Endpoint Security Suite Enterprise

Guide d'installation de base v2.1

Remarques, précautions et avertissements

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

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

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

2018 - 11

Rév. A01

Table des matières

1

Introduction

Ce guide décrit comment installer et configurer l'application en utilisant le programme d'installation principal d'Endpoint Security Suite Enterprise. Ce guide permet d'obtenir une aide basique à l'installation. Voir le *Guide d'installation avancée* si vous avez besoin d'informations sur l'installation des programmes d'installation enfants, la configuration de Security Management Server/Security Management Server Virtual ou des informations allant au-delà de l'assistance de base à propos du programme d'installation principal Endpoint Security Suite Enterprise.

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

Avant de commencer

1 Installez le Serveur Dell 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 Serveur Dell.

2 Configuration d'un locataire pour Advanced Threat Prevention Un locataire doit être provisionné dans Serveur Dell 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 :

- Reportez-vous à Configuration requise pour accéder à la configuration requise du client.
- Sélectionnez 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

Contacter Dell ProSupport

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

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

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

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

2

Configuration requise

Tous les clients

- Les meilleures pratiques informatiques doivent être suivies pendant le déploiement. Ceci inclut, sans s'y limiter, les environnements de test contrôlés pour les premiers tests et les déploiements échelonnés pour les utilisateurs.
- Le compte utilisateur servant à l'installation/la mise à 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 ou Quest KACE. Les utilisateurs non-administrateurs et disposant de privilèges particuliers ne sont pas pris en charge.
- Sauvegardez toutes les données importantes avant de démarrer l'installation ou la désinstallation.
- Lors de l'installation, n'apportez aucune modification à l'ordinateur, notamment, n'insérez ou ne retirez pas de lecteurs externes (USB).
- Les administrateurs doivent s'assurer que tous les ports nécessaires sont disponibles.
- Consultez régulièrement la rubrique www.dell.com/support pour obtenir la dernière documentation et conseils techniques.
- **REMARQUE : La ligne de produits Dell Data Security ne prend pas en charge les versions de Windows Insider Preview.**

Configuration requise pour tous les clients

- Le programme d'installation principal installe les conditions suivantes si elles ne sont pas déjà installées sur l'ordinateur.

Conditions requises
– Visual C++ 2012 Redistributable Package (x86 and x64) Mise à jour 4 ou ultérieure
– Visual C++ 2015 Redistributable Package (x86 et x64) Mise à jour 3 ou ultérieure

Visual C++ 2015 nécessite Windows Update KB2999226 s'il est installé sous Windows 7.

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* le composant Microsoft .Net Framework.

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

Matériel pour tous les clients

- 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 crypter les fichiers sur le point de terminaison. Cette taille varie en fonction des stratégies et de la taille du lecteur.

Tous les clients - Localisation

- Les clients Encryption, Advanced Threat Prevention et Gestionnaire BitLocker sont compatibles avec l'interface utilisateur multilingue (MUI) et sont localisés dans les langues suivantes. Le cryptage complet du disque est uniquement pris en charge avec les systèmes d'exploitation en anglais. Les données Advanced Threat Prevention présentées sur la console de gestion sont disponibles en anglais uniquement.

Langues prises en charge

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

Client Encryption

- L'ordinateur client doit posséder une connexion active au réseau pour être activé.
- Désactivez le mode Veille lors du balayage de cryptage initial pour prévenir la mise en veille d'un ordinateur lors des périodes d'inactivité. Le cryptage ne peut pas être exécuté sur un ordinateur en veille (le décryptage non plus).
- Le client Encryption ne prend pas en charge les configurations à double démarrage dans la mesure où il est possible de crypter les fichiers système de l'autre système d'exploitation, ce qui perturberait son fonctionnement.
- Le client Encryption 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 prévenir les incompatibilités entre le balayage et le cryptage des antivirus. Le client Encryption a aussi été testé avec Microsoft Enhanced Mitigation Experience Toolkit.

  Si votre entreprise utilise un fournisseur d'antivirus qui n'est pas répertorié, consultez http://www.dell.com/support/article/us/en/19/SLN288353/ ou contactez Dell ProSupport.
- 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.

Configuration requise du client Encryption

Systèmes d'exploitation du client Encryption

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

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

- Windows 7 SP1 : Entreprise, Professionnel, Ultimate
- Windows Embedded Standard 7 avec modèle de compatibilité des applications
- Windows 8 : Enterprise, Pro
- Windows 8.1 : Enterprise, Pro
- Windows Embedded 8.1 Industry Enterprise
- Windows 10 : Éducation, Entreprise, Pro Version 1607 (Mise à jour anniversaire/Redstone 1) jusqu'à la version 1803 (Mise à jour avril 2018/Redstone 4)

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

- VMWare Workstation 12.5 et version ultérieure

REMARQUE :
La règle de mise en veille prolongée n'est pas prise en charge en mode UEFI.

Systèmes d'exploitation pour le client Encryption avec activation différée

- 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 Serveur Dell qui les valide par rapport aux domaines Active Directory configurés. Pour en savoir plus, voir http://www.dell.com/support/article/us/en/19/sln306341.
- Le tableau suivant décrit les systèmes d'exploitation pris en charge avec l'activation différée.

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

- Windows 7 SP1 : Entreprise, Professionnel, Ultimate
- Windows Embedded Standard 7 avec modèle de compatibilité des applications
- Windows 8 : Enterprise, Pro
- Windows 8.1 : Enterprise, Pro
- Windows Embedded 8.1 Industry Enterprise
- Windows 10 : Éducation, Entreprise, Pro Version 1607 (Mise à jour anniversaire/Redstone 1) jusqu'à la version 1803 (Mise à jour avril 2018/Redstone 4)

Encryption External Media Les systèmes d'exploitation cryptage média externe

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

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

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

- Windows 7 SP1 : Entreprise, Professionnel, Ultimate
- Windows Embedded Standard 7 avec modèle de compatibilité des applications
- Windows 8 : Enterprise, Pro
- Windows 8.1 : Enterprise, Pro
- Windows Embedded 8.1 Industry Enterprise
- Windows 10 : Éducation, Entreprise, Pro Version 1607 (Mise à jour anniversaire/Redstone 1) jusqu'à la version 1803 (Mise à jour avril 2018/Redstone 4)

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

- macOS Sierra 10.12.6
- macOS High Sierra 10.13.5 - 10.13.6

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

- macOS Mojave 10.14

Cryptage complet du disque

Le cryptage complet du disque peut **uniquement** être installé au moyen de l'interface de ligne de commande (CLI). Si vous souhaitez installer le cryptage complet du disque, téléchargez le Guide d'installation avancée Endpoint Security Suite Enterprise pour plus d'instructions.

- Le cryptage 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 des configurations à plusieurs disques n'est pas pris en charge.
- 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 connexion active au 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 cryptage 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 cryptage complet du disque n'est pas pris en charge avec BitLocker ou BitLocker Manager. N'installez pas le cryptage complet du disque sur un ordinateur sur lequel le BitLocker ou BitLocker Manager est installé.
- Tout disque NVMe utilisé pour PBA : l'opération SATA du BIOS doit être définie sur RAID ON, car la PBA Management de Dell ne prend pas en charge AHCI sur les disques NVMe.
- Tout disque NVMe utilisé pour PBA : le mode de démarrage du BIOS doit être UEFI et les ROM de l'option Hérité doivent être désactivés.
- Tout disque non NVMe utilisé pour PBA : l'opération SATA du BIOS doit être définie sur AHCI, car PBA Management de Dell ne prend pas en charge RAID avec les disques non NVMe.
  - RAID ON n'est pas pris en charge, car l'accès à la lecture et l'écriture des données RAID (sur un secteur non disponible sur un lecteur non NVMe verrouillé) n'est pas disponible au démarrage et ne peut attendre de lire ces données après la connexion de l'utilisateur.
  - Le système d'exploitation plante lorsqu'il est transféré de RAID ON à AHCI si les disques du contrôleur AHCI ne sont pas préinstallés. Pour obtenir des instructions sur le transfert de RAID à AHCI (ou vice-versa), voir http://www.dell.com/support/article/us/en/19/SLN306460.

    Dell recommande Intel Rapid Storage Technology Driver version 15.2.0.0 ou ultérieure avec les disques NVMe.
- Désactivez le mode Veille lors du balayage de cryptage initial pour prévenir la mise en veille d'un ordinateur lors des périodes d'inactivité. Le cryptage ne peut pas être exécuté sur un ordinateur en veille (le décryptage non plus).
- Le client de cryptage complet du disque ne prend pas en charge les configurations à double démarrage dans la mesure où il est possible de crypter les fichiers système de l'autre système d'exploitation, ce qui perturberait son fonctionnement.
- 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.
- **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 : Le cryptage complet du disque doit être configuré avec des algorithmes de cryptage définis sur AES 256 et Mode de cryptage défini pour CBC.

Prérequis du client de cryptage complet du disque

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

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

Matériel du client de cryptage complet du disque

- Le tableau suivant répertorie en détail le matériel compatible.

Matériel intégré en option
– TPM 1.2 ou 2.0

Systèmes d'exploitation du client de cryptage complet du disque

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

Systèmes d'exploitation Windows (64 bits)
– Windows 7 SP1 : Entreprise, Professionnel, Édition Intégrale (mode de démarrage hérité requis)
– Windows 10 : Éducation, Entreprise, Pro Version 1607 (Mise à jour anniversaire/Redstone 1) jusqu'à la version 1803 (Mise à jour avril 2018/Redstone 4) (mode de démarrage UEFI requis)

Client Advanced Threat Prevention

- Pour terminer l'installation d'Advanced Threat Prevention lorsque le Serveur Dell 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 Serveur Dell de gestion est exécuté en mode Déconnecté.
- Pour configurer un locataire pour Advanced Threat Prevention, le Serveur Dell 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 Serveur Dell 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 Serveur Dell ainsi qu'aux autres applications. Pour obtenir des instructions sur l'ajout d'exceptions à Advanced Threat Prevention dans le Serveur Dell, voir http://www.dell.com/support/article/us/en/04/SLN300970. Pour obtenir la liste des exclusions à ajouter à l'autre applications anti-virus, reportez-vous à http://www.dell.com/support/article/us/en/04/sln301562.

Systèmes d'exploitation d'Advanced Threat Prevention

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

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

- Windows 7 SP1 : Entreprise, Professionnel, Ultimate
- Windows Embedded Standard 7
- Windows 8 : Enterprise, Pro
- Windows 8.1 : Enterprise, Pro
- Windows 10 : Éducation, Entreprise, Pro Version 1607 (Mise à jour anniversaire/Redstone 1) jusqu'à la version 1803 (Mise à jour avril 2018/Redstone 4)
- Windows Server 2008 R2
- Windows Server 2012 R2
- Windows Server 2016

Ports Advanced Threat Prevention

- 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 : http://www.dell.com/support/article/us/en/19/SLN303898

Vérification de l'intégrité de l'image BIOS

Si la règle *Activer l'assurance BIOS* est sélectionnée dans la console de gestion, le locataire 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 Serveur Dell 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
- Latitude 7370
- Latitude E5270
- Latitude E5470
- OptiPlex 5040
- OptiPlex 7040
- OptiPlex 7440
- Precision Mobile Workstation 3510
- Precision Mobile Workstation 5510
- Precision Workstation 3620

Modèles d'ordinateur Dell pris en charge avec la vérification de l'intégrité de l'image BIOS

- Latitude E5570
- Latitude E7270
- Latitude E7470
- Latitude Rugged 5414
- Latitude Rugged 7214 Extrême
- Latitude Rugged 7414
- OptiPlex 3040
- OptiPlex 3240
- 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

Pare-feu client et clients de protection Web

- L'installation du pare-feu client et des clients de protection Web exige la connexion de l'ordinateur au réseau.
- Désinstallez les applications antivirus, anti-programmes malveillants, anti-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.
- La fonction Web Protection n'est prise en charge que par Internet Explorer.

Systèmes d'exploitation pour le pare-feu client et le client de protection Web

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

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

- Windows 7 SP1 : Entreprise, Professionnel, Ultimate
- Windows 8 : Enterprise, Pro
- Windows 8.1 : Enterprise, Pro
- Windows 10 : Éducation, Entreprise, Pro Version 1607 (Mise à jour anniversaire/Redstone 1) jusqu'à la version 1803 (Mise à jour avril 2018/Redstone 4)

Ports du pare-feu client et des clients de protection Web

- Pour garantir que le pare-feu client et les clients de protection Web 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 anti-virus (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	Remarques
Service de réputation	SSL	TCP	443	tunnel.web.trustedsource.org	Sortant	
Commentaires relatif au service de réputation	SSL	TCP	443	gtifeedback.trustedsource.org	Sortant	

Utilisation	Protocole d'application	Protocole de transport :	Numéro de port	Destination	Direction	Remarques
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	

Client SED

- Pour que l'installation de SED réussisse, l'ordinateur doit disposer d'une connectivité à un 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 Management 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 pas pris en charge avec les configurations à plusieurs disques.
- 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-cryptage prenant en charge le module HCA. Cette configuration non prise en charge est une configuration après-vente.
- Si l'ordinateur ciblé pour cryptage est équipé d'un accélérateur d'un lecteur à cryptage automatique, vérifiez que l'option Active Directory, *l'utilisateur doit changer de mot passe lors de la prochaine connexion*, est désactivée. L'authentification avant démarrage ne prend pas en charge cette option Active Directory.
- Dell vous déconseille de changer de méthode d'authentification après avoir activé la règle PBA. Si vous devez changer de méthode d'authentification, vous devez :
  - Supprimez tous les utilisateurs de la PBA.

    ou
  - Désactivez la PBA, changez de méthode d'authentification, puis ré-activez la PBA.

  IMPORTANT:

  En raison de la nature du RAID et des SED, la gestion des SED ne prend pas en charge le RAID. *RAID=On* avec disques SED présente un problème : le RAID exige un accès au disque pour la lecture et l'écriture des données associées au RAID dans un secteur élevé non disponible sur un SED verrouillé dès le début, et, pour lire ces données, ne peut pas attendre que l'utilisateur se connecte. Pour résoudre le problème, dans le BIOS, définissez l'opération SATA sur *AHCI* au lieu de *RAID=On*. Si les pilotes de contrôleur AHCI ne sont pas pré-installés sur le système d'exploitation, ce dernier plante lors du passage de *RAID=On* à *AHCI*.
- La configuration des disques à cryptage automatique pour SED management de Dell est différente entre les disques NVMe et non NVMe (SATA).
  - Tout disque NVMe utilisé en tant que SED : l'opération SATA du BIOS doit être définie sur RAID ON, car SED Management de Dell ne prend pas en charge AHCI sur les disques NVMe.
  - Tout disque NVMe utilisé en tant que SED : le mode de démarrage du BIOS doit être UEFI et les ROM de l'option Hérité doivent être désactivés.
  - Tout disque non NVMe utilisé en tant que SED : l'opération SATA du BIOS doit être définie sur AHCI, car SED Management de Dell ne prend pas en charge RAID avec les disques non NVMe.
    - RAID ON n'est pas pris en charge, car l'accès à la lecture et l'écriture des données RAID (sur un secteur non disponible sur un lecteur non NVMe verrouillé) n'est pas disponible au démarrage et ne peut attendre de lire ces données après la connexion de l'utilisateur.

- Le système d'exploitation plante lorsqu'il est transféré de RAID ON à AHCI si les disques du contrôleur AHCI ne sont pas préinstallés. Pour obtenir des instructions sur le transfert de RAID à AHCI (ou vice-versa), voir http://www.dell.com/support/article/us/en/19/SLN306460.

Les lecteurs SED compatibles OPAL pris en charge exigent les pilotes Intel Rapid Storage Technology mis à jour, disponibles à l'adresse http://www.dell.com/support. Dell recommande Intel Rapid Storage Technology Driver version 15.2.0.0 ou ultérieure avec les disques NVMe.

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

- SED Management n'est pas pris en charge avec Server Encryption ou Advanced Threat Prevention sur un système d'exploitation de serveur.
- **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.**

Matériel du client SED

Claviers internationaux pour le client SED

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

Clavier international pris en charge - UEFI

- DE-FR - Suisse (français)
- DE-CH - Suisse (allemand)
- EN-US - Anglais (anglais américain)
- EN-GB - Anglais (anglais britannique)
- EN-CA - Anglais (anglais canadien)

Clavier International prise en charge : Non-UEFI

- AR - Arabe (avec lettres latines)
- DE-FR - Suisse (français)
- DE-CH - Suisse (allemand)
- EN-US - Anglais (anglais américain)
- EN-GB - Anglais (anglais britannique)
- EN-CA - Anglais (anglais canadien)

Emplacement du client SED

Le client SED est compatible avec l'interface utilisateur multilingue (MUI – Multilingual User Interface) et a été traduit dans les langues suivantes. Le mode UEFI et l'authentification avant démarrage prennent en charge les langues suivantes (**à l'exception** du russe, du chinois traditionnel et du chinois simplifié).

Langues prises en charge

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

Systèmes d'exploitation du client SED

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

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

– Windows 7 SP0-SP1 : Entreprise, Professionnel, Édition Intégrale (pris en charge pour le mode de démarrage hérité, mais pas pour UEFI)

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

– Windows 8 : Enterprise, Pro
– Windows 8.1 : Enterprise, Pro
– Windows 10 : Éducation, Entreprise, Pro Version 1607 (Mise à jour anniversaire/Redstone 1) jusqu'à la version 1803 (Mise à jour avril 2018/Redstone 4)

Client Gestionnaire BitLocker

- 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 Gestionnaire BitLocker avant de configurer la partition PBA, vous ne pourrez pas activer BitLocker et Gestionnaire BitLocker ne sera pas opérationnel.
- Un Serveur Dell est nécessaire pour utiliser BitLocker Manager.
- Assurez-vous qu'un certificat de signature est disponible dans la base de données. Voir http://www.dell.com/support/article/us/en/19/sln307028 pour plus d'informations.
- 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 Gestionnaire BitLocker s'approprie le TPM sans nécessiter de redémarrage. Toutefois, si le TPM est déjà propriétaire, Gestionnaire BitLocker lance le processus de configuration du cryptage (aucun redémarrage n'est nécessaire). Ce qui compte, c'est que le TPM soit propriétaire et activé.
- Gestionnaire BitLocker n'est pas pris en charge avec Server Encryption ou Advanced Threat Prevention sur un système d'exploitation de serveur.

Matériel du client BitLocker Manager

- Le tableau suivant répertorie en détail le matériel compatible.

Matériel intégré en option
– TPM 1.2 ou 2.0

Systèmes d'exploitation du client Gestionnaire BitLocker

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

Systèmes d'exploitation Windows
– Windows 7 SP0-SP1 : Enterprise, Ultimate (32 et 64 bits)
– Windows 8 : Enterprise (64 bits)
– Windows 8.1 : Enterprise Edition, Pro Edition (64 bits)
– Windows 10 : Entreprise, Pro Version 1607 (Mise à jour anniversaire/Redstone 1) jusqu'à la version 1803 (Mise à jour avril 2018/ Redstone 4)
– Windows Server 2008 R2 : Standard Edition, Enterprise Edition (64 bits)
– Windows Server 2012 R2 : Standard Edition, Enterprise Edition (64 bits)
– Windows Server 2016

Les mises à jour Windows KB3133977 et KB3125574 **ne doivent pas** être installées en cas d'installation de BitLocker Manager sous Windows 7.

3

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.**
- 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 du client Encryption, voir *Aide concernant Dell Encrypt*. Accédez à l'aide depuis **<Install dir>:\Program Files\Dell\Dell Data Protection\Encryption\Help**.
  - Pour apprendre à utiliser les fonctions d'*Encryption External Media*, voir l'Aide concernant Encryption External Media. Accédez à l'aide depuis **<Install dir>:\Program Files\Dell\Dell Data Protection\Encryption\EMS**.
  - Voir l'Aide d'*Endpoint Security Suite Enterprise* pour savoir comment utiliser les fonctions de et d'Advanced Threat Prevention. Accédez à l'aide depuis **<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 le fichier **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 Management local*, saisissez le nom d'hôte complet du Serveur Dell pour gérer l'utilisateur cible, comme serveur.organisation.com.

   Dans le champ *URL de Dell Device Server*, saisissez l'URL du Serveur Dell avec lequel le client communiquera.

   e format est le suivant : https://serveur.organisation.com:**8443**/xapi**/** (barre oblique de fin incluse).

   Cliquez sur **Suivant** .

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

7 Sélectionnez les composants à installer.

Security Framework installe le cadre de sécurité sous-jacent.

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.

Threat Protection permet d'installer les clients Threat Protection qui constituent une protection contre les programmes malveillants et les virus. Ils permettent de rechercher les virus, les programmes espions et indésirables, les pare-feu du client pour surveiller les communications entre l'ordinateur et les ressources existantes sur le réseau et Internet, puis de filtrer le Web afin d'afficher les niveaux de sécurité ou de bloquer l'accès à certains sites Internet lors de la navigation en ligne.

Gestionnaire BitLocker permet d'installer le client Gestionnaire BitLocker, 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 cryptage de BitLocker.

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 machine 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 les fonctionnalités facultatives : protection Web et 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.

REMARQUE : Si vous tentez d'installer la fonction Advanced Threat Prevention sur un ordinateur Windows 10 avec la mise à jour octobre 2018 (Redstone 5) ou version ultérieure, un message d'avertissement d'incompatibilité s'affiche.

REMARQUE : Si vous tentez d'installer les fonctionnalités facultatives Web Protection et Firewall sur un ordinateur Windows 10 avec la mise à jour octobre 2018 (Redstone 5) ou version ultérieure, un message d'avertissement d'incompatibilité s'affiche.

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.

REMARQUE : Advanced Threat Prevention n'est pas pris en charge pour Windows 10 avec la mise à jour octobre 2018 (Redstone 5) ou version ultérieure.

Commutateur	Description
-y -gm2	Extraction préalable du programme d'installation principal d'Endpoint Security Suite Enterprise. Vous devez utiliser les commutateurs -y et -gm2 ensemble. Ne les séparez pas.
/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 Serveur Dell.
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 = Gestionnaire BitLocker SED = SED Management (EMAgent/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 Serveur Dell 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 gestion SED.

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 Serveur Dell spécifié.

```
"DDSSuite.exe" -y -gm2 /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 Serveur Dell spécifié.

```
"DDSSuite.exe" -y -gm2 /S /z"\"SERVER=server.organization.com, FEATURES=DE-ATP\""
```

- (Sur le système d'exploitation d'un poste de travail) Cet exemple correspond à l'installation d'Advanced Threat Prevention, d'Encryption et de SED Management 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 Serveur Dell spécifié.

```
"DDSSuite.exe" -y -gm2 /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 Serveur Dell spécifié.

```
"DDSSuite.exe" -y -gm2 /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 Serveur Dell spécifié.

```
"DDSSuite.exe" -y -gm2 /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 par défaut **C:\Program Files\Dell\Dell Data Protection**

```
"DDSSuite.exe" -y -gm2 /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 Serveur Dell spécifié.

```
"DDSSuite.exe" -y -gm2 /S /z"\"SERVER=server.organization.com, FEATURES=ATP\""
```

- (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 Serveur Dell spécifié.

```
"DDSSuite.exe" -y -gm2 /S /z"\"SERVER=server.organization.com, FEATURES=DE\""
```

4

Désinstallation du 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 :

  a Désinstallez le client Encryption.

  b Désinstallez Advanced Threat Prevention.

  c Désinstallez le client SED (cette opération désinstalle le Dell Encryption Management/Agent, qui ne peut pas être désinstallé avant la désinstallation d'Advanced Threat Prevention).

  d Désinstaller le client 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" -y -gm2 /S /x
  ```

  Lorsque vous avez terminé, redémarrez l'ordinateur.

5

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
/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 du client Encryption et Server Encryption

- 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).
- Dell Encryption et Encryption External Media mettent à jour le Serveur Dell pour faire passer le statut à *Non protégé* au début d'un processus de désinstallation du Client Encryption. Toutefois, lorsque le client ne peut pas contacter le Serveur Dell, 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 flux de travail 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 le rapporteur de conformité.

Processus

- 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.

Désinstallation de ligne de commande

- Après son extraction du programme d'installation principal d'Endpoint Security Suite Enterprise, le programme d'installation du client Encryption se trouve dans **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 Serveur Dell 0 : ne pas installer Encryption Removal Agent
CMGSILENTMODE	Propriété permettant d'activer la désinstallation silencieuse : 1 : silencieuse 0 : pas silencieuse
Propriétés requises	
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).
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 Serveur Dell, 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 du client Encryption et au téléchargement des clés de cryptage 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 du client Encryption et au téléchargement des clés de cryptage 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.

IMPORTANT:

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.

REMARQUE :

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"
```

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.

- **IMPORTANT: 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"
  ```

Désinstaller le client SED

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

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.
- Désinstaller le client SED.

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 Serveur Dell à l'ordinateur cible de la désactivation.

   Désinstallez les clients SED et d'authentification après la désactivation de la PBA.

Désinstaller le client SED

Désinstallation avec ligne de commande

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

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

    Après avoir terminé, éteignez et redémarrez l'ordinateur.

Désinstallation du client Gestionnaire BitLocker

Désinstallation avec ligne de commande

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

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

Lorsque vous avez terminé, redémarrez l'ordinateur.

6

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.

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

Pour plus d'informations ou pour utiliser l'interface de ligne de commande (CLI), voir l'article de la base de connaissances SLN307791.

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

Pour exécuter l'utilitaire, ouvrez le dossier le contenant, cliquez avec le bouton droit de la souris sur **DataSecurityUninstaller.exe**, et **exécutez-le en tant qu'administrateur**.

Cliquez sur **Suivant**.

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

REMARQUE : 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.

7

Provision a Tenant

Un locataire doit être provisionné dans Serveur Dell 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 Serveur Dell.
- 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 Serveur Dell.

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 Serveur Dell 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 Serveur Dell. 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**.

8

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 Serveur Dell.

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**.

Extraction des programmes d'installation enfant

- 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 /z"\"EXTRACT_INSTALLERS=C:\extracted\""
```

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

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

10

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.
- 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 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 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 »).

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.

Écran des services - Redémarrage du service Key Server

1 Retournez au panneau 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 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.

11

Utiliser l'utilitaire Administrative Download (CMGAd)

- Cet utilitaire permet de télécharger un ensemble de matériel clé à utiliser sur un ordinateur non connecté à un Security Management Server/Security Management Server Virtual.
- Cet utilitaire utilise l'une des méthodes suivantes pour télécharger un ensemble 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

Utiliser l'utilitaire de téléchargement administratif en mode d'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/.

Admin Dell : nom de l'administrateur doté des identifiants d'administrateur d'analyse approfondie (activés dans la console de gestion à distance), tel que jdupond

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.

> **CONSEIL:**
> Normalement, 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 des informations différentes concernant le client et l'ordinateur client.

Cliquez sur **Suivant**.

3 Dans le champ Phrase de passe : entrez la phrase de passe afin de 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 par défaut et l'emplacement auquel le fichier sera enregistré, ou bien 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.

Utiliser l'utilitaire de téléchargement administratif en 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 Security Management Server Virtualce dernier n'utilise pas le Key Server. Utiliser le mode Analyse approfondie pour obtenir l'ensemble de clés si le client est activé auprès d'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.

> **CONSEIL:**
> Normalement, 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 des informations différentes concernant le client et l'ordinateur client.

Cliquez sur **Suivant**.

3 Dans le champ Phrase de passe : entrez la phrase de passe afin de 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 par défaut et l'emplacement auquel le fichier sera enregistré, ou bien 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.

12

Dépannage

Tous les clients - Dépannage

- Les fichiers journaux du programme d'installation principal 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). DDP|A n'est compatible avec cette suite de produits.

Tous les Clients - état de la protection

Dell Security Management 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 cryptage par périphérique.

L'état protégé est désormais 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.
- Dell Data Guardian est installé et activé.
- Self-Encrypting Drive Management est installé et activé et l'authentification avant démarrage (PBA) est activée.
- BitLocker Manager est installé et activé, et le cryptage est terminé.
- Dell Encryption (MAC) est installé et activé, et le cryptage basé sur des règles a été appliqué.
- 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 du client Encryption et Server Encryption

Mise à niveau vers Windows 10 Creators Update

Pour effectuer la mise à niveau vers Windows 10 avec la mise à jour octobre 2018, suivez les instructions figurant dans l'article suivant : http://www.dell.com/support/article/us/en/19/SLN298382.

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 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 Serveur Dell 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 Serveur Dell doit être 9.1 ou ultérieure. Si nécessaire, mettez à niveau votre Serveur Dell à la version 9.1 ou ultérieure.
- Vérifiez l'adresse URL de Serveur Dell 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 initniale de Server Encryption 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.

La boîte de dialogue Activation s'affiche lorsque l'un des deux événements suivants se produit :

- Un nouvel utilisateur (non géré) se connecte à l'ordinateur.
- Un nouvel utilisateur fait un clic droit sur l'icône du client Encryption dans la barre d'état système et sélectionne Activer Dell Encryption.

La procédure d'activation initiale se déroule comme suit :

1 L'utilisateur se connecte.
2 Détectant 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 du client 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 Server Encryption d'être déployé dans d'autres environnements de serveur qui ne le prennent pas en charge. Pour désactiver l'exigence des informations d'identification de l'administrateur de domaine, voir Avant de commencer.

6 Serveur Dell 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, Serveur Dell crée un nouveau compte utilisateur pour l'utilisateur du serveur virtuel et stocke ces informations d'identification dans le coffre de Serveur Dell.

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, Server Encryption se connecte automatiquement en tant qu'utilisateur du serveur virtuel, en demandant la clé d'ordinateur auprès de Serveur Dell. Cette opération intervient avant même que tout utilisateur puisse ouvrir une session.

- Ouvrez la boîte de dialogue À propos pour vérifier que Server Encryption est authentifié et en mode Serveur.
- Si l'ID du Client Encryption 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<2><2><2><2> </2></2></2></2>*pour procéder à de nouvelles tentatives de récupération de la clé à intervalles définis.

    Pour en savoir plus sur la règle d'*Intervalle entre les tentatives en cas d'échec du réseau*, voir 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 Serveur Dell :

   - Si l'ordinateur n'a pas encore été activé par un périphérique, Serveur Dell attribue à l'ordinateur un MCID, un DCID et un certificat de confiance, et stocke toutes ces informations dans le coffre de Serveur Dell.
   - Si l'ordinateur avait été précédemment activé par un périphérique, Serveur Dell vérifie le certificat de confiance.

3 Une fois que Serveur Dell 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.

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 le client Encryption, d'afficher l'état de chiffrement et d'identifier les fichiers non cryptés qui devraient être décryptés.
- Des privilèges d'administrateur sont requis pour exécuter cet utilitaire.

Exécutez l'

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 du client Encryption. Suivez votre processus actuel de décryptage des données, par exemple l'envoi d'une mise à jour de règle de décryptage. Une fois les données décryptées mais avant de redémarrer l'ordinateur en préparation de la désinstallation, exécutez WSScan afin de vous assurer que toutes les données sont décryptées.
- *Fichiers non cryptés* : pour identifier les fichiers qui ne sont pas cryptés, avec une mention indiquant si les fichiers doivent être cryptés (Y/N).
- *Tous les fichiers* : pour répertorier tous les fichiers cryptés et non cryptés, avec une mention indiquant si les fichiers doivent être cryptés (Y/N).
- *Fichiers non cryptés en violation* : pour identifier les fichiers qui ne sont pas cryptés, mais qui devraient l'être.

6 Cliquez sur **Rechercher**.

OU

1 Cliquez sur **Avancé** pour basculer la vue vers **Simple** afin d'analyser un dossier particulier.

2 Accédez à Paramètres d'analyse, puis saisissez le chemin du dossier dans le champ *Rechercher un chemin d'accès*. Si vous utilisez ce champ, la sélection dans le menu est ignorée.

3 Si vous ne voulez pas écrire la sortie WSScan dans un fichier, décochez la case **Sortie vers un fichier**.

4 Si vous le souhaitez, changez le chemin et le nom de fichier par défaut à partir du champ *Chemin*.

5 Sélectionnez **Ajouter au fichier existant** si vous ne souhaitez remplacer aucun des fichiers WSScan de sortie existants.

6 Choisissez le format de sortie :

- Sélectionnez l'option Format du rapport, si vous souhaitez que les résultats de l'analyse apparaissent sous forme de liste de rapport. Il s'agit du format par défaut.
- Sélectionnez Fichier à valeur délimitée pour que les résultats puissent être exportés dans un tableur. Le séparateur par défaut est « | », mais il peut être remplacé par un maximum de 9 caractères alphanumériques, espaces ou symboles de ponctuation.
- Sélectionnez Valeurs désignées pour mettre chaque valeur entre doubles guillemets.
- Sélectionnez Fichier à largeur fixe si vous souhaitez un fichier cible non délimité contenant une ligne continue d'informations à longueur fixe sur chaque fichier crypté.

7 Cliquez sur **Rechercher**.

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

Fichier cible WSScan

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

Exemple :

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

Sortie	Signification
Date/heure	Date et heure d'analyse du fichier.
Type de cryptage	Type de cryptage utilisé pour le fichier. **SysData** : clé SDE. **Utilisateur :** clé de chiffrement utilisateur. **Commun** : clé de chiffrement commun. Le rapport de cryptage ne prend pas en compte les fichiers cryptés avec l'option Encrypt for Sharing.

Sortie	Signification
KCID	Identification de l'ordinateur principal. Dans l'exemple ci-dessus : « **7vdlxrsb** » Si vous analysez un disque réseau mappé, le rapport d'analyse ne comporte pas de KCID.
UCID	ID d'utilisateur. Comme dans l'exemple ci-dessus , « **_SDENCR_** » Tous les utilisateurs de l'ordinateur partagent le même UCID.
Fichier	Chemin d'accès du fichier crypté. Comme dans l'exemple ci-dessus, « **c:\temp\Dell - test.log** »
Algorithme	Algorithme utilisé pour crypter le fichier. Dans l'exemple ci-dessus, « **cryptage AES 256 toujours en place** » RIJNDAEL 128 RIJNDAEL 256 AES-128 AES-256 3DES

Vérification de l'état d'Encryption Removal Agent.

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

- **Attente de la désactivation SDE** - Le client Encryption est toujours installé, toujours configuré ou les deux. Le déchiffrement ne démarrera pas tant que le client Encryption ne sera pas désinstallé.
- **Balayage initial** - Le service procède à un premier balayage en calculant le nombre de fichiers chiffrés et les octets. L'analyse initiale n'a lieu qu'une seule fois.
- **Balayage de décryptage** - Le service déchiffre les fichiers et demande éventuellement à déchiffrer des fichiers verrouillés.
- **Decrypter au redémarrage (partiel)** - Le balayage de décryptage est terminé et certains fichiers verrouillés (mais pas tous) devront être décryptés au prochain redémarrage.
- **Décrypter au redémarrage** - Le balayage de décryptage est terminé et tous les fichiers verrouillés devront être décryptés au prochain redémarrage.
- **Tous les fichiers n'ont pas pu être décryptés** - Le balayage de décryptage est terminé, mais tous les fichiers n'ont pas pu être décryptés. Cet état signifie que l'une des situations suivantes s'applique :
  - Les fichiers verrouillés n'ont pas pu être programmés pour être décryptés, en raison d'une taille trop importante ou du fait qu'une erreur s'est produite lors de la requête de déverrouillage.
  - Une erreur au niveau de la source / de la cible s'est produite lors du décryptage des fichiers.
  - Les fichiers n'ont pas pu être décryptés par la règle.
  - Les fichiers ont le statut « devraient être cryptés ».
  - Une erreur s'est produite lors de l'analyse de décryptage.
  - Dans tous les cas, un fichier de consignation est créé (si vous avez configuré la consignation) si la valeur LogVerbosity est supérieure ou égale à 2. Pour résoudre le problème, choisissez la valeur de verbosité de consignation 2, puis relancez le service Encryption Removal Agent pour forcer l'exécution d'un nouveau balayage de déchiffrement.

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

Dépannage du client Advanced Threat Prevention

Trouver le code de produit avec Windows PowerShell

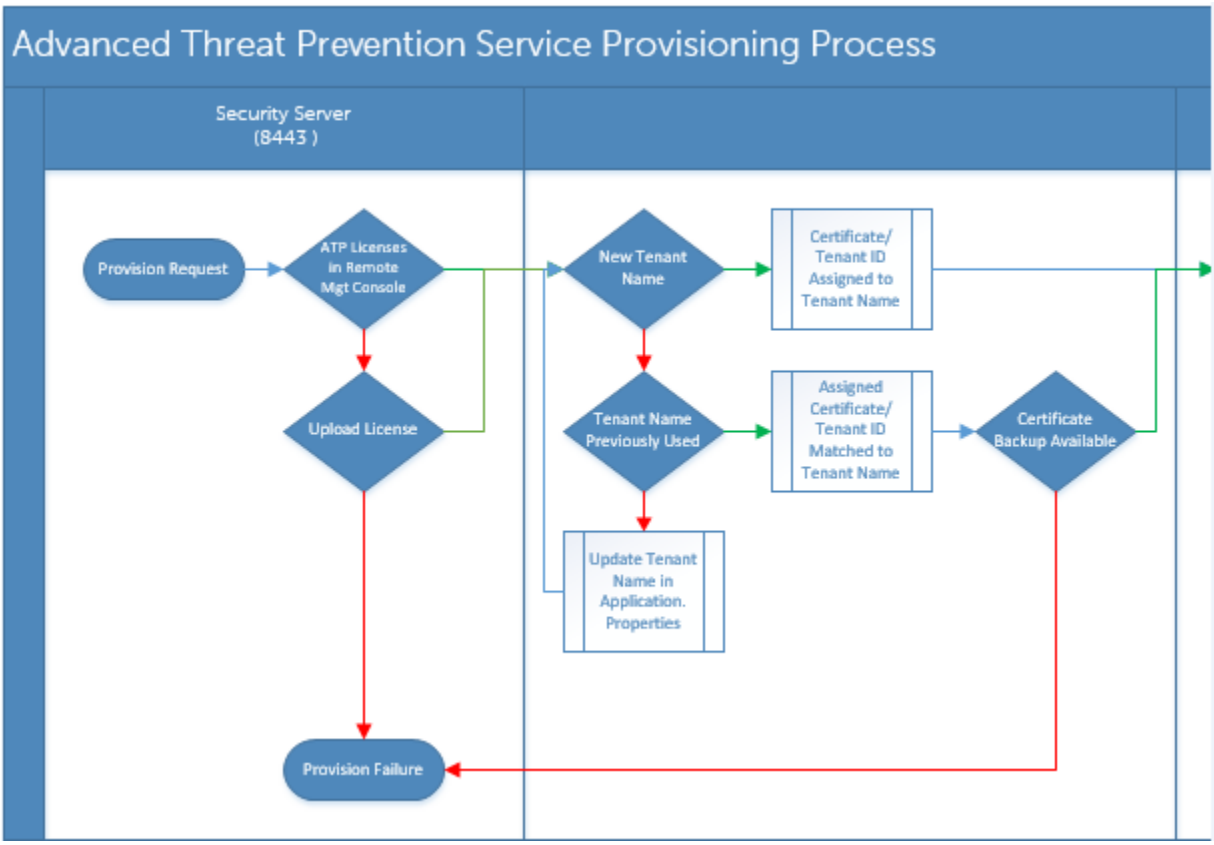
- Vous pouvez facilement identifier le code de produit, si le code de produit change à l'avenir, à l'aide de cette méthode.

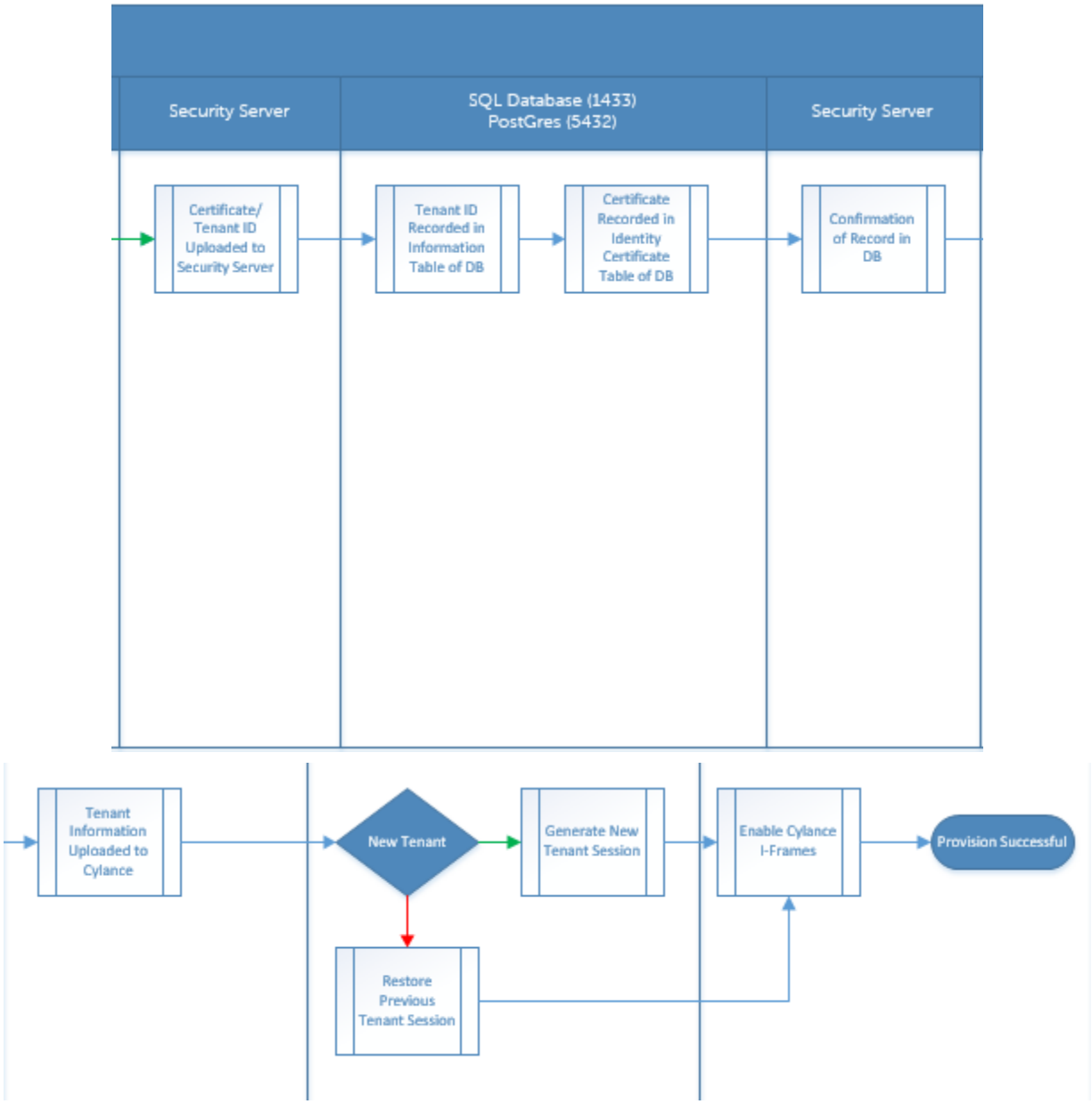
  ```
  Get-WmiObject  Win32_Product | Where-Object {$_.Name -like '*Cylance*'} | FT
  IdentifyingNumber, Name, LocalPackage
  ```

  La sortie génère le chemin complet et le nom du fichier .msi (le nom du fichier converti en valeur hexadécimale).

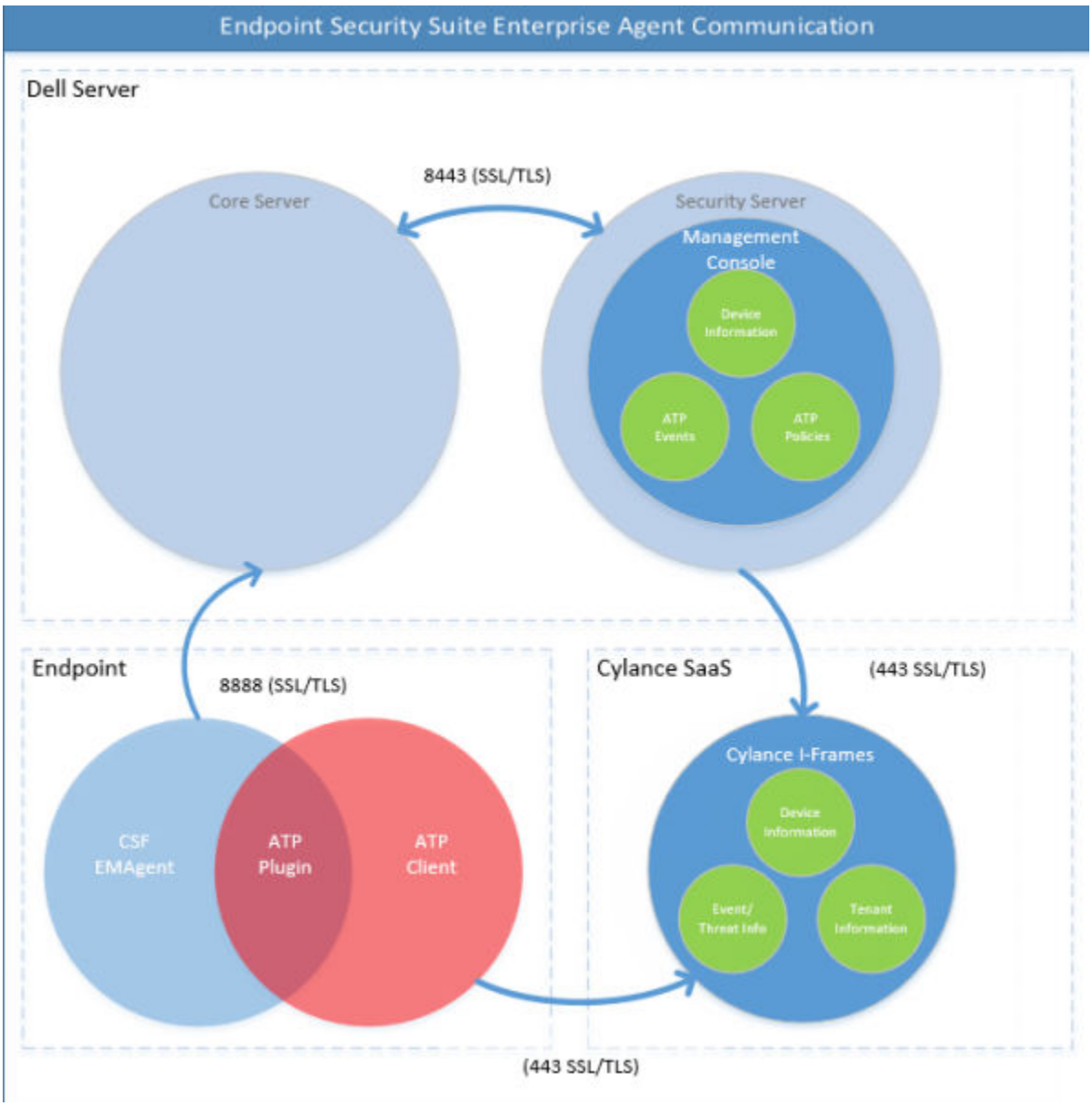
Provisionnement d'Advanced Threat Prevention et communication agent

Les diagrammes suivants illustrent le processus de provisionnement du service Advanced Threat Prevention



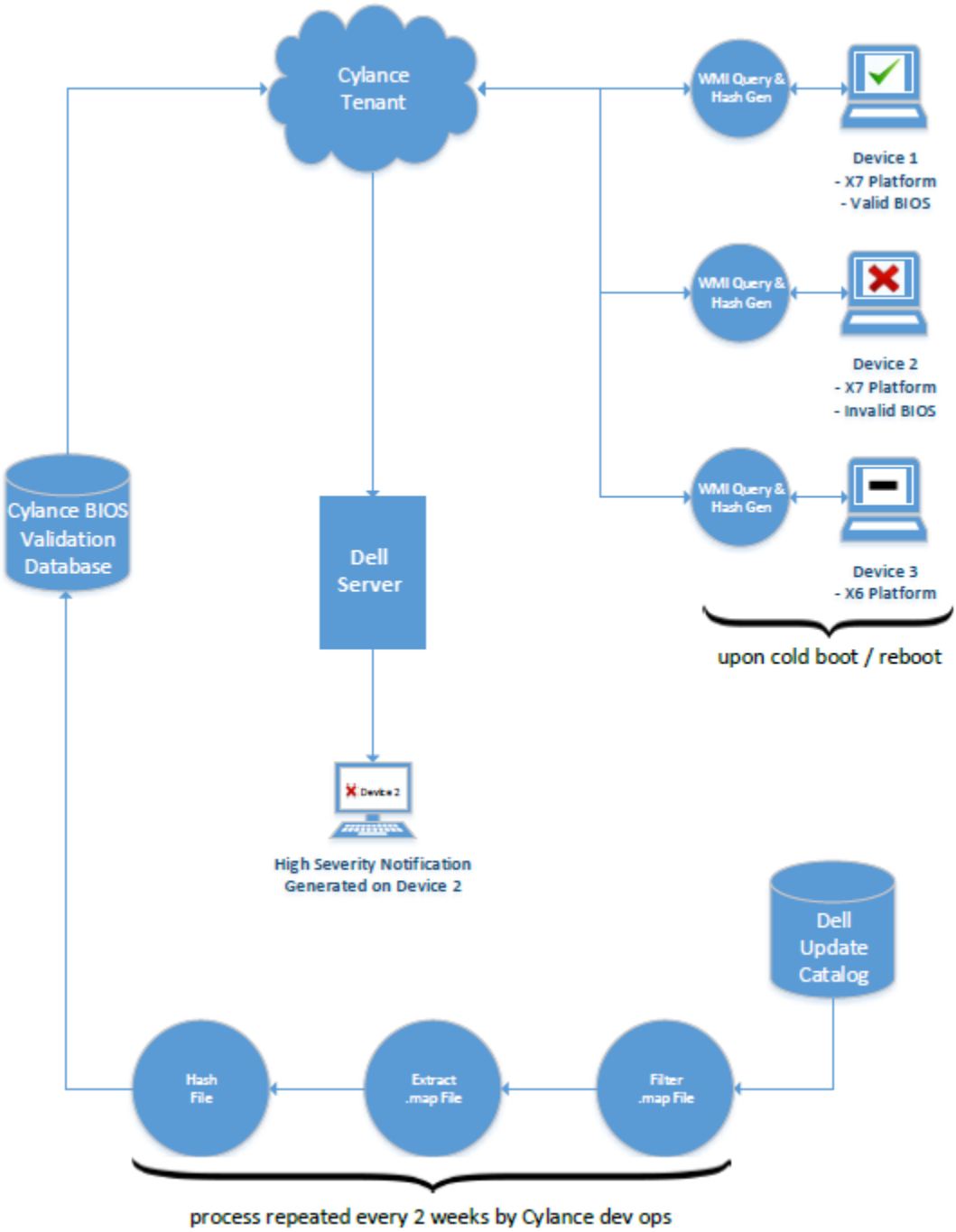


Le diagramme suivant illustre le processus de communication agent d'Advanced Threat Prevention.



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 ».



Pilotes Dell ControlVault

Mettre à jour les pilotes et le micrologiciel Dell ControlVault

Les pilotes et le micrologiciel Dell ControlVault installés en usine sur les ordinateurs Dell sont obsolètes et doivent être mis à jour à l'aide de la procédure suivante dans l'ordre indiqué.

Si, pendant l'installation du client, un message d'erreur vous invite à quitter le programme d'installation afin de mettre à jour les pilotes Dell ControlVault, vous pouvez ignorer ce message en toute sécurité et poursuivre l'installation du client. Les pilotes (et le micrologiciel) Dell ControlVault peuvent être mis à jour une fois l'installation du client terminée.

Télécharger les derniers pilotes

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

Installation du pilote Dell ControlVault

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

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

:

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

Cliquez sur **Continuer** pour commencer.

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

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

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

Le dossier contenant les fichiers s'affiche après l'extraction. Sinon, naviguez vers le dossier dans lequel vous avez extrait les fichiers. Dans ce cas, le dossier est **JW22F**.

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

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

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

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

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

Facultativement, cochez la case permettant d'afficher le fichier journal du programme d'installation. Cliquez sur **Terminer** pour fermer l'Assistant.

Vérifiez l'installation du pilote.

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

Installer le micrologiciel Dell ControlVault

1 Accédez au dossier dans lequel vous avez téléchargé le fichier d'installation du micrologiciel.
2 Double-cliquez sur le micrologiciel Dell ControlVault pour lancer le fichier exécutable à extraction automatique.
3 Cliquez sur **Continuer** pour commencer.
4 Cliquez sur **Ok** pour décompresser les fichiers de pilote dans l'emplacement par défaut de C:\Dell\Drivers\<Nouveaudossier>.
5 Cliquez sur **Oui** pour permettre la création d'un nouveau dossier.
6 Cliquez sur **OK** lorsque le message décompression réussie s'affiche.
7 Le dossier contenant les fichiers s'affiche après l'extraction. Sinon, naviguez vers le dossier dans lequel vous avez extrait les fichiers. Sélectionnez le dossier **micrologiciel**.
8 Double-cliquez sur **ushupgrade.exe** pour lancer le programme d'installation du micrologiciel.

9 Cliquez sur **Démarrer** pour commencer la mise à niveau du micrologiciel.

:

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

Plusieurs messages d'état s'affichent.

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

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

13

Glossaire

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.

Gestionnaire BitLocker : 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. Gestionnaire BitLocker prend en charge le cryptage BitLocker des systèmes d'exploitation, des lecteurs fixes et de BitLocker To Go. Gestionnaire BitLocker vous permet d'intégrer facilement BitLocker à vos besoins existants en terme de cryptage et de gérer BitLocker à moindre effort lors de la rationalisation de la conformité et de la sécurité. BitLocker Manager fournit la gestion intégrée de la récupération de clé, la gestion des règles et leur application, la gestion automatisée du TPM, la conformité à FIPS et des rapports de conformité.

Désactiver : la désactivation se produit lorsque vous désactivez la gestion SED dans la console de gestion. 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 du client Dell Encryption applique les règles aux supports amovibles et aux périphériques de stockage externes.

Code d'accès d'Encryption External Media : ce service de Serveur Dell 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.

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

Point de terminaison : un ordinateur géré par Serveur Dell.

Balayage de cryptage : un balayage de cryptage est un processus d'analyse des dossiers à crypter sur un point de terminaison géré afin de s'assurer que les fichiers contenus se trouvent en état de cryptage adéquat. Les opérations de création de fichier et de renommage ne déclenchent pas de balayage de cryptage. Il est important de savoir à quel moment un balayage de cryptage peut avoir lieu et ce qui risque d'affecter les temps de balayage résultants et ce de la manière suivante : un balayage de cryptage se 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 crypter seront analysés à chaque connexion de l'utilisateur. - Un balayage peut être déclenché à nouveau en raison de certaines modifications ultérieures apportées à des règles. Toute modification de règle en relation avec la définition des dossiers de cryptage, les algorithmes de cryptage, l'utilisation de clés de cryptage (communes par rapport à celles de l'utilisateur), déclenchent un balayage. De plus, le basculement entre l'activation et la désactivation du cryptage déclenche un balayage de cryptage.

Gestion SED : la gestion SED fournit une plateforme permettant de gérer les disques à auto-cryptage de manière sécurisée. Les disques à auto-cryptage assurent leur propre cryptage, mais ils ont besoin d'une plate-forme pour gérer le cryptage et les règles disponibles. SED

Management est un élément de gestion centrale évolutif, qui vous permet de protéger et de gérer vos données plus efficacement. SED Management vous permet d'administrer votre entreprise plus rapidement et plus facilement.

Utilisateur du serveur : compte d'utilisateur virtuel créé par Serveur Dell Encryption dans le but de gérer les clés de cryptage et les mises à jour de règles. 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.