des ports standard, de manière silencieuse, à l'emplacement par défaut C:\Program Files\Dell\Dell Data Protection\ et avec la configuration pour utiliser le Dell Server spécifié.

```
"DDSSuite.exe" /s /z"\"SERVER=server.organization.com, FEATURES=DE\""
```

5

Désinstaller le programme d'installation principal

- Dell recommande d'utiliser le programme de désinstallation de Data Security pour supprimer la suite Data Security.
- Chaque composant doit être désinstallé séparément, avant la désinstallation à l'aide du programme d'installation principal d'Endpoint Security Suite Enterprise. Les clients doit être désinstallée dans un **ordre spécifique pour éviter les échecs de désinstallation.**
- Suivez les instructions de la section Extraire les programmes d'installation enfants du programme d'installation principal pour obtenir les programmes d'installation enfants.
- Assurez-vous d'utiliser la même version du programme d'installation principal d'Endpoint Security Suite Enterprise (et des clients) pour la désinstallation et l'installation.
- Ce chapitre vous réfère à d'autres chapitres contenant des instructions *détaillées* sur le processus de 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 Encryption.
  2. Désinstallez Advanced Threat Prevention.
  3. Désinstallez le chiffrement complet du disque (cette opération désinstalle le Dell Encryption Management Agent, qui ne peut pas être désinstallé avant la désinstallation d'Advanced Threat Prevention).
  4. Désinstallez SED Manager (cette opération désinstalle le Dell Encryption Management Agent, qui ne peut pas être désinstallé avant la désinstallation d'Advanced Threat Prevention).
  5. Désinstaller BitLocker Manager
- Passez à l'étape Désinstallation à l'aide du programme d'installation principal.

Désinstallation du programme d'installation principal d'Endpoint Security Suite Enterprise

Maintenant que tous les clients individuels ont été désinstallés, le programme d'installation principal peut être désinstallé.

Désinstallation avec ligne de commande

- L'exemple suivant correspond à la désinstallation silencieuse du programme d'installation principal d'Endpoint Security Suite Enterprise.

  ```
  "DDSSuite.exe" /s /x
  ```

  Lorsque vous avez terminé, redémarrez l'ordinateur.

6

Installation à l'aide des programmes d'installation enfants

- Pour installer ou mettre à niveau chaque client individuellement, vous devez d'abord extraire les fichiers exécutables enfants du programme d'installation principal d'Endpoint Security Suite Enterprise, tel qu'indiqué dans la section Extraire les programmes d'installation enfants du programme d'installation principal.
- Les exemples de commande inclus dans cette section supposent que les commandes sont exécutées à partir de `C:\extracted`.
- 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.

  Remarque : le chiffrement basé sur les règles 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 `/l*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 l'élément setup.exe. Le contenu doit toujours être entouré de guillemets en texte brut.
`/s`	Mode Silencieux
`/x`	Mode Désinstallation

REMARQUE :

Avec `/v`, les options Microsoft par défaut sont disponibles. Pour obtenir la liste des options, reportez-vous à cet article.

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

Option	Signification
/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
/norestart	Suppression du redémarrage

- Dirigez les utilisateurs vers les documents suivants et les fichiers d'aide en cas de besoin au moment de l'application :
  - Pour apprendre à utiliser les fonctions d'Encryption, reportez-vous à *Dell Encrypt Help* (Aide concernant Dell Encrypt). Accédez à l'aide depuis `<Install dir>\Program Files\Dell\Dell Data Protection\Encryption\Help`.
  - Voir *Encryption External Media Help* (Aide concernant Encryption External Media) pour apprendre à utiliser les fonctions d'Encryption External Media. Accédez à l'aide depuis `<Install dir>:\Program Files\Dell\Dell Data Protection\Encryption\EMS`.
  - Reportez-vous à l'aide d'*Endpoint Security Suite Enterprise* pour savoir comment utiliser les fonctions de Advanced Threat Prevention. Accédez à l'aide depuis `<Install dir>\Program Files\Dell\Dell Data Protection\Client Security Framework\Help`.

Installer les pilotes

- Les pilotes et le micrologiciel de ControlVault, les lecteurs d'empreintes et les cartes à puce ne sont pas inclus dans les fichiers exécutables du programme d'installation principal Endpoint Security Suite Enterprise ou des programmes d'installation enfants. 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.
  - 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.

Installation d'Encryption

- Passez en revue les exigences d'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.
- Après l'installation, l'utilisateur doit mettre à jour ses règles en faisant un clic droit sur l'icône Dell Encryption située dans la zone de notification et en sélectionnant *Rechercher les mises à jour des règles*.
- Vous pouvez localiser le programme d'installation d'Encryption de la manière suivante :
  - **À partir de votre compte FTP Dell** : repérez le lot d'installation Endpoint-Security-SuiteEnt-1.x.x.xxx.zip, puis extrayez les programmes d'installation enfant depuis le programme d'installation principal. Après l'extraction, localisez le fichier dans `C:\extracted\Encryption`.
  - **REMARQUE :** Les journaux Dell Encryption n'indiquent pas si un espace disque insuffisant a provoqué l'échec de l'installation.

Installation par ligne de commande

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

Paramètres
SERVERHOSTNAME= <ServerName> (nom de domaine complet de Dell Server pour la réactivation)
POLICYPROXYHOSTNAME=<RGKName> (nom de domaine complet du proxy de la stratégie par défaut)
MANAGEDDOMAIN=<MyDomain> (domaine à utiliser pour le périphérique)
DEVICESERVERURL=<DeviceServerName/SecurityServerName> (utilisée pour l'activation, cette URL comprend généralement le nom du serveur, le port et xapi)
GKPORT=<NewGKPort> (port du contrôleur d'accès)
MACHINEID=<MachineName> (nom de l'ordinateur)
RECOVERYID=<RecoveryID> (identifiant de récupération)
REBOOT=ReallySuppress (Null permet les redémarrages automatiques, ReallySuppress désactive le redémarrage)
HIDEOVERLAYICONS=1 (0 active la superposition des icônes, 1 désactive la superposition des icônes)
HIDESYSTRAYICON=1 (0 active l'icône dans la zone de notification, 1 désactive l'icône dans la zone de notification)
ENABLE_FDE_LM=1 (Permet l'installation de Dell Encryption sur un ordinateur avec le chiffrement complet de disque actif)
EME=1 (Installez le mode Encryption External Media)

Pour obtenir la liste des commutateurs .msi de base et des options d'affichage pouvant être utilisés dans la ligne de commande, voir la section « Installation à l'aide des programmes d'installation enfants ».

- Le tableau suivant détaille les autres paramètres facultatifs liés à l'activation.

Paramètres
SLOTTEDACTIVATON=1 (0 désactive les activations retardées/planifiées, 1 active les activations retardées/planifiées)
SLOTINTERVAL=45,120 (planifie les activations par la notation x,x où la première valeur est la limite inférieure de la planification et la deuxième valeur est la limite supérieure, en secondes)
CALREPEAT=600 (doit correspondre à ou dépasser la limite maximale définie dans SLOTINTERVAL. Durée d'attente, en secondes, d'Encryption avant de générer une tentative d'activation en fonction de SLOTINTERVAL.)

Exemples de ligne de commande

REMARQUE : Remplacez`DEVICESERVERURL=https://server.organization.com:`**8081/xapi** (sans barre oblique à la fin) si la version de votre Security Management Server est antérieure à 7.7.

- L'exemple suivant correspond à l'installation de Dell Encryption avec les paramètres par défaut (Encryption, Encrypt for Sharing, pas de boîte de dialogue, pas de barre de progression, redémarrage automatique, installation à l'emplacement par défaut `C:\Program Files\Dell\Dell Data Protection\Encryption`).

```
DDPE_XXbit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com
POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION
DEVICESERVERURL=https://server.organization.com:8443/xapi/ /qn"
```

Commande MSI :

```
msiexec.exe /i "Dell Data Protection Encryption.msi" /qn REBOOT="ReallySuppress"
SERVERHOSTNAME="server.organization.com" POLICYPROXYHOSTNAME="rgk.organization.com"
MANAGEDDOMAIN="ORGANIZATION" DEVICESERVERURL="https://server.organization.com:8443/xapi/"
```

- L'exemple suivant correspond à l'installation d'Encryption et d'Encrypt for Sharing, avec masquage de l'icône Dell Encryption dans la zone de notification, masquage des icônes en transparence, aucune boîte de dialogue, aucune barre

de progression, suppression du redémarrage, installation à l'emplacement par défaut : `C:\Program Files\Dell\Dell Data Protection\Encryption`.

```
DDPE_XXbit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com
POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION
DEVICESERVERURL=https://server.organization.com:8443/xapi/ HIDESYSTRAYICON=1
HIDEOVERLAYICONS=1 REBOOT=ReallySuppress /qn"
```

Commande MSI :

```
msiexec.exe /i "Dell Data Protection Encryption.msi" /qn REBOOT="ReallySuppress"
SERVERHOSTNAME="server.organization.com" POLICYPROXYHOSTNAME="rgk.organization.com"
MANAGEDDOMAIN="ORGANIZATION" DEVICESERVERURL="https://server.organization.com:8443/xapi/"
HIDESYSTRAYICON="1" HIDEOVERLAYICONS="1"
```

Exemple de ligne de commande pour installer Encryption External Media uniquement

- Installation silencieuse, pas de barre de progression, redémarrage automatique, installation à l'emplacement par défaut `C:\Program Files\Dell\Dell Data Protection\Encryption`.

  ```
  DDPE_XXbit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com
  POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION
  DEVICESERVERURL=https://server.organization.com:8443/xapi/ EME=1 /qn"
  ```

  Commande MSI :

  ```
  msiexec.exe /i "Dell Data Protection Encryption.msi" /qn REBOOT="ReallySuppress"
  SERVERHOSTNAME="server.organization.com" POLICYPROXYHOSTNAME="rgk.organization.com"
  MANAGEDDOMAIN="ORGANIZATION" DEVICESERVERURL="https://server.organization.com:8443/xapi/"
  ```

- Installation silencieuse, pas de redémarrage, installation à l'emplacement par défaut `C:\Program Files\Dell\Dell Data Protection\Encryption`).

  ```
  DDPE_XXbit_setup.exe /s /v"EME=1
  SERVERHOSTNAME=server.organization.com POLICYPROXYHOSTNAME=rgk.organization.com
  DEVICESERVERURL=https://server.organization.com:8443/xapi/ MANAGEDDOMAIN=ORGANIZATION /
  norestart /qn"
  ```

  Commande MSI :

  ```
  msiexec.exe /i "Dell Data Protection Encryption.msi" /qn REBOOT="ReallySuppress" EME="1"
  SERVERHOSTNAME="server.organization.com" POLICYPROXYHOSTNAME="rgk.organization.com"
  DEVICESERVERURL="https://server.organization.com:8443/xapi/" MANAGEDDOMAIN="ORGANIZATION"
  ```

- **REMARQUE :**

  Sur le client, la section À propos affiche le numéro de version du logiciel, mais n'indique pas si Encryption (installation complète) ou uniquement Encryption External Media, a été installé. Pour localiser cette information, allez à `C:\ProgramData\Dell\Dell Data Protection\Encryption\CMGShield.log` et cherchez l'entrée suivante :

  [<date/timestamp> DeviceInfo: < >] ***Shield Information - SM=External Media Only***, SB=DELL, UNF=FQUN, last sweep={0, 0}

Exemple de ligne de commande pour convertir Encryption External Media en Encryption (installation complète)

REMARQUE : La conversion de Encryption External Media en Encryption (installation complète) n'est pas prise en charge avec les mises à niveau.

- Le déchiffrement n'est pas nécessaire pour convertir Encryption External Media en Encryption (installation complète).

  ```
  DDPE_XXbit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com
  POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION
  DEVICESERVERURL=https://server.organization.com:8443/xapi/ REINSTALL=ALL EME=0
  REINSTALLMODE=vamus /qn"
  ```

  Commande MSI :

  ```
  msiexec.exe /i "Dell Data Protection Encryption.msi" /qn REBOOT="ReallySuppress"
  SERVERHOSTNAME="server.organization.com" POLICYPROXYHOSTNAME="rgk.organization.com"
  MANAGEDDOMAIN="ORGANIZATION" DEVICESERVERURL="https://server.organization.com:8443/xapi/"
  REINSTALL="ALL" EME="0" REINSTALLMODE="vamus"
  ```

- **Exemple de ligne de commande pour installer Dell Encryption avec chiffrement complet du disque**

\Chiffrement

- L'exemple suivant correspond à l'installation de Dell Encryption avec les paramètres par défaut (Encryption, Encrypt for Sharing, pas de boîte de dialogue, pas de barre de progression, redémarrage automatique, installation à l'emplacement par défaut `C:\Program Files\Dell\Dell Data Protection\Encryption`).

  ```
  DDPE_XXbit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com
  POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION
  DEVICESERVERURL=https://server.organization.com:8443/xapi/ /qn"
  ```

  Puis :

  \Encryption Management Agent

  L'exemple suivant correspond à l'installation du chiffrement complet de disque géré à distance et permet l'installation sur un ordinateur protégé par Dell Encryption (installation silencieuse, pas de redémarrage, aucune entrée dans la liste Programmes du Panneau de configuration, installation à l'emplacement par défaut `C:\Program Files\Dell\Dell Data Protection\Encryption`).

  ```
  EMAgent_64bit_setup.exe /s /v"CM_EDITION=1 ENABLE_FDE_LM=1
  FEATURE=FDE SERVERHOST=server.organization.com SERVERPORT=8888
  SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443 ARPSYSTEMCOMPONENT=1 /
  norestart /qn"
  ```

- **Exemple de ligne de commande pour installer Encryption External Media et le chiffrement complet du disque.**

  \Chiffrement

  L'exemple suivant correspond à l'installation d'Encryption External Media avec installation silencieuse, pas de barre de progression, redémarrage automatique, installation à l'emplacement par défaut `C:\Program Files\Dell\Dell Data Protection\Encryption.`

  ```
  DDPE_XXbit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com
  POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION
  DEVICESERVERURL=https://server.organization.com:8443/xapi/ EME=1 /qn"
  ```

  Puis :

  \Encryption Management Agent

  L'exemple suivant installe le chiffrement complet du disque géré à distance et permet l'installation sur un ordinateur protégé Dell Encryption (installation silencieuse, pas de redémarrage, aucune entrée dans la liste Programmes du Panneau de configuration, installation à l'emplacement par défaut de `C:\Program Files\Dell\Dell Data Protection`).

  ```
  EMAgent_64bit_setup.exe /s /v"CM_EDITION=1 ENABLE_FDE_LM=1
  FEATURE=FDE SERVERHOST=server.organization.com SERVERPORT=8888
  SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443 ARPSYSTEMCOMPONENT=1 /
  norestart /qn"
  ```

- **Exemple de ligne de commande pour installer Encryption External Media sur une installation existante avec chiffrement complet du disque.**

  L'exemple suivant correspond à l'installation d'Encryption External Media sur une installation existante avec chiffrement complet du disque avec installation discrète, pas de barre de progression, redémarrage automatique et installation à l'emplacement par défaut `C:\Program Files\Dell\Dell Data Protection`.

  ```
  DDPE_XXbit_setup.exe /s /v"EME=1 SERVERHOSTNAME=server.organization.com
  POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION
  DEVICESERVERURL=https://server.organization.com:8443/xapi/ ENABLE_FDE_LM=1 /
  norestart /qn"
  ```

- **Exemple ligne de commande pour installer le client Encryption géré à distance sur une installation existante avec chiffrement complet du disque.**

  L'exemple suivant correspond à l'installation de Dell Encryption sur une installation existante du chiffrement complet de disque avec les paramètres par défaut (client Encryption, Encrypt for Sharing, pas de boîte de dialogue, pas de barre de progression, redémarrage automatique, installation à l'emplacement par défaut `C:\Program Files\Dell\Dell Data Protection\Encryption`) et logs d'installation sous `C:\Dell`. **Remarque :** pour que les logs puissent être générés correctement, le répertoire `C:\Dell` doit exister avant l'installation.

  ```
  DDPE_XXbit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com
  POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION
  ```

```
DEVICESERVERURL=https://server.organization.com:8443/xapi/ ENABLE_FDE_LM=1 /
norestart /qn /l*v C:\Dell\DellEncryptionInstall.log"
```

REMARQUE : il est possible que certaines versions anciennes nécessitent des caractères d'échappement \" autour des valeurs de paramètres. Par exemple :

DDPE_XXbit_setup.exe /v"CMG_DECRYPT=\"1\" CMGSILENTMODE=\"1\" DA_SERVER=\"server.organization.com\" DA_PORT=\"8050\" SVCPN=\"administrator@organization.com\" DA_RUNAS=\"domain\username\" DA_RUNASPWD=\"password\" /qn

Installer le chiffrement complet du disque

- Passez en revue les exigences pour le chiffrement complet du disque 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 d'approbation SSL/TLS.
- Les utilisateurs se connectent par l'intermédiaire de l'authentification avant démarrage au moyen de leur mot de passe Windows.

Installation par ligne de commande

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

Paramètres
CM_EDITION=1 (gestion à distance)
INSTALLDIR=(modifier la destination d'installation)
SERVERHOST=(securityserver.organization.com)
SERVERPORT=8888
SECURITYSERVERHOST=(securityserver.organization.com)
SECURITYSERVERPORT=8443
FEATURE=FDE
ENABLE_FDE_LM=1 <Permet l'installation du chiffrement complet du disque sur un ordinateur avec Dell Encryption actif>

Pour obtenir la liste des commutateurs .msi de base et des options d'affichage pouvant être utilisés dans la ligne de commande, voir la section « Installation à l'aide des programmes d'installation enfants ».

Exemples de ligne de commande

Encryption Management/Agent

- L'exemple suivant correspond à l'installation du chiffrement complet du disque géré à distance (installation silencieuse, pas de redémarrage et installation dans l'emplacement par défaut `C:\Program Files\Dell\Dell Data Protection\Encryption`).

```
EMAgent_64bit_setup.exe /s /v"CM_EDITION=1 FEATURE=FDE SERVERHOST=server.organization.com
SERVERPORT=8888 SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443 /
norestart /qn"
```

- **Encryption Management/Agent**
- L'exemple suivant correspond à l'installation du chiffrement complet du disque géré à distance et permet l'installation sur un ordinateur protégé par Dell Encryption (installation silencieuse, pas de redémarrage, installation à l'emplacement par défaut `C:\Program Files\Dell\Dell Data Protection\Encryption`).

```
EMAgent_64bit_setup.exe /s /v"CM_EDITION=1 ENABLE_FDE_LM=1
FEATURE=FDE SERVERHOST=server.organization.com SERVERPORT=8888
SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443 /norestart /qn"
```

- **Exemple de ligne de commande pour installer le chiffrement complet du disque et Encryption External Media.**

  Cryptage

  L'exemple suivant correspond à l'installation d'Encryption External Media avec installation silencieuse, pas de barre de progression, redémarrage automatique, installation à l'emplacement par défaut `C:\Program Files\Dell\Dell Data Protection\Encryption`.

  ```
  DDPE_XXbit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com
  POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION
  DEVICESERVERURL=https://server.organization.com:8443/xapi/ EME=1 /qn"
  ```

  Puis :

  Encryption Management/Agent

  L'exemple suivant correspond à l'installation du chiffrement complet de disque géré à distance et permet l'installation sur un ordinateur protégé par Dell Encryption (installation silencieuse, pas de redémarrage, aucune entrée dans la liste Programmes du Panneau de configuration, installation à l'emplacement par défaut `C:\Program Files\Dell\Dell Data Protection\Encryption`).

  ```
  EMAgent_64bit_setup.exe /s /v"CM_EDITION=1 ENABLE_FDE_LM=1
  FEATURE=FDE SERVERHOST=server.organization.com SERVERPORT=8888
  SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443 /norestart /qn"
  ```

Installer Encryption sur un système d'exploitation de serveur

Il existe deux méthodes pour installer Encryption sur un système d'exploitation de serveur. Sélectionnez l'une des méthodes suivantes :

- Installer Encryption sur un système d'exploitation de serveur de façon interactive

  Encryption sur un système d'exploitation de serveur peut être installé manière interactive uniquement sur les ordinateurs dotés d'un système d'exploitation de serveur. L'installation sur des ordinateurs dotés d'un système d'exploitation non-serveur doit être effectuée via la ligne de commande, en spécifiant le paramètre SERVERMODE=1.

- Installer Encryption sur un système d'exploitation de serveur à l'aide de la ligne de commande

Compte d'utilisateur virtuel

- Dans le cadre de l'installation, un **compte d'utilisateur de serveur virtuel** est créé ; il sera exclusivement utilisé par Encryption sur un système d'exploitation de serveur. L'authentification DPAPI et le mot de passe sont désactivés : seul l'utilisateur du serveur virtuel peut accéder aux clés de chiffrement.

Avant de commencer

- Le compte de l'utilisateur qui exécute l'installation doit correspondre à un utilisateur de domaine doté de droits de niveau Administrateur.
- Pour ignorer la configuration requise ou pour exécuter Encryption sur un système d'exploitation de serveur sur des serveurs hors domaine ou multidomaines, définissez la propriété *ssos.domainadmin.verify* sur *false* dans le fichier application.properties. Le fichier est stocké dans les chemins de fichier suivants, en fonction du serveur Dell Server que vous utilisez :

  Security Management Server - *<rép installation>*/Security Server/conf/application.properties

  Security Management Server Virtual - /opt/dell/server/security-server/conf/application.properties

- Le serveur doit prendre en charge les contrôles de port.

  Les règles du système de contrôle de port affectent le support amovible des serveurs protégés, en contrôlant par exemple l'accès et l'utilisation des ports USB du serveur par des périphériques USB. La règle du port USB s'applique aux ports USB externes. La fonction du port USB interne n'est pas affectée par la règle du port USB. Si la règle du port USB est désactivée,

le clavier et la souris USB ne fonctionnent pas et l'utilisateur n'est pas en mesure d'utiliser l'ordinateur à moins qu'une connexion du bureau à distance soit définie avant l'application de la règle.

- Pour que l'activation réussisse, l'ordinateur doit avoir accès à une connexion réseau.
- Lorsque le module TPM (Trusted Platform Module) est disponible, il est utilisé pour sceller la clé GPK (General Purpose Key, clé générale) sur le matériel Dell. Si le module TPM n'est pas disponible, l'API Microsoft Data Protection (DPAPI) est utilisée pour protéger la clé GPK.

  Lors de l'installation d'un nouveau système d'exploitation sur un ordinateur Dell avec module TPM qui exécute Server Encryption, effacez le TPM dans le BIOS. Reportez-vous à cet article pour obtenir des instructions.
- Le fichier log de l'installation se trouve dans le répertoire %temp% de l'utilisateur, à savoir `C:\Users\<user name>\AppData\Local\Temp`. Pour localiser le fichier log approprié, recherchez un nom de fichier qui commence par MSI et finit par l'extension .log. Le fichier inclut un horodatage de date/heure qui correspond à l'heure à laquelle le programme d'installation a été exécuté.
- Encryption n'est pas pris en charge sur des serveurs qui font partie de DFS (distributed file systems).

Extraction du programme d'installation enfant

- Pour installer Encryption sur un système d'exploitation de serveur, vous devez d'abord extraire le programme d'installation enfant (**DDPE_xxbit_setup.exe**) du programme d'installation principal. Voir Extraire les programmes d'installation enfants du programme d'installation principal.

Installation interactive

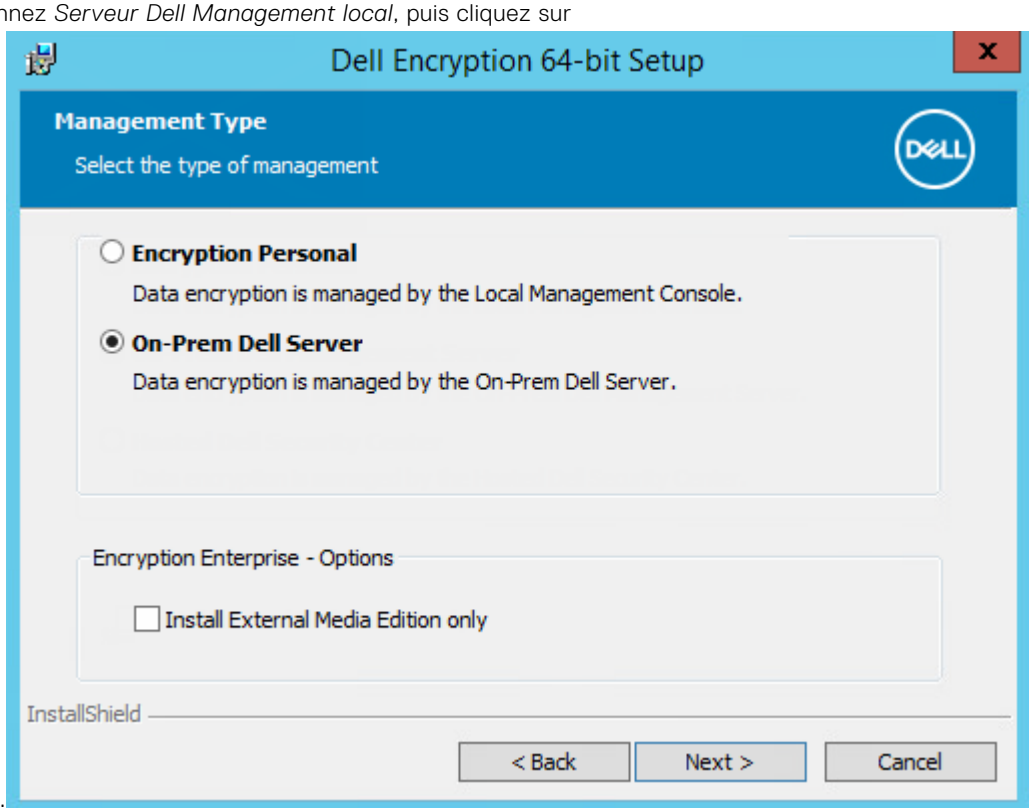
- Utilisez ces instructions pour installer Encryption sur un système d'exploitation de serveur de façon interactive. Ce programme d'installation comprend les composants requis pour le chiffrement au niveau logiciel.

1. Localisez **DDPE_XXbit_setup.exe** dans le dossier `C:\extracted\Encryption`. Copiez-le sur l'ordinateur local.
2. Si vous installez Encryption sur un système d'exploitation de serveur, double-cliquez sur **DDPE_XXbit_setup.exe** pour lancer le programme d'installation.

   REMARQUE :

   Lorsque Encryption sur un système d'exploitation de serveur est installé sur un ordinateur qui exécute un système d'exploitation de serveur tel que Windows Server 2012 R2, le programme d'installation installe automatiquement Encryption en SERVERMODE.
3. Dans le dialogue d'accueil, cliquez sur **Suivant.**
4. Sur l'écran Contrat de Licence, lisez le contrat de licence, acceptez-en les termes, puis cliquez sur **Suivant**.

5. Sélectionnez *Serveur Dell Management local*, puis cliquez sur **Suivant**.



6. Cliquez sur **Suivant** pour effectuer l'installation à l'emplacement par défaut.
7. Cliquez sur **Suivant** pour ignorer la boîte de dialogue *Type de gestion*.
8. Dans le champ *Nom Security Management Server*, entrez/validez le nom d'hôte complet de Dell Server pour gérer l'utilisateur cible (par exemple, *server.organization.com)*.

   Entrez le nom de domaine dans *Domaine géré* (par exemple, « entreprise »). Cliquez sur **Suivant**.
9. Dans le nom d'hôte et le port Proxy de règles, entrez/validez les informations et cliquez sur **Suivant**.
10. Dans l'URL du serveur du périphérique, entrez/validez les informations et cliquez sur **Suivant**.
11. Cliquez sur **Installer** pour démarrer l'installation.

    L'installation peut prendre quelques minutes.
12. Une fois la configuration terminée, cliquez sur **Terminer**.

    L'installation est terminée.
13. Redémarrez l'ordinateur. Dell recommande de mettre en attente le redémarrage uniquement s'il vous faut du temps pour enregistrer votre travail et fermer les applications. Le cryptage ne pourra commencer que lorsque l'ordinateur aura redémarré.

Installation à l'aide de la ligne de commande

Recherche du programme d'installation dans `C:\extracted\Encryption`

- Utilisez **DDPE_xxbit_setup.exe** pour une installation ou mise à niveau par installation scriptée, à l'aide de fichiers batch ou toute autre technologie Push disponible dans votre entreprise.

Commutateurs

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

Commutateur	Signification
/v	Transmission des variables au fichier .msi dans DDPE_XXbit_setup.exe

Commutateur	Signification
/a	Installation administrateur
/s	Mode Silencieux

Paramètres

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

Composant	Fichier journal	Paramètres de ligne de commande
Tous	/l*v [chemin-complet][nom-fichier].log *	SERVERHOSTNAME=<Security Management Server Name>
		SERVERMODE=1
		POLICYPROXYHOSTNAME=<RGK Name>
		MANAGEDDOMAIN=<My Domain>
		DEVICESERVERURL=<Activation Server Name>
		GKPORT=<New GK Port>
		MACHINEID=<Machine Name>
		RECOVERYID=<Recovery ID>
		REBOOT=ReallySuppress
		HIDEOVERLAYICONS=1
		HIDESYSTRAYICON=1
		EME=1

REMARQUE :

Le redémarrage peut être supprimé, mais il sera nécessaire à la fin du processus. Le cryptage ne pourra commencer que lorsque l'ordinateur aura redémarré.

Options

Le tableau suivant détaille les options d'affichage que vous pouvez spécifier à la fin de l'argument transmis au commutateur /v.

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

Option	Signification
REMARQUE : N'utilisez pas **/q** et **/qn** dans la même ligne de commande. Utilisez uniquement « **!** » et « - » après **/qb**.	

- Le paramètre de ligne de commande SERVERMODE=1 est respecté uniquement lors d'une nouvelle installation. Le paramètre est ignoré lors des désinstallations.
- Si une valeur contient un ou plusieurs caractères spéciaux, comme un espace, placez-la entre guillemets avec caractères d'échappement.
- Le paramètre DEVICESERVERURL est sensible à la casse.

Exemple d'installation par ligne de commande

- L'exemple suivant permet d'installer Encryption en mode système d'exploitation de serveur avec les paramètres par défaut (Encryption, installation silencieuse, Encrypt for Sharing, pas de boîte de dialogue, pas de barre de progression, redémarrage automatique, installation à l'emplacement par défaut `C:\Program Files\Dell\Dell Data Protection`).

  ```
  DDPE_XXbit_setup.exe /s /v"SERVERMODE=1 SERVERHOSTNAME=server.organization.com
  POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION
  DEVICESERVERURL=https://server.organization.com:8443/xapi/ /qn"
  ```

  Commande MSI :

  ```
  msiexec.exe /i "Dell Data Protection Encryption.msi" /qn
  REBOOT="ReallySuppress" SERVERMODE="1" SERVERHOSTNAME="server.organization.com"
  POLICYPROXYHOSTNAME="rgk.organization.com" MANAGEDDOMAIN="ORGANIZATION"
  DEVICESERVERURL="https://server.organization.com:8443/xapi/"
  ```

- L'exemple suivant permet d'installer Encryption en mode système d'exploitation de serveur avec un fichier log et les paramètres par défaut (Encryption, installation silencieuse, Encrypt for Sharing, pas de boîte de dialogue, pas de barre de progression, pas de redémarrage, installation à l'emplacement par défaut `C:\Program Files\Dell\Dell Data Protection\Encryption`), et précise un nom de fichier log personnalisé finissant par un numéro (DDP_ssos-090.log) qui doit être incrémenté si la ligne de commande est exécutée plusieurs fois sur le même serveur. Pour placer les fichiers journaux à un autre emplacement que l'emplacement par défaut (le dossier du fichier exécutable), vous devez spécifier le chemin complet dans la commande. Par exemple, la commande /l*v C:\Logs\DDP_ssos-090.log crée les logs d'installation dans C:\Logs.

  ```
  DDPE_XXbit_setup.exe /s /v"SERVERMODE=1 SERVERHOSTNAME=server.organization.com
  POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION
  DEVICESERVERURL=https://server.organization.com:8443/xapi/ /l*v DDP_ssos-090.log /
  norestart/qn"
  ```

  Commande MSI :

  ```
  msiexec.exe /i "Dell Data Protection Encryption.msi" /qn SERVERMODE="1"
  SERVERHOSTNAME="server.organization.com" POLICYPROXYHOSTNAME="rgk.organization.com"
  MANAGEDDOMAIN="ORGANIZATION" DEVICESERVERURL="https://server.organization.com:8443/
  xapi/" /l*v DDP_ssos-090.log /norestart/qn"
  ```

Redémarrez l'ordinateur après l'installation. Dell recommande de mettre en attente le redémarrage uniquement s'il vous faut du temps pour enregistrer votre travail et fermer les applications. Le cryptage ne pourra commencer que lorsque l'ordinateur aura redémarré.

Activer

- Vérifiez que le nom d'ordinateur du serveur est bien le nom de point de terminaison à afficher dans la console de gestion.
- Pour l'activation initiale, un utilisateur interactif doté d'informations d'identification d'administrateur de domaine doit se connecter au serveur au moins une fois. L'utilisateur connecté peut être de n'importe quel type : membre du domaine ou non, connecté en mode Bureau à distance ou utilisateur interactif sur le serveur. Cependant, l'activation exige des informations d'identification d'administrateur de domaine.
- Une fois le redémarrage après installation terminé, la boîte de dialogue d'activation s'affiche. L'administrateur doit entrer ses références d'administrateur de domaine et préciser un nom d'utilisateur au format UPN (Nom principal utilisateur). Le chiffrement des systèmes d'exploitation de serveur ne s'active pas automatiquement.
- Pendant l'activation initiale, un compte d'utilisateur de serveur virtuel est créé. Après l'activation initiale, l'ordinateur est redémarré afin que l'activation des périphériques puisse commencer.

- Au cours de la phase d'authentification et d'activation des périphériques, un ID d'ordinateur unique est attribué à l'ordinateur, des clés de cryptage sont créées et regroupées en jeux de clés, et une relation est établie entre le jeu de clés de cryptage et l'utilisateur du serveur virtuel. Ce jeu de clés de cryptage associe les clés et les règles de cryptage au nouvel utilisateur de serveur virtuel, afin de créer une relation solide entre les données cryptées, l'ordinateur concerné et l'utilisateur du serveur virtuel. Après l'activation du périphérique, l'utilisateur du serveur virtuel apparaît dans la console de gestion sous la mention « UTILISATEUR-SERVEUR@<*fully qualified server name*>. Pour plus d'informations sur l'activation, voir la section « Activation sur un système d'exploitation serveur ».

REMARQUE :

Si vous renommez le serveur après l'activation, son nom d'affichage ne change pas dans la console de gestion. Toutefois, si le chiffrement des systèmes d'exploitation de serveur est de nouveau activé après que vous avez renommé le serveur, le nouveau nom du serveur s'affiche dans la console de gestion.

La boîte de dialogue Activation s'affiche une seule fois à chaque redémarrage pour inviter l'utilisateur à activer Encryption sur un système d'exploitation de serveur. Pour effectuer l'activation, procédez comme suit :

1. Connectez-vous au serveur, directement sur ce serveur ou avec Connexion de Bureau à distance.
2. Entrez le nom d'utilisateur d'un administrateur de domaine au format UPN, ainsi que le mot de passe, puis cliquez sur **Activer**. La même boîte de dialogue Activation s'affiche à chaque nouveau démarrage du système non activé.

   Dell Server émet une clé de cryptage pour l'ID d'ordinateur, crée le **compte d'utilisateur de serveur virtuel** et une clé de cryptage pour ce compte d'utilisateur, regroupe les clés en un jeu de clés de cryptage, puis crée la relation entre le jeu de clés de cryptage et le compte d'utilisateur de serveur virtuel.

3. Cliquez sur **Fermer**.

   Après l'activation, le cryptage commence.

4. Une fois le balayage de cryptage terminé, redémarrez l'ordinateur pour traiter tous les fichiers précédemment en cours d'utilisation. Ceci constitue une étape importante à effectuer pour des raisons de sécurité.

   REMARQUE :

   Si la règle *Sécuriser les informations d'identification Windows* est activée, Encryption sur systèmes d'exploitation de serveur chiffre les fichiers du dossier `\Windows\system32\config`, y compris les informations d'identification Windows. Les fichiers du dossier `\Windows\system32 \config` sont chiffrés même si la règle *Cryptage SDE activé* est désactivée. Par défaut, la règle *Sécuriser les informations d'authentification Windows* est sélectionnée.

   REMARQUE :

   Après le redémarrage de l'ordinateur, l'authentification avec la clé de chiffrement commune exige *toujours* la clé d'ordinateur du serveur protégé. Dell Server renvoie une clé de déverrouillage pour accéder aux clés de chiffrement et aux règles dans le coffre (les clés et les règles sont pour le serveur, pas pour l'utilisateur). Sans la clé d'ordinateur du serveur, la clé de chiffrement commune ne peut pas être déverrouillée et l'ordinateur ne peut pas recevoir les mises à jour des règles.

Confirmation de l'activation

Sur la console locale, ouvrez la boîte de dialogue **À propos** pour vérifier que Encryption sur systèmes d'exploitation de serveur est installé, authentifié et en mode Serveur. Si l'ID du client Encryption est **rouge**, cela signifie que le chiffrement n'a pas encore été activé.

Utilisateur de serveur virtuel

- Dans la console de gestion, un serveur protégé peut être identifié grâce au nom de son ordinateur. De plus, chaque serveur protégé possède son propre d'utilisateur de serveur virtuel. Chaque compte est doté d'un nom d'utilisateur statique unique et d'un nom d'ordinateur unique.
- Le compte d'utilisateur de serveur virtuel est utilisé uniquement par Encryption sur systèmes d'exploitation de serveur. Sinon, il est transparent pour le fonctionnement du serveur protégé. L'utilisateur de serveur virtuel est associé au jeu de clés de cryptage et à la règle proxy.
- Après l'activation, le compte d'utilisateur de serveur virtuel est le compte d'utilisateur qui est activé et associé au serveur.
- Après l'activation du compte de l'utilisateur de serveur virtuel, toutes les notifications de connexion/déconnexion du serveur sont ignorées. Au lieu de cela, au cours du démarrage, l'ordinateur s'authentifie automatiquement auprès de l'utilisateur de serveur virtuel, puis télécharge la clé d'ordinateur depuis le Dell Server.

Installer le client Advanced Threat Prevention

- **REMARQUE :** Si votre entreprise nécessite l'utilisation de fournisseurs d'informations d'identification tiers, Encryption Management Agent doit être installé ou mis à niveau en utilisant le paramètre FEATURE=BLM ou FEATURE=BASIC.

  REMARQUE : Avant d'installer Advanced Threat Prevention, les dossiers de destination pour l'installation et les journaux doivent être créés.

- Les programmes d'installation doivent être exécuté dans un ordre spécifique. Si vous ne suivez pas la bonne séquence d'installation des composants, l'installation échoue. Exécutez les programmes d'installation dans l'ordre suivant :

1. **(Sous un système d'exploitation de station de travail uniquement)** \Encryption Management Agent : Advanced Threat Prevention nécessite Encryption Management Agent.

   (Sous un système d'exploitation serveur uniquement) Composant Dell Encryption Management Agent, tel qu'illustré dans la section Installation depuis la ligne de commande.

2. Client Advanced Threat Prevention, tel qu'illustré dans la section Installation depuis la ligne de commande.
3. Plug-in Advanced Threat Prevention, tel qu'illustré dans la section Installation depuis la ligne de commande.

- Vous pouvez récupérer le programme d'installation du client Advanced Threat Prevention de la manière suivante :
  - **À partir de votre compte FTP Dell** - Repérez le lot d'installation Endpoint-Security-Suite-Ent-2.x.x.xxx.zip, puis extrayez les programmes d'installation enfants depuis le programme d'installation principal. Après l'extraction, localisez le fichier dans `C:\extracted\Advanced Threat Prevention\WinXXR\` et `C:\extracted\Advanced Threat Prevention\WinNtAll\`.
- Le programme d'installation d'Encryption Management Agent se trouve à l'adresse suivante :
  - **À partir de votre compte FTP Dell** - Repérez le lot d'installation Endpoint-Security-Suite-Ent-2.x.x.xxx.zip, puis extrayez les programmes d'installation enfants depuis le programme d'installation principal. Après l'extraction, localisez le fichier dans `C:\extracted\Encryption Management Agent`.

Installation par ligne de commande

- Des commandes .msi de base sont disponibles pour l'installation.
- Le tableau suivant indique les paramètres disponibles dans le cadre de l'installation.

Paramètres
CM_EDITION=1 <remote management>
INSTALLDIR=<change the installation destination>
SERVER=<securityserver.organization.com>
SERVERPORT=8888
SECURITYSERVERHOST=<securityserver.organization.com>
SECURITYSERVERPORT=8443
ARPSYSTEMCOMPONENT=1 <no entry in the Control Panel Programs list>
REBOOT=ReallySuppress <suppresses the reboot>
FEATURE=BASIC <***requis*** sur le système d'exploitation d'un serveur ; peut également être utilisé sur le système d'exploitation d'un poste de travail ; empêche l'installation des plugin de gestion SED et BitLocker Manager>

Pour obtenir la liste des commutateurs .msi de base et des options d'affichage pouvant être utilisés dans la ligne de commande, voir la section « Installation à l'aide des programmes d'installation enfants ».

Exemples de ligne de commande

- L'exemple suivant correspond à l'installation d'Encryption Management Agent de base, sans la gestion SED ni BitLocker Manager (installation silencieuse, pas de redémarrage, aucune entrée dans la liste Programmes du Panneau de configuration, installation à l'emplacement par défaut `C:\Program Files\Dell\Dell Data Protection`).

  ```
  EMAgent_XXbit_setup.exe /s /v"FEATURE=BASIC
  CM_EDITION=1 SERVERHOST=server.organization.com SERVERPORT=8888
  SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443 ARPSYSTEMCOMPONENT=1 /
  norestart /qn"
  ```

- L'exemple suivant correspond à l'installation d'Advanced Threat Prevention (installation silencieuse, pas de redémarrage, fichier journal d'installation et dossier d'installation aux emplacements spécifiés)

  ```
  MSIEXEC.EXE /I "ATP_CSF_Plugins_x64.msi" /qn REBOOT="ReallySuppress" APPFOLDER="C:
  \Program Files\Dell\Dell Data Protection\Advanced Threat Prevention\Plugins"
  ARPSYSTEMCOMPONENT="1" /l*v "C:\ProgramData\Dell\Dell Data Protection\Installer
  Logs\ATP_Plugins_x64.msi.log"
  ```

  et

  ```
  "\Advanced Threat Prevention\WinNtAll\ATP_AgentSetup.exe" /s EXTRACT_INSTALLERS /v"/qb!"
  ```

REMARQUE : ces composants doivent uniquement être installés avec la ligne de commande. Double-cliquer pour installer ce composant installe une version non-Dell, non gérée du produit, qui n'est pas prise en charge. Si cela est effectué par inadvertance, allez à Ajouter/Supprimer des programmes et désinstallez cette version.

Exemple de script

L'exemple suivant correspond à l'installation d'Advanced Threat Prevention sans la gestion SED ni BitLocker Manager (installation silencieuse, pas de redémarrage, aucune entrée dans la liste Programmes du Panneau de configuration, installation à l'emplacement par défaut `C:\Program Files\Dell\Dell Data Protection`).

:: Installation d'Encryption Management Agent

".\Encryption Management Agent\EMAgent_64bit_setup.exe" /s /v" FEATURE=BASIC CM_EDITION=1 SERVERHOST=%SERVER% SERVERPORT=8888 SECURITYSERVERHOST=%SERVER% SECURITYSERVERPORT=8443 ARPSYSTEMCOMPONENT=1 /norestart /qn"

:: Installation des plug-ins ATP

MSIEXEC.EXE /I "Advanced Threat Prevention\Win64R\ATP_CSF_Plugins_x64.msi" /qn REBOOT=ReallySuppress APPFOLDER="C:\Program Files\Dell\Dell Data Protection\Advanced Threat Prevention\Plugins" ARPSYSTEMCOMPONENT=1 /l*v "C:\ProgramData\Dell\Dell Data Protection\Installer Logs\ATP_CSF_Plugins_x64.msi.log"

:: Installation d'Advanced Threat Prevention

".\Advanced Threat Prevention\WinNtAll\ATP_AgentSetup.exe" /s EXTRACT_INSTALLERS /v"/qb!"

Installation des clients du pare-feu client et de la protection Web

- Envisagez de vérifier les exigences du pare-feu client et de la protection Web avant l'installation.
- **REMARQUE :** Si votre entreprise nécessite l'utilisation de fournisseurs d'informations d'identification tiers, Encryption Management Agent doit être installé ou mis à niveau en utilisant le paramètre FEATURE=BLM ou FEATURE=BASIC.

  REMARQUE : Encryption Management Agent **doit** être installé avant de procéder à l'installation du pare-feu client et de la protection Web.

  REMARQUE : Les répertoires de sortie **doivent** exister avant l'exécution des commandes ci-dessous.

- Les programmes d'installation doivent être exécuté dans un ordre spécifique. Si vous ne suivez pas la bonne séquence d'installation des composants, l'installation échoue. Exécutez les programmes d'installation dans l'ordre décroissant dans l'installation par ligne de commande.

  Les commandes de programmes d'installation enfants **doivent** être exécutées à partir de leurs répertoires d'extraction, sinon un problème se produira.

Installation par ligne de commande

- Le tableau suivant indique les paramètres disponibles pour le fichier **`EnsMgmtSdkInstaller.exe`**.

Paramètres	Description
LoadCert	Charger le certificat dans le répertoire spécifié.
InstallSDK	Installe le SDK à l'emplacement spécifié.
RemoveRightClick	Supprime l'option de menu clic droit pour les utilisateurs.
RemoveMcTray	Supprime la zone de notification.

- Le tableau suivant indique les paramètres disponibles pour le fichier **`EPsetup.exe`**.

Paramètres	Description
ADDLOCAL="fw,wc"	Identifie les modules à installer : fw=Client Firewall wc=Web Protection
override"hips"	Ne pas installer Host Intrusion Prevention
INSTALLDIR	Emplacement d'installation autre que par défaut
/nocontentupdate	Avertit le programme d'installation de ne pas mettre à jour le contenu des fichiers automatiquement au cours du processus d'installation. Dell recommande la planification d'une mise à jour dès que l'installation est terminée.
/nopreservesettings	N'enregistre pas les paramètres.

- Le tableau suivant indique les paramètres disponibles pour le fichier **`DellThreatProtection.msi`**.

Paramètres	Description
Reboot=ReallySuppress	Supprime le redémarrage.
ARP	0=Aucune entrée dans Ajout/Suppression de programmes 1=Entrée dans Ajout/Suppression de programmes

Pour effectuer une installation ou une mise à niveau, utilisez le flux de travail suivant :

- **Exemples de ligne de commande**

  \Threat Protection\EndPointSecurity

  L'exemple suivant correspond à l'installation de Web Protection et Client Firewall à l'aide de paramètres par défaut (mode silencieux, installer Client Firewall et Web Protection, remplacer Host Intrusion Prevention, pas de mise à jour du contenu, pas de paramètres enregistrés avec des fichiers journaux sous C:\ProgramData\Dell\Dell Data Protection).

  ```
  ".\Threat Protection\EndPointSecurity\EPsetup.exe" ADDLOCAL="fw,wc" /override"hips" /
  nocontentupdate /qb! /L*v"C:\ProgramData\Dell\Dell Data Protection\Installer Logs\"
  ```

  Puis :

  \Threat Protection\ThreatProtection\WinXXR

- L'exemple suivant correspond à l'installation du client à l'aide de paramètres par défaut (supprimer le redémarrage, pas de boîte de dialogue, pas de barre de progression, pas d'entrée dans la liste des programmes du panneau de configuration).

  ```
  "Threat Protection\ThreatProtection\WinXXR\DellThreatProtection.msi" /qn
  REBOOT=ReallySuppress ARPSYSTEMCOMPONENT=1
  ```

  Puis :

\Threat Protection\SDK

- La ligne de commande suivante correspond au chargement des paramètres par défaut du certificat.

  ```
  "Threat Protection\SDK\EnsMgmtSdkInstaller.exe" -LoadCert >"C:\ProgramData\Dell\Dell Data Protection\Installer Logs\McAfeeSDKInstallerBeforeEndPoint.log"
  ```

  Puis :

  \Threat Protection\SDK

- L'exemple suivant permet d'installer le SDK.

  ```
  "Threat Protection\SDK\EnsMgmtSDKInstaller.exe" -InstallSDK -RemoveRightClick -RemoveMcTray >> "<OUTPUTDIRECTORY>\McAfeeSDKInstallerAfterEndPoint.log"
  ```

Installation de SED Manager et PBA Advanced Authentication

- Passez en revue les exigences SED 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 d'approbation SSL/TLS.
- Les utilisateurs se connectent par l'intermédiaire de l'authentification avant démarrage au moyen de leur mot de passe Windows.
- Les programmes d'installation de SED Manager et PBA Advanced Authentication peuvent se trouver à l'adresse suivante :
  - **À partir de votre compte FTP Dell** : repérez le lot d'installation Endpoint-Security-Suite-Ent-2.x.x.xxx.zip, puis extrayez les programmes d'installation enfant depuis le programme d'installation principal. Après l'extraction, localisez le fichier dans `C:\extracted\Encryption Management Agent`.

Installation par ligne de commande

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

Paramètres
CM_EDITION=1 <remote management>
INSTALLDIR=<change the installation destination>
SERVER=<securityserver.organization.com>
SERVERPORT=8888
SECURITYSERVERHOST=<securityserver.organization.com>
SECURITYSERVERPORT=8443
ARPSYSTEMCOMPONENT=1 <no entry in the Control Panel Programs list>

Pour obtenir la liste des commutateurs .msi de base et des options d'affichage pouvant être utilisés dans la ligne de commande, voir la section « Installation à l'aide des programmes d'installation enfants ».

Les exemples de commande suivants permettent d'installer ou de mettre à niveau Encryption Management Agent.

Exemples de ligne de commande

\Encryption Management Agent

- L'exemple suivant correspond à l'installation de SED Manager, d'Encryption Management Agent et de la console de sécurité locale gérés à distance (installation silencieuse, pas de redémarrage, aucune entrée dans la liste Programmes du Panneau de configuration, installation à l'emplacement par défaut `C:\Program Files\Dell\Dell Data Protection\Encryption`).

```
EMAgent_XXbit_setup.exe /s /v"CM_EDITION=1 SERVERHOST=server.organization.com
SERVERPORT=8888 SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443
ARPSYSTEMCOMPONENT=1 /norestart /qn"
```

Installer BitLocker Manager

- **REMARQUE :** Si votre entreprise nécessite l'utilisation de fournisseurs d'informations d'identification tiers, Encryption Management Agent doit être installé ou mis à niveau en utilisant le paramètre FEATURE=BLM ou FEATURE=BASIC.

- Passez en revue les conditions requises du client BitLocker Manager si votre organisation utilise un certificat signé par une autorité racine telle que EnTrust ou Verisign. Une modification de paramètre de registre est nécessaire sur l'ordinateur client pour activer la validation d'approbation SSL/TLS.
- Les programmes d'installation du client BitLocker Manager se trouvent à l'adresse suivante :
  - **À partir de votre compte FTP Dell** : repérez le lot d'installation Endpoint-Security-Suite-Ent-2.x.x.xxx.zip, puis extrayez les programmes d'installation enfant depuis le programme d'installation principal. Après l'extraction, localisez le fichier dans `C:\extracted\Encryption Management Agent`.

Installation avec ligne de commande

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

Paramètres
CM_EDITION=1 <remote management>
INSTALLDIR=<change the installation destination>
SERVER=<securityserver.organization.com>
SERVERPORT=8888
SECURITYSERVERHOST=<securityserver.organization.com>
SECURITYSERVERPORT=8443
FEATURE=BLM <install BitLocker Manager only>
FEATURE=BLM,SED <install BitLocker Manager with SED>
ARPSYSTEMCOMPONENT=1 <no entry in the Control Panel Programs list>

Pour obtenir la liste des commutateurs .msi de base et afficher les options utilisables dans les lignes de commande, reportez-vous à Installer à l'aide des programmes d'installation enfants.

Exemple de ligne de commande

- L'exemple suivant correspond à l'installation de BitLocker Manager seulement (installation silencieuse, pas de redémarrage, pas d'entrée dans la liste des Programmes du panneau de configuration, installation à l'emplacement par défaut `C:\Program Files\Dell\Dell Data Protection`).

  ```
  EMAgent_XXbit_setup.exe /s /v"CM_EDITION=1 SERVERHOST=server.organization.com
  SERVERPORT=8888 SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443
  FEATURE=BLM /norestart /qn"
  ```

- L'exemple suivant correspond à l'installation de BitLocker Manager avec SED (installation silencieuse, pas de redémarrage, pas d'entrée dans la liste des Programmes du panneau de configuration, installation à l'emplacement par défaut `C:\Program Files\Dell\Dell Data Protection`).

  ```
  EMAgent_XXbit_setup.exe /s /v"CM_EDITION=1 SERVERHOST=server.organization.com
  SERVERPORT=8888 SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443
  FEATURE=BLM,SED /norestart /qn"
  ```

- **Exemple de ligne de commande pour installer BitLocker Manager et Dell Encryption**

  L'exemple suivant correspond à l'installation de BitLocker Manager seulement (installation silencieuse, pas de redémarrage, pas d'entrée dans la liste des Programmes du panneau de configuration, installation à l'emplacement par défaut `C:\Program Files\Dell\Dell Data Protection`).

  ```
  EMAgent_XXbit_setup.exe /s /v"CM_EDITION=1 SERVERHOST=server.organization.com
  SERVERPORT=8888 SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443
  FEATURE=BLM /norestart /qn"
  ```

  Puis :

  L'exemple suivant correspond à l'installation du client avec les paramètres par défaut (client Encryption, Encrypt for Sharing, pas de boîte de dialogue, pas de barre d'avancement, redémarrage automatique, installation à l'emplacement par défaut : `C:\Program Files\Dell\Dell Data Protection`).

  ```
  DDPE_XXbit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com
  POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION
  DEVICESERVERURL=https://server.organization.com:8443/xapi/ /qn"
  ```

7

Désinstaller à l'aide des programme d'installation enfants

- Dell recommande d'utiliser le programme de désinstallation de Data Security pour supprimer la suite Data Security.
- Pour désinstaller chaque client individuellement, vous devez d'abord extraire les fichiers exécutables enfant du programme d'installation principal d'Endpoint Security Suite Enterprise ; tel qu'indiqué dans la section Extraire les programmes d'installation enfants du programme d'installation principal. Sinon, exécutez une installation administrative pour extraire le fichier .msi.
- Assurez-vous que la version de client utilisée pour la désinstallation est identique à celle utilisée pour l'installation.
- 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 des fichiers journaux de désinstallation du programme d'installation enfant 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 standard .msi peut être utilisée pour créer un fichier journal à l'aide de /l `C:\<any directory>\<any log file name>.log`. Dell recommande de ne pas utiliser la consignation détaillée « /l*v » dans une désinstallation avec ligne de commande, car le nom d'utilisateur/mot de passe est enregistré dans le fichier journal.

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

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

Commutateur	Signification
/v	Transmission des variables au fichier .msi dans l'élément setup.exe. Le contenu doit toujours être entouré de guillemets en texte brut.
/s	Mode Silencieux
/x	Mode Désinstallation
/a	Installation administrative (copie tous les fichiers dans le fichier .msi)

REMARQUE :

Avec /v, les options Microsoft par défaut sont disponibles. Pour obtenir la liste des options, voir https://msdn.microsoft.com/en-us/library/windows/desktop/aa367988(v=vs.85).aspx.

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

Option	Signification
/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

Désinstallation de Web Protection et Firewall

Si Web Protection et Firewall ne sont pas installés, procédez à la désinstallation du client Encryption.

Désinstallation avec ligne de commande

- Après son extraction du programme d'installation principal Endpoint Security Suite Enterprise, le programme d'installation client Web Protection et Firewall est disponible sur `C:\extracted\Dell Threat Protection\ThreatProtection\WinXXR\DellThreatProtection.msi`.
- Rendez-vous dans la section Ajoute/Supprimer des programmes dans le panneau de configuration et désinstallez les composants suivants dans cet ordre :
  - McAfee Endpoint Security Firewall
  - McAfee Endpoint Security Web Control
  - McAfee Agent
- Puis :
- L'exemple suivant désinstalle Web Protection et Firewall.

```
MSIEXEC.EXE /x "DellThreatProtection.msi"
```

Désinstallation d'Advanced Threat Prevention

Désinstallation de ligne de commande

- L'exemple suivant illustre la désinstallation du client Advanced Threat Prevention. ***Vous devez exécuter cette commande à partir d'une invite de commande d'administration.***

  ```
  wmic path win32_product WHERE (CAPTION LIKE "%%CYLANCE%%") call uninstall
  ```

  Arrêtez et redémarrez l'ordinateur, puis désinstallez le composant Dell Encryption Management Agent.

- **REMARQUE :** Si vous avez installé le client SED ou activé l'authentification avant démarrage, suivez les instructions de désinstallation de la section Désinstaller le client SED.

  L'exemple suivant désinstalle uniquement le composant Dell Encryption Management Agent, et non le client SED.

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

Installez le chiffrement complet du disque

- La désactivation de l'authentification avant démarrage requiert une connexion réseau au Dell Server.

Processus

- Désactivation de l'authentification avant démarrage, ce qui supprime toutes les données d'authentification avant démarrage de l'ordinateur et déverrouille les clés de chiffrement complet du disque.
- Désinstallez le chiffrement complet du disque.

Désactiver l'authentification avant démarrage

1. Connectez-vous à la console de gestion en tant qu'administrateur Dell.
2. Dans le volet de gauche, cliquez sur **Populations** > **Points de terminaison**.
3. Sélectionnez le type de point final approprié.
4. Sélectionnez Afficher >*Visible*, *Masqué*, ou *Tout*.
5. Si vous connaissez le nom d'hôte de l'ordinateur, saisissez-le dans le champ Nom d'hôte (les jokers sont pris en charge). Pour afficher tous les ordinateurs, laissez ce champ vide. Cliquez sur **Rechercher**.

   Si vous ne connaissez pas le nom d'hôte, faites défiler la liste des ordinateurs disponibles afin d'identifier celui qui vous intéresse.

   Selon le filtre de recherche utilisé, un ordinateur ou une liste d'ordinateurs s'affiche.
6. Sélectionnez le nom d'hôte de l'ordinateur souhaité.
7. Cliquez sur **Règles de sécurité** sur le menu supérieur.
8. Sélectionnez le **chiffrement complet du disque** dans le groupe de **Chiffrement Windows**.
9. Passez le **chiffrement complet du disque** et la stratégie de *On* sur ***Off***.
10. Cliquez sur **Enregistrer**.
11. Dans le volet de gauche, cliquez sur la bannière **Valider les règles**.
12. Cliquez sur **Valider les règles**.

    Attendez que la règle se propage du Dell Server à l'ordinateur cible de la désactivation.

    Désinstallez le chiffrement complet du disque et PBA Advanced Authentication une fois que l'authentification avant démarrage est désactivée.

Installation d'un client de chiffrement complet du disque

Désinstallation avec ligne de commande

- Après son extraction du programme d'installation principal, le chiffrement complet du disque est disponible à l'emplacement `C:\extracted\Encryption Management Agent\EMAgent_XXbit_setup.exe`.
  - L'exemple suivant permet de désinstaller silencieusement le chiffrement complet du disque.

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

    Après avoir terminé, éteignez et redémarrez l'ordinateur.

Désinstallation de SED Manager

- La désactivation de l'authentification avant démarrage requiert une connexion réseau au Dell Server.

Processus

- Désactivation de l'authentification avant démarrage, ce qui supprime toutes les données d'authentification avant démarrage de l'ordinateur et déverrouille les clés SED.
- Désinstallez SED Manager

Désactiver l'authentification avant démarrage

1. Connectez-vous à la console de gestion en tant qu'administrateur Dell.
2. Dans le volet de gauche, cliquez sur **Populations** > **Points de terminaison**.
3. Sélectionnez le type de point final approprié.
4. Sélectionnez Afficher >*Visible*, *Masqué*, ou *Tout*.
5. Si vous connaissez le nom d'hôte de l'ordinateur, saisissez-le dans le champ Nom d'hôte (les jokers sont pris en charge). Pour afficher tous les ordinateurs, laissez ce champ vide. Cliquez sur **Rechercher**.

   Si vous ne connaissez pas le nom d'hôte, faites défiler la liste des ordinateurs disponibles afin d'identifier celui qui vous intéresse.

   Selon le filtre de recherche utilisé, un ordinateur ou une liste d'ordinateurs s'affiche.
6. Sélectionnez le nom d'hôte de l'ordinateur souhaité.
7. Cliquez sur **Règles de sécurité** sur le menu supérieur.
8. Sélectionnez **Disques à cryptage automatique** à partir de la page **Catégorie de règle**.
9. Modifiez le **lecteur à cryptage automatique (SED)** et la règle en passant de `On` à ***`Off`***.
10. Cliquez sur **Enregistrer**.
11. Dans le volet de gauche, cliquez sur la bannière **Valider les règles**.
12. Cliquez sur **Valider les règles**.

    Attendez que la règle se propage du Dell Server à l'ordinateur cible de la désactivation.

    Désinstallez SED Manager et PBA Advanced Authentication une fois que l'authentification avant démarrage est désactivée.

Désinstaller le client SED

Désinstallation avec ligne de commande

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

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

    Après avoir terminé, éteignez et redémarrez l'ordinateur.

Désinstaller Encryption et Encryption sur système d'exploitation de serveur

- Pour réduire la durée du décryptage, lancez l'Assistant Nettoyage de disque Windows qui supprimera les fichiers temporaires et toute autre donnée inutile.
- 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.
- Lorsque la désinstallation est terminée alors que le décryptage est toujours en cours, désactivez toute connectivité réseau. Sinon, de nouvelles règles peuvent être acquises et réactiver le cryptage.
- Suivez votre processus actuel de décryptage des données (envoi d'une mise à jour de règle, par exemple).
- Encryption et Encryption External Media mettent à jour le Dell Server pour faire passer le statut à *Non protégé* au début du processus de désinstallation d'un client. Toutefois, lorsque le client ne peut pas contacter le Dell Server, quelle qu'en soit la raison, le statut ne peut pas être mis à jour. Dans ce cas, vous devez *supprimer le point de terminaison* manuellement dans la console de gestion. Si votre organisation utilise ce workflow à des fins de conformité, Dell recommande de vérifier que le statut *Non protégé* a été défini correctement, dans la console de gestion ou dans les rapports gérés.

Processus

- **Avant de lancer la désinstallation**, voir (Facultatif) Créer un fichier journal de Encryption Removal Agent. Ce fichier journal permet de diagnostiquer les erreurs, si vous rencontrez un problème lors de la désinstallation / du déchiffrement Si vous ne souhaitez pas déchiffrer les fichiers à la désinstallation, il n'est pas nécessaire de créer un fichier journal Encryption Removal Agent.
- Le Key Server (et Security Management Server) doit être configuré avant de procéder à la désinstallation si on utilise l'option **Télécharger les clés d'Encryption Removal Agent depuis un serveur**. Voir Configuration du Key Server pour procéder à la désinstallation du client Encryption activé auprès de Security Management Server pour obtenir les instructions. Aucune action préalable n'est nécessaire si le client à désinstaller est activé auprès d'un Security Management Server Virtual, car le Security Management Server Virtual n'utilise pas le Key Server.
- Vous devez utiliser l'utilitaire Dell Administrative Utility (CMGAd) avant de lancer Encryption Removal Agent si vous utilisez l'option **Importer les clés d'Encryption Removal Agent depuis un fichier**. Cet utilitaire est utilisé pour l'obtention du paquet de clés de cryptage. Reportez-vous à Utiliser l'utilitaire de téléchargement administratif (CMGAd) pour obtenir des instructions. L'utilitaire est disponible sur le support d'installation Dell.
- Exécutez WSScan pour vous assurer que toutes les données sont dédéchiffrée une fois la désinstallation terminée, mais avant de redémarrer l'ordinateur. Reportez-vous à Utiliser WSScan pour obtenir des instructions.
- A intervalles réguliers, Vérifiez l'état de l'agent Encryption Removal. Le déchiffrement de données est encore en cours si le service Encryption Removal Agent existe encore dans le panneau de services.

Désinstallation avec ligne de commande

- Après son extraction du programme d'installation principal d'Endpoint Security Suite Enterprise, le programme d'installation d'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 : 3 - Utiliser le bundle LSARecovery 2 - Utiliser les clés d'analyse approfondie précédemment téléchargées 1 : télécharger les clés depuis Dell Server 0 : ne pas installer Encryption Removal Agent
CMGSILENTMODE	Propriété permettant d'activer la désinstallation silencieuse : 1 - Silencieux : requis lors de l'exécution avec des variables msiexec contenant /q ou /qn 0 - Non silencieux : possible uniquement lorsque les variables msiexec contenant /q ne sont pas présentes dans la syntaxe de ligne de commande
Propriétés requises	
DA_KM_PATH	Chemin d'accès complet à l'ensemble de clés.
DA_KM_PW	Mot de passe défini sur l'ensemble de clés.
DA_SERVER	FQHN pour le Security Management Server hébergeant la session de négociation.
DA_PORT	Port sur Security Management Server pour requête (la valeur par défaut est 8050).

Paramètre	Sélection
SVCPN	Nom d'utilisateur au format UPN employé par le service Key Server pour se connecter comme sur Security Management Server.
DA_RUNAS	Nom d'utilisateur dans un format compatible SAM, dans le contexte duquel la demande d'extraction de clé est exécutée. Cet utilisateur doit être répertorié dans la liste des comptes Key Server, dans Security Management Server.
DA_RUNASPWD	Mot de passe de l'utilisateur d'exécution
FORENSIC_ADMIN	Compte administrateur d'analyse approfondie sur Dell Server, qui peut être utilisé pour des demandes d'analyse approfondie, des désinstallations ou des clés.
FORENSIC_ADMIN_PWD	Mot de passe du compte d'administrateur d'analyse approfondie.
Propriétés facultatives	
SVCLOGONUN	Nom d'utilisateur au format UPN pour le paramètre Connexion en tant que service Encryption Removal Agent.
SVCLOGONPWD	Mot de passe pour se connecter en tant qu'utilisateur.

- L'exemple suivant correspond à la désinstallation silencieuse d'Encryption et au téléchargement des clés de chiffrement depuis Security Management Server.

  ```
  DDPE_XXbit_setup.exe /s /x /v"CMG_DECRYPT=1 CMGSILENTMODE=1
  DA_SERVER=server.organization.com DA_PORT=8050 SVCPN=administrator@organization.com
  DA_RUNAS=domain\username DA_RUNASPWD=password /qn"
  ```

  Commande MSI :

  ```
  msiexec.exe /s /x "Dell Data Protection Encryption.msi" /qn REBOOT="ReallySuppress"
  CMG_DECRYPT="1" CMGSILENTMODE="1" DA_SERVER="server.organization.com" DA_PORT="8050"
  SVCPN="administrator@domain.com" DA_RUNAS="domain\username" DA_RUNASPWD="password" /qn
  ```

  Lorsque vous avez terminé, redémarrez l'ordinateur.

- L'exemple suivant correspond à la désinstallation silencieuse d'Encryption et au téléchargement des clés de chiffrement à l'aide d'un compte de l'administrateur d'analyse approfondie.

  ```
  DDPE_XXbit_setup.exe /s /x /v"CMG_DECRYPT=1 CMGSILENTMODE=1
  FORENSIC_ADMIN=forensicadmin@organization.com FORENSIC_ADMIN_PWD=tempchangeit /qn"
  ```

  Commande MSI :

  ```
  msiexec.exe /s /x "Dell Data Protection Encryption.msi" /qn
  CMG_DECRYPT=1 CMGSILENTMODE=1 FORENSIC_ADMIN=forensicadmin@organization.com
  FORENSIC_ADMIN_PWD=tempchangeit REBOOT=REALLYSUPPRESS
  ```

  Lorsque vous avez terminé, redémarrez l'ordinateur.

- L'exemple suivant correspond à la désinstallation silencieuse d'Encryption à l'aide de clés pré-téléchargées disponibles sur C:\Users\administrator\Desktop\Admin\ avec le mot de passe d'administrateur d'analyse approfondie et l'écriture de journaux au chemin C:\SheildUninstall.

  ```
  DDPE_XXbit_setup.exe /s /x /v"CMG_DECRYPT=2 CMGSILENT=1 DA_KM_PATH=C:
  \Users\administrator\Desktop\Admin\<HOSTNAME>.bin DA_KM_PW=qwert12345 /l*v c:
  \ShieldUninstall.log /qn /norestart"
  ```

  Commande de module MSI

```
msiexec.exe /s /x "Dell Data Protection Encryption.msi" CMG_DECRYPT=2 CMGSILENT=1
DA_KM_PATH=C:\Users\administrator\Desktop\Admin\<HOSTNAME>.bin DA_KM_PW=qwert12345 /l*v
c:\ShieldUninstall.log /qn /norestart
```

REMARQUE :

Dell recommande les actions suivantes lors de l'utilisation d'un mot de passe d'administrateur d'analyse approfondie sur la ligne de commande :

1. crée un compte d'administrateur d'analyse approfondie sur la console de gestion, dans le but d'effectuer la désinstallation silencieuse ;
2. utilise un mot de passe temporaire, applicable uniquement à ce compte et pendant cette période.
3. retire le compte temporaire de la liste des administrateurs ou en modifie le mot de passe une fois la désinstallation silencieuse terminée.

Il est possible que quelques anciens clients nécessitent des caractères d'échappement \" autour des valeurs de paramètres. Par exemple :

```
DDPE_XXbit_setup.exe /x /v"CMG_DECRYPT=\"1\"
CMGSILENTMODE=\"1\" DA_SERVER=\"server.organization.com\" DA_PORT=\"8050\"
SVCPN=\"administrator@organization.com\" DA_RUNAS=\"domain\username\"
DA_RUNASPWD=\"password\" /qn"
```

Désinstaller BitLocker Manager

Désinstallation avec ligne de commande

- Après son extraction du programme d'installation principal d'Endpoint Security Suite Enterprise, le programme d'installation de BitLocker Manager se trouve dans `C:\extracted\Encryption Management Agent\EMAgent_XXbit_setup.exe`.
- L'exemple suivant correspond à la désinstallation silencieuse de BitLocker Manager.

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

  Lorsque vous avez terminé, redémarrez l'ordinateur.

8

Programme de désinstallation de Data Security

Désinstaller Endpoint Security Suite Enterprise

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

REMARQUE : Lors de la désinstallation de FDE, Dell recommande de redémarrer l'ordinateur une fois la désactivation de FDE terminée afin d'éviter les problèmes de veille prolongée de l'ordinateur.

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

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

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

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

Cliquez sur **Suivant**.

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

Les dépendances requises sont automatiquement sélectionnées ou effacées.

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

Sélectionnez **Encryption Removal Agent : télécharger des clés depuis un serveur**.

Saisissez les informations d'identification complètes d'un administrateur d'analyse approfondie et sélectionnez **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.

9

Scénarios couramment utilisés

- Pour installer chaque client individuellement, vous devez d'abord extraire les fichiers exécutables enfant du programme d'installation principal d'Endpoint Security Suite Enterprise ; tel qu'indiqué dans la section Extraire les programmes d'installation enfants du programme d'installation principal.
- Le composant du programme d'installation enfant Advanced Threat Prevention doit être installé par la ligne de commande uniquement. Double-cliquer pour installer ce composant installe une version non-Dell, non gérée du produit, qui n'est pas prise en charge. Si cela est effectué par inadvertance, allez à Ajouter/Supprimer des programmes et désinstallez cette version.
- 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 /l*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 dotée du bouton **Annuler** : vous invite à effectuer un redémarrage
/qb-	Boîte de dialogue de progression avec bouton **Annuler**: redémarre automatiquement à la fin du processus
/qb!	Boîte de dialogue de progression sans bouton **Annuler** : vous invite à effectuer un redémarrage
/qb!-	Boîte de dialogue de progression sans le bouton **Annuler**, redémarre automatiquement une fois le processus terminé

Option	Signification
/qn	Pas d'interface utilisateur

- Dirigez les utilisateurs vers les documents suivants et les fichiers d'aide en cas de besoin au moment de l'application :
  - Pour apprendre à utiliser les fonctions d'Encryption, reportez-vous à *Dell Encrypt Help* (Aide concernant Dell Encrypt). Accédez à l'aide depuis `<Install dir>:\Program Files\Dell\Dell Data Protection\Encryption\Help`.
  - Voir *Encryption External Media Help* (Aide concernant Encryption External Media) pour apprendre à utiliser les fonctions d'Encryption External Media. Accédez à l'aide depuis `<Install dir>:\Program Files\Dell\Dell Data Protection\Encryption\EMS`
  - Voir (Aide d'Encryption Enterprise) d'*Endpoint Security Suite Enterprise* pour savoir comment utiliser les fonctions de et d'Advanced Threat Prevention. Accédez à l'aide à partir de `<Install dir>:\Program Files\Dell\Dell Data Protection\Advanced Threat Prevention\Help`.

Client Encryption et Advanced Threat Prevention

- L'exemple suivant correspond à l'installation de la gestion SED et d'Encryption Management Agent (installation silencieuse, pas de redémarrage, aucune entrée dans la liste Programmes du Panneau de configuration, installation à l'emplacement par défaut `C:\Program Files\Dell\Dell Data Protection\Encryption`). Ce composant installe Encryption Management Agent, qui est requis par Advanced Threat Prevention.

  ```
  EMAgent_XXbit_setup.exe /s /v"CM_EDITION=1 SERVERHOST=server.organization.com
  SERVERPORT=8888 SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443
  ARPSYSTEMCOMPONENT=1 /norestart /qn"
  ```

  Puis :

  Puis :

- L'exemple suivant correspond à l'installation d'Advanced Threat Prevention (installation silencieuse, pas de redémarrage, fichier journal d'installation et dossier d'installation aux emplacements spécifiés)

  ```
  MSIEXEC.EXE /I "ATP_CSF_Plugins_x64.msi" /qn REBOOT="ReallySuppress" APPFOLDER="C:
  \Program Files\Dell\Dell Data Protection\Advanced Threat Prevention\Plugins"
  ARPSYSTEMCOMPONENT="1" /l*v "C:\ProgramData\Dell\Dell Data Protection\Installer
  Logs\AdvancedThreatProtectionPlugins.msi.log"
  ```

  et

  ```
  ATP_AgentSetup.exe" /s EXTRACT_INSTALLERS /v"/qb!"
  ```

- L'exemple suivant correspond à l'installation d'Encryption avec les paramètres par défaut (Encryption et Encrypt for Sharing, pas de boîte de dialogue, pas de barre de progression, pas de redémarrage, installation à l'emplacement par défaut `C:\Program Files\Dell\Dell Data Protection\Encryption`).

  ```
  DDPE_XXbit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com
  POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION
  DEVICESERVERURL=https://server.organization.com:8443/xapi/ /norestart /qn"
  ```

- Les exemples suivants correspondent à l'installation des fonctionnalités ***facultatives*** : protection Web et pare-feu.
- **\Threat Protection\SDK**

  La ligne de commande suivante correspond au chargement des paramètres par défaut du certificat.

  ```
  EnsMgmtSdkInstaller.exe -LoadCert >"C:\ProgramData\Dell\Dell Data Protection\Installer
  Logs\McAfeeSDKInstallerBeforeEndPoint.log"
  ```

  REMARQUE :

  Vous ne pouvez pas ignorer ce programme d'installation si vous procédez à une mise à niveau.

  Puis :

  \Threat Protection\EndPointSecurity

- L'exemple suivant correspond à l'installation des *fonctionnalités facultatives* : protection Web et pare-feu à l'aide de paramètres par défaut (mode silencieux, installer Threat Protection, Client Firewall et Web Protection, remplacer Host Intrusion Prevention, pas de mise à jour du contenu, pas de paramètres enregistrés).

```
"Threat Protection\EndPointSecurity\EPsetup.exe" ADDLOCAL="fw,wc" /override"hips" /
nocontentupdate /nopreservesettings /qn
```

Puis :

\Threat Protection\ThreatProtection\WinXXR

- L'exemple suivant correspond à l'installation du client à l'aide de paramètres par défaut (supprimer le redémarrage, pas de boîte de dialogue, pas de barre de progression, pas d'entrée dans la liste des programmes du panneau de configuration).

```
"DellThreatProtection.msi" /qn REBOOT=ReallySuppress ARPSYSTEMCOMPONENT=1
```

\Threat Protection\SDK

- L'exemple suivant permet d'installer le SDK.

```
EnsMgmtSdkInstaller.exe "C:\Program Files\Dell\Dell Data
Protection\Threat Protection\DellAVAgent.exe" -InstallSDK -RemoveRightClick
-RemoveMcTray >"C:\ProgramData\Dell\Dell Data Protection\Installer
Logs\McAfeeSDKInstallerAfterEndPoint.log"
```

SED Manager et Encryption External Media

- L'exemple suivant correspond à l'installation de SED Manager, d'Encryption Management Agent et de la console de sécurité locale (installation silencieuse, pas de redémarrage, aucune entrée dans la liste Programmes du Panneau de configuration, installation à l'emplacement par défaut de `C:\Program Files\Dell\Dell Data Protection\Encryption`).

```
EMAgent_XXbit_setup.exe /s /v"CM_EDITION=1 SERVERHOST=server.organization.com
SERVERPORT=8888 SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443
ARPSYSTEMCOMPONENT=1 /norestart /qn"
```

Puis :

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

```
DDPE_XXbit_setup.exe /s /v"EME=1
SERVERHOSTNAME=server.organization.com POLICYPROXYHOSTNAME=rgk.organization.com
DEVICESERVERURL=https://server.organization.com:8443/xapi/ MANAGEDDOMAIN=ORGANIZATION /
norestart /qn"
```

BitLocker Manager et Encryption External Media

- BitLocker Manager et Encryption External Media interagissent en fonction d'une séquence de chiffrement. Si un disque BitLocker Manager est inséré dans un ordinateur avec Encryption External Media, le mot de passe BitLocker Manager **doit** être saisi pour que Encryption External Media puisse lire et crypter le lecteur.
- Si Encryption External Media est actif sur un lecteur, BitLocker Manager peut être appliqué au même lecteur.
- L'exemple suivant correspond à l'installation de BitLocker Manager (installation silencieuse, pas de redémarrage, pas d'entrée dans la liste des Programmes du panneau de configuration, installation à l'emplacement par défaut `C:\Program Files\Dell\Dell Data Protection`).

```
EMAgent_XXbit_setup.exe /s /v"CM_EDITION=1 SERVERHOST=server.organization.com
SERVERPORT=8888 SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443
FEATURE=BLM /norestart /qn"
```

Ensuite :

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

```
DDPE_XXbit_setup.exe /s /v"EME=1
SERVERHOSTNAME=server.organization.com POLICYPROXYHOSTNAME=rgk.organization.com
DEVICESERVERURL=https://server.organization.com:8443/xapi/ MANAGEDDOMAIN=ORGANIZATION /
norestart /qn"
```

BitLocker Manager et Advanced Threat Prevention

- L'exemple suivant correspond à l'installation de BitLocker Manager (installation silencieuse, pas de redémarrage, pas d'entrée dans la liste des Programmes du panneau de configuration, installation à l'emplacement par défaut `C:\Program Files\Dell\Dell Data Protection`). Ce composant installe Encryption Management Agent, qui est requis par Advanced Threat Prevention.

  ```
  EMAgent_XXbit_setup.exe /s /v"CM_EDITION=1 SERVERHOST=server.organization.com
  SERVERPORT=8888 SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443
  FEATURE=BLM /norestart /qn"
  ```

  Puis :

- L'exemple suivant correspond à l'installation d'Advanced Threat Prevention (installation silencieuse, pas de redémarrage, fichier journal d'installation et dossier d'installation aux emplacements spécifiés)

  ```
  MSIEXEC.EXE /I "ATP_CSF_Plugins_x64.msi" /qn REBOOT="ReallySuppress"
  ARPSYSTEMCOMPONENT="1" /l*v "C:\ProgramData\Dell\Dell Data Protection\Installer
  Logs\ATP.log" APPFOLDER="C:\Program Files\Dell\Dell Data Protection\Advanced Threat
  Prevention"
  ```

  et

  ```
  "\Advanced Threat Prevention\WinNtAll\ATP_AgentSetup.exe" /s EXTRACT_INSTALLERS /v"/qb!"
  ```

10

Provision a Tenant

Un locataire doit être provisionné dans Dell Server pour que l'application des stratégies Advanced Threat Prevention devienne active.

Pré-requis

- Doit être effectué par un administrateur doté du rôle Administrateur système.
- Doit disposer d'une connexion à Internet pour provisionner sur Dell Server.
- Doit disposer d'une connexion à Internet sur le client pour afficher l'intégration de service en ligne Advanced Threat Prevention dans la console de gestion.
- Le provisionnement est basé sur un jeton qui est généré à partir d'un certificat pendant le provisionnement.
- Les licences Advanced Threat Prevention doivent être présentes sur Dell Server.

Provisionner un service partagé

1. Connectez-vous à la console de gestion en tant qu'administrateur Dell.
2. Dans le volet de gauche de la console de gestion, cliquez sur **Gestion > Services de gestion.**
3. Cliquez sur **Configurer le service Advanced Threat Protection**. Importez vos licences Advanced Threat Prevention en cas d'échec à ce stade.
4. La configuration guidée commence une fois que les licences sont importées. Cliquez sur **Suivant** pour commencer.
5. Lisez et acceptez les termes du CLUF et cliquez sur **Suivant**.
6. Fournissez les identifiants à Dell Server pour le provisionnement du service partagé. Cliquez sur **Suivant**. *Le provisionnement d'un service partagé existant de marque Cylance n'est pas pris en charge.*
7. Téléchargez le certificat. Celui-ci est nécessaire à la récupération en cas de sinistre affectant Dell Server. Ce certificat n'est pas automatiquement sauvegardé. Sauvegardez le certificat à un emplacement sûr sur un autre ordinateur. Cochez la case pour confirmer que vous avez sauvegardé le certificat et cliquez sur **Suivant**.
8. La configuration est terminée. Cliquez sur **OK**.

11

Configuration de la mise à jour automatique de l'agent Advanced Threat Prevention

Pour recevoir les mises à jour automatiques de l'agent Advanced Threat Prevention, vous pouvez vous inscrire dans la console de gestion. Le fait de s'inscrire pour recevoir les mises à jour automatiques de l'agent permet aux clients de télécharger et d'appliquer les mises à jour depuis le service Advanced Threat Prevention. Mises à jour et publications mensuelles.

REMARQUE :

Les mises à jour automatiques de l'agent sont prises en charge par la version 9.4.1 ou les versions ultérieures du Dell Server.

Mises à jour automatique de l'agent de réception

Pour vous inscrire et recevoir les mises à jour automatique de l'agent :

1. Dans le volet de gauche de la console de gestion, cliquez sur **Gestion** > **Services de gestion**.
2. Sur l'onglet *Menaces avancées*, sous *Mise à jour automatique de l'agent*, cliquez sur le bouton **Activé**, puis cliquez sur **Enregistrer les préférences**.

   Le renseignement des informations et l'affichage des mises à jour automatiques peuvent prendre quelques instants.

Arrêter la réception de mises à jour automatiques de l'agent

Pour ne plus recevoir les mises à jour automatiques de l'agent :

1. Dans le volet de gauche de la console de gestion, cliquez sur **Gestion** > **Services de gestion**.
2. Sur l'onglet *Menaces avancées*, sous *Mise à jour automatique de l'agent*, cliquez sur le bouton **Désactivé**, puis cliquez sur **Enregistrer les préférences**.

12

Configuration préalable à l'installation pour SED UEFI, et BitLocker Manager

Initialiser le module TPM

- Vous devez être membre du groupe des administrateurs locaux, ou équivalent.
- L'ordinateur doit être pourvu d'un BIOS compatible et d'un TPM.
- Suivez les instructions sous http://technet.microsoft.com/en-us/library/cc753140.aspx.

Configuration de la pré-Installation avant démarrage sur les ordinateurs UEFI

Activer la connectivité réseau au cours de l'authentification avant démarrage UEFI

Pour que l'authentification avant démarrage réussisse sur un ordinateur équipé du micrologiciel UEFI, l'authentification avant démarrage (PBA) doit disposer de la connectivité réseau. Par défaut, les ordinateurs équipés d'un micrologiciel UEFI ne disposent pas de connectivité réseau tant que le système d'exploitation n'est pas chargé, ce qui intervient après le mode d'authentification avant démarrage.

La procédure suivante active la connectivité réseau au cours de la PBA pour les ordinateurs activés UEFI. Comme les étapes de configuration varient d'un modèle d'ordinateur à l'autre, la procédure suivante n'est donnée qu'à titre d'exemple.

1. Démarrez en mode de configuration du micrologiciel UEFI :
2. Appuyez continuellement sur la touche F2 pendant le démarrage, jusqu'à ce qu'un message de type « préparation du menu de démarrage ponctuel » apparaisse dans l'angle supérieur droit de l'écran.
3. Entrez le mot de passe d'administrateur du BIOS si on vous le demande.

   REMARQUE :

   Généralement, vous ne verrez pas cette invite s'il s'agit d'un nouvel ordinateur, car le mot de passe du BIOS n'aura pas encore été configuré.
4. Sélectionnez **Configuration système**
5. Sélectionnez **NIC intégrée**.
6. Cochez la case **Activer la pile réseau UEFI**.
7. Sélectionnez **Activé** ou **Activé avec PXE**.
8. Sélectionnez **Appliquer**

   REMARQUE :

   Les ordinateurs ne disposant *pas* du micrologiciel UEFI n'ont pas besoin de configuration.

Désactiver les ROM de l'option Héritée :

Assurez-vous que le paramètre **Activer les ROM de l'option Héritée** est désactivé dans le BIOS.

1. Redémarrez l'ordinateur.
2. Au cours du redémarrage, appuyez sur **F12** à plusieurs reprises jusqu'à appeler les paramètres d'amorçage de l'ordinateur UEFI.

3. Appuyez sur la flèche vers le bas, mettez en surbrillance l'option **Paramètres du BIOS**, puis appuyez sur **Entrée**.
4. Sélectionnez **Paramètres** > **généraux** > **Options de démarrage avancées**.
5. Décochez la case **Activer les ROM de l'option Héritée** et cliquez sur **Appliquer**.

Configuration préalable à l'installation d'une partition d'authentification avant démarrage BitLocker

- Vous devez créer la partition d'authentification avant démarrage (PBA) **avant** d'installer BitLocker Manager.
- Mettez sous tension et activez le TPM **avant** d'installer BitLocker Manager. BitLocker Manager s'approprie le TPM sans nécessiter de redémarrage. Toutefois, si le TPM a déjà un propriétaire, BitLocker Manager lance le processus de configuration du cryptage. Ce qui compte, c'est que le TPM soit propriétaire et activé.
- Vous devrez peut-être partitionner le disque manuellement. Pour obtenir des informations supplémentaires, reportez-vous à la description de l'outil de préparation de lecteur BitLocker de Microsoft.
- Utilisez la commande BdeHdCfg.exe pour créer la partition d'authentification avant démarrage. Avec le paramètre par défaut, l'outil de ligne de commande suit le même processus que l'Assistant Configuration BitLocker.

  ```
  BdeHdCfg -target default
  ```

  REMARQUE :

  Pour plus d'options disponibles pour la commande BdeHdCfg, voir Référence des paramètres de BdeHdCfg.exe de Microsoft.

13

Définir le Dell Server par le biais du registre

- Si les droits sont accordés à vos clients par le biais de Dell Digital Delivery, suivez les instructions ci-dessous pour définir un registre à l'aide d'objets de la stratégie de groupe afin de prédéfinir le serveur Dell à utiliser après l'installation.
- La station de travail doit être membre de l'unité organisationnelle dans laquelle les objets de stratégie de groupe sont appliqués. Sinon, les paramètres du registre doivent être définis manuellement sur le point de terminaison.
- Assurez-vous que le port sortant 443 est disponible pour communiquer avec le Dell Server sur cloud.dell.com. Si le port 443 est bloqué (quelle que soit la raison), l'obtention de l'autorisation échoue et une autorisation est consommée à partir du pool disponible.

  REMARQUE : Si vous ne définissez pas cette valeur de registre lorsque vous tentez l'installation par le biais de Dell Digital Delivery ou si vous ne spécifiez pas un SERVEUR dans le programme d'installation principal, l'URL d'activation est définie par défaut sur 199.199.199.199.

Définir manuellement la clé de registre

Pour les points de terminaison qui ne sont pas joints au domaine ou pour lesquels la configuration d'un objet de stratégie de groupe est impossible, prédéfinissez une clé de registre pour les activer sur un Dell Server spécifique lors de l'installation.

1. Dans la zone de recherche de la barre des tâches, saisissez **regedit**, puis cliquez avec le bouton droit de la souris et sélectionnez **Exécuter en tant qu'administrateur**.
2. Accédez aux clés de registre et créez la clé de registre suivante :

   HKEY_LOCAL_MACHINE\SOFTWARE\Dell\Dell Data Protection

   REG_SZ: Server

   Value: <FQDN or IP address of the Dell Server>

3. Installez le chiffrement par le biais de Dell Digital Delivery ou du programme d'installation principal.

Créer l'objet de stratégie de groupe

1. Sur le contrôleur de domaine permettant de gérer les clients, cliquez sur **Démarrer** > **Outils d'administration** > **Gestion des règles de groupe**.
2. Cliquez avec le bouton droit sur l'unité organisationnelle à laquelle la règle doit être appliquée, puis sélectionnez **Créer un objet GPO dans ce domaine** et **Le lier ici**.
3. Saisissez le nom du nouvel objet GPO, sélectionnez (aucun) dans le champ Objet GPO Starter source, puis cliquez sur **OK**.
4. Cliquez-droit sur l'objet GPO créé et sélectionnez **Modifier**.
5. L'Éditeur de gestion des règles de groupe se charge. Accédez à **Configuration ordinateur** > **Préférences** > **Paramètres Windows** > **Registre**.
6. Cliquez avec le bouton droit sur le registre, puis sélectionnez **Nouveau** > **Élément du Registre**. Renseignez les éléments suivants :

   Action : Create

   Ruche : HKEY_LOCAL_MACHINE

   Chemin d'accès à la clé : SOFTWARE\Dell\Dell Data Protection

   Nom de la valeur : Server

   Type de valeur : REG_SZ

   Value data: <FQDN or IP address of the Dell Server>

7. Cliquez sur **OK**.
8. Déconnectez-vous, puis reconnectez-vous au poste de travail, ou exécutez **`gpupdate /force`** pour appliquer la règle de groupe.

14

Extraire les programmes d'installation enfant

- Pour installer chaque client individuellement, vous devez d'abord extraire les fichiers exécutables du programme d'installation.
- Le programme d'installation principal n'est pas un *programme de désinstallation* principal. Chaque client doit être désinstallé séparément avant la désinstallation du programme d'installation principal. 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 **DDSSuite.exe** sur l'ordinateur local.
2. Ouvrez une invite de commande dans le même emplacement que le fichier **DDSSuite.exe** et saisissez :

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

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

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

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

15

Configurer Key Server

- Cette section explique comment configurer les composants requis pour utiliser l'authentification/autorisation Kerberos avec un Security Management Server. Security Management Server Virtual n'utilise pas Key Server.

  Key Server est un service qui écoute pour savoir quels clients se connectent à un socket. Dès qu'un client est connecté, une connexion sécurisée est négociée, authentifiée et cryptée à l'aide des API Kerberos (en cas d'échec de la négociation de la connexion sécurisée, le client est déconnecté).

  Dell Key Server vérifie ensuite auprès du Security Server (anciennement dénommé Device Server) si l'utilisateur exécutant le client est autorisé à accéder aux clés. Cet accès est accordé via des domaines individuels dans la console de gestion.

- Pour utiliser l'authentification/autorisation Kerberos, il est nécessaire d'intégrer le serveur qui contient le composant Key Server dans le domaine concerné.
- La désinstallation classique est affectée car le Security Management Server Virtual n'utilise pas le Key Server. Lors de la désinstallation d'un client Encryption activé par rapport à un Security Management Server Virtual, la récupération de la clé d'analyse approfondie standard s'effectue par le biais de Security Server plutôt que par la méthode Kerberos de Key Server. Reportez-vous à Désinstallation par la ligne de commande pour plus d'informations.

Écran des services - Ajouter un utilisateur du compte de domaine

1. Dans Security Management Server, accédez au volet de services (Démarrer > Exécuter > services.msc > OK).
2. Effectuez un clic droit sur Key Server, puis sélectionnez **Propriétés**.
3. Sélectionnez l'onglet Connexion puis l'option **Ce compte :**.

   Dans le champ *Ce compte :*, ajoutez l'utilisateur de compte de domaine. Cet utilisateur de domaine doit au minimum disposer des droits d'administrateur local sur le dossier Key Server (il doit disposer de droits d'écriture sur le fichier de configuration Key Server ainsi que sur le fichier log.txt).

   Saisissez et confirmez un nouveau mot de passe pour l'utilisateur.

   Cliquez sur **OK**.
4. Redémarrez le service Key Server (laissez ouvert le panneau de services pour pouvoir y revenir ultérieurement).
5. Accédez au fichier log.txt qui se trouve dans <Key Server install dir> pour vérifier que le service a correctement démarré.

Fichier de configuration de Key Server - Ajouter un utilisateur pour la communication avec le Security Management Server

1. Naviguez jusqu'au <Key Server install dir>.
2. Ouvrez *Credant.KeyServer.exe.config* dans un éditeur de texte.
3. Naviguez jusqu'à <add key="user" value="superadmin" /> et remplacez la valeur « superadmin » par le nom de l'utilisateur concerné (vous pouvez également laisser la valeur « superadmin »).

   Le format « superadmin » peut correspondre à n'importe quelle méthode permettant l'authentification sur le Security Management Server. Vous pouvez utiliser le nom de compte SAM, l'UPN ou le format DOMAINE\Nom d'utilisateur. Toutes les méthodes permettant l'authentification sur le Security Management Server sont acceptées, car la validation est requise pour ce compte utilisateur pour l'autorisation sur Active Directory.

   Par exemple, dans un environnement à domaines multiples, si vous saisissez uniquement un nom de compte SAM tel que « jdupont », l'authentification risque d'échouer, car le Security Management Server ne peut pas authentifier « jdupont », puisque « jdupont » est introuvable. Bien que le format DOMAINE\Nom d'utilisateur soit accepté, nous vous recommandons

d'utiliser l'UPN dans un environnement à domaines multiples. Dans un environnement à domaine unique, vous pouvez utiliser le nom de compte SAM.

4. Accédez à <add key="epw" value="<encrypted value of the password>" /> et remplacez « epw » par « password ». Remplacez ensuite « <encrypted value of the password> » par le mot de passe de l'utilisateur que vous avez configuré à l'étape 3. Ce mot de passe est à nouveau crypté au redémarrage du Security Management Server.

   Si vous avez utilisé « superadmin » à l'étape 3, et si le mot de passe superadmin n'est pas « changeit », vous devez le modifier ici. Enregistrez le fichier, puis fermez-le.

Exemple de fichier de configuration

<?xml version="1.0" encoding="utf-8" ?>

<configuration>

<appSettings>

<add key="port" value="8050" /> [port TCP sur lequel Dell Key Server écoutera. La valeur par défaut est 8050.]

<add key="maxConnections" value="2000" /> [nombre de connexions de socket actives que le Key Server autorisera]

<add key="url" value="https://keyserver.domain.com:8443/xapi/" /> [URL du Security Server (anciennement dénommé Device Server) (le format est 8081/xapi si votre version de Security Management Server est antérieure à 7.7)]

<add key="verifyCertificate" value="false" /> [la valeur « vrai » vérifie les certificats ; définissez-la sur « faux » si vous ne souhaitez pas vérifier les certificats ou si vous utilisez des certificats auto-signés]

<add key="user" value="superadmin" /> [Nom d'utilisateur utilisé pour communiquer avec le Security Server. Le rôle Administrateur doit être sélectionné pour cet utilisateur dans la Console de gestion. Le format « superadmin » peut correspondre à n'importe quelle méthode permettant l'authentification sur le Security Management Server. Vous pouvez utiliser le nom de compte SAM, l'UPN ou le format DOMAINE\Nom d'utilisateur. Toutes les méthodes permettant l'authentification sur le Security Management Server sont acceptées, car la validation est requise pour ce compte utilisateur pour l'autorisation sur Active Directory. Par exemple, dans un environnement à domaines multiples, si vous saisissez uniquement un nom de compte SAM tel que « jdupont », l'authentification risque d'échouer, car le Security Management Server ne peut pas authentifier « jdupont », puisque « jdupont » est introuvable. Bien que le format DOMAINE\Nom d'utilisateur soit accepté, nous vous recommandons d'utiliser l'UPN dans un environnement à domaines multiples. Dans un environnement à domaine unique, vous pouvez utiliser le nom de compte SAM.]

<add key="cacheExpiration" value="30" /> [Fréquence (en secondes) à laquelle le service doit vérifier les personnes autorisées à demander des clés. Le service conserve un cache et assure le suivi de son ancienneté. Lorsque l'ancienneté du cache dépasse la valeur définie, le service établit une nouvelle liste. Lorsqu'un utilisateur se connecte, le Key Server doit télécharger les utilisateurs autorisés à partir du Security Server. S'il n'existe aucun cache pour ces utilisateurs, ou si la liste n'a pas été téléchargée au cours des « x » dernières secondes, elle est de nouveau téléchargée. Aucune interrogation n'est exécutée, mais cette valeur permet de configurer le délai d'expiration de la liste après lequel une actualisation est nécessaire.]

<add key="epw" value="encrypted value of the password" /> [Mot de passe utilisé pour communiquer avec Security Management Server. Si vous avez modifié le mot de passe superadmin, vous devez également le modifier ici.]

</appSettings>

</configuration>

Écran des services - Redémarrage du service Key Server

1. Retournez au panneau de services (Démarrer > Exécuter > services.msc > OK).
2. Redémarrez le service Key Server.
3. Accédez au fichier log.txt qui se trouve dans <Key Server install dir> pour vérifier que le service a correctement démarré.
4. Fermez le volet de services.

Console de gestion - Ajouter un administrateur d'analyse approfondie

1. Connectez-vous à la console de gestion en tant qu'administrateur Dell.
2. Cliquez sur **Populations** > **Domaines**.
3. Sélectionnez le Domaine pertinent.
4. Cliquez sur l'onglet **Key Server**.
5. Dans *Compte*, ajoutez l'utilisateur pour effectuer les activités d'administrateur. Le format est DOMAINE\Nom d'utilisateur. Cliquez sur **Ajouter un compte**.
6. Cliquez sur **Utilisateurs** dans le menu de gauche. Dans la zone de recherche, recherchez le nom d'utilisateur que vous avez ajouté à l'étape 5. Cliquez sur **Rechercher**.
7. Une fois que vous avez localisé l'utilisateur approprié, cliquez sur l'onglet **Admin**.
8. Sélectionnez **Administrateur d'analyse approfondie**, puis cliquez sur **Mettre à jour**.

   La configuration des composants pour l'authentification/autorisation Kerberos est maintenant terminée.

16

Utiliser l'utilitaire Administrative Download (CMGAd)

- Cet utilitaire permet de télécharger un bundle de matériel clé à utiliser sur un ordinateur non connecté à un Dell Server.
- Cet utilitaire utilise l'une des méthodes suivantes pour télécharger un bundle de ressources de clé, selon le paramètre de ligne de commande passé à l'application :
  - Mode d'analyse approfondie : utilisé si -f est passé sur la ligne de commande ou si aucun paramètre de ligne de commande n'est utilisé.
  - Mode Admin : utilisé si -f est passé sur la ligne de commande.

    Les fichiers journaux se trouvent à `C:\ProgramData\CmgAdmin.log`

Utilisation du mode Analyse approfondie

1. Double-cliquez sur **`cmgad.exe`** pour lancer l'utilitaire ou ouvrez une invite de commande où se trouve CMGAd et tapez `cmgad.exe -f`**`cmgad.exe -f`** (ou`cmgad.exe` **`cmgad.exe`**).
2. Entrez les informations suivantes (certains champs peuvent être déjà renseignés).

   URL du Device Server : URL complète du Security Server (Device Server). Le format est le suivant https://securityserver.domain.com:8443/xapi/.

   Dell Admin : nom de l'administrateur avec les informations d'identification de l'administrateur d'analyse approfondie comme jdupont (activé dans la console de gestion)

   Mot de passe : mot de passe d'administrateur d'analyse approfondie

   MCID : ID de la machine, tel que IDmachine.domaine.com

   DCID : huit premiers caractères de l'ID de Bouclier comportant 16 caractères.

   REMARQUE :

   Généralement, il suffit de spécifier MCID *ou* DCID. Cependant, si les deux sont connus, il peut être utile de les entrer tous les deux. Chaque paramètre contient différentes informations utilisées par cet utilitaire.

   Cliquez sur **Suivant**.

3. Dans le champ *Phrase de passe :*, entrez la phrase de passe pour protéger le fichier de téléchargement. La phrase de passe doit contenir au moins huit caractères, au moins un caractère alphabétique et un caractère numérique. Confirmer la phrase de passe.

   Acceptez le nom et l'emplacement par défaut auquel le fichier sera enregistré, ou cliquez sur ... pour sélectionner un emplacement différent.

   Cliquez sur **Suivant**.

   Le message qui s'affiche indique que le matériel clé a été déverrouillé avec succès. Les fichiers sont désormais accessibles.

4. Cliquez sur **Terminer** lorsque vous avez terminé.

Utilisation du mode Admin

Le mode Admin ne peut pas être utilisé pour l'obtention d'un ensemble de clés depuis un Security Management Server Virtual, car le Security Management Server Virtual n'utilise pas le Key Server. Utilisez le mode Analyse approfondie pour obtenir l'ensemble de clés si le client est activé par rapport à un Security Management Server Virtual.

1. Ouvrez une invite de commande à l'emplacement de CMGAd et saisissez la commande **`cmgad.exe -a`**.

2. Entrez les informations suivantes (certains champs peuvent être déjà renseignés).

   Serveur : nom d'hôte complet du Key Server, tel que keyserver.domaine.com

   Numéro de port : le port par défaut est 8050.

   Compte de serveur : l'utilisateur de domaine sous le nom duquel le Key Server s'exécute. Le format est DOMAINE\Nom d'utilisateur. L'utilisateur de domaine qui exécute l'utilitaire doit être autorisé à effectuer le téléchargement depuis le Key Server

   MCID : ID de la machine, tel que IDmachine.domaine.com

   DCID : huit premiers caractères de l'ID de Bouclier comportant 16 caractères.

   REMARQUE :

   Généralement, il suffit de spécifier MCID *ou* DCID. Cependant, si les deux sont connus, il peut être utile de les entrer tous les deux. Chaque paramètre contient différentes informations utilisées par cet utilitaire.

   Cliquez sur **Suivant**.

3. Dans le champ *Phrase de passe :*, entrez la phrase de passe pour protéger le fichier de téléchargement. La phrase de passe doit contenir au moins huit caractères, au moins un caractère alphabétique et un caractère numérique.

   Confirmer la phrase de passe.

   Acceptez le nom et l'emplacement par défaut auquel le fichier sera enregistré, ou cliquez sur ... pour sélectionner un emplacement différent.

   Cliquez sur **Suivant**.

   Le message qui s'affiche indique que le matériel clé a été déverrouillé avec succès. Les fichiers sont désormais accessibles.

4. Cliquez sur **Terminer** lorsque vous avez terminé.

17

Configuration d'Encryption sur un système d'exploitation de serveur

Activer Encryption sur un système d'exploitation de serveur

REMARQUE :

Le chiffrement des systèmes d'exploitation de serveur convertit le chiffrement Utilisateur en chiffrement Courant.

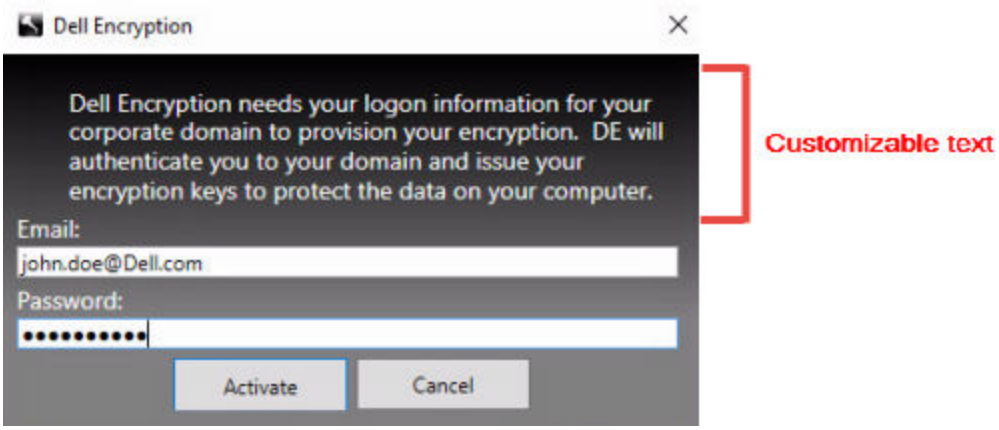
1. Connectez-vous à la console de gestion en tant qu'administrateur Dell.
2. Sélectionnez **Groupe de points de terminaison** (ou **Point de terminaison**), recherchez le point de terminaison ou le groupe de points de terminaison à activer, sélectionnez **Règles de sécurité**, puis la catégorie de règles **Server Encryption**.
3. Définissez les règles suivantes :
   - Server Encryption : **sélectionnez cette option** pour activer Encryption sur un système d'exploitation de serveur et les règles connexes.
   - SDE Encryption activé : **sélectionnez cette option** pour activer le cryptage SDE.
   - Encryption activé - **Sélectionnez cette option** pour activer le cryptage courant.
   - Sécuriser les informations d'identification Windows : cette stratégie est **sélectionnée** par défaut.

     Lorsque la stratégie *Sécuriser les informations d'identification Windows* est **sélectionnée** (par défaut), tous les fichiers du dossier \Windows\system32\config sont cryptés, y compris les informations d'identification Windows. Pour éviter le cryptage des informations d'identification Windows, **désélectionnez** la stratégie *Sécuriser les informations d'identification Windows*. Le cryptage des informations d'identification Windows se produit indépendamment de la définition de la stratégie *SDE Encryption activé*.
4. Enregistrez et validez les règles.

Personnaliser la boîte de dialogue de connexion Activation

La boîte de dialogue de connexion Activation affiche :

- Lorsqu'un utilisateur non géré se connecte.
- Lorsque l'utilisateur sélectionne l'option Activer Dell Encryption dans le menu de l'icône Encryption, situé dans la zone de notification.



Configuration de règles Encryption External Media

L'***ordinateur de cryptage d'origine*** est l'ordinateur qui crypte un périphérique amovible à l'origine. Lorsque l'ordinateur d'origine est un ***serveur protégé*** (un serveur sur lequel Encryption sur un système d'exploitation de serveur est installé et activé) et dès que le serveur protégé détecte la présence d'un périphérique amovible, l'utilisateur est invité à le chiffrer.

- Les règles d'Encryption External Media contrôlent aussi l'accès du support amovible au serveur, l'authentification et le cryptage, entre autres.
- Les règles du système de contrôle de port affectent le support amovible des serveurs protégés, en contrôlant par exemple l'accès et l'utilisation des ports USB du serveur par des périphériques USB.

Les règles de cryptage des supports amovibles se trouvent dans la console de gestion, dans le groupe de technologie *Server Encryption*.

Encryption sur un système d'exploitation de serveur et supports externes

Lorsque la stratégie de *cryptage EMS des supports externes* est **sélectionnée**, les supports externes sont cryptés. Encryption lie le périphérique au serveur protégé avec la clé d'ordinateur et à l'utilisateur avec la clé Utilisateur itinérant de l'utilisateur/du propriétaire du périphérique amovible. Tous les fichiers ajoutés au périphérique amovible sont cryptés à l'aide de ces mêmes clés, quel que soit l'ordinateur auquel il est connecté.

REMARQUE :

Encryption sur un système d'exploitation de serveur convertit le chiffrement Utilisateur en chiffrement Courant, sauf sur les périphériques amovibles. Sur les périphériques amovibles, le cryptage est effectué à l'aide de la clé Utilisateur itinérant associée à l'ordinateur.

Lorsqu'un utilisateur ne souhaite pas crypter un périphérique amovible, l'accès de l'utilisateur au périphérique peut être défini sur *Bloqué* lorsqu'il est utilisé sur le serveur protégé, *En lecture seule* lors de son utilisation sur le serveur protégé ou bien sur *Accès total*. Les stratégies du serveur protégé déterminent le niveau d'accès à un périphérique amovible non protégé.

Les mises à jour des règles se produisent lorsque le périphérique amovible est réinséré dans le serveur protégé d'origine.

Authentification et Support externe

Les stratégies du serveur protégé déterminent la fonction d'authentification.

Après le cryptage d'un périphérique amovible, seul son propriétaire/utilisateur peut y accéder sur le serveur protégé. D'autres utilisateurs ne peuvent pas accéder aux fichiers cryptés sur le support amovible.

L'authentification automatique locale permet d'authentifier automatiquement le périphérique amovible protégé lorsqu'il est inséré dans l'ordinateur de cryptage d'origine et que le propriétaire de ce support est connecté. Lorsque l'authentification automatique est désactivée, le propriétaire/l'utilisateur doit s'authentifier pour accéder au périphérique amovible protégé.

Lorsque l'ordinateur de cryptage d'origine d'un périphérique amovible est un serveur protégé, le propriétaire/l'utilisateur doit toujours se connecter au périphérique amovible lorsqu'il l'utilise sur des ordinateurs qui ne sont pas d'origine, quels que soient les paramètres de la règle Encryption External Media définis sur les autres ordinateurs.

Reportez-vous à AdminHelp pour plus d'informations à propos des règles de contrôle des ports de Server Encryption et d'Encryption External Media.

Interruption d'Encryption sur un système d'exploitation de serveur

L'interruption d'un serveur crypté empêche l'accès à ses données cryptées après un redémarrage. L'utilisateur du serveur virtuel ne peut pas être interrompu. À la place, la clé d'ordinateur du serveur crypté est interrompue.

REMARQUE :

L'interruption d'un point final du serveur n'entraîne pas l'interruption immédiate du serveur. L'interruption se produit lors de la demande suivante de la clé, ce qui correspond en général au redémarrage suivant du serveur.

REMARQUE :

À utiliser avec soin. L'interruption d'un serveur crypté peut entraîner une instabilité, selon les paramètres de la règle et si le serveur protégé est interrompu lorsqu'il est déconnecté du réseau.

Pré-requis

- Des droits d'administrateur du service d'assistance technique, attribués dans la console de gestion, sont requis pour interrompre un point de terminaison.
- L'administrateur doit être connecté à la console de gestion.

  Dans le volet de gauche de la console de gestion, cliquez sur **Populations** > **Points de terminaison**.

  Recherchez ou sélectionnez un nom d'hôte, puis cliquez sur l'onglet **Détails et actions**.

  Sous *Contrôle des périphériques du serveur*, cliquez sur **Suspendre**, puis sur **Oui**.

  REMARQUE :

  Cliquez sur **Rétablir** pour permettre à Encryption sur systèmes d'exploitation de serveur d'accéder aux données chiffrées sur le serveur après son redémarrage.

18

Configuration de l'activation différée

Le client Encryption avec activation différée est différent de l'activation du client Encryption sur deux aspects :

Règles de cryptage basées sur le périphérique

Les règles du client Encryption reposent sur l'utilisateur, tandis que les règles de cryptage du client Encryption avec activation différée sont basées sur le périphérique. Le cryptage Utilisateur est converti en cryptage Courant. Cette différence permet à l'utilisateur d'apporter un périphérique personnel pour l'utiliser au sein du domaine de l'organisation, tout en permettant à l'organisation de conserver son niveau de sécurité grâce à une gestion centralisée des règles de cryptage.

Activation

Avec le client Encryption, l'activation est automatique. Lorsque Endpoint Security Suite Enterprise est installé avec l'activation différée, l'activation automatique est désactivée. Cette option permet à l'utilisateur de choisir s'il active ou non le cryptage, et à quel moment.

REMARQUE :

Avant de quitter définitivement l'organisation et pendant que son adresse e-mail est toujours active, l'utilisateur doit exécuter l'agent Encryption Removal et désinstaller le client Encryption de son ordinateur personnel.

Personnalisation de l'activation différée

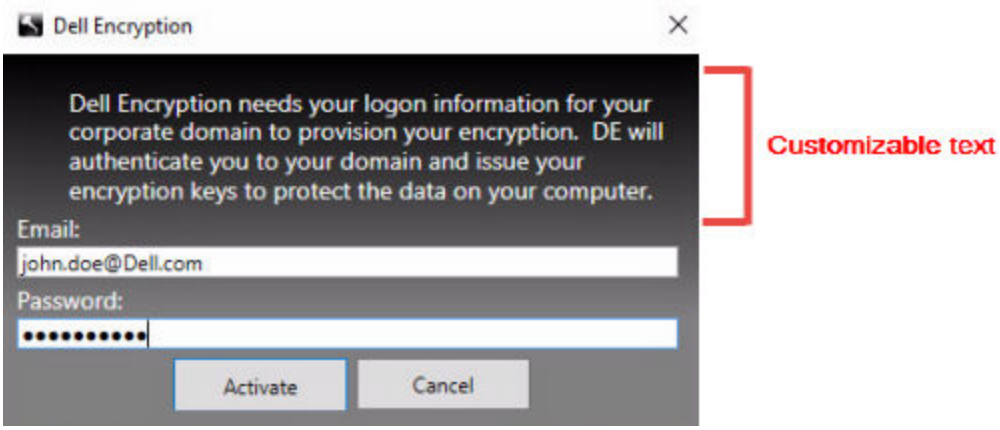
Ces tâches côté client permettent de personnaliser l'activation différée.

- Ajoutez une exclusion dans la boîte de dialogue de connexion Activation
- Désactivez la réactivation automatique (facultatif)

Ajoutez une exclusion dans la boîte de dialogue de connexion Activation

La boîte de dialogue de connexion Activation s'affiche dans ces situations :

- Lorsqu'un utilisateur non géré se connecte.
- Lorsque l'utilisateur sélectionne l'option Activer Dell Encryption dans le menu de l'icône Encryption, situé dans la zone de notification.



Préparation de l'ordinateur pour l'installation

Si les données sont cryptées à l'aide d'un produit de cryptage autre que Dell, avant d'installer le client Encryption, décryptez les données à l'aide du logiciel de cryptage existant, puis désinstallez-le. Si l'ordinateur ne redémarre pas automatiquement, redémarrez-le manuellement.

Créer un mot de passe Windows

Dell vous recommande vivement de créer un mot de passe Windows (s'il n'en existe pas déjà un) pour protéger l'accès aux données cryptées. La création d'un mot de passe sur l'ordinateur permet de bloquer l'accès à votre compte utilisateur à toute personne qui ne dispose pas du mot de passe.

Désinstaller les versions précédentes du client Encryption

Avant de désinstaller une version précédente du client Encryption, arrêtez ou suspendez le balayage de cryptage, si nécessaire.

Si la version de Dell Encryption de l'ordinateur est antérieure à la version 8.6, désinstallez le client Encryption à partir de la ligne de commande. Pour obtenir davantage d'instructions, voir la section *Désinstaller Encryption et le client Server Encryption*.

REMARQUE :

Si vous envisagez d'installer la dernière version du client Encryption immédiatement après la désinstallation, il n'est pas nécessaire d'exécuter l'agent Encryption Removal pour décrypter les fichiers.

Pour mettre à niveau une version précédente du client Encryption installée avec l'activation différée, désinstallez le Programme de désinstallation de Data Security ou les Programmes d'installation enfant. Ces méthodes de désinstallation sont possibles même si le paramètre OPTIN est désactivé.

REMARQUE :

Si aucun utilisateur n'a été activé précédemment, le client Encryption efface le paramètre OPTIN du coffre SDE (SDE Vault) étant donné que ce paramètre est hérité d'une installation précédente. Le client Encryption bloque les activations différées si les utilisateurs ont été précédemment activés mais que l'indicateur OPTIN n'est pas défini dans le coffre SDE.

Installer Encryption avec activation différée

Pour installer le client Encryption avec l'activation différée, installez le client Encryption avec le paramètre OPTIN=1. Pour plus d'informations sur l'installation du client avec le paramètre OPTIN=1, reportez-vous à Installer Encryption.

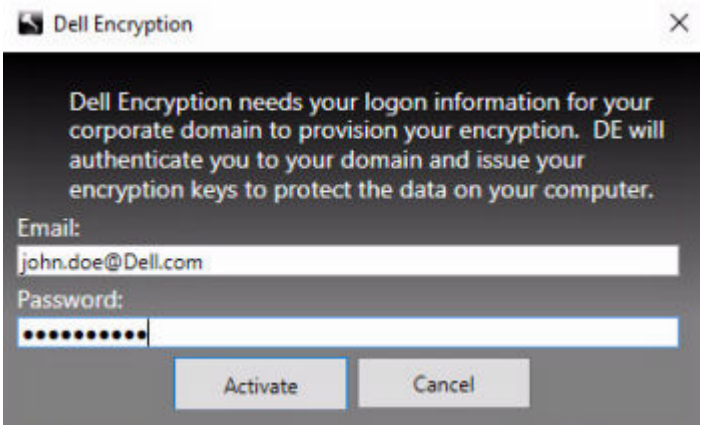
Activer Encryption avec activation différée

- Le processus d'activation associe un utilisateur de domaine à un compte d'utilisateur local et un ordinateur spécifique.
- Plusieurs utilisateurs peuvent procéder à l'activation depuis le même ordinateur, à condition qu'ils utilisent des comptes locaux uniques et qu'ils disposent d'adresses e-mail de domaine uniques.
- Un utilisateur peut activer le client de cryptage une seule fois par compte de domaine.

Avant d'activer le client de cryptage, vous devez procéder comme suit :

- Connectez-vous au compte local que vous utilisez le plus souvent. Ce sont les données qui sont associées à ce compte qui seront cryptées.
- Connectez-vous au réseau de votre entreprise.

1. Connectez-vous au poste de travail ou au serveur.
2. Saisissez l'adresse e-mail du domaine et le mot de passe associé, puis cliquez sur **Activer**.



REMARQUE :

Les adresses e-mail personnelles ou extérieures au domaine ne peuvent pas être utilisées pour l'activation.

3. Cliquez sur **Fermer**.

   Le serveur Dell regroupe le jeu de clés de cryptage et les identifiants de l'utilisateur ainsi que l'ID unique de l'ordinateur (ID d'ordinateur), créant ainsi une relation solide entre le jeu de clés, l'ordinateur concerné et l'utilisateur.

4. Redémarrez l'ordinateur afin de commencer l'analyse de cryptage.

REMARQUE :

La console de gestion locale, accessible depuis l'icône de la zone de notification, affiche les règles envoyées par le serveur, et non la règle appliquée.

Résolution des problèmes d'activation différée

Résolution des problèmes d'activation

Problème : accès impossible à certains fichiers et dossiers

L'impossibilité d'accéder à certains fichiers et dossiers est le signe que l'utilisateur a ouvert une session avec un compte différent de celui pour lequel il est activé.

La boîte de dialogue de connexion Activation s'affiche automatiquement, même si l'utilisateur a été activé au préalable.

Solution possible

Déconnectez-vous, puis reconnectez-vous avec les informations d'identification du compte activé et essayez d'accéder à nouveau aux fichiers.

Dans les rares cas où le client Encryption ne parvient pas à authentifier l'utilisateur, la boîte de dialogue de connexion Activation invite l'utilisateur à saisir ses informations d'identification pour authentifier les clés de cryptage et y accéder. Pour utiliser la fonction de réactivation automatique, les clés de registre *AutoReactivation* et *AutoPromptForActivation* doivent être activées toutes les DEUX. Bien que la fonction soit activée par défaut, il est possible de la désactiver manuellement. Pour plus d'informations, voir la section Désactiver la réactivation automatique.

Message d'erreur : Échec du serveur d'authentification

Le serveur n'est pas parvenu à authentifier l'adresse e-mail et le mot de passe.

Solutions possibles

- Utilisez l'adresse e-mail associée à l'organisation. Les adresses e-mail personnelles ne peuvent pas être utilisées pour l'activation.
- Entrez de nouveau l'adresse e-mail et le mot de passe et assurez-vous qu'ils ne comportent aucune erreur typographique.
- Demandez à l'administrateur de vérifier que le compte de messagerie est activé et qu'il n'est pas verrouillé.
- Demandez à l'administrateur de réinitialiser le mot de passe du domaine de l'utilisateur.

  Message d'erreur : Erreur de connexion réseau

  Le client Encryption ne parvient pas à communiquer avec le serveur Dell.

  Solutions possibles

- Connectez-vous directement au réseau de l'organisation, puis relancez l'activation.
- Si l'accès VPN est requis pour se connecter au réseau, vérifiez la connexion VPN et faites une nouvelle tentative.
- Vérifiez l'adresse URL de Dell Server pour vous assurer qu'elle correspond à l'URL fournie par l'administrateur.

  L'adresse URL ainsi que d'autres données saisies par l'utilisateur dans le programme d'installation sont stockées dans le répertoire. Assurez-vous que les données sous [HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield] et [HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield\Servlet] sont correctes.

- Déconnexion et reconnexion :

  Déconnectez l'ordinateur du réseau.

  Reconnectez au réseau.

  Redémarrez l'ordinateur.

Tentez de connecter au réseau à nouveau.

Message d'erreur : Serveur hérité non pris en charge

Impossible d'activer Encryption sur un serveur hérité ; la version de Dell Server doit être 9.1 ou ultérieure.

Solution possible

- Vérifiez l'adresse URL de Dell Server pour vous assurer qu'elle correspond à l'URL fournie par l'administrateur.

  L'adresse URL ainsi que d'autres données saisies par l'utilisateur dans le programme d'installation sont stockées dans le répertoire.

- Assurez-vous que les données sous [HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield] et [HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield\Servlet] sont correctes.

Message d'erreur : Utilisateur de domaine déjà activé

Un deuxième utilisateur s'est connecté à l'ordinateur local et a tenté d'activer un compte de domaine qui a déjà été activé.

Un utilisateur peut activer le client de cryptage une seule fois par compte de domaine.

Solution possible

Décryptez et désinstallez le client Encryption quand vous êtes connecté en tant que second utilisateur activé.

Message d'erreur : Erreur générale sur le serveur

Une erreur est survenue sur le serveur.

Solution possible

Il est recommandé à l'administrateur de vérifier les journaux du serveur pour s'assurer que les services sont en cours d'exécution.

L'utilisateur doit tenter l'activation ultérieurement.

Outils

CMGAd

Ouvrez l'utilitaire CMGAd avant de lancer l'agent Encryption Removal pour obtenir le jeu de clés de cryptage. L'utilitaire CMGAd et ses instructions se trouvent sur le support d'installation Dell (Dell-Offline-Admin-XXbit)

Fichiers journaux

Dans `C:\ProgramData\Dell\Dell Data Protection\Encryption`, recherchez le fichier journal appelé **CmgSysTray**.

Recherchez la phrase « Résultat de l'activation manuelle ».

Le code d'erreur est sur la même ligne, suivi de « état = » ; l'état indique ce qui a échoué.

19

Dépannage

Tous les clients - Dépannage

- Les fichiers log du programme d'installation de la suite principale d'**Endpoint Security Suite Enterprise** se trouvent dans `C:\ProgramData\Dell\Dell Data Protection\Installer`.
- Windows crée des **fichiers journaux d'installation du programme d'installation enfant** uniques destinés à l'utilisateur connecté à %temp%, à l'adresse `C:\Users\<NomUtilisateur>\AppData\Local\Temp`.
- Windows crée des fichiers journaux pour les conditions préalables du client (par exemple, Visual C++), pour l'utilisateur connecté à %temp%, à l'adresse `C:\Users\<NomUtilisateur>\AppData\Local\Temp`. Par exemple, `C:\Users\<NomUtilisateur>\AppData\Local\Temp\dd_vcredist_amd64_20160109003943.log`
- Suivez les instructions sur http://msdn.microsoft.com pour vérifier la version de Microsoft.Net qui est installée sur l'ordinateur ciblé pour l'installation.

  Pour télécharger la version complète de Microsoft .Net Framework 4.5.2 ou version ultérieure, consultez https://www.microsoft.com/en-us/download/details.aspx?id=30653.

- Reportez-vous à *ce document* si Dell Access est installé sur l'ordinateur ciblé pour l'installation (ou l'a été dans le passé). Dell Access n'est pas compatible avec cette suite de produits.

Tous les clients - État de la protection

Dell Server v9.8.2. intègre une nouvelle méthode d'extraction de l'état protégé d'un périphérique. Auparavant, la section État protégé du point de terminaison sur le tableau de bord de la console de gestion n'indiquait que l'état de chiffrement par périphérique.

Depuis Dell Server v9.8.2, l'état protégé est indiqué si l'un des critères suivants est satisfait :

- Advanced Threat Prevention est installé et activé.
- Le client Web Protection ou Client Firewall est installé et la stratégie correspondante est activée.
- Self-Encrypting Drive Manager est installé et activé, et l'authentification avant démarrage (PBA) est activée.
- Full Disk Encryption est installé et activé, et la PBA est activée.
- BitLocker Manager est installé et activé, et le cryptage est terminé.
- Dell Encryption (MAC) est installé et activé, et la règle *Chiffrer en utilisant FileVault pour Mac* a été appliquée.
- La solution Dell Encryption (Windows) est installée et activée, le cryptage basé sur des règles a été configuré pour le point de terminaison et les balayages du périphérique ont été effectués.

Dépannage de Dell Encryption (client et serveur)

Activation sur un système d'exploitation de serveur

Lorsque Encryption est installé sur le système d'exploitation d'un serveur, son activation nécessite deux phases : l'activation initiale et l'activation du terminal.

Activation initiale du dépannage

L'activation initiale échoue lorsque :

- Un code nom d'utilisateur principal valide ne peut pas être obtenu à l'aide des références fournies.
- Les informations d'identification sont introuvable dans le coffre de l'entreprise.
- Les informations d'identification utilisées pour l'activation ne sont pas celles de l'administrateur de domaine.

Message d'erreur : nom d'utilisateur inconnu ou mot de passe erroné

Le nom d'utilisateur ou le mot de passe n'est pas valide.

Solution possible : connectez-vous à nouveau en vous assurant de saisir le nom d'utilisateur et le mot de passe correctement.

Message d'erreur : l'activation a échoué car le compte d'utilisateur ne dispose pas de droits d'administrateur du domaine.

Les informations d'identification utilisées pour l'activation ne sont pas dotées des droits d'administrateur de domaine ou bien le nom d'utilisateur de l'administrateur n'était pas au format UPN.

Solution possible **:** dans la boîte de dialogue Activation, saisissez les informations d'identification au format UPN pour un administrateur de domaine.

Messages d'erreur : Impossible d'établir une connexion avec le serveur.

ou

```
The operation timed out.
```

Server Encryption ne peut pas communiquer sur HTTPS avec le port 8449 vers Dell Server.

Solutions possibles

- Connectez-vous directement à votre réseau, puis relancez l'activation.
- Si vous êtes connecté via VPN, essayez de vous connecter directement au réseau et de relancer l'activation.
- Vérifiez l'adresse URL de Dell Server pour vous assurer qu'elle correspond à l'URL fournie par l'administrateur. L'adresse URL ainsi que d'autres données saisies par l'utilisateur dans le programme d'installation sont stockées dans le répertoire. Assurez-vous que les données sous [HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield] et [HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield\Servlet] sont correctes.
- Déconnectez le serveur du réseau. Redémarrez le serveur et reconnectez-le au réseau.

Message d'erreur : L'activation a échoué car le serveur ne peut pas prendre en charge cette demande.

Solutions possibles

- Impossible d'activer Server Encryption sur un serveur hérité ; la version de Dell Server doit être 9.1 ou ultérieure. Si nécessaire, mettez à niveau votre Dell Server à la version 9.1 ou ultérieure.
- Vérifiez l'adresse URL de Dell Server pour vous assurer qu'elle correspond à l'URL fournie par l'administrateur. L'adresse URL ainsi que d'autres données saisies par l'utilisateur dans le programme d'installation sont stockées dans le répertoire.
- Assurez-vous que les données sous [HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield] et [HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield\Servlet] sont correctes.

Processus d'activation initiale

Le schéma suivant illustre une activation initiale réussie.

Le processus d'activation initiale d'Encryption pour systèmes d'exploitation de serveur requiert qu'un utilisateur accède directement au serveur. L'utilisateur peut être de n'importe quel type : membre du domaine ou non, connecté en mode Bureau à distance ou utilisateur interactif. Cependant, l'utilisateur doit avoir accès aux informations d'identification de l'administrateur de domaine.

Le dialogue d'activation s'affiche lorsque l'un des deux flux de travail se produit :

- Un nouvel utilisateur (non géré) se connecte à l'ordinateur.
- Un nouvel utilisateur fait un clic droit sur l'icône d'*Encryption* dans la zone de notification et sélectionne *Activer Dell Encryption*.

  La procédure d'activation initiale se déroule comme suit :

1. L'utilisateur se connecte.
2. Lors de la détection d'un nouvel utilisateur (non géré), la boîte de dialogue *Activer* s'affiche. L'utilisateur clique sur **Annuler**.
3. L'utilisateur ouvre la boîte À propos de Server Encryption pour confirmer que ce dernier est en cours d'exécution en mode Serveur.
4. L'utilisateur fait un clic droit sur l'icône d'*Encryption* dans la zone de notification et sélectionne *Activer Dell Encryption*.
5. L'utilisateur entre les références de l'administrateur de domaine dans la boîte de dialogue Activer.

   REMARQUE :

   La nécessité de fournir les informations d'identification de l'administrateur de domaine est une mesure de sécurité qui empêche Encryption pour systèmes d'exploitation de serveur d'être déployé dans d'autres environnements de serveur non pris en charge. Pour désactiver l'exigence des informations d'identification de l'administrateur de domaine, voir Avant de commencer.
6. Dell Server vérifie les informations d'identification dans le coffre de l'entreprise (Active Directory ou équivalent) afin de s'assurer que ces informations appartiennent bien à un administrateur de domaine.

7. Un UPN est construit à l'aide des références.
8. Avec l'UPN, Dell Server crée un nouveau compte utilisateur pour l'utilisateur du serveur virtuel et stocke ces informations d'identification dans le coffre de Dell Server.

   Un **compte d'utilisateur de serveur virtuel** est réservé à l'utilisation du client Encryption. Il est utilisé pour s'authentifier auprès du serveur, gérer les clés de chiffrement commun et recevoir des mises à jour des règles.

   REMARQUE :

   L'authentification DPAPI et l'authentification par mot de passe sont désactivées pour ce compte, afin que *seul* l'utilisateur de serveur virtuel puisse accéder aux clés de cryptage sur l'ordinateur. Ce compte ne correspond à aucun autre compte utilisateur sur l'ordinateur ou dans le domaine.
9. Lorsque l'activation est réussie, l'utilisateur redémarre l'ordinateur, lequel lance la deuxième phase, l'authentification et l'activation du périphérique.

Dépannage de l'authentification et de l'activation du périphérique

L'activation du périphérique échoue lorsque :

- L'activation initiale a échoué.
- Aucune connexion n'a pu être établie avec le serveur.
- Le certificat de confiance n'a pas pu être validé.

Après l'activation, lorsque l'ordinateur a redémarré, Encryption pour systèmes d'exploitation de serveur se connecte automatiquement en tant qu'utilisateur du serveur virtuel, en demandant la clé d'ordinateur auprès de Dell Server. Cette opération intervient avant même que tout utilisateur puisse ouvrir une session.

- Ouvrez la boîte de dialogue À propos pour vérifier que Encryption pour systèmes d'exploitation de serveur est authentifié et en mode Serveur.
- Si l'ID du Encryption client est rouge, le cryptage n'a pas encore été activé.
- Dans la Console de gestion, la version d'un serveur équipé de Server Encryption est répertoriée comme *Bouclier de serveur*.
- Si la récupération de la clé d'ordinateur échoue en raison d'une défaillance réseau, Server Encryption s'enregistre auprès du système d'exploitation pour les notifications du réseau.
- Si la récupération de la clé d'ordinateur échoue :
  - La connexion de l'utilisateur du serveur virtuel fonctionne malgré tout.
  - Définissez la règle d'*Intervalle entre les tentatives en cas d'échec du réseau* pour procéder à de nouvelles tentatives de récupération de la clé à intervalles définis.

    Pour plus de détails sur la règle d'*Intervalle entre les tentatives en cas d'échec du réseau*, reportez-vous à AdminHelp, disponible dans la console de gestion.

Authentification et activation du périphérique

Le schéma suivant illustre une authentification et une activation réussies d'un périphérique.

1. Après un redémarrage suite à une activation initiale réussie, un ordinateur équipé de Server Encryption s'authentifie automatiquement à l'aide du compte d'utilisateur de serveur virtuel et exécute le client Encryption en mode Serveur.
2. L'ordinateur vérifie l'état d'activation du périphérique auprès de Dell Server :
   - Si l'ordinateur n'a pas encore été activé par un périphérique, Dell Server attribue à l'ordinateur un MCID, un DCID et un certificat de confiance, et stocke toutes ces informations dans le coffre de Dell Server.
   - Si l'ordinateur avait été précédemment activé par un périphérique, Dell Server vérifie le certificat de confiance.
3. Une fois que Dell Server a attribué le certificat de confiance au serveur, ce dernier peut accéder à ses clés de cryptage.
4. L'activation du périphérique a réussi.

   REMARQUE :

   Lors de l'exécution en mode Serveur, le client Encryption doit avoir accès au même certificat qui a été utilisé pour l'activation du périphérique afin de pouvoir accéder aux clés de chiffrement.

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

- Avant de lancer la désinstallation, vous pouvez, si vous le souhaitez, créer un fichier journal Encryption Removal Agent. Ce fichier journal permet de diagnostiquer les erreurs, si vous rencontrez un problème lors de la désinstallation / du décryptage. Si vous ne souhaitez pas décrypter les fichiers à la désinstallation, il n'est pas nécessaire de créer ce fichier journal.

- Le fichier log d'Encryption Removal Agent n'est créé qu'après l'exécution du service Encryption Removal Agent, après le redémarrage de l'ordinateur. Une fois la désinstallation du client et le décryptage de l'ordinateur terminés, le fichier est définitivement supprimé.
- Le chemin du fichier journal est `C:\ProgramData\Dell\Dell Data Protection\Encryption.`
- Créez l'entrée de registre suivante sur l'ordinateur cible pour le décryptage.

  [HKLM\Software\Credant\DecryptionAgent].

  "LogVerbosity"=DWORD:2

  0: aucune consignation

  1 : erreurs bloquant l'exécution du service

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

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

  5 : consigne des informations de débogage

Trouver la version de TSS

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

Encryption External Media et interactions PCS

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

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

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

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

Utiliser WSScan

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

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

Exécutez l'

1. À partir du support d'installation Dell, copiez le fichier WSScan.exe sur l'ordinateur à analyser.
2. Lancez une ligne de commande à l'emplacement spécifié ci-dessus et entrez **wsscan.exe** à l'invite de commande. WSScan démarre.
3. Cliquez sur **Avancé**.
4. Sélectionnez le type du lecteur à rechercher : *Tous les lecteurs, Lecteurs fixes*, *Lecteurs amovibles*, ou *CD-ROM/DVD-ROM*.
5. Sélectionnez le type de rapport de chiffrement : *Fichiers cryptés*, *Fichiers non cryptés*, *Tous les fichiers*, ou *Fichiers non cryptés en violation* :
   - *Fichiers cryptés* : pour vérifier que toutes les données sont décryptées lors de la désinstallation d'Encryption. Suivez votre processus actuel de décryptage des données, par exemple l'envoi d'une mise à jour de règle de décryptage. Une

fois les données décryptées mais avant de redémarrer l'ordinateur en préparation de la désinstallation, exécutez WSScan afin de vous assurer que toutes les données sont décryptées.

- *Fichiers non cryptés* : pour identifier les fichiers qui ne sont pas cryptés, avec une mention indiquant si les fichiers doivent être cryptés (Y/N).
- *Tous les fichiers* : pour répertorier tous les fichiers cryptés et non cryptés, avec une mention indiquant si les fichiers doivent être cryptés (Y/N).
- *Fichiers non cryptés en violation* : pour identifier les fichiers qui ne sont pas cryptés, mais qui devraient l'être.

6. Cliquez sur **Rechercher**.

OU

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

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

Utilisation de la ligne de commande WSScan

```
WSScan [-ta] [-tf] [-tr] [-tc] [drive] [-s] [-o<filepath>] [-a] [-f<format specifier>] [-r]
[-u[a][-|v]] [-d<delimeter>] [-q] [-e] [-x<exclusion directory>] [-y<sleep time>]
```

Commutateur	Signification
Lecteur	Disque à analyser. S'il n'est pas défini, tous les disques durs fixes locaux sont utilisés par défaut. Il peut s'agir d'un lecteur réseau mappé.
-ta	Analyser tous les disques
-tf	Analyser les disques fixes (valeur par défaut)
-tr	Analyser les lecteurs amovibles
-tc	Analyser les CDROM/DVDROM
-s	Opération silencieuse
-o	Chemin d'accès au fichier de sortie.
-a	Ajouter au fichier de sortie . Par défaut, le fichier de sortie est tronqué.
-f	Spécificateur de format de rapport (Rapport, Fixe, Délimité)
-r	Exécutez WSScan dans les privilèges administrateur. **Certains fichiers peuvent ne pas être visibles si ce mode est utilisé.**
-u	Inclure les fichiers non cryptés dans le fichier de sortie.

Commutateur	Signification
	Ce commutateur est sensible à l'ordre : “u” doit être en première position, “a” doit être en deuxième position (ou omis), “-” ou “v” doit être en dernière position.
-u-	Inclure uniquement les fichiers décryptés dans le fichier de sortie
-ua	Signale également les fichiers non cryptés, mais utilise toutes les règles utilisateur pour afficher le champ « should ».
-ua-	Signale les fichiers non cryptés uniquement, mais utilise toutes les règles utilisateur pour afficher le champ « should ».
-uv	Signale les fichiers non cryptés qui violent la règle uniquement (Is=No / Should=Y)
-uav	Signale les fichiers non cryptés qui violent la règle uniquement (Is=No / Should=Y), en utilisant toutes les règles utilisateur.
-d	Spécifie l'élément à utiliser comme séparateur de valeurs pour la sortie délimitée
q	Spécifie les valeurs qui doivent être placées entre guillemets pour la sortie délimitée
-e	Inclure les champs de cryptage étendu dans la sortie délimité
-x	Exclure un répertoire de l'analyse. Plusieurs exclusions sont autorisées.
-y	Inactivité (en millisecondes) entre les répertoires. Ce commutateur ralentit les analyses, mais rend le processeur plus réactif.

Fichier cible WSScan

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

Exemple :

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

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

Sortie	Signification
	Comme dans l'exemple ci-dessus, « **c:\temp\Dell - test.log** »
Algorithme	Algorithme utilisé pour crypter le fichier. Dans l'exemple ci-dessus, « **cryptage AES 256 toujours en place** » RIJNDAEL 128 RIJNDAEL 256 AES-128 AES-256 3DES

Utiliser WSProbe

L'utilitaire Probing est destiné à être utilisé avec toutes les versions d'Encryption, à l'exception des règles Encryption External Media. Utilisez cet utilitaire pour :

- Analyser ou planifier l'analyse d'un ordinateur crypté. Il respecte la règle de priorité d'analyse de poste de travail.
- Désactiver ou réactiver temporairement la liste de cryptage des données d'application de l'utilisateur.
- Ajouter ou supprimer des noms de processus dans la liste privilégiée.
- Exécuter les opérations de dépannage indiquées par Dell ProSupport.

Approches du cryptage des données

Si vous définissez des règles pour crypter les données sur des appareils Windows, vous pouvez utiliser n'importe laquelle des approches suivantes :

- La première approche consiste à accepter le comportement par défaut du client. Si vous définissez des dossiers dans Dossiers cryptés communs ou Dossiers cryptés utilisateur, ou spécifiez Sélectionné pour Crypter « Mes documents », Crypter les dossiers personnels Outlook, Crypter les fichiers temporaires, Crypter les fichiers Internet temporaires ou Crypter le fichier de pagination Windows, les fichiers affectés sont cryptés lors de leur création ou (après leur création par un utilisateur non géré) lorsque l'utilisateur se connecte. Le client analyse également les dossiers d'analyses définis dans ou associés à ces règles pour le cryptage/Décryptage possible lorsqu'un dossier est renommé ou que le client reçoit des modifications de ces règles.
- Vous pouvez aussi sélectionner Analyser la station de travail à la connexion. Dans ce cas, lorsqu'un utilisateur se connecte, le client compare la manière dont les fichiers dans les dossiers actuellement et précédemment cryptés sont cryptés par rapport aux règles utilisateur, et il effectue les modifications appropriées.
- Pour crypter les fichiers qui répondent aux critères de cryptage, mais qui ont été créés avant l'entrée en vigueur des règles de cryptage, vous pouvez utiliser cette règle pour analyser et planifier l'analyse de l'ordinateur si vous ne voulez pas subir l'impact des analyses fréquentes.

Pré-requis

- Le périphérique Windows que vous voulez utiliser doit être chiffré.
- L'utilisateur que vous voulez utiliser doit être connecté.

Utilisation de l'utilitaire de détection

WSProbe.exe se trouve dans le support d'installation.

Syntaxe

```
wsprobe [path]

wsprobe [-h]

wsprobe [-f path]

wsprobe [-u n] [-x process_names] [-i process_names]
```

Paramètres

Paramètre	À
Chemin d'accès	Éventuellement, définissez un chemin particulier sur le périphérique à analyser pour un chiffrement/déchiffrement possible. Si vous ne définissez pas de chemin, cet utilitaire analyse tous les dossiers associés aux règles de cryptage.
-h	Afficher l'aide de la ligne de commande.
-f	Exécuter le dépannage comme indiqué par Dell ProSupport
-u	Activer ou réactiver la liste de cryptage des données d'application d'un utilisateur. Cette liste est effective uniquement si Chiffrement activé est sélectionné pour l'utilisateur en cours. Spécifiez 0 pour désactiver ou 1 pour réactiver. L'état de la règle en cours pour l'utilisateur est restauré lors de la connexion suivante.
-x	Ajouter des noms de processus à la liste privilégiée. L'ordinateur et les noms de processus d'installation dans cette liste, et ceux que vous ajoutez en utilisant ce paramètre ou HKLM\Software\CREDANT\CMGShield\EUWPrivilegedList, sont ignorés s'ils se trouvent dans la liste de cryptage des données d'application. Séparez les noms de processus avec une virgule. Si la liste contient un ou plusieurs espaces, placez-la entre des guillemets doubles.
-i	Supprimez les noms de processus précédemment ajoutés à la liste des privilèges (vous ne pouvez pas supprimer les noms de processus codés en dur). Séparez les noms de processus avec une virgule. Si la liste contient un ou plusieurs espaces, placez-la entre des guillemets doubles.

Vérification de l'état d'Encryption Removal Agent.

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

- **Attente de la désactivation SDE** - Encryption est toujours installé, toujours configuré ou les deux. Le décryptage ne démarrera pas tant qu'Encryption ne sera pas désinstallé.
- **Balayage initial** - Le service procède à un premier balayage en calculant le nombre de fichiers chiffrés et les octets. L'analyse initiale n'a lieu qu'une seule fois.
- **Balayage de décryptage** - Le service déchiffre les fichiers et demande éventuellement à déchiffrer des fichiers verrouillés.
- **Decrypter au redémarrage (partiel)** - Le balayage de décryptage est terminé et certains fichiers verrouillés (mais pas tous) devront être décryptés au prochain redémarrage.
- **Décrypter au redémarrage** - Le balayage de décryptage est terminé et tous les fichiers verrouillés devront être décryptés au prochain redémarrage.
- **Tous les fichiers n'ont pas pu être décryptés** - Le balayage de décryptage est terminé, mais tous les fichiers n'ont pas pu être décryptés. Cet état signifie que l'une des situations suivantes s'applique :
  - Les fichiers verrouillés n'ont pas pu être programmés pour être décryptés, en raison d'une taille trop importante ou du fait qu'une erreur s'est produite lors de la requête de déverrouillage.
  - Une erreur au niveau de la source / de la cible s'est produite lors du décryptage des fichiers.
  - Les fichiers n'ont pas pu être décryptés par la règle.
  - Les fichiers ont le statut « devraient être cryptés ».
  - Une erreur s'est produite lors de l'analyse de décryptage.
  - Dans tous les cas, un fichier de consignation est créé (si vous avez configuré la consignation) si la valeur LogVerbosity est supérieure ou égale à 2. Pour résoudre le problème, choisissez la valeur de verbosité de consignation 2, puis relancez le service Encryption Removal Agent pour forcer l'exécution d'un nouveau balayage de déchiffrement. Voir Création d'un fichier journal Encryption Removal Agent (facultatif) pour obtenir des instructions.
- **Terminé** : l'analyse de déchiffrage est terminée. Le service, le fichier exécutable, le pilote et le fichier exécutable du pilote seront supprimés au prochain redémarrage.

Dépannage d'Advanced Threat Prevention

Trouver le code de produit avec Windows PowerShell

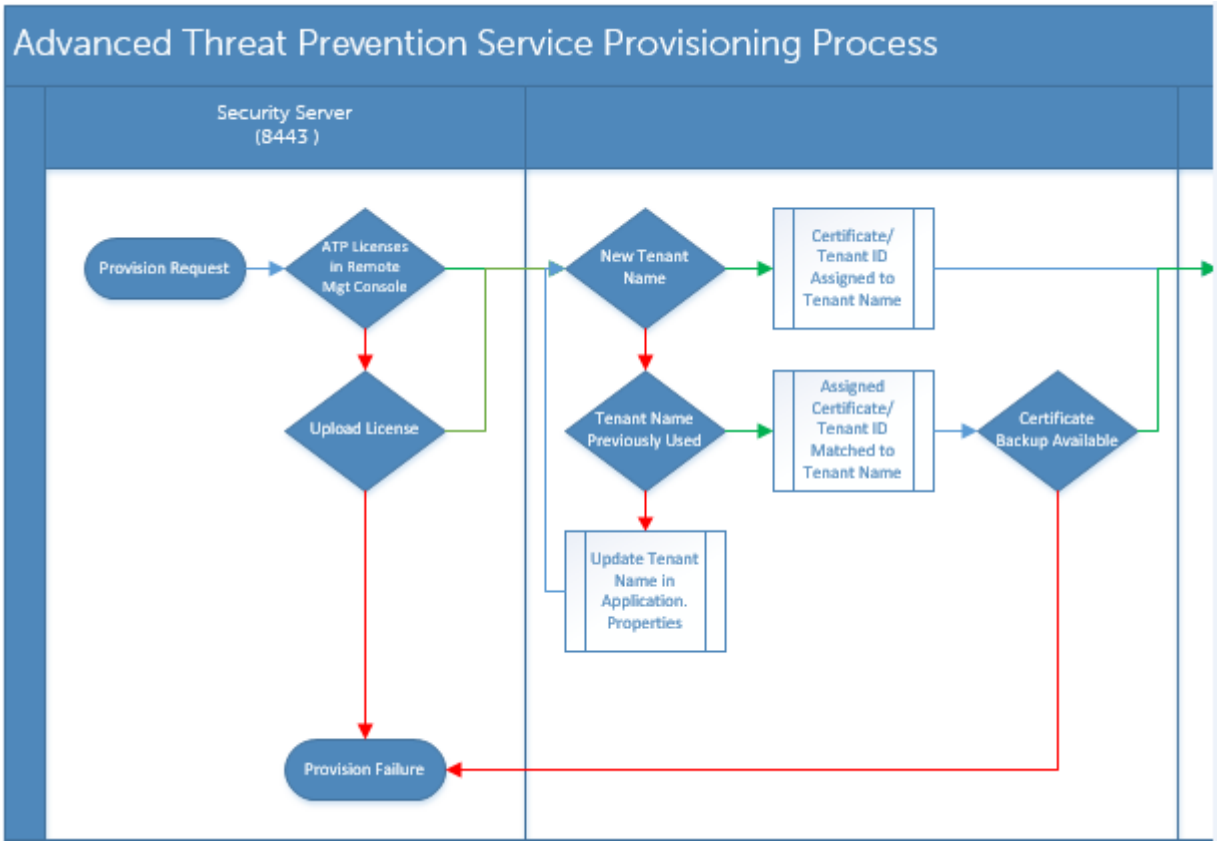
- Vous pouvez facilement identifier le code de produit, si le code de produit change à l'avenir, à l'aide de cette méthode.

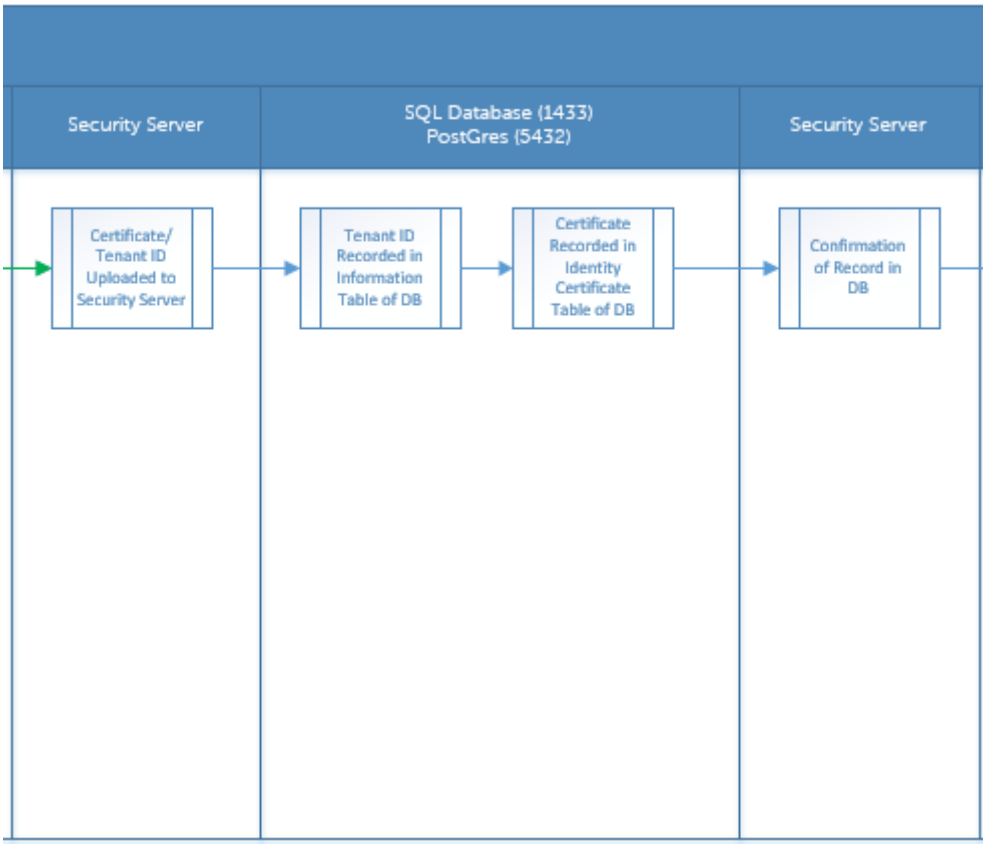
  ```
  Get-WmiObject  Win32_Product | Where-Object {$_.Name -like '*Cylance*'} | FT
  IdentifyingNumber, Name, LocalPackage
  ```

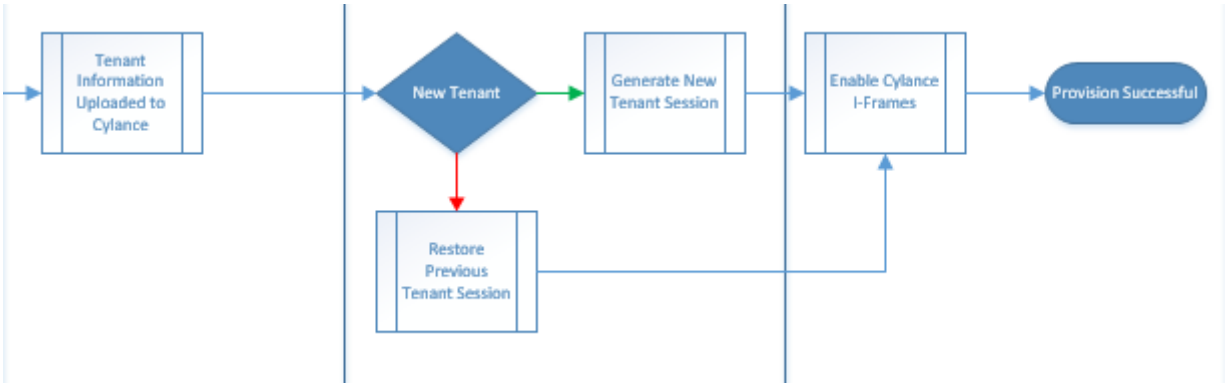
  La sortie génère le chemin complet et le nom du fichier .msi (le nom du fichier converti en valeur hexadécimale).

Provisionnement d'Advanced Threat Prevention et communication agent

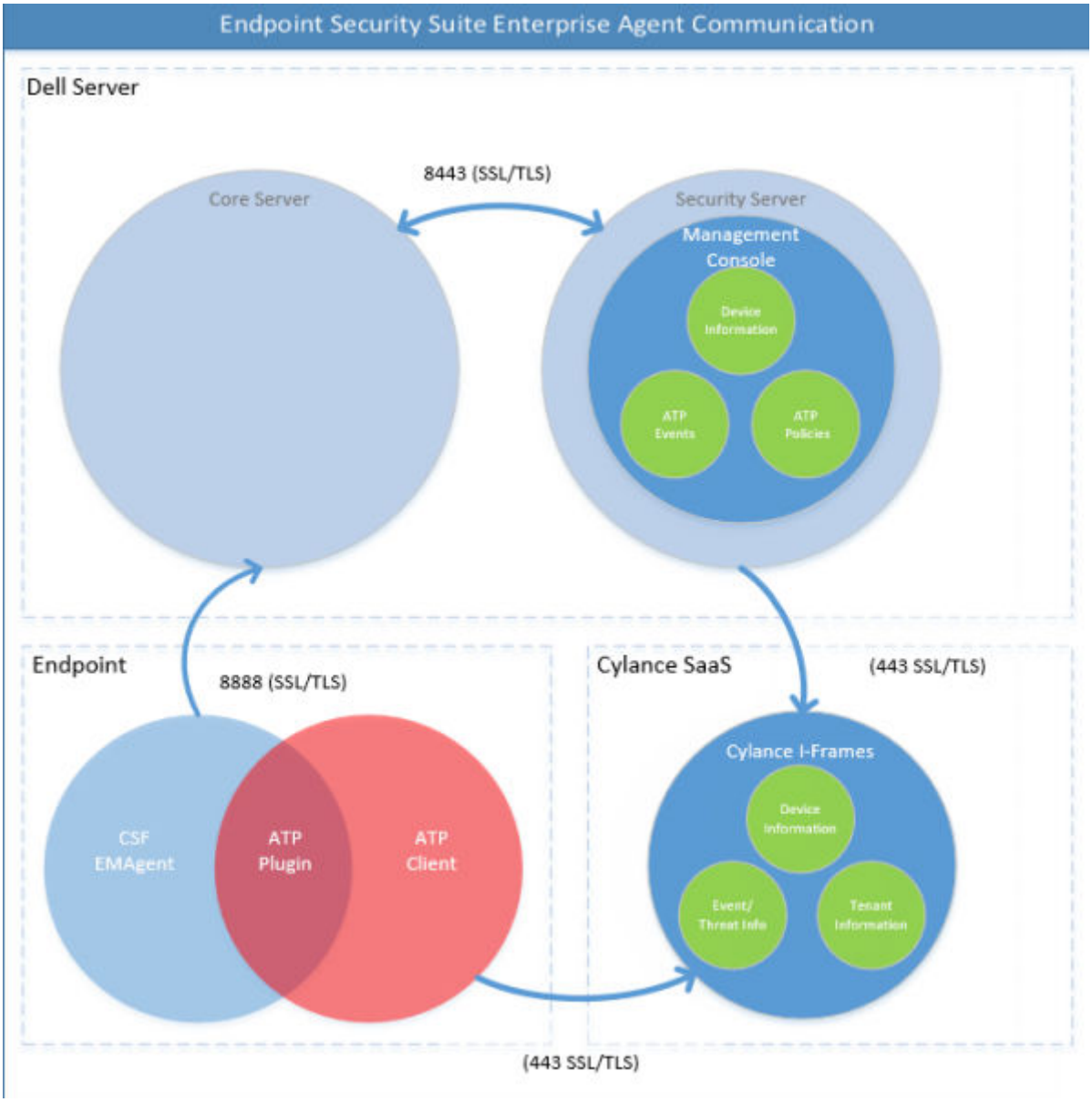
Les diagrammes suivants illustrent le processus de provisionnement du service Advanced Threat Prevention





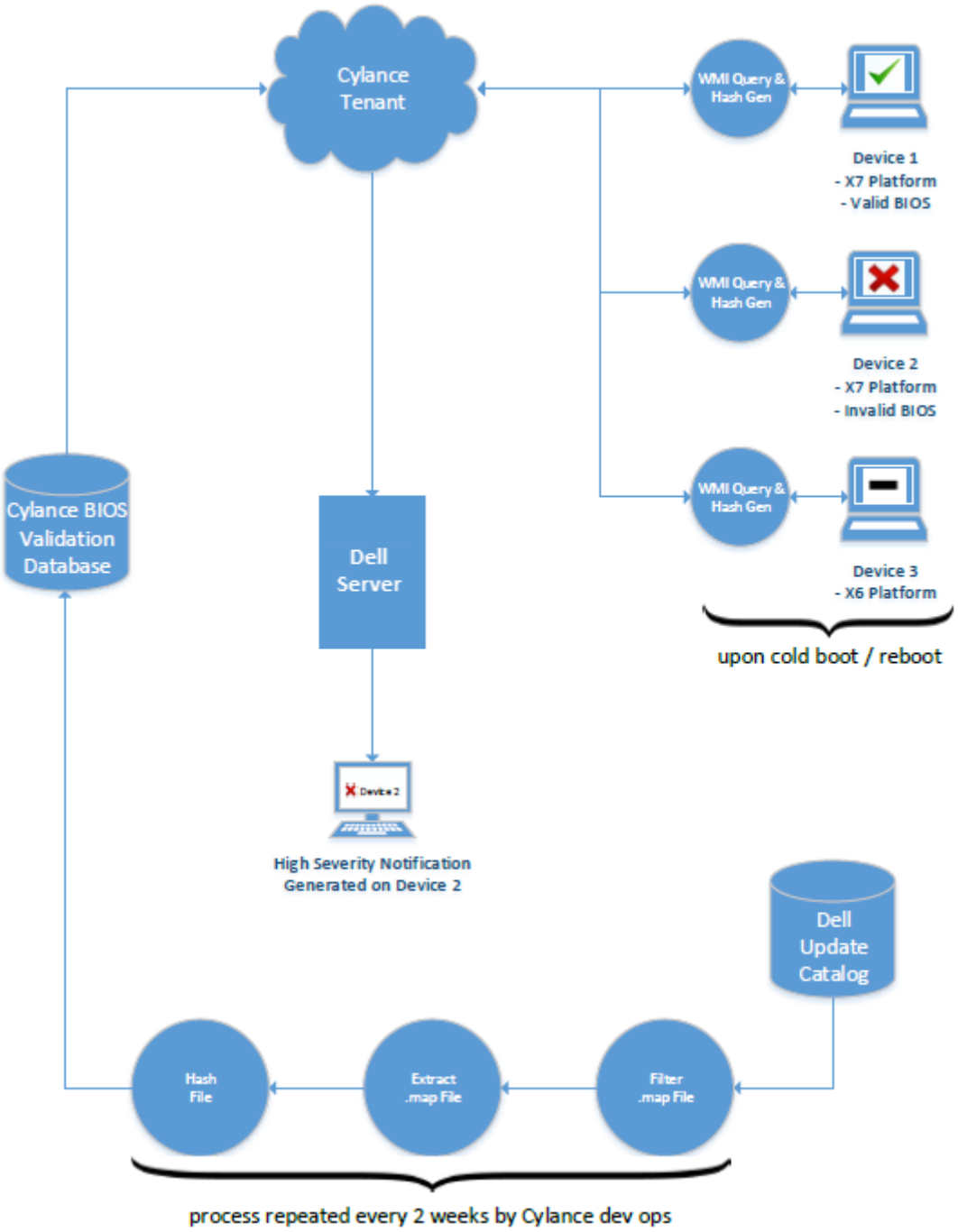


Le diagramme suivant illustre le processus de communication agent d'Advanced Threat Prevention.



Processus de vérification de l'intégrité de l'image BIOS

Le diagramme suivant illustre le processus de vérification de l'intégrité de l'image BIOS. Pour consulter la liste des modèles d'ordinateur Dell pris en charge avec la vérification de l'intégrité de l'image du BIOS, voir la section « Configuration requise : vérification de l'intégrité de l'image BIOS ».



Dépannage SED

Utiliser le code d'accès initial

- Cette règle permet la connexion à un ordinateur lorsqu'il est impossible de se connecter au réseau, c'est-à-dire lorsque le Dell Server et Active Directory (AD) sont indisponibles. Utilisez la règle *Code d'accès initial* uniquement en cas de nécessité absolue. Dell ne conseille pas d'utiliser cette méthode pour se connecter. L'utilisation de la règle *Code d'accès initial* n'assure pas le même degré de sécurité que la méthode de connexion usuelle à l'aide d'un nom d'utilisateur, domaine et mot de passe.

  C'est une méthode de connexion moins sécurisée et en outre, si un utilisateur est activé à l'aide de la règle *Code d'accès initial*, l'activation de cet utilisateur sur cet ordinateur n'est pas consignée sur le Dell Server. Il n'y a alors aucun moyen de générer un code de réponse à partir du Dell Server pour l'utilisateur s'il oublie son mot de passe et ne répond pas correctement aux questions de support autonome.

- Le *Code d'accès initial* ne peut être utilisé qu**'une seule** fois, immédiatement après l'activation. Dès lors qu'un utilisateur s'est connecté, le *Code d'accès initial* n'est plus disponible. La première connexion au domaine survenant après saisie du *Code d'accès initial* occasionnera une mise en cache, et le champ de saisie du *Code d'accès initial* ne sera plus affiché.
- Le *Code d'accès initial* s'affiche **uniquement** dans les conditions suivantes :
  - L'utilisateur n'a jamais été activé dans l'authentification avant démarrage.
  - Le client n'est pas connecté au réseau ou au Dell Server.

Utiliser le code d'accès initial

1. Définissez une valeur pour la règle du **Code d'accès initial** dans la console de gestion.
2. Enregistrez et validez la règle.
3. Démarrez l'ordinateur local.
4. Lorsque l'écran Code d'accès s'affiche, saisissez le **Code d'accès initial**.
5. Cliquez sur la **flèche bleue**.
6. Lorsque la fenêtre d'avertissement légal s'affiche, cliquez sur **OK**.
7. Connectez-vous à Windows avec les identifiants d'utilisateur de cet ordinateur. Ces identifiants doivent faire partie du domaine.
8. Une fois connecté, ouvrez la console Data Security Console et vérifiez que l'utilisateur avec authentification avant démarrage a bien été créé.

   Cliquez sur **Journal** dans le menu supérieur et recherchez le message *Utilisateur avec authentification avant démarrage créé pour <DOMAIN\Username>*, qui indique que le processus a abouti.
9. Éteignez et redémarrez l'ordinateur.
10. Sur l'écran d'ouverture de session, saisissez le nom d'utilisateur, le domaine et le mot de passe que vous avez utilisé précédemment pour vous connecter à Windows.

    Vous devez appliquer le même format de nom d'utilisateur que pour la création de l'utilisateur avec authentification avant démarrage. Ainsi, si vous avez utilisé le format DOMAINE\Nom d'utilisateur, vous devez saisir DOMAINE\Nom d'utilisateur dans Nom d'utilisateur.
11. Lorsque la fenêtre d'avertissement légal s'affiche, cliquez sur **Connexion**.

    Windows démarre et l'ordinateur peut être utilisé comme d'habitude.

Créer un fichier journal d'authentification avant démarrage dans une optique de dépannage

- Dans certains cas, un fichier journal PBA est nécessaire pour résoudre les problèmes PBA, notamment :
  - L'icône de connexion réseau ne s'affiche pas, alors que la connectivité réseau fonctionne. Le fichier journal contient des informations DHCP permettant de résoudre le problème.
  - L'icône de connexion du Dell Server ne s'affiche pas. Le fichier log contient des informations permettant de diagnostiquer les problèmes de connectivité.
  - L'authentification échoue même si les bons identifiants ont été saisis. Le fichier log utilisé avec les journaux de serveur Dell Server peut vous aider à diagnostiquer le problème.

Capturer les journaux lors du démarrage dans l'authentification avant démarrage (Hérité)

1. Créez un dossier sur un lecteur USB en le nommant**`\CredantSED`** au niveau de la racine du lecteur USB.
2. Créez un fichier nommé actions.txt et placez-le dans le dossier **`\CredantSED`** folder.
3. Dans actions.txt, ajoutez la ligne :

   ```
   get logs
   ```
4. Enregistrez le fichier, puis fermez-le.

   N'insérez pas le lecteur USB lorsque l'ordinateur est hors tension. Si le lecteur USB est déjà inséré quand l'ordinateur est à l'arrêt, retirez-le.
5. Allumez l'ordinateur pour reproduire le problème. Insérez le lecteur USB dans l'ordinateur d'où les journaux doivent être collectés au cours de cette étape.
6. Après l'insertion du lecteur USB, patientez 5 à 10 secondes, puis retirez-le.

   Un fichier credpbaenv.tgz est créé dans le dossier **`\CredantSED`** contenant les fichiers journaux nécessaires.

Capturer les journaux lors du démarrage dans l'authentification avant démarrage (UEFI)

1. Créez un fichier appelé **PBAErr.log** au niveau de la racine du lecteur USB.
2. Insérez le lecteur USB **avant** la mise sous tension de l'ordinateur.
3. Retirez le lecteur USB **après** avoir reproduit le problème nécessitant les journaux.

Le fichier PBAErr.log est mis à jour et écrit en temps réel.

Pilotes Dell ControlVault

Mettre à jour les pilotes et le firmware Dell ControlVault

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

Télécharger les derniers pilotes

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

Installation du pilote Dell ControlVault

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

   REMARQUE :

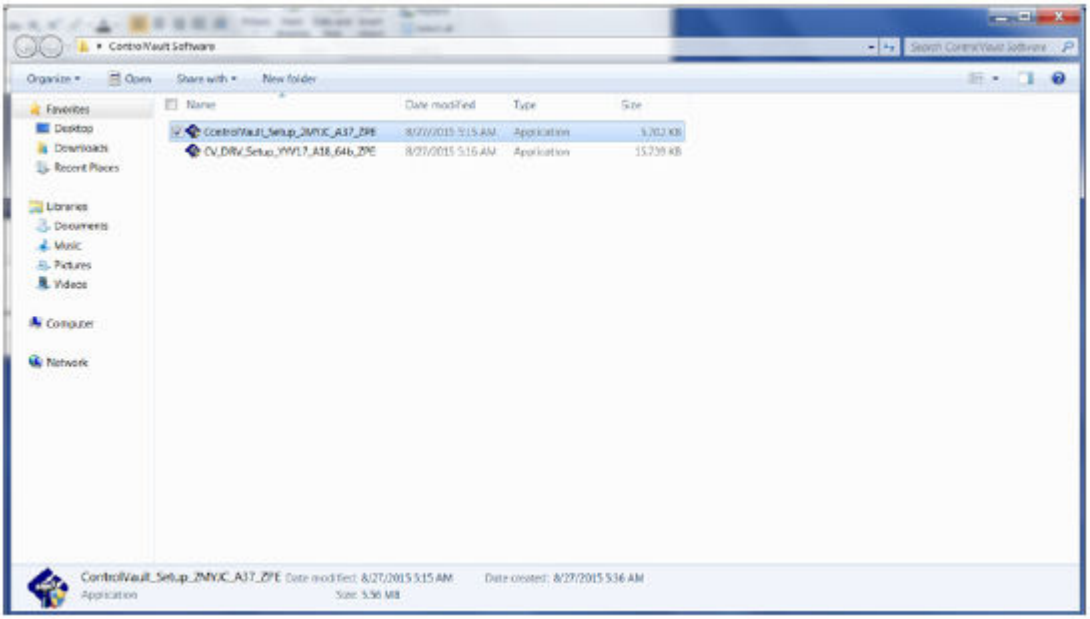
   Assurez-vous d'installer le pilote en premier. Le nom de fichier du pilote *au moment de la création de ce document* est ControlVault_Setup_2MYJC_A37_ZPE.exe.
3. Cliquez sur **Continuer** pour commencer.
4. Cliquez sur **Ok** pour décompresser les fichiers de pilote dans l'emplacement par défaut `C:\Dell\Drivers\<New Folder>`.
5. Cliquez sur **Oui** pour permettre la création d'un nouveau dossier.
6. Cliquez sur **OK** lorsque le message décompression réussie s'affiche.
7. Le dossier contenant les fichiers s'affiche après l'extraction. Sinon, naviguez vers le dossier dans lequel vous avez extrait les fichiers. Dans ce cas, le dossier est **JW22F**.
8. Double-cliquez sur **CVHCI64.MSI** pour lancer le programme d'installation du pilote. [**CVHCI64.MSI** dans cet exemple, (CVHCI pour un ordinateur 32 bits)].
9. Cliquez sur **Suivant** sur l'écran de bienvenue.
10. Cliquez sur **Suivant** pour installer les pilotes à l'emplacement par défaut `C:\Program Files\Broadcom Corporation\Broadcom USH Host Components\.`
11. Sélectionnez l'option **Terminer**, puis cliquez sur **Suivant**.
12. Cliquez sur **Installer** pour démarrer l'installation des pilotes.
13. Facultativement, cochez la case permettant d'afficher le fichier journal du programme d'installation. Cliquez sur **Terminer** pour fermer l'Assistant.

Vérifiez l'installation du pilote.

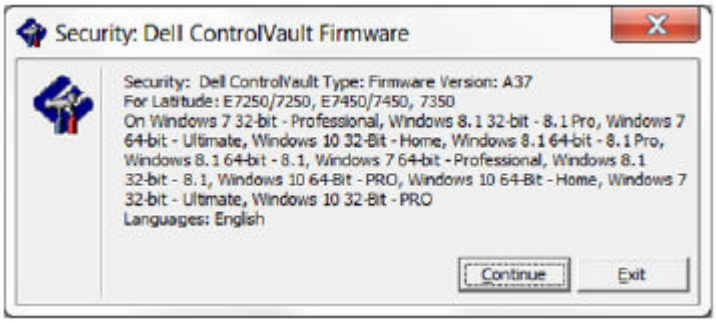
- Le Gestionnaire de périphérique disposera d'un périphérique Dell ControlVault (et d'autres périphériques) en fonction du système d'exploitation et de la configuration matérielle.

Installer le firmware Dell ControlVault

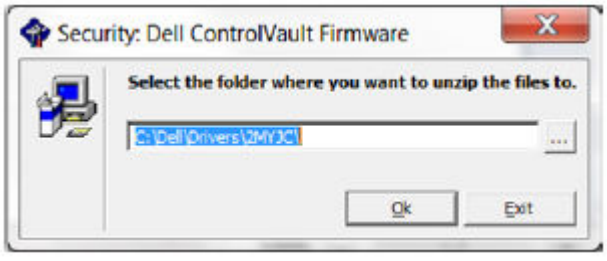
1. Accédez au dossier dans lequel vous avez téléchargé le fichier d'installation du firmware.



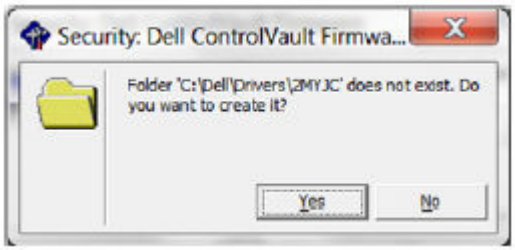
2. Double-cliquez sur le firmware Dell ControlVault pour lancer le fichier exécutable à extraction automatique.
3. Cliquez sur **Continuer** pour commencer.



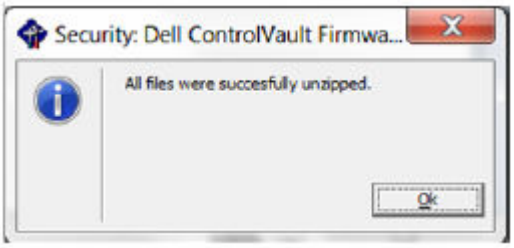
4. Cliquez sur **Ok** pour décompresser les fichiers de pilote dans l'emplacement par défaut `C:\Dell\Drivers\<New Folder>`.



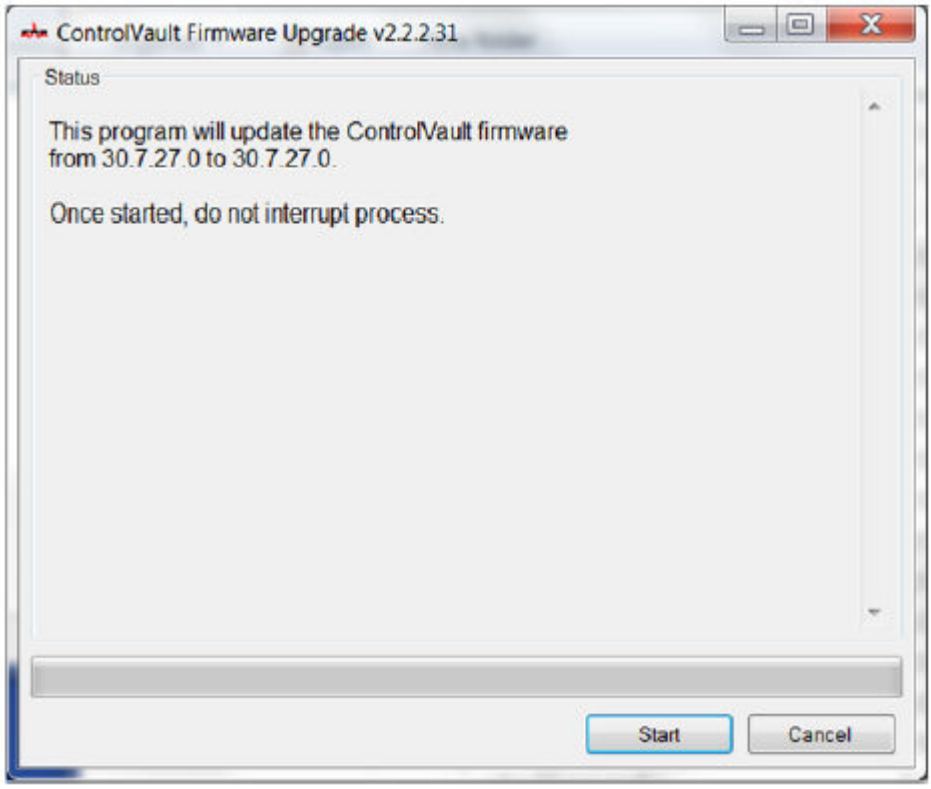
5. Cliquez sur **Oui** pour permettre la création d'un nouveau dossier.



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



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



REMARQUE :

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

Plusieurs messages d'état s'affichent.

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

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

UEFI Computers

Résolution des problèmes de réseau

- Pour que l'authentification avant démarrage réussisse sur un ordinateur équipé du micrologiciel UEFI, le mode d'authentification avant démarrage (PBA) doit disposer de la connectivité réseau. Par défaut, les ordinateurs équipés d'un micrologiciel UEFI ne disposent pas de connectivité réseau tant que le système d'exploitation n'est pas chargé, ce qui intervient après le mode d'authentification avant démarrage. Lorsque la procédure informatique décrite dans Configuration préalable à l'installation pour les ordinateurs UEFI aboutit et qu'elle est correctement configurée, l'icône de connexion réseau apparaît dans l'écran d'authentification avant démarrage lorsque l'ordinateur est connecté au réseau.

- Vérifiez le câble réseau pour vous assurer qu'il est connecté à l'ordinateur si l'icône de connexion réseau ne s'affiche toujours pas pendant l'authentification avant le démarrage. Redémarrez l'ordinateur pour relancer le mode PBA s'il n'était pas connecté ou s'il était désactivé.

TPM et BitLocker

Codes d'erreur TPM et BitLocker

Constante/Valeur	Description
TPM_E_ERROR_MASK 0x80280000	Il s'agit d'un masque d'erreurs pour convertir les erreurs du module de plateforme sécurisée (TPM) en erreurs win.
TPM_E_AUTHFAIL 0x80280001	Échec d'authentification.
TPM_E_BADINDEX 0x80280002	L'index d'un registre PCR, DIR ou autre est incorrect.
TPM_E_BAD_PARAMETER 0x80280003	Au moins un paramètre n'est pas valide
TPM_E_AUDITFAILURE 0x80280004	Une opération s'est déroulée correctement, mais son audit a échoué.
TPM_E_CLEAR_DISABLED 0x80280005	L'indicateur de désactivation de l'effacement est défini et toutes les opérations de suppression nécessitent à présent un accès physique.
TPM_E_DEACTIVATED 0x80280006	Activer le module de plateforme sécurisée (TPM).
TPM_E_DISABLED 0x80280007	Activer le module de plateforme sécurisée (TPM).
TPM_E_DISABLED_CMD 0x80280008	La commande cible a été désactivée.

Constante/Valeur	Description
TPM_E_FAIL 0x80280009	L'opération a échoué.
TPM_E_BAD_ORDINAL 0x8028000A	L'ordinal était inconnu ou incohérent.
TPM_E_INSTALL_DISABLED 0x8028000B	La fonction d'installation d'un propriétaire est désactivée.
TPM_E_INVALID_KEYHANDLE 0x8028000C	Impossible d'interpréter le descripteur de clé.
TPM_E_KEYNOTFOUND 0x8028000D	Le descripteur de clé pointe vers une clé non valide.
TPM_E_INAPPROPRIATE_ENC 0x8028000E	Schéma de cryptage inacceptable.
TPM_E_MIGRATEFAIL 0x8028000F	Échec de l'autorisation de migration.
TPM_E_INVALID_PCR_INFO 0x80280010	Impossible d'interpréter les informations PCR.
TPM_E_NOSPACE 0x80280011	Aucun espace pour charger la clé.
TPM_E_NOSRK 0x80280012	Aucune clé racine de stockage (Storage Root Key, SRK) n'est définie.
TPM_E_NOTSEALED_BLOB 0x80280013	Un objet blob crypté n'est pas valide ou n'a pas été créé par ce module TPM.
TPM_E_OWNER_SET 0x80280014	Le module TPM a déjà un propriétaire.
TPM_E_RESOURCES 0x80280015	Le module TPM ne dispose pas des ressources suffisantes pour exécuter l'action demandée.
TPM_E_SHORTRANDOM 0x80280016	Une chaîne aléatoire était trop courte.
TPM_E_SIZE 0x80280017	Le module TPM ne dispose pas de l'espace approprié pour exécuter l'opération.
TPM_E_WRONGPCRVAL 0x80280018	La valeur PCR nommée ne correspond pas à la valeur PCR actuelle.
TPM_E_BAD_PARAM_SIZE 0x80280019	L'argument paramSize dans la commande a une valeur incorrecte.

Constante/Valeur	Description
TPM_E_SHA_THREAD 0x8028001A	Il n'existe pas d'unité d'exécution SHA-1 existante
TPM_E_SHA_ERROR 0x8028001B	Le calcul ne peut pas être exécuté, car une erreur s'est déjà produite sur l'unité d'exécution SHA-1.
TPM_E_FAILEDSELFTEST 0x8028001C	Le périphérique matériel du Module de plateforme sécurisée (TPM) a signalé une erreur lors de son auto-test interne. Essayez de redémarrer l'ordinateur pour résoudre le problème. Si le problème persiste, vous devrez peut-être remplacer le matériel du Module de plateforme sécurisée (TPM) ou la carte mère.
TPM_E_AUTH2FAIL 0x8028001D	Échec de l'autorisation pour la seconde clé d'une fonction à deux clés.
TPM_E_BADTAG 0x8028001E	La valeur d'indicateur envoyée pour une commande n'est pas valide.
TPM_E_IOERROR 0x8028001F	Une erreur d'E/S sortie s'est produite lors de la transmission des informations au module TPM.
TPM_E_ENCRYPT_ERROR 0x80280020	Un problème est apparu dans le processus de cryptage.
TPM_E_DECRYPT_ERROR 0x80280021	Le processus de cryptage ne s'est pas terminé.
TPM_E_INVALID_AUTHHANDLE 0x80280022	Un handle non valide a été utilisé.
TPM_E_NO_ENDORSEMENT 0x80280023	Le module TPM n'a pas de clé EK (Endorsement Key) installée.
TPM_E_INVALID_KEYUSAGE 0x80280024	L'utilisation d'une clé n'est pas autorisée.
TPM_E_WRONG_ENTITYTYPE 0x80280025	Le type d'entité envoyé n'est pas autorisé.
TPM_E_INVALID_POSTINIT 0x80280026	La commande a été reçue dans la séquence inappropriée par rapport à TPM_Init et à une commande TPM_Startup subséquente.
TPM_E_INAPPROPRIATE_SIG 0x80280027	Les données signées ne peuvent pas contenir des informations DER supplémentaires.
TPM_E_BAD_KEY_PROPERTY 0x80280028	Les propriétés de clé dans TPM_KEY_PARMs ne sont pas compatibles avec ce module TPM.
TPM_E_BAD_MIGRATION 0x80280029	Les propriétés de migration de cette clé sont incorrectes.

Constante/Valeur	Description
TPM_E_BAD_SCHEME 0x8028002A	La signature ou le schéma de cryptage de cette clé sont incorrects ou non autorisés dans ce cas.
TPM_E_BAD_DATASIZE 0x8028002B	La taille du paramètre de données (ou blob) est incorrecte ou incohérente avec la clé référencée.
TPM_E_BAD_MODE 0x8028002C	Un paramètre de mode est incorrect, par exemple capArea ou subCapArea pour TPM_GetCapability ; physicalPresence pour TPM_PhysicalPresence ou migrationType pour TPM_CreateMigrationBlob.
TPM_E_BAD_PRESENCE 0x8028002D	La valeur de bits physicalPresence ou physicalPresenceLock est erronée.
TPM_E_BAD_VERSION 0x8028002E	Le module TPM ne peut pas exécuter cette version de la fonctionnalité.
TPM_E_NO_WRAP_TRANSPORT 0x8028002F	Le module de plateforme sécurisée (TPM) ne tient pas compte des sessions de transport encapsulées.
TPM_E_AUDITFAIL_UNSUCCESSFUL 0x80280030	La construction de l'audit du module de plateforme sécurisée (TPM) a échoué ; la commande sous-jacente renvoyait également un code d'échec.
TPM_E_AUDITFAIL_SUCCESSFUL 0x80280031	La construction de l'audit du module de plateforme sécurisée TPM a échoué et la commande sous-jacente a retourné un succès.
TPM_E_NOTRESETABLE 0x80280032	Tentative de réinitialisation d'un registre PCR dépourvu de l'attribut réinitialisable.
TPM_E_NOTLOCAL 0x80280033	Tentative de réinitialiser un registre PCR qui nécessite une localité, et le modificateur de localité de fait pas partie du transport de commande.
TPM_E_BAD_TYPE 0x80280034	Rendre la saisie de l'objet BLOB d'identité incorrecte.
TPM_E_INVALID_RESOURCE 0x80280035	Lors de l'enregistrement du contexte, la ressource identifiée ne correspond pas à la ressource réelle.
TPM_E_NOTFIPS 0x80280036	Le module TPM tente d'exécuter une commande uniquement disponible en mode iFIPS.
TPM_E_INVALID_FAMILY 0x80280037	La commande tente d'utiliser un ID de famille non valide.
TPM_E_NO_NV_PERMISSION 0x80280038	L'autorisation de manipuler le stockage NV n'est pas disponible.
TPM_E_REQUIRES_SIGN 0x80280039	L'opération nécessite une commande signée.
TPM_E_KEY_NOTSUPPORTED	Opération erronée pour charger une clé NV.

Constante/Valeur	Description
0x8028003A	
TPM_E_AUTH_CONFLICT 0x8028003B	L'objet blob NV_LoadKey nécessite un propriétaire et une autorisation blob.
TPM_E_AREA_LOCKED 0x8028003C	La zone NV est verrouillée et non inscriptible.
TPM_E_BAD_LOCALITY 0x8028003D	La localité est incorrecte pour l'opération tentée.
TPM_E_READ_ONLY 0x8028003E	La zone NV est en lecture seule et aucune donnée ne peut y être écrite.
TPM_E_PER_NOWRITE 0x8028003F	Aucune protection d'écriture dans la zone NV.
TPM_E_FAMILYCOUNT 0x80280040	La valeur du compteur de familles ne correspond pas.
TPM_E_WRITE_LOCKED 0x80280041	Des données ont déjà été écrites dans la zone NV.
TPM_E_BAD_ATTRIBUTES 0x80280042	Conflit d'attributs de zone NV.
TPM_E_INVALID_STRUCTURE 0x80280043	L'indicateur et la version de structure ne sont pas valides ou sont incohérents.
TPM_E_KEY_OWNER_CONTROL 0x80280044	La clé demeure sous le contrôle du propriétaire du module de plateforme sécurisée (TPM), il est le seul à pouvoir l'expulser.
TPM_E_BAD_COUNTER 0x80280045	Le handle du compteur est incorrect.
TPM_E_NOT_FULLWRITE 0x80280046	L'écriture ne représente pas l'écriture complète de la zone.
TPM_E_CONTEXT_GAP 0x80280047	L'écart entre les nombres de contextes enregistrés est trop important.
TPM_E_MAXNVWRITES 0x80280048	Le nombre maximum d'écritures NV sans propriétaire a été atteint.
TPM_E_NOOPERATOR 0x80280049	Aucune valeur AuthData d'opérateur n'est définie.
TPM_E_RESOURCEMISSING 0x8028004A	La ressource désignée par le contexte n'est pas chargée.
TPM_E_DELEGATE_LOCK	L'administration de délégation est verrouillée.

Constante/Valeur	Description
0x8028004B	
TPM_E_DELEGATE_FAMILY 0x8028004C	Tentative de gestion d'une famille autre que la famille déléguée.
TPM_E_DELEGATE_ADMIN 0x8028004D	Gestion de table de délégation non activée.
TPM_E_TRANSPORT_NOTEXCLUSIVE 0x8028004E	Une commande a été exécutée en dehors d'une session de transport exclusive.
TPM_E_OWNER_CONTROL 0x8028004F	Tentative d'enregistrer en contexte une clé dont l'expulsion est contrôlée par le propriétaire.
TPM_E_DAA_RESOURCES 0x80280050	La commande DAA n'a pas de ressources disponibles pour exécuter la commande.
TPM_E_DAA_INPUT_DATA0 0x80280051	La vérification de cohérence sur le paramètre DAA inputData0 a échoué.
TPM_E_DAA_INPUT_DATA1 0x80280052	La vérification de cohérence sur le paramètre DAA inputData1 a échoué.
TPM_E_DAA_ISSUER_SETTINGS 0x80280053	La vérification de cohérence sur DAA_issuerSettings a échoué.
TPM_E_DAA_TPM_SETTINGS 0x80280054	La vérification de cohérence sur DAA_tpmSpecific a échoué.
TPM_E_DAA_STAGE 0x80280055	Le processus automatique indiqué par la commande DAA soumise n'est pas le processus attendu.
TPM_E_DAA_ISSUER_VALIDITY 0x80280056	La vérification de validité de l'émetteur a détecté une incohérence.
TPM_E_DAA_WRONG_W 0x80280057	La vérification de cohérence sur w a échoué.
TPM_E_BAD_HANDLE 0x80280058	Le gestionnaire n'est pas correct.
TPM_E_BAD_DELEGATE 0x80280059	La délégation n'est pas correcte.
TPM_E_BADCONTEXT 0x8028005A	L'objet blob de contexte n'est pas valide.
TPM_E_TOOMANYCONTEXTS 0x8028005B	Trop de contextes détenus par le module TPM.
TPM_E_MA_TICKET_SIGNATURE	La validation de la signature de migration a échoué.

Constante/Valeur	Description
0x8028005C	
TPM_E_MA_DESTINATION 0x8028005D	Destination de migration non authentifiée.
TPM_E_MA_SOURCE 0x8028005E	Source de migration incorrecte.
TPM_E_MA_AUTHORITY 0x8028005F	Autorité de migration incorrecte.
TPM_E_PERMANENTEK 0x80280061	Tentative de révocation de EK alors qu'EK n'est pas révocable.
TPM_E_BAD_SIGNATURE 0x80280062	Signature incorrecte du ticket CMK.
TPM_E_NOCONTEXTSPACE 0x80280063	Aucune place dans la liste de contextes pour d'autres contextes.
TPM_E_COMMAND_BLOCKED 0x80280400	La commande a été bloquée.
TPM_E_INVALID_HANDLE 0x80280401	Le descripteur défini est introuvable.
TPM_E_DUPLICATE_VHANDLE 0x80280402	Le module TPM a retourné un descripteur en double, et la commande doit être resoumise.
TPM_E_EMBEDDED_COMMAND_BLOCKED 0x80280403	La commande a été bloquée dans le transport.
TPM_E_EMBEDDED_COMMAND_UNSUPPORTED 0x80280404	La commande dans le transport n'est pas prise en charge.
TPM_E_RETRY 0x80280800	Le module de plateforme sécurisée (TPM) est trop occupé pour répondre immédiatement à la commande, mais celle-ci pourra de nouveau être soumise ultérieurement.
TPM_E_NEEDS_SELFTEST 0x80280801	SelfTestFull n'a pas été exécuté.
TPM_E_DOING_SELFTEST 0x80280802	Le module TPM exécute un autotest complet.
TPM_E_DEFEND_LOCK_RUNNING 0x80280803	Le module de plateforme sécurisée (TPM) se défend actuellement contre les attaques par dictionnaire et il observe un délai d'attente.
TBS_E_INTERNAL_ERROR 0x80284001	Une erreur logicielle interne a été détectée.
TBS_E_BAD_PARAMETER	Au moins un paramètre d'entrée n'est pas valide.

Constante/Valeur	Description
0x80284002	
TBS_E_INVALID_OUTPUT_POINTER 0x80284003	Un pointeur de sortie défini est incorrect.
TBS_E_INVALID_CONTEXT 0x80284004	Le handle de contexte défini ne fait pas référence à un contexte valide.
TBS_E_INSUFFICIENT_BUFFER 0x80284005	Une mémoire tampon de sortie définie est trop petite.
TBS_E_IOERROR 0x80284006	Erreur de communication avec le module TPM.
TBS_E_INVALID_CONTEXT_PARAM 0x80284007	Au moins un paramètre de contexte n'est pas valide
TBS_E_SERVICE_NOT_RUNNING 0x80284008	Le service TBS n'est pas actif ou n'a pas pu démarrer.
TBS_E_TOO_MANY_TBS_CONTEXTS 0x80284009	Aucun contexte n'a pu être créé, car un trop grand nombre de contextes sont ouverts.
TBS_E_TOO_MANY_RESOURCES 0x8028400A	Aucune ressource n'a pu être créée, car un trop grand nombre de ressources virtuelles sont ouvertes.
TBS_E_SERVICE_START_PENDING 0x8028400B	Le service TBS a été démarré, mais il n'est pas actif.
TBS_E_PPI_NOT_SUPPORTED 0x8028400C	L'interface de présence physique n'est pas prise en charge.
TBS_E_COMMAND_CANCELED 0x8028400D	La commande a été annulée.
TBS_E_BUFFER_TOO_LARGE 0x8028400E	Le tampon d'entrée ou de sortie est trop volumineux.
TBS_E_TPM_NOT_FOUND 0x8028400F	Aucun périphérique de sécurité TPM n'a été trouvé sur cet ordinateur.
TBS_E_SERVICE_DISABLED 0x80284010	Le service TBS a été désactivé.
TBS_E_NO_EVENT_LOG 0x80284011	Aucun journal d'événements TCG disponible.
TBS_E_ACCESS_DENIED 0x80284012	L'appelant ne dispose pas des droits appropriés pour exécuter l'opération demandée
TBS_E_PROVISIONING_NOT_ALLOWED	L’action de configuration du module de plateforme sécurisée (TPM) n’est pas autorisée par les indicateurs.

Constante/Valeur	Description
0x80284013	Pour que la configuration soit prise en compte, l'une des nombreuses actions peut être requise. L'action de la console de gestion du module de plateforme sécurisée (tpm.msc) permettant de préparer le module de plateforme sécurisée (TPM) peut s'avérer utile. Pour plus d'informations, consultez la documentation relative à la méthode WMI Win32_Tpm « Provision ». (Parmi les actions qui peuvent être nécessaires figurent l'importation de la valeur d'autorisation du propriétaire du module de plateforme sécurisée dans le système, l'appel de la méthode Win32_Tpm WMI pour la configuration du module de plateforme sécurisée (TPM) et la spécification de la valeur TRUE pour « ForceClear_Allowed » ou « PhysicalPresencePrompts_Allowed » (comme indiqué par la valeur retournée dans les Informations supplémentaires), ou l'activation du module de plateforme sécurisée (TPM) dans le BIOS du système.)
TBS_E_PPI_FUNCTION_UNSUPPORTED 0x80284014	L'interface de présence physique de ce microprogramme ne prend pas en charge la méthode demandée.
TBS_E_OWNERAUTH_NOT_FOUND 0x80284015	La valeur d'autorisation du propriétaire du module de plateforme sécurisée (TPM) demandée est introuvable.
TBS_E_PROVISIONING_INCOMPLETE 0x80284016	Impossible de terminer la configuration du module de plateforme sécurisée (TPM). Pour plus d'informations sur l'exécution de la configuration, appelez la méthode WMI Win32_Tpm pour configurer le module de plateforme sécurisée (« Provision »), puis vérifiez les informations retournée.
TPMAPI_E_INVALID_STATE 0x80290100	Le tampon de la commande n'est pas en état correct.
TPMAPI_E_NOT_ENOUGH_DATA 0x80290101	Les données contenues dans le tampon de commande ne sont pas suffisantes pour satisfaire la demande.
TPMAPI_E_TOO_MUCH_DATA 0x80290102	Les données contenues dans le tampon de commande ne sont pas suffisantes pour satisfaire la demande.
TPMAPI_E_INVALID_OUTPUT_POINTER 0x80290103	Au moins un paramètre de sortie était de valeur NULL ou incorrect.
TPMAPI_E_INVALID_PARAMETER 0x80290104	Au moins un paramètre d'entrée n'est pas valide
TPMAPI_E_OUT_OF_MEMORY 0x80290105	Mémoire insuffisante pour satisfaire la demande.
TPMAPI_E_BUFFER_TOO_SMALL 0x80290106	Le tampon spécifié était trop petit.
TPMAPI_E_INTERNAL_ERROR 0x80290107	Une erreur interne a été détectée.

Constante/Valeur	Description
TPMAPI_E_ACCESS_DENIED 0x80290108	L'appelant ne dispose pas des droits appropriés pour exécuter l'opération demandée
TPMAPI_E_AUTHORIZATION_FAILED 0x80290109	Les informations d'autorisation spécifiées étaient inexactes.
TPMAPI_E_INVALID_CONTEXT_HANDLE 0x8029010A	Le handle de contexte spécifié était incorrect.
TPMAPI_E_TBS_COMMUNICATION_ERROR 0x8029010B	Erreur de communication avec le TBS.
TPMAPI_E_TPM_COMMAND_ERROR 0x8029010C	La plateforme sécurisée (TPM) a renvoyé un résultat imprévu.
TPMAPI_E_MESSAGE_TOO_LARGE 0x8029010D	Le message était trop volumineux pour le schéma de codage.
TPMAPI_E_INVALID_ENCODING 0x8029010E	Le codage de l'objet BLOB n'a pas été reconnu.
TPMAPI_E_INVALID_KEY_SIZE 0x8029010F	La taille de clé n'est pas valide.
TPMAPI_E_ENCRYPTION_FAILED 0x80290110	L'opération de cryptage a échoué.
TPMAPI_E_INVALID_KEY_PARAMS 0x80290111	La structure des paramètres de clé n'était pas valide
TPMAPI_E_INVALID_MIGRATION_AUTHORIZATION_BLOB 0x80290112	Les données requises fournies ne semblent pas correspondre à un objet BLOB d'autorisation de migration valide.
TPMAPI_E_INVALID_PCR_INDEX 0x80290113	L'index PCR spécifié était incorrect.
TPMAPI_E_INVALID_DELEGATE_BLOB 0x80290114	Les données en question ne semblent pas correspondre à un objet BLOB de délégation valide.
TPMAPI_E_INVALID_CONTEXT_PARAMS 0x80290115	Au moins un paramètre de contexte n'était pas valide.
TPMAPI_E_INVALID_KEY_BLOB 0x80290116	Les données en question ne semblent pas correspondre à un objet BLOB de clé valide.
TPMAPI_E_INVALID_PCR_DATA 0x80290117	Les données PCR définies n'étaient pas corrects.
TPMAPI_E_INVALID_OWNER_AUTH 0x80290118	Le format des données auth du propriétaire n'étaient pas valides.

Constante/Valeur	Description
TPMAPI_E_FIPS_RNG_CHECK_FAILED 0x80290119	Le nombre aléatoire généré n'a pas passé avec succès le contrôle FIPS RNG.
TPMAPI_E_EMPTY_TCG_LOG 0x8029011A	Le journal des événements TCG ne contient pas de données.
TPMAPI_E_INVALID_TCG_LOG_ENTRY 0x8029011B	Une entrée du journal d'événements TCG n'était pas valide.
TPMAPI_E_TCG_SEPARATOR_ABSENT 0x8029011C	Un séparateur TCG est introuvable.
TPMAPI_E_TCG_INVALID_DIGEST_ENTRY 0x8029011D	Une valeur digest contenue dans une entrée du journal TCG ne correspond pas aux données hachées.
TPMAPI_E_POLICY_DENIES_OPERATION 0x8029011E	L'opération demandée a été bloquée par la stratégie actuelle du module de plateforme sécurisée (TPM). Contactez votre administrateur système pour obtenir de l'aide.
TBSIMP_E_BUFFER_TOO_SMALL 0x80290200	Le tampon spécifié était trop petit.
TBSIMP_E_CLEANUP_FAILED 0x80290201	Le contexte n'a pas pu être nettoyé.
TBSIMP_E_INVALID_CONTEXT_HANDLE 0x80290202	Le handle de contexte spécifié est incorrect.
TBSIMP_E_INVALID_CONTEXT_PARAM 0x80290203	Un paramètre de contexte incorrect a été spécifié.
TBSIMP_E_TPM_ERROR 0x80290204	Erreur de communication avec la plateforme sécurisée (TPM).
TBSIMP_E_HASH_BAD_KEY 0x80290205	Aucune entrée avec la clé spécifiée n'a été trouvée.
TBSIMP_E_DUPLICATE_VHANDLE 0x80290206	Le handle virtuel spécifié correspond à un handle virtuel déjà utilisé.
TBSIMP_E_INVALID_OUTPUT_POINTER 0x80290207	La valeur du pointeur vers l'emplacement de handle spécifié était NUL ou incorrecte.
TBSIMP_E_INVALID_PARAMETER 0x80290208	Au moins un paramètre est incorrect.
TBSIMP_E_RPC_INIT_FAILED 0x80290209	L'initialisation du sous-système RPC était impossible.
TBSIMP_E_SCHEDULER_NOT_RUNNING 0x8029020A	Le planificateur TBS ne s'exécute pas.

Constante/Valeur	Description
TBSIMP_E_COMMAND_CANCELED 0x8029020B	La commande a été annulée.
TBSIMP_E_OUT_OF_MEMORY 0x8029020C	Mémoire insuffisante pour répondre à la demande
TBSIMP_E_LIST_NO_MORE_ITEMS 0x8029020D	La liste spécifiée est vide ou l'itération a atteint la fin de la liste.
TBSIMP_E_LIST_NOT_FOUND 0x8029020E	L'élément spécifié est introuvable dans la liste.
TBSIMP_E_NOT_ENOUGH_SPACE 0x8029020F	L'espace offert par le module de plateforme sécurisée (TPM) est insuffisant pour charger la ressource demandée.
TBSIMP_E_NOT_ENOUGH_TPM_CONTEXTS 0x80290210	Les contextes du module TPM en cours d'utilisation sont trop nombreux.
TBSIMP_E_COMMAND_FAILED 0x80290211	La commande de plateforme sécurisée (TPM) a échoué.
TBSIMP_E_UNKNOWN_ORDINAL 0x80290212	Le service TBS ne reconnaît pas l'ordinal spécifié.
TBSIMP_E_RESOURCE_EXPIRED 0x80290213	La ressource demandée n'est plus disponible.
TBSIMP_E_INVALID_RESOURCE 0x80290214	Le type de ressource ne correspondait pas.
TBSIMP_E_NOTHING_TO_UNLOAD 0x80290215	Aucune ressource ne peut être déchargée.
TBSIMP_E_HASH_TABLE_FULL 0x80290216	Aucune nouvelle entrée ne peut être ajoutée à la table de hachage.
TBSIMP_E_TOO_MANY_TBS_CONTEXTS 0x80290217	Impossible de créer un nouveau contexte TBS, car il y a trop de contextes ouverts.
TBSIMP_E_TOO_MANY_RESOURCES 0x80290218	Aucune ressource n'a pu être créée, car un trop grand nombre de ressources virtuelles sont ouvertes.
TBSIMP_E_PPI_NOT_SUPPORTED 0x80290219	L'interface de présence physique n'est pas prise en charge.
TBSIMP_E_TPM_INCOMPATIBLE 0x8029021A	TBS non compatible avec la version du TPM qui figure sur le système.
TBSIMP_E_NO_EVENT_LOG 0x8029021B	Aucun journal d'événements TCG disponible.

Constante/Valeur	Description
TPM_E_PPI_ACPI_FAILURE 0x80290300	Une erreur générale a été détectée lors de l'acquisition de la réponse du BIOS à la commande Physical Presence.
TPM_E_PPI_USER_ABORT 0x80290301	L'utilisateur n'a pas pu confirmer la demande d'opération du module de plateforme sécurisée (TPM).
TPM_E_PPI_BIOS_FAILURE 0x80290302	L'exécution de l'opération TPM demandée n'a pu se dérouler correctement en raison de l'échec du BIOS (par ex. demande d'opération TPM non valide, erreur de communication BIOS avec le module TPM).
TPM_E_PPI_NOT_SUPPORTED 0x80290303	Le BIOS ne prend pas en charge l'interface de présence physique?
TPM_E_PPI_BLOCKED_IN_BIOS 0x80290304	La commande de présence physique a été bloquée par les paramètres du BIOS actuels. Le propriétaire du système peut être en mesure de reconfigurer les paramètres du BIOS pour autoriser la commande.
TPM_E_PCP_ERROR_MASK 0x80290400	Il s'agit d'un masque d'erreurs destiné à convertir les erreurs du fournisseur de cryptage de plateforme en erreurs win.
TPM_E_PCP_DEVICE_NOT_READY 0x80290401	Le périphérique de cryptage de plateforme n'est pas prêt pour le moment. Il doit être entièrement déployé pour être opérationnel.
TPM_E_PCP_INVALID_HANDLE 0x80290402	Le handle communiqué au fournisseur de cryptage de plateforme n'est pas valide.
TPM_E_PCP_INVALID_PARAMETER 0x80290403	Un paramètre communiqué au fournisseur de cryptage de plateforme n'est pas valide.
TPM_E_PCP_FLAG_NOT_SUPPORTED 0x80290404	Un indicateur communiqué au fournisseur de cryptage de plateforme n'est pas pris en charge.
TPM_E_PCP_NOT_SUPPORTED 0x80290405	L'opération demandée n'est pas prise en charge par ce fournisseur de cryptage de plateforme.
TPM_E_PCP_BUFFER_TOO_SMALL 0x80290406	Le tampon est trop petit pour contenir toutes les données. Aucune information écrite dans le tampon.
TPM_E_PCP_INTERNAL_ERROR 0x80290407	Une erreur interne imprévue s'est produite dans le fournisseur de cryptage de plateforme.
TPM_E_PCP_AUTHENTICATION_FAILED 0x80290408	Échec de l'autorisation d'utiliser un objet fournisseur.
TPM_E_PCP_AUTHENTICATION_IGNORED 0x80290409	Le périphérique de cryptage de plateforme a ignoré l'autorisation accordée à l'objet fournisseur de se défendre contre une attaque par dictionnaire.
TPM_E_PCP_POLICY_NOT_FOUND 0x8029040A	La règle référencée est introuvable.

Constante/Valeur	Description
TPM_E_PCP_PROFILE_NOT_FOUND 0x8029040B	Le profil référencé est introuvable.
TPM_E_PCP_VALIDATION_FAILED 0x8029040C	La validation n'a pas réussi.
PLA_E_DCS_NOT_FOUND 0x80300002	Ensemble Data Collector introuvable.
PLA_E_DCS_IN_USE 0x803000AA	L'ensemble de collecteurs de données ou l'une des ses dépendances est déjà utilisé.
PLA_E_TOO_MANY_FOLDERS 0x80300045	Impossible de démarrer l'ensemble de collecteurs de données car le nombre de dossiers est trop important.
PLA_E_NO_MIN_DISK 0x80300070	L'espace disque disponible est insuffisant pour lancer l'ensemble de collecteurs de données.
PLA_E_DCS_ALREADY_EXISTS 0x803000B7	Le collecteur de données existe déjà.
PLA_S_PROPERTY_IGNORED 0x00300100	La valeur de propriété sera ignorée.
PLA_E_PROPERTY_CONFLICT 0x80300101	Conflit de valeur de propriété.
PLA_E_DCS_SINGLETON_REQUIRED 0x80300102	La configuration actuelle de cet ensemble de collecteurs de données spécifie qu'il ne peut contenir qu'un seul collecteur de données.
PLA_E_CREDENTIALS_REQUIRED 0x80300103	Un compte d'utilisateur est nécessaire pour valider les propriétés de l'actuel ensemble de collecteurs de données.
PLA_E_DCS_NOT_RUNNING 0x80300104	L'ensemble de collecteurs de données ne fonctionne pas actuellement.
PLA_E_CONFLICT_INCL_EXCL_API 0x80300105	Un conflit a été détecté dans les listes d'inclusion et d'exclusion des API. Ne spécifiez pas la même API dans ces deux listes.
PLA_E_NETWORK_EXE_NOT_VALID 0x80300106	Le chemin d'accès de l'exécutable spécifié fait référence à un partage réseau ou à un chemin d'accès UNC.
PLA_E_EXE_ALREADY_CONFIGURED 0x80300107	Le chemin d'accès de l'exécutable que vous avez spécifié est déjà configuré pour le suivi de l'API.
PLA_E_EXE_PATH_NOT_VALID 0x80300108	Le chemin d'accès de l'exécutable que vous avez spécifié n'existe pas. Vérifiez que ce chemin est correct.
PLA_E_DC_ALREADY_EXISTS 0x80300109	Le collecteur de données existe déjà.

Constante/Valeur	Description
PLA_E_DCS_START_WAIT_TIMEOUT 0x8030010A	Le délai d'attente avant que l'ensemble de collecteurs de données lance les notifications a expiré.
PLA_E_DC_START_WAIT_TIMEOUT 0x8030010B	Le délai d'attente avant que l'ensemble de collecteurs de données démarre a expiré.
PLA_E_REPORT_WAIT_TIMEOUT 0x8030010C	Le délai d'attente avant que l'outil de génération de rapport se termine a expiré.
PLA_E_NO_DUPLICATES 0x8030010D	Les doublons ne sont pas autorisés.
PLA_E_EXE_FULL_PATH_REQUIRED 0x8030010E	Lorsque vous spécifiez l'exécutable à suivre, vous devez indiquer un chemin d'accès complet vers cet exécutable et pas seulement un nom de fichier.
PLA_E_INVALID_SESSION_NAME 0x8030010F	Le nom de session fourni n'est pas valide.
PLA_E_PLA_CHANNEL_NOT_ENABLED 0x80300110	Le canal Microsoft-Windows-Diagnosis-PLA/Operational du journal des événements doit être activé pour effectuer cette opération.
PLA_E_TASKSCHED_CHANNEL_NOT_ENABLED 0x80300111	Le canal Microsoft-Windows-TaskScheduler du journal des événements doit être activé pour effectuer cette opération.
PLA_E_RULES_MANAGER_FAILED 0x80300112	Échec de l'exécution du Gestionnaire de messages.
PLA_E_CABAPI_FAILURE 0x80300113	Une erreur s'est produite lors de la tentative de compression ou d'extraction des données.
FVE_E_LOCKED_VOLUME 0x80310000	Ce disque est verrouillé par le cryptage de disque de BitLocker. Vous devez déverrouiller ce disque depuis le Panneau de configuration.
FVE_E_NOT_ENCRYPTED 0x80310001	Le disque n'est pas crypté.
FVE_E_NO_TPM_BIOS 0x80310002	Le BIOS n'a pas communiqué correctement avec le module de plateforme sécurisée (TPM). Contactez le fabricant de l'ordinateur pour obtenir des instructions de mise à niveau du BIOS.
FVE_E_NO_MBR_METRIC 0x80310003	Le BIOS n'a pas communiqué correctement avec le secteur de démarrage principal. Contactez le fabricant de l'ordinateur pour obtenir des instructions de mise à niveau du BIOS.
FVE_E_NO_BOOTSECTOR_METRIC 0x80310004	Une mesure TPM requise est manquante. Si un CD/DVD de démarrage est présent dans l'ordinateur, retirez-le, redémarrez l'ordinateur, puis activez de nouveau BitLocker. Si le problème persiste, assurez-vous que l'enregistrement de démarrage principal est à jour.

Constante/Valeur	Description
FVE_E_NO_BOOTMGR_METRIC 0x80310005	Le secteur de démarrage de ce lecteur n'est pas compatible avec le cryptage de lecteur BitLocker. Utilisez l'outil bootrec.exe de l'environnement de récupération Windows pour mettre à jour ou réparer le gestionnaire de démarrage (BOOTMGR).
FVE_E_WRONG_BOOTMGR 0x80310006	Le gestionnaire de démarrage de ce système d'exploitation n'est pas compatible avec le cryptage de lecteur BitLocker. Utilisez l'outil bootrec.exe de l'environnement de récupération Windows pour mettre à jour ou réparer le gestionnaire de démarrage (BOOTMGR).
FVE_E_SECURE_KEY_REQUIRED 0x80310007	Au moins un protecteur de clé sécurisée est requis pour réaliser cette opération.
FVE_E_NOT_ACTIVATED 0x80310008	Le cryptage de lecteur BitLocker n'est pas activé sur ce lecteur. Activez le cryptage de lecteur.
FVE_E_ACTION_NOT_ALLOWED 0x80310009	Le cryptage de lecteur BitLocker ne peut pas exécuter l'action demandée. Cette erreur peut se produire lorsque deux demandes sont effectuées en même temps. Patientez quelques instants, puis réessayez.
FVE_E_AD_SCHEMA_NOT_INSTALLED 0x8031000A	La forêt des services de domaine Active Directory ne contient pas les attributs et les classes nécessaires pour héberger les informations de cryptage de lecteur BitLocker ou celles du module de plateforme sécurisée TPM. Contactez votre administrateur de domaine pour vérifier que toutes les extensions de schéma Active Directory BitLocker requises ont été installées.
FVE_E_AD_INVALID_DATATYPE 0x8031000B	Le type de donnée obtenu à partir d'Active Directory était inattendu. Il est possible que les informations de récupération BitLocker soient manquantes ou endommagées.
FVE_E_AD_INVALID_DATASIZE 0x8031000C	La taille des données obtenues à partir d'Active Directory était inattendue. Il est possible que les informations de récupération BitLocker soient manquantes ou endommagées.
FVE_E_AD_NO_VALUES 0x8031000D	L'attribut lu à partir d'Active Directory ne contient aucune valeur. Il est possible que les informations de récupération BitLocker soient manquantes ou endommagées.
FVE_E_AD_ATTR_NOT_SET 0x8031000E	L'attribut n'a pas été défini. L'attribut n'était pas défini. Vérifiez que vous êtes connecté à l'aide d'un compte de domaine autorisé à écrire des informations dans les objets Active Directory.
FVE_E_AD_GUID_NOT_FOUND 0x8031000F	L'attribut défini est introuvable dans les services de domaine Active Directory. Contactez votre administrateur de domaine pour vérifier que toutes les extensions de schéma Active Directory BitLocker requises ont été installées.
FVE_E_BAD_INFORMATION 0x80310010	Les métadonnées BitLocker du lecteur crypté ne sont pas valides. Vous pouvez essayer de réparer le lecteur pour restaurer l'accès.

Constante/Valeur	Description
FVE_E_TOO_SMALL 0x80310011	Le lecteur ne peut pas être crypté car il ne contient pas suffisamment d'espace libre. Supprimez toutes données inutiles pour libérer de l'espace, puis réessayez.
FVE_E_SYSTEM_VOLUME 0x80310012	Le lecteur ne peut pas être crypté car il contient les informations de démarrage du système. Créez une première partition contenant les informations de démarrage qui sera utilisée comme lecteur système et une seconde qui sera utilisée comme lecteur du système d'exploitation, puis chiffrez le lecteur du système d'exploitation.
FVE_E_FAILED_WRONG_FS 0x80310013	Impossible de crypter le disque, car le système de fichiers n'est pas pris en charge.
FVE_E_BAD_PARTITION_SIZE 0x80310014	La taille du système de fichiers dépasse celle des partitions dans la table de partitions. Ce disque peut être corrompu ou a peut-être été altéré. Pour l'utiliser avec BitLocker, vous devez reformater la partition.
FVE_E_NOT_SUPPORTED 0x80310015	Ce disque ne peut pas être crypté.
FVE_E_BAD_DATA 0x80310016	Les données ne sont pas valides.
FVE_E_VOLUME_NOT_BOUND 0x80310017	Le lecteur de données spécifié n'est pas configuré pour le déverrouillage automatique sur l'ordinateur actuel et ne peut donc pas être déverrouillé automatiquement.
FVE_E_TPM_NOT_OWNED 0x80310018	Vous devez initialiser le module de plateforme sécurisée (TPM) pour pouvoir utiliser le cryptage de lecteur BitLocker.
FVE_E_NOT_DATA_VOLUME 0x80310019	Impossible d'effectuer l'opération tentée sur un disque du système d'exploitation.
FVE_E_AD_INSUFFICIENT_BUFFER 0x8031001A	La mémoire tampon dédiée à une fonction était insuffisante pour contenir les données renvoyées. Augmentez la taille de la mémoire tampon avant d'exécuter de nouveau cette fonction.
FVE_E_CONV_READ 0x8031001B	Une opération de lecture a échoué lors de la conversion du disque. Le disque n'a pas été converti. Veuillez réactiver BitLocker.
FVE_E_CONV_WRITE 0x8031001C	Une opération d'écriture a échoué lors de la conversion du disque. Le disque n'a pas été converti. Veuillez réactiver BitLocker.
FVE_E_KEY_REQUIRED 0x8031001D	Au moins un protecteur de clé BitLocker est requis. Vous ne pouvez pas supprimer la dernière clé sur ce lecteur.
FVE_E_CLUSTERING_NOT_SUPPORTED 0x8031001E	Les configurations de cluster ne sont pas prises en charge par le cryptage de lecteur BitLocker.
FVE_E_VOLUME_BOUND_ALREADY 0x8031001F	Le lecteur spécifié est déjà configuré pour être automatiquement déverrouillé sur l'ordinateur actuel.

Constante/Valeur	Description
FVE_E_OS_NOT_PROTECTED 0x80310020	Le lecteur du système d'exploitation n'est pas protégé par le cryptage de lecteur BitLocker.
FVE_E_PROTECTION_DISABLED 0x80310021	Le cryptage de lecteur BitLocker a été suspendu sur ce lecteur. Tous les protecteurs de clés BitLocker configurés pour ce lecteur sont désactivés et le lecteur sera automatiquement déverrouillé à l'aide d'une clé non cryptée (claire).
FVE_E_RECOVERY_KEY_REQUIRED 0x80310022	Aucun protecteur de clé pour le chiffrage n'est disponible pour le lecteur que vous essayez de verrouiller car la protection BitLocker est actuellement suspendue. Activez de nouveau BitLocker pour verrouiller ce lecteur.
FVE_E_FOREIGN_VOLUME 0x80310023	BitLocker ne peut pas utiliser le module de plateforme sécurisée (TPM) pour protéger un lecteur de données. La protection du module de plateforme sécurisée ne peut être utilisée qu'avec le lecteur du système d'exploitation.
FVE_E_OVERLAPPED_UPDATE 0x80310024	Les métadonnées BitLocker du lecteur crypté ne peuvent pas être mises à jour car elles ont été verrouillées pour mise à jour par un autre processus. Veuillez réessayer.
FVE_E_TPM_SRK_AUTH_NOT_ZERO 0x80310025	Les données d'autorisation de la clé de racine de stockage (SRK) du module de plateforme sécurisée (TPM) n´ayant pas la valeur zéro, sont incompatibles avec BitLocker. Veuillez initialiser le TPM avant de tenter de l'utiliser avec BitLocker.
FVE_E_FAILED_SECTOR_SIZE 0x80310026	L'algorithme de cryptage du lecteur ne peut pas être utilisé avec cette taille de secteur.
FVE_E_FAILED_AUTHENTICATION 0x80310027	Impossible de déverrouiller le lecteur avec la clé fournie. Vérifiez que la clé est correcte, puis réessayez.
FVE_E_NOT_OS_VOLUME 0x80310028	Le lecteur spécifié ne contient pas le système d'exploitation.
FVE_E_AUTOUNLOCK_ENABLED 0x80310029	Le cryptage de lecteur BitLocker ne peut pas être désactivé sur le lecteur du système d'exploitation tant que la fonction de déverrouillage automatique n'a pas été désactivée pour les lecteurs de données fixes et amovibles associés à cet ordinateur.
FVE_E_WRONG_BOOTSECTOR 0x8031002A	Le secteur de démarrage de la partition système n'effectue pas de mesures TPM. Utilisez l'outil bootrec.exe de l'environnement de récupération Windows pour mettre à jour ou réparer le secteur de démarrage.
FVE_E_WRONG_SYSTEM_FS 0x8031002B	Les lecteurs du système d'exploitation doivent être formatés avec le système de fichiers NTFS pour pouvoir être cryptés avec le cryptage de lecteur BitLocker. Convertissez le lecteur en NTFS, puis activez BitLocker.
FVE_E_POLICY_PASSWORD_REQUIRED 0x8031002C	Les paramètres de stratégie de groupe exigent qu'un mot de passe de récupération soit spécifié avant de crypter le lecteur.

Constante/Valeur	Description
FVE_E_CANNOT_SET_FVEK_ENCRYPTED 0x8031002D	L'algorithme et la clé de cryptage du volume ne peuvent pas être définis sur un lecteur déjà crypté. Pour crypter ce lecteur avec le cryptage de lecteur BitLocker, retirez le cryptage précédent, puis activez BitLocker.
FVE_E_CANNOT_ENCRYPT_NO_KEY 0x8031002E	Le cryptage de lecteur BitLocker ne peut pas crypter le lecteur spécifié car aucune clé de cryptage n'est disponible. Ajoutez un protecteur de clé pour crypter ce lecteur.
FVE_E_BOOTABLE_CDDVD 0x80310030	Le cryptage de lecteur BitLocker a détecté la présence d'un média de démarrage amovible (CD ou DVD) dans l'ordinateur. Retirez le média, puis redémarrez l'ordinateur avant de configurer BitLocker.
FVE_E_PROTECTOR_EXISTS 0x80310031	Impossible d'ajouter ce protecteur de clé. Un seul protecteur de clé de ce type est autorisé pour ce lecteur.
FVE_E_RELATIVE_PATH 0x80310032	Le fichier de mot de passe de récupération est introuvable car un chemin d'accès relatif a été spécifié. Les mots de passe de récupération doivent être enregistrés dans un chemin d'accès complet. Les variables d'environnement configurées sur l'ordinateur peuvent être utilisées dans le chemin d'accès.
FVE_E_PROTECTOR_NOT_FOUND 0x80310033	Le protecteur de clé spécifié est introuvable sur le lecteur. Essayez-en un autre.
FVE_E_INVALID_KEY_FORMAT 0x80310034	La clé de récupération fournie est endommagée et ne peut pas être utilisée pour accéder au lecteur. Une autre méthode de récupération comme un mot de passe de récupération, un agent de récupération de données ou une version de sauvegarde de la clé de récupération doit être utilisée pour retrouver l'accès au lecteur.
FVE_E_INVALID_PASSWORD_FORMAT 0x80310035	Le format du mot de passe de récupération n'est pas valide. Les mots de passe de récupération BitLocker sont formés de 48 chiffres. Vérifiez que le mot de passe de restauration est correct, puis réessayez.
FVE_E_FIPS_RNG_CHECK_FAILED 0x80310036	Échec du test de contrôle du générateur de nombres aléatoires.
FVE_E_FIPS_PREVENTS_RECOVERY_PASSWORD 0x80310037	Le paramètre de stratégie de groupe qui nécessite la compatibilité FIPS empêche la génération ou l'utilisation d'un mot de passe de récupération local par le cryptage de lecteur BitLocker. En mode de compatibilité FIPS, les options de récupération BitLocker peuvent être une clé de récupération stockée sur un disque USB ou un agent de récupération de données.
FVE_E_FIPS_PREVENTS_EXTERNAL_KEY_EXPORT 0x80310038	Le paramètre de stratégie de groupe qui nécessite la compatibilité FIPS empêche l'enregistrement du mot de passe de récupération dans Active Directory. En mode de compatibilité FIPS, les options de récupération BitLocker peuvent être une clé de récupération stockée sur un disque USB ou un agent de récupération de données. Vérifiez la configuration des paramètres de stratégie de groupe.

Constante/Valeur	Description
FVE_E_NOT_DECRYPTED 0x80310039	Pour terminer l'opération, le lecteur doit être intégralement décrypté.
FVE_E_INVALID_PROTECTOR_TYPE 0x8031003A	Le protecteur de clé spécifié ne peut pas être utilisé pour cette opération.
FVE_E_NO_PROTECTORS_TO_TEST 0x8031003B	Aucun protecteur de clé n'existe sur le lecteur pour effectuer le test du matériel.
FVE_E_KEYFILE_NOT_FOUND 0x8031003C	Impossible de trouver la clé de démarrage ou le mot de passe de récupération BitLocker sur le périphérique USB. Assurez-vous que le périphérique USB correct est connecté à un port USB actif de l'ordinateur, redémarrez l'ordinateur, puis réessayez. Si le problème persiste, demandez au fabricant de l'ordinateur comment mettre à niveau le BIOS.
FVE_E_KEYFILE_INVALID 0x8031003D	La clé de démarrage ou le fichier de mot de passe de récupération BitLocker est endommagé ou non valide. Vérifiez que vous disposez de la bonne clé de démarrage ou du bon fichier de mot de passe de restauration, puis réessayez.
FVE_E_KEYFILE_NO_VMK 0x8031003E	Impossible d'obtenir la clé de cryptage BitLocker à partir de la clé de démarrage ou du mot de passe de récupération. Vérifiez que la clé de démarrage ou le mot de passe de récupération correct sont utilisés, puis réessayez.
FVE_E_TPM_DISABLED 0x8031003F	Le module TPM est désactivé. Le module de plateforme sécurisée (TPM) est désactivé. Celui-ci doit être activé, initialisé et avoir un propriétaire valide pour pouvoir être utilisé avec le cryptage de lecteur BitLocker.
FVE_E_NOT_ALLOWED_IN_SAFE_MODE 0x80310040	La configuration BitLocker du lecteur spécifié ne peut pas être gérée car cet ordinateur fonctionne en mode sans échec. En mode sans échec, le cryptage de lecteur BitLocker ne peut être utilisé qu'à des fins de récupération.
FVE_E_TPM_INVALID_PCR 0x80310041	Le module de plateforme sécurisée (TPM) n'a pas réussi à déverrouiller le lecteur car les informations de démarrage système ont été modifiées ou le code confidentiel fourni est incorrect. Vérifiez que le lecteur n'a pas été falsifié et que les informations de démarrage système ont été modifiées par une source approuvée. Après avoir vérifié que l'accès au lecteur est sécurisé, utilisez la console de récupération BitLocker pour déverrouiller le lecteur, puis suspendez et reprenez BitLocker pour mettre à jour les informations de démarrage système que BitLocker associe à ce lecteur.
FVE_E_TPM_NO_VMK 0x80310042	Impossible d'obtenir la clé de cryptage BitLocker du module de plateforme sécurisée (TPM).
FVE_E_PIN_INVALID 0x80310043	Impossible d'obtenir la clé de cryptage du module de plateforme sécurisée et de PIN.
FVE_E_AUTH_INVALID_APPLICATION 0x80310044	Une application de démarrage a changé depuis l'activation du cryptage de lecteur BitLocker.

Constante/Valeur	Description
FVE_E_AUTH_INVALID_CONFIG 0x80310045	Les paramètres des données de configuration de démarrage (BCD) ont changé depuis l'activation du cryptage de lecteur BitLocker.
FVE_E_FIPS_DISABLE_PROTECTION_NOT_ALLOWED 0x80310046	Le paramètre de stratégie de groupe qui nécessite la compatibilité FIPS interdit l'utilisation de clés non cryptées, ce qui empêche la suspension de BitLocker sur ce lecteur. Pour en savoir plus, contactez l'administrateur de domaine.
FVE_E_FS_NOT_EXTENDED 0x80310047	Ce disque ne peut pas être crypté par le cryptage de disque BitLocker, car le système de fichiers ne s'étend pas jusqu'à l'extrémité du disque. Repartitionnez ce lecteur et réessayez.
FVE_E_FIRMWARE_TYPE_NOT_SUPPORTED 0x80310048	Impossible d'activer le cryptage de disque BitLocker sur un disque du système d'exploitation. Contactez le fabricant de l'ordinateur pour obtenir des instructions de mise à niveau du BIOS.
FVE_E_NO_LICENSE 0x80310049	Cette version de Windows ne comprend pas BitLocker Drive Encryption. Pour utiliser BitLocker Drive Encryption, veuillez mettre à niveau le système d'exploitation.
FVE_E_NOT_ON_STACK 0x8031004A	Le cryptage de lecteur BitLocker ne peut pas être utilisé car les fichiers système BitLocker sont manquants ou endommagés. Restaurez-les sur votre ordinateur à l'aide de l'outil de redémarrage système Windows.
FVE_E_FS_MOUNTED 0x8031004B	Le disque ne peut pas être verrouillé lorsqu'il est en cours d'utilisation.
FVE_E_TOKEN_NOT_IMPERSONATED 0x8031004C	Le jeton d'accès associé au thread en cours n'est pas un jeton représenté.
FVE_E_DRY_RUN_FAILED 0x8031004D	Impossible d'obtenir la clé de cryptage BitLocker. Vérifiez que le module de plateforme sécurisée (TMP) est activé et que la propriété a été acquise. Si cet ordinateur n'a pas de module TPM, vérifiez que le lecteur USB est inséré et disponible.
FVE_E_REBOOT_REQUIRED 0x8031004E	Vous devez redémarrer votre ordinateur pour continuer d'utiliser BitLocker Drive Encryption.
FVE_E_DEBUGGER_ENABLED 0x8031004F	Le lecteur ne peut pas être crypté tant que le débogage de démarrage est activé. Utilisez l'outil de ligne de commande bcdedit pour le désactiver.
FVE_E_RAW_ACCESS 0x80310050	Aucune action n'a été prise car le cryptage de lecteur BitLocker est en mode d'accès brut.
FVE_E_RAW_BLOCKED 0x80310051	Le cryptage de lecteur BitLocker ne peut pas adopter le mode d'accès RAW pour ce lecteur car ce dernier est en cours d'utilisation.
FVE_E_BCD_APPLICATIONS_PATH_INCORRECT 0x80310052	Le chemin d'accès spécifié dans les données de configuration de démarrage (BCD) pour une application à intégrité protégée par cryptage de lecteur BitLocker est

Constante/Valeur	Description
	incorrect. Veuillez vérifier et corriger vos paramètre BCD et réessayer.
FVE_E_NOT_ALLOWED_IN_VERSION 0x80310053	Le cryptage de lecteur BitLocker peut uniquement être utilisé à des fins d'approvisionnement limité ou de récupération lorsque l'ordinateur s'exécute dans des environnements de préinstallation ou de récupération Windows.
FVE_E_NO_AUTOUNLOCK_MASTER_KEY 0x80310054	La clé principale de déverrouillage automatique n'est pas disponible à partir du volume du système d'exploitation.
FVE_E_MOR_FAILED 0x80310055	Le microprogramme du système n'a pas pu libérer la mémoire système au redémarrage de l'ordinateur.
FVE_E_HIDDEN_VOLUME 0x80310056	Le lecteur masqué ne peut pas être crypté.
FVE_E_TRANSIENT_STATE 0x80310057	Les clés de cryptage BitLocker ont été ignorées du fait de l'état transitoire du lecteur.
FVE_E_PUBKEY_NOT_ALLOWED 0x80310058	Les protecteurs basés sur une clé publique ne sont pas autorisés sur ce lecteur.
FVE_E_VOLUME_HANDLE_OPEN 0x80310059	Le cryptage de lecteur BitLocker exécute déjà une opération sur ce lecteur. Veuillez terminer toutes les opérations avant de continuer.
FVE_E_NO_FEATURE_LICENSE 0x8031005A	Cette version de Windows ne prend pas en charge cette fonction de BitLocker Drive Encryption. Pour utiliser cette fonction, mettez à niveau le système d'exploitation.
FVE_E_INVALID_STARTUP_OPTIONS 0x8031005B	Les paramètres de stratégie de groupe pour les options de démarrage BitLocker sont en conflit et ne peuvent pas être appliqués. Pour plus d'informations, contactez votre administrateur système.
FVE_E_POLICY_RECOVERY_PASSWORD_NOT_ALLOWED 0x8031005C	Les paramètres de stratégie de groupe ne permettent pas la création d'un mot de passe de récupération.
FVE_E_POLICY_RECOVERY_PASSWORD_REQUIRED 0x8031005D	Les paramètres de règle de groupe exigent la création d'un mot de passe de restauration.
FVE_E_POLICY_RECOVERY_KEY_NOT_ALLOWED 0x8031005E	Les paramètres de stratégie de groupe ne permettent pas la création d'une clé de récupération.
FVE_E_POLICY_RECOVERY_KEY_REQUIRED 0x8031005F	Les paramètres de règle de groupe exigent la création d'une clé de restauration.
FVE_E_POLICY_STARTUP_PIN_NOT_ALLOWED 0x80310060	Les paramètres de stratégie de groupe ne permettent pas l'utilisation d'un code confidentiel au démarrage. Veuillez choisir une autre option de démarrage de BitLocker.

Constante/Valeur	Description
FVE_E_POLICY_STARTUP_PIN_REQUIRED 0x80310061	Les paramètres de règle de groupe exigent l'utilisation d'un code confidentiel au démarrage. Veuillez choisir cette option de démarrage de BitLocker.
FVE_E_POLICY_STARTUP_KEY_NOT_ALLOWED 0x80310062	Les paramètres de règle de groupe ne permettent pas l'utilisation d'une clé de démarrage. Veuillez choisir une autre option de démarrage de BitLocker.
FVE_E_POLICY_STARTUP_KEY_REQUIRED 0x80310063	Les paramètres de règle de groupe exigent l'utilisation d'une clé de démarrage. Veuillez choisir cette option de démarrage de BitLocker.
FVE_E_POLICY_STARTUP_PIN_KEY_NOT_ALLOWED0x80310064	Les paramètres de règle de groupe ne permettent pas l'utilisation d'une clé de démarrage et d'un code confidentiel. Veuillez choisir une autre option de démarrage de BitLocker.
FVE_E_POLICY_STARTUP_PIN_KEY_REQUIRED 0x80310065	Les paramètres de règle de groupe exigent l'utilisation d'une clé de démarrage et d'un code personnel. Veuillez choisir cette option de démarrage de BitLocker.
FVE_E_POLICY_STARTUP_TPM_NOT_ALLOWED 0x80310066	La stratégie de groupe ne permet pas l'utilisation exclusive d'un module de plateforme sécurisée au démarrage. Veuillez choisir une autre option de démarrage de BitLocker.
FVE_E_POLICY_STARTUP_TPM_REQUIRED 0x80310067	Les paramètres de règle de groupe exigent l'utilisation d'un module TPM uniquement au démarrage. Veuillez choisir cette option de démarrage de BitLocker.
FVE_E_POLICY_INVALID_PIN_LENGTH 0x80310068	Le code confidentiel fourni ne respecte pas les exigences de longueurs minimale ou maximale.
FVE_E_KEY_PROTECTOR_NOT_SUPPORTED 0x80310069	Le protecteur de clé n'est pas pris en charge par la version du cryptage de lecteur BitLocker actuellement présent sur le lecteur. Mettez à niveau le lecteur pour ajouter le protecteur de clé.
FVE_E_POLICY_PASSPHRASE_NOT_ALLOWED 0x8031006A	Les paramètres de règle de groupe ne permettent pas la création d'un mot de passe.
FVE_E_POLICY_PASSPHRASE_REQUIRED 0x8031006B	Les paramètres de règle de groupe exigent la création d'un mot de passe.
FVE_E_FIPS_PREVENTS_PASSPHRASE 0x8031006C	Le paramètre de stratégie de groupe nécessitant la conformité FIPS n'a pas permis de générer ou d'utiliser le mot de passe. Pour en savoir plus, contactez l'administrateur de domaine.
FVE_E_OS_VOLUME_PASSPHRASE_NOT_ALLOWED 0x8031006D	Impossible d'ajouter un mot de passe au lecteur du système d'exploitation.
FVE_E_INVALID_BITLOCKER_OID 0x8031006E	L'identificateur d'objet (OID) BitLocker sur le lecteur n'est pas valide ou est endommagé. Utilisez manage-BDE pour réinitialiser l'OID sur ce lecteur.
FVE_E_VOLUME_TOO_SMALL 0x8031006F	Le lecteur est trop exigu pour être protégé à l'aide du cryptage de lecteur BitLocker.

Constante/Valeur	Description
FVE_E_DV_NOT_SUPPORTED_ON_FS 0x80310070	Le type de lecteur de détection sélectionné est incompatible avec le système de fichiers du lecteur. Les lecteurs de détection BitLocker To Go doivent être créés sur des lecteurs au format FAT.
FVE_E_DV_NOT_ALLOWED_BY_GP 0x80310071	Le type de lecteur de détection sélectionné n'est pas autorisé par les paramètres de stratégie de groupe de l'ordinateur. Vérifiez que les paramètres de stratégie de groupe autorisent la création de lecteurs de détection qui seront utilisés avec BitLocker To Go
FVE_E_POLICY_USER_CERTIFICATE_NOT_ALLOWED 0x80310072	Les paramètres de stratégie de groupe ne permettent pas d'utiliser les certificats utilisateur, tels que les cartes à puce, avec le cryptage de lecteur BitLocker.
FVE_E_POLICY_USER_CERTIFICATE_REQUIRED 0x80310073	Les paramètres de stratégie de groupe exigent l'utilisation d'un certificat utilisateur valide, tel qu'une carte à puce, avec le cryptage de lecteur BitLocker.
FVE_E_POLICY_USER_CERT_MUST_BE_HW 0x80310074	Les paramètres de stratégie de groupe exigent l'utilisation d'un protecteur de clé de type carte à puce avec le cryptage de lecteur BitLocker.
FVE_E_POLICY_USER_CONFIGURE_FDV_AUTOUNLOCK_NOT_ALLOWED 0x80310075	Les paramètres de stratégie de groupe ne permettent pas le déverrouillage automatique des lecteurs de données fixes protégés par BitLocker.
FVE_E_POLICY_USER_CONFIGURE_RDV_AUTOUNLOCK_NOT_ALLOWED 0x80310076	Les paramètres de stratégie de groupe ne permettent pas le déverrouillage automatique des lecteurs de données amovibles protégés par BitLocker.
FVE_E_POLICY_USER_CONFIGURE_RDV_NOT_ALLOWED 0x80310077	Les paramètres de stratégie de groupe ne permettent pas la configuration du cryptage de lecteur BitLocker sur les lecteurs de données amovibles.
FVE_E_POLICY_USER_ENABLE_RDV_NOT_ALLOWED 0x80310078	Les paramètres de stratégie de groupe ne permettent pas l'activation du cryptage de lecteur BitLocker sur les lecteurs de données amovibles. Veuillez contacter l'administrateur du système si vous avez besoin d'activer BitLocker.
FVE_E_POLICY_USER_DISABLE_RDV_NOT_ALLOWED 0x80310079	Les paramètres de stratégie de groupe n'autorisent pas la désactivation du cryptage de lecteur BitLocker sur des lecteurs de données amovibles. Veuillez contacter l'administrateur du système si vous avez besoin de désactiver BitLocker.
FVE_E_POLICY_INVALID_PASSPHRASE_LENGTH 0x80310080	Votre mot de passe ne respecte pas les exigences de longueur minimale. Par défaut, les mots de passe doivent comprendre au moins 8 caractères. Votre mot de passe ne répond pas aux exigences de longueur minimale.
FVE_E_POLICY_PASSPHRASE_TOO_SIMPLE 0x80310081	Votre mot de passe ne répond pas aux exigences de complexité définies par votre administrateur système. Ajoutez des caractères majuscules et minuscules, des nombres et des symboles.
FVE_E_RECOVERY_PARTITION 0x80310082	Le lecteur ne peut pas être crypté car il est réservé pour les options de récupération système de Windows.

Constante/Valeur	Description
FVE_E_POLICY_CONFLICT_FDV_RK_OFF_AUK_ON 0x80310083	Le cryptage de lecteur BitLocker ne peut pas être appliqué à ce lecteur en raison de paramètres de stratégie de groupe en conflit. BitLocker ne peut pas être configuré pour déverrouiller automatiquement les lecteurs de données fixes lorsque les options de récupération utilisateur sont désactivées. Si vous souhaitez que les lecteurs de données fixes protégés par BitLocker soient automatiquement déverrouillés après validation de la clé, demandez à votre administrateur système de résoudre les conflits de paramètres avant d'activer BitLockerBit.
FVE_E_POLICY_CONFLICT_RDV_RK_OFF_AUK_ON 0x80310084	Le cryptage de lecteur BitLocker ne peut pas être appliqué à ce lecteur en raison de paramètres de stratégie de groupe en conflit. BitLocker ne peut pas être configuré pour déverrouiller automatiquement les lecteurs de données fixes lorsque les options de récupération utilisateur sont désactivées. Si vous souhaitez que les lecteurs de données amovibles protégés par BitLocker soient automatiquement déverrouillés après validation de la clé, demandez à votre administrateur système de résoudre les conflits de paramètres avant d'activer BitLocker.
FVE_E_NON_BITLOCKER_OID 0x80310085	L'attribut d'utilisation avancée de la clé du certificat spécifié ne permet pas au certificat spécifié d'être utilisé pour le cryptage de lecteur BitLocker. BitLocker n'exige pas qu'un certificat possède un attribut d'utilisation avancée de la clé. Toutefois, si un tel attribut est configuré, il doit être égal à un identificateur d'objet correspondant à l'identificateur d'objet configuré pour BitLocker.
FVE_E_POLICY_PROHIBITS_SELFSIGNED 0x80310086	Le cryptage de lecteur BitLocker tel qu'il est configuré ne peut pas être appliqué à ce lecteur en raison des paramètres de la stratégie de groupe. Le certificat fourni pour le cryptage de lecteur est auto-signé. Les paramètres actuels de la stratégie de groupe n'autorisent pas l'utilisation de certificats auto-signés. Obtenez un nouveau certificat auprès de l'autorité de certification avant d'essayer d'activer BitLocker.
FVE_E_POLICY_CONFLICT_RO_AND_STARTUP_KEY_REQUIRED 0x80310087	Le cryptage de lecteur BitLocker ne peut pas être appliqué à ce lecteur en raison de paramètres de stratégie de groupe en conflit. Lorsque l'accès en lecture aux lecteurs non protégés par BitLocker est refusé, l'utilisation d'une clé de démarrage USB ne peut pas être exigée. Demandez à votre administrateur système de résoudre ces conflits de stratégie avant d'essayer d'activer BitLocker.
FVE_E_CONV_RECOVERY_FAILED 0x80310088	Le cryptage de lecteur BitLocker ne peut pas être appliqué à ce lecteur en raison de paramètres de stratégie de groupe en conflit pour les options de récupération sur les lecteurs du système d'exploitation. Le stockage des informations de récupération dans les services de domaine Active Directory ne peut pas être requis lorsque la génération de mots de passe de récupération n'est pas autorisée. Demandez à votre administrateur système de résoudre ces conflits de stratégie avant d'essayer d'activer BitLocker.
FVE_E_VIRTUALIZED_SPACE_TOO_BIG 0x80310089	La taille de virtualisation demandée est trop grande.

Constante/Valeur	Description
FVE_E_POLICY_CONFLICT_OSV_RP_OFF_ADB_ON 0x80310090	Le cryptage de lecteur BitLocker ne peut pas être appliqué à ce lecteur en raison de paramètres de stratégie de groupe en conflit pour les options de récupération sur les lecteurs du système d'exploitation. Le stockage des informations de récupération dans les services de domaine Active Directory ne peut pas être requis lorsque la génération de mots de passe de récupération n'est pas autorisée. Demandez à votre administrateur système de résoudre ces conflits de stratégie avant d'essayer d'activer BitLocker.
FVE_E_POLICY_CONFLICT_FDV_RP_OFF_ADB_ON 0x80310091	Le cryptage de lecteur BitLocker ne peut pas être appliqué à ce lecteur en raison de paramètres de stratégie de groupe en conflit pour les options de récupération sur les lecteurs de données fixes. Le stockage des informations de récupération dans les services de domaine Active Directory ne peut pas être requis lorsque la génération de mots de passe de récupération n'est pas autorisée. Demandez à votre administrateur système de résoudre ces conflits de stratégie avant d'essayer d'activer BitLocker.
FVE_E_POLICY_CONFLICT_RDV_RP_OFF_ADB_ON 0x80310092	Le cryptage de lecteur BitLocker ne peut pas être appliqué à ce lecteur en raison de paramètres de stratégie de groupe en conflit pour les options de récupération sur les lecteurs de données amovibles. Le stockage des informations de récupération dans les services de domaine Active Directory ne peut pas être requis lorsque la génération de mots de passe de récupération n'est pas autorisée. Demandez à votre administrateur système de résoudre ces conflits de stratégie avant d'essayer d'activer BitLocker.
FVE_E_NON_BITLOCKER_KU 0x80310093	L'attribut d'utilisation de la clé ne permet pas au certificat spécifié d'être utilisé pour le cryptage de lecteur BitLocker. BitLocker n'exige pas qu'un certificat possède un attribut d'utilisation de la clé. Toutefois, si un tel attribut est configuré, il doit avoir la valeur Chiffrement de la clé ou Accord de la clé.
FVE_E_PRIVATEKEY_AUTH_FAILED 0x80310094	Impossible d'autoriser la clé privée associée au certificat spécifié. L'autorisation de la clé privée n'a pas été fournie ou l'autorisation fournie n'est pas valide.
FVE_E_REMOVAL_OF_DRA_FAILED 0x80310095	La suppression du certificat de l'agent de récupération de données doit être effectuée à l'aide du composant logiciel enfichable Certificats.
FVE_E_OPERATION_NOT_SUPPORTED_ON_VISTA_VOLUME 0x80310096	Ce lecteur a été crypté à l'aide de la version de cryptage de lecteur BitLocker fournie avec Windows Vista et Windows Server 2008, et qui ne prend pas en charge les identificateurs d'organisation. Pour spécifier les identificateurs d'organisation de ce lecteur, mettez à niveau le cryptage du lecteur à la dernière version, à l'aide de la commande « manage-bde -upgrade ».
FVE_E_CANT_LOCK_AUTOUNLOCK_ENABLED_VOLUME 0x80310097	Le lecteur ne peut pas être verrouillé parce qu'il est automatiquement déverrouillé sur cet ordinateur. Supprimez le protecteur de déverrouillage automatique pour verrouiller ce lecteur.
FVE_E_FIPS_HASH_KDF_NOT_ALLOWED 0x80310098	La fonction de dérivation de clés BitLocker par défaut SP800-56A pour les cartes à puces ECC n'est pas prise en charge par votre carte à puce. Le paramètre Stratégie

Constante/Valeur	Description
	de groupe, qui nécessite la compatibilité FIPS, empêche BitLocker d'utiliser toute autre fonction de dérivation de clés pour le cryptage. Vous devez utiliser une carte à puce compatible FIPS dans les environnements limités à FIPS.
FVE_E_ENH_PIN_INVALID 0x80310099	Impossible d'obtenir la clé de cryptage du module de plateforme sécurisée et du code confidentiel étendu. Utilisez un code confidentiel contenant uniquement des chiffres.
FVE_E_INVALID_PIN_CHARS 0x8031009A	Le PIN TPM demandé contient des caractères non valides.
FVE_E_INVALID_DATUM_TYPE 0x8031009B	Les informations de gestion stockées sur le disque contenaient un type inconnu. Si vous utilisez une version plus ancienne de Windows, accédez au disque à partir de la dernière version.
FVE_E_EFI_ONLY 0x8031009C	Cette fonction n'est prise en charge que sur les systèmes EFI.
FVE_E_MULTIPLE_NKP_CERTS 0x8031009D	Plusieurs certificats de protecteur de clé réseau ont été trouvés sur le système.
FVE_E_REMOVAL_OF_NKP_FAILED 0x8031009E	La suppression du certificat de protecteur de clé réseau doit être effectuée à l'aide du composant logiciel enfichable Certificats.
FVE_E_INVALID_NKP_CERT 0x8031009F	Un certificat non valide a été trouvé dans le magasin de certificats de protecteur de clé réseau.
FVE_E_NO_EXISTING_PIN 0x803100A0	Ce disque n'est pas protégé par un PIN.
FVE_E_PROTECTOR_CHANGE_PIN_MISMATCH 0x803100A1	Veuillez enter le code confidentiel correct actuel.
FVE_E_PROTECTOR_CHANGE_BY_STD_USER_DISALLOWED 0x803100A2	Vous devez vous connecter avec un compte d'administrateur pour pouvoir changer le code confidentiel ou le mot de passe. Cliquez sur le lien pour réinitialiser le code confidentiel ou le mot de passe en tant qu'administrateur.
FVE_E_PROTECTOR_CHANGE_MAX_PIN_CHANGE_ATTEMPTS_REACHED 0x803100A3	BitLocker a désactivé les modifications de code confidentiel et de mot de passe après un trop grand nombre d'échecs de demande. Cliquez sur le lien pour réinitialiser le code confidentiel ou le mot de passe en tant qu'administrateur.
FVE_E_POLICY_PASSPHRASE_REQUIRES_ASCII 0x803100A4	Votre administrateur système requiert que les mots de passe contiennent uniquement des caractères ASCII imprimables. Cela inclut les lettres non accentuées (A-Z, a-z), les nombres (0-9), l'espace, les signes arithmétiques, la ponctuation courante, les séparateurs et les symboles suivants : # $ & @ ^ _ ~ .
FVE_E_FULL_ENCRYPTION_NOT_ALLOWED_ON_TP_STORAGE 0x803100A5	Le cryptage de lecteur BitLocker ne prend en charge que le cryptage d'espace utilisé uniquement sur un stockage alloué dynamiquement.

Constante/Valeur	Description
FVE_E_WIPE_NOT_ALLOWED_ON_TP_STORAGE 0x803100A6	Le cryptage de lecteur BitLocker ne prend pas en charge l'effacement d'espace libre sur un stockage alloué dynamiquement.
FVE_E_KEY_LENGTH_NOT_SUPPORTED_BY_EDRIVE 0x803100A7	La longueur de la clé d'authentification requise n'est pas prise en charge par le lecteur.
FVE_E_NO_EXISTING_PASSPHRASE 0x803100A8	Ce disque n'est pas protégé par un mot de passe.
FVE_E_PROTECTOR_CHANGE_PASSPHRASE_MISMATCH 0x803100A9	Veuillez enter le bon mot de passe actuel.
FVE_E_PASSPHRASE_TOO_LONG 0x803100AA	Les mots de passe ne doivent pas comporter plus de 256 caractères.
FVE_E_NO_PASSPHRASE_WITH_TPM 0x803100AB	Impossible d'ajouter un protecteur de clé de mot de passe car un protecteur de module de plateforme sécurisée (TPM) existe sur le lecteur.
FVE_E_NO_TPM_WITH_PASSPHRASE 0x803100AC	Impossible d'ajouter un protecteur de module de plateforme sécurisée (TPM) car un protecteur de mot de passe existe sur le lecteur.
FVE_E_NOT_ALLOWED_ON_CSV_STACK 0x803100AD	Cette commande ne peut être exécutée qu'à partir du nœud coordinateur du volume CSV spécifié.
FVE_E_NOT_ALLOWED_ON_CLUSTER 0x803100AE	Impossible d'exécuter cette commande sur un volume lorsque celui-ci fait partie d'un cluster.
FVE_E_EDRIVE_NO_FAILOVER_TO_SW 0x803100AF	BitLocker n'a pas rétabli le cryptage au niveau logiciel BitLocker en raison de la stratégie de groupe.
FVE_E_EDRIVE_BAND_IN_USE 0x803100B0	Le lecteur ne peut pas être géré par BitLocker, car la fonction de cryptage matériel du lecteur est déjà en cours d'utilisation.
FVE_E_EDRIVE_DISALLOWED_BY_GP 0x803100B1	Les paramètres de stratégie de groupe ne permettent pas l'utilisation du cryptage matériel.
FVE_E_EDRIVE_INCOMPATIBLE_VOLUME 0x803100B2	Le lecteur spécifié ne prend pas en charge le cryptage au niveau matériel.
FVE_E_NOT_ALLOWED_TO_UPGRADE_WHILE_CONVERTING 0x803100B3	Impossible de mettre à niveau BitLocker lors du cryptage ou du décryptage d'un disque.
FVE_E_EDRIVE_DV_NOT_SUPPORTED 0x803100B4	Les volumes de découverte ne sont pas pris en charge pour les volumes utilisant le cryptage au niveau matériel.
FVE_E_NO_PREBOOT_KEYBOARD_DETECTED 0x803100B5	Aucun clavier préalable au démarrage détecté. Il se peut que l'utilisateur ne puisse pas fournir l'entrée requise pour déverrouiller le volume.

Constante/Valeur	Description
FVE_E_NO_PREBOOT_KEYBOARD_OR_WINRE_DETECTED 0x803100B6	Aucun clavier préalable au démarrage ou environnement de récupération Windows détecté. Il se peut que l'utilisateur ne puisse pas fournir l'entrée requise pour déverrouiller le volume.
FVE_E_POLICY_REQUIRES_STARTUP_PIN_ON_TOUCH_DEVICE 0x803100B7	Les paramètres de stratégie de groupe nécessitent de créer un code confidentiel de démarrage, mais aucun clavier préalable au démarrage n'est disponible sur ce périphérique. Il se peut que l'utilisateur ne puisse pas fournir l'entrée requise pour déverrouiller le volume.
FVE_E_POLICY_REQUIRES_RECOVERY_PASSWORD_ON_TOUCH_DEVICE 0x803100B8	Les paramètres de stratégie de groupe nécessitent de créer un mot de passe de récupération, mais aucun clavier préalable au démarrage ou environnement de récupération Windows n'est disponible sur ce périphérique. Il se peut que l'utilisateur ne puisse pas fournir l'entrée requise pour déverrouiller le volume.
FVE_E_WIPE_CANCEL_NOT_APPLICABLE 0x803100B9	Aucun effacement d'espace libre n'a lieu actuellement.
FVE_E_SECUREBOOT_DISABLED 0x803100BA	BitLocker ne peut pas utiliser le démarrage sécurisé pour l'intégrité de la plateforme car le démarrage sécurisé est désactivé.
FVE_E_SECUREBOOT_CONFIGURATION_INVALID 0x803100BB	BitLocker ne peut pas utiliser le démarrage sécurisé pour l'intégrité de la plateforme car la configuration du démarrage sécurisé ne répond pas aux conditions requises pour BitLocker.
FVE_E_EDRIVE_DRY_RUN_FAILED 0x803100BC	Votre ordinateur ne prend pas en charge le cryptage au niveau matériel BitLocker. Contactez le fabricant de votre ordinateur afin de savoir si des mises à jour du microprogramme sont disponibles.
FVE_E_SHADOW_COPY_PRESENT 0x803100BD	BitLocker ne peut pas activer le volume car il contient un cliché instantané de volume. Supprimez tous les clichés instantanés de volumes avant de crypter le volume.
FVE_E_POLICY_INVALID_ENHANCED_BCD_SETTINGS 0x803100BE	Impossible d'appliquer le cryptage de lecteur BitLocker à ce lecteur car le paramètre de stratégie de groupe pour les données de configuration de démarrage améliorées contient des données non valides. Demandez à votre administrateur système de corriger cette configuration non valide avant de tenter d'activer BitLocker.
FVE_E_EDRIVE_INCOMPATIBLE_FIRMWARE 0x803100BF	Le micrologiciel du PC ne prend pas en charge le cryptage au niveau matériel.
FVE_E_PROTECTOR_CHANGE_MAX_PASSPHRASE_CHANGE_ATTEMPTS_REACHED 0x803100C0	BitLocker a désactivé les modifications de mot de passe après un trop grand nombre d'échecs de demandes. Cliquez sur le lien pour réinitialiser le mot de passe en tant qu'administrateur.
FVE_E_PASSPHRASE_PROTECTOR_CHANGE_BY_STD_USER_DISALLOWED 0x803100C1	Vous devez avoir ouvert une session avec un compte d'administrateur pour pouvoir modifier le mot de passe. Cliquez sur le lien pour réinitialiser le mot de passe en tant qu'administrateur.

Constante/Valeur	Description
FVE_E_LIVEID_ACCOUNT_SUSPENDED 0x803100C2	BitLocker ne peut pas enregistrer le mot de passe de récupération, car le compte Microsoft spécifié est suspendu.
FVE_E_LIVEID_ACCOUNT_BLOCKED 0x803100C3	BitLocker ne peut pas enregistrer le mot de passe de récupération, car le compte Microsoft spécifié est bloqué.
FVE_E_NOT_PROVISIONED_ON_ALL_VOLUMES 0x803100C4	Ce PC n'est pas configuré pour prendre en charge le cryptage de l'appareil. Activez BitLocker sur l'ensemble des volumes afin de vous conformer à la stratégie de cryptage de l'appareil.
FVE_E_DE_FIXED_DATA_NOT_SUPPORTED 0x803100C5	Ce PC ne peut pas prendre en charge le cryptage de l'appareil en raison de la présence de volumes de données fixes non cryptés.
FVE_E_DE_HARDWARE_NOT_COMPLIANT 0x803100C6	Ce PC ne possède pas la configuration matérielle requise pour la prise en charge du cryptage de l'appareil.
FVE_E_DE_WINRE_NOT_CONFIGURED 0x803100C7	Ce PC ne peut pas prendre en charge le cryptage de l'appareil, car WinRE n'est pas configuré correctement.
FVE_E_DE_PROTECTION_SUSPENDED 0x803100C8	La protection est activée sur le volume, mais elle a été interrompue vraisemblablement en raison d'une mise à jour en cours d'application sur votre système. Veuillez réessayer après un redémarrage.
FVE_E_DE_OS_VOLUME_NOT_PROTECTED 0x803100C9	Ce PC n'est pas configuré pour prendre en charge le cryptage de l'appareil.
FVE_E_DE_DEVICE_LOCKEDOUT 0x803100CA	Le verrouillage appareil a été déclenché en raison d'un nombre trop élevé d'entrées de mots de passe incorrects.
FVE_E_DE_PROTECTION_NOT_YET_ENABLED 0x803100CB	La protection n'a pas été activée sur le volume. L'activation de la protection requiert un compte connecté. Si vous possédez déjà un compte connecté et que vous obtenez cette erreur, référez-vous au journal des événements pour plus d'informations.
FVE_E_INVALID_PIN_CHARS_DETAILED 0x803100CC	Votre PIN ne peut contenir que des chiffres allant de 0 à 9.
FVE_E_DEVICE_LOCKOUT_COUNTER_UNAVAILABLE 0x803100CD	BitLocker ne peut pas utiliser la protection de la relecture matérielle car aucun compteur n'est disponible sur l'ordinateur.
FVE_E_DEVICELOCKOUT_COUNTER_MISMATCH 0x803100CE	Échec de validation de l'état de verrouillage du périphérique en raison d'une incohérence de comptage.
FVE_E_BUFFER_TOO_LARGE 0x803100CF	Le tampon d'entrée est trop volumineux.

20

Glossaire

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

Active Directory (AD) : service de répertoire créé par Microsoft pour les réseaux de domaine Windows.

Advanced Threat Prevention : le produit Advanced Threat Prevention est une protection antivirus de nouvelle génération qui utilise la science des algorithmes et l'apprentissage machine pour identifier, classifier et prévenir les cybermenaces connues ou inconnues et les empêcher d'exécuter ou d'endommager les points de terminaison. La fonction facultative Pare-feu client surveille la communication entre l'ordinateur et les ressources du réseau et d'Internet et intercepte les communications potentiellement malveillantes. La fonction facultative Web Protection bloque les sites Web et les téléchargements dangereux lors des consultations et des recherches, selon les rapports et cotes de sécurité des sites Web.

Cryptage des données d'application : crypte tous les fichiers écrits par une application protégée, à l'aide d'un remplacement de catégorie 2. Cela signifie que, dans tous les répertoires dotés d'une protection de catégorie 2 ou supérieure, ainsi que dans tous les dossiers où des extensions spécifiques sont protégées avec la catégorie 2 ou supérieure, ADE ne crypte aucun fichier.

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

Identifiants mis en cache : les identifiants mis en cache sont les identifiants qui sont ajoutés à la base de données d'authentification avant démarrage lorsqu'un utilisateur s'authentifie pour accéder à Active Directory. Ces informations relatives à l'utilisateur sont conservées afin qu'il puisse accéder à l'ordinateur lorsqu'il n'est pas connecté à Active Directory (lorsqu'il emporte son ordinateur portable chez lui, par exemple).

Cryptage Courant : la clé Courant rend les fichiers accessibles à tous les utilisateurs gérés sur leur périphérique de création.

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

Encryption External Media : ce service d'Encryption protège les supports amovibles et les périphériques de stockage externes.

Code d'accès d'Encryption External Media : ce service permet de récupérer les périphériques protégés par Encryption External Media lorsque l'utilisateur oublie son mot de passe et ne peut plus se connecter. Cette manipulation permet à l'utilisateur de réinitialiser le mot de passe défini sur le support.

Encryption : composant du périphérique qui permet d'appliquer les règles de sécurité, qu'un point de terminaison soit connecté au réseau, déconnecté du réseau, perdu ou volé. En créant un environnement de calcul de confiance pour les points de terminaison, Encryption opère à un niveau supérieur du système d'exploitation du périphérique et fournit une authentification, un chiffrement et une autorisation appliqués de façon cohérente qui permettent d'optimiser la protection des données sensibles.

Point de terminaison : en fonction du contexte, il peut s'agir d'un ordinateur, d'un appareil mobile ou d'un support externe.

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) protégé.

Balayage de chiffrement : processus d'analyse des dossiers à chiffrer afin de s'assurer que les fichiers contenus se trouvent dans l'état de chiffrement 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 produit lors de 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 *Analyser la station de travail lors de la connexion* est activée, les dossiers à chiffrer seront analysés à

chaque connexion de l'utilisateur. - Un balayage peut être déclenché à nouveau en raison de certaines modifications ultérieures apportées à des règles. Toute modification de règle en relation avec la définition des dossiers de chiffrement, les algorithmes de chiffrement, l'utilisation de clés de chiffrement (commun par rapport à utilisateur), déclenchera une analyse. De plus, le basculement entre l'activation et la désactivation du cryptage déclenche 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.

Contrôle des scripts : le contrôle des scripts protège les périphériques en empêchant les scripts malveillants de s'exécuter.

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

Utilisateur du serveur : compte d'utilisateur virtuel créé par Encryption dans le but de gérer les clés de chiffrement et les mises à jour de règles sur un système d'exploitation de serveur. Ce compte utilisateur ne correspond à aucun autre compte utilisateur sur l'ordinateur ou à l'intérieur du domaine, et il ne possède pas de nom d'utilisateur et de mot de passe pouvant être utilisés physiquement. Une valeur UCID unique est attribuée à ce compte dans la console de gestion.

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 communes et d'utilisateur sont destinées aux données sensibles de l'utilisateur, 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. Les règles SDE ne nécessitent pas d'authentification avant démarrage et n'affectent en rien l'enregistrement de démarrage principal. Au démarrage de l'ordinateur, les fichiers cryptés sont disponibles avant l'identification de l'utilisateur (pour permettre la gestion des correctifs, les SMS et l'utilisation des outils de sauvegarde et de récupération). La désactivation de SDE déclenche le déchiffrement automatique de tous les fichiers et répertoires SDE chiffrés pour les utilisateurs pertinents, quelles que soient les autres règles SDE, par exemple les règles de chiffrement 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.

Cryptage utilisateur : la clé utilisateur ne rend les fichiers accessibles qu'à l'utilisateur qui les a créés et uniquement sur le périphérique d'origine. Lors de l'exécution de Dell Server Encryption, le cryptage Utilisateur est converti en cryptage Commun. Il existe cependant une exception pour les périphériques de support amovible : lorsque des fichiers sont insérés dans un serveur sur lequel est installé Encryption, les fichiers sont cryptés à l'aide de la clé Utilisateur itinérant.