Dell Data Protection | Encryption

Enterprise Edition Basic Installation Guide v8.13 (Guide d'installation de base d'Enterprise Edition v8.10)

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.

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

Enterprise Edition Basic Installation Guide (Guide d'installation de base d'Enterprise Edition)

2017 - 04

Rév. A01

Table des matières

1

Introduction

Ce guide explique en détails comment installer et configurer l'application à l'aide du programme d'installation principal . Ce guide permet d'obtenir une aide basique à l'installation. Reportez-vous au *Guide d'installation avancée* si vous avez besoin d'informations sur l'installation des programmes d'installation enfants, la configuration d'EE Server/VE Server ou des informations allant au-delà de l'assistance de base à propos du programme d'installation principal .

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

Avant de commencer

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

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

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

2 Lisez attentivement le chapitre Configuration requise de ce document.

3 Déployez les clients sur les utilisateurs finaux.

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 de manière interactive à l'aide du programme d'installation principal

    ou
  - Installation par 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 Data Protection.

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

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

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

2

Configuration requise

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 jour/la désinstallation doit correspondre à un administrateur local ou de domaine, qui peut être affecté temporairement par un outil de déploiement tel que Microsoft SMS ou Dell KACE. Les utilisateurs non-administrateurs et disposant de privilèges particuliers ne sont pas pris en charge.
- Sauvegardez toutes les données importantes avant de démarrer l'installation 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).
- Assurez-vous que le port de sortie 443 est disponible pour communiquer avec l'EE Server/VE Server si les clients du programme d'installation principal possèdent le droit d'utiliser Dell Digital Delivery (DDD). La fonctionnalité de droit ne fonctionnera pas si le port 443 est bloqué (pour quelque raison que ce soit). DDD n'est pas utilisé si l'installation est effectuée à l'aide des programmes d'installation enfants.
- Consultez régulièrement la rubrique www.dell.com/support pour obtenir la dernière documentation et conseils techniques.

Configuration requise pour tous les clients

- 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.

  La version complète de Microsoft .Net Framework 4.5.2. (ou version ultérieure) est pré-installée sur tous les ordinateurs expédiés par l'usine Dell. Cependant, si vous n'effectuez pas l'installation sur du matériel Dell ou que vous procédez à une mise à niveau sur du matériel Dell plus ancien, vous devez vérifier la version de Microsoft .Net installée et la mettre à jour **avant d'installer le client** pour éviter tout échec d'installation/de mise à niveau. 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.
- Les pilotes et le micrologiciel de ControlVault, les lecteurs d'empreintes et les cartes à puce (répertoriés ci-dessous) ne sont pas inclus dans le programme d'installation principal ni dans les fichiers exécutables des programmes d'installation enfants. Les pilotes et le micrologiciel doivent être conservés à jour et peuvent être téléchargés à partir de http://www.dell.com/support en sélectionnant votre modèle d'ordinateur. Téléchargez les pilotes et le logiciel appropriés en fonction de votre matériel d'authentification.

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

  Si vous installez du matériel autre que Dell, téléchargez les pilotes et le logiciel mis à jour depuis le site internet du fournisseur. Des instructions d'installation pour les pilotes ControlVault sont fournies dans Mise à jour des pilotes et du micrologiciel Dell ControlVault.

Matériel pour tous les clients

- Le tableau suivant répertorie les matériels informatiques compatibles.

Matériel

- La configuration minimale requise doit répondre aux spécifications minimales du système d'exploitation.

Tous les clients - Langues prises en charge

- Les clients BitLocker Manager, Encryption et sont compatibles avec l'interface utilisateur multilingue (MUI) et prennent en charge les langues suivantes.

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)

- Les clients SED et Advanced Authentication sont compatibles avec l'interface utilisateur multilingue (MUI – Multilingual User Interface) et prennent en charge les langues suivantes. Le mode UEFI et l'authentification avant démarrage ne sont pas pris en charge en russe, chinois traditionnel et 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

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 a été testé et est compatible avec McAfee, le client Symantec, Kaspersky et MalwareBytes. Les exclusions codées en dur sont en place afin que ces fournisseurs d'antivirus puissent prévenir les incompatibilités entre le balayage et le cryptage des antivirus. Le client Encryption a aussi été testé avec Microsoft Enhanced Mitigation Experience Toolkit.

  Si votre entreprise utilise un fournisseur d'antivirus qui n'est pas répertorié, consultez http://www.dell.com/support/Article/us/en/19/SLN298707 ou contactez Dell ProSupport
- La mise à niveau du système d'exploitation sur place n'est pas prise en charge avec le client Encryption installé. Effectuez une désinstallation et un décryptage du client Encryption et une mise à niveau au nouveau système d'exploitation, puis réinstallez le client Encryption.

Par ailleurs, la réinstallation du système d'exploitation n'est pas prise en charge. Pour réinstaller le système d'exploitation, effectuez une sauvegarde de l'ordinateur cible, effacez le contenu de l'ordinateur, installez le système d'exploitation, puis récupérez les données cryptées selon les procédures de récupération établies ci-après.

Configuration requise du client Encryption

- Le programme d'installation principal installe Microsoft Visual C++ 2012 Mise à jour 4 s'il n'est pas déjà installé sur l'ordinateur.

Conditions requises

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

Systèmes d'exploitation du client Encryption

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

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

- Windows 7 SP0-SP1 : Enterprise, Professional, Ultimate
- Windows Embedded Standard 7 doté du modèle Application Compatibility (Compatibilité de l'application) (le matériel de cryptage n'est pas pris en charge)
- Windows 8 : Enterprise, Pro
- Windows 8.1 Mise à jour 0-1 : Enterprise Edition, Pro Edition
- Windows Embedded 8.1 Industry Enterprise (le matériel de cryptage n'est pas pris en charge)
- Windows 10 : Education, Enterprise, Pro
- VMWare Workstation 5.5 et version supérieure

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

Systèmes d'exploitation prenant en charge External Media Shield (EMS)

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

> **REMARQUE :**
> Pour héberger EMS, 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.

> **REMARQUE :**
> Windows XP est pris en charge lors de l'utilisation de EMS Explorer uniquement.

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

- Windows 7 SP0-SP1 : Enterprise, Professional, Ultimate, Home Premium
- Windows 8 : Enterprise, Pro, Grand public
- Windows 8.1 Mise à jour 0-1 : Enterprise Edition, Pro Edition
- Windows 10 : Education, Enterprise, Pro

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

- Mac OS X Yosemite 10.10.5
- Mac OS X El Capitan 10.11.6
- Mac OS Sierra 10.12.0

Client SED

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

  - Supprimez tous les utilisateurs de la PBA.

  ou

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

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

Conditions préalables du client SED

- Le programme d'installation principal installe Microsoft Visual C++ 2010 SP1 **et** Microsoft Visual C++ 2012 Mise à jour 4 s'ils ne sont pas déjà installés sur l'ordinateur.

Pré-requis

- Visual C++ 2010 SP1 ou version ultérieure - Package redistribuable (x86 et x64)
- Visual C++ 2012 Redistributable Package (x86 and x64) Mise à jour 4 ou ultérieure

Matériel du client SED

Claviers internationaux

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

Clavier international pris en charge - UEFI

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

Clavier International prise en charge : Non-UEFI

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

Systèmes d'exploitation du client SED

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

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

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

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

- Windows 8 : Enterprise, Pro
- Windows 8.1 : Enterprise Edition, Pro Edition
- Windows 10 : Education, Enterprise, Pro

Client Advanced Authentication

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

  Pour continuer à utiliser le système d'exploitation Microsoft pour gérer vos identifiants, désinstallez Security Tools ou ne l'installez pas.
- La fonctionnalité de mot de passe à usage unique (OTP) des outils de sécurité nécessite qu'un TPM soit présent, activé et détenu. OTP est pas pris en charge avec TPM 2.0 . Pour effacer et configurer la propriété du TPM, voir https://technet.microsoft.com.

Matériel de client d'authentification avancée

- Le tableau suivant répertorie le matériel d'authentification informatique compatible.

Lecteurs de cartes à puces et d'empreintes digitales

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

Cartes sans contact

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

Cartes à puce

- Cartes à puce PKCS #11 utilisant le client ActivIdentity

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

- Cartes CSP
- Cartes CAC (Common Access Cards)
- Cartes réseau de catégorie B/SIPR

Systèmes d'exploitation du client Advanced Authentication (Authentification avancée)

Systèmes d'exploitation Windows

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

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

- Windows 7 SP0-SP1 : Enterprise, Professional, Ultimate
- Windows 8 : Enterprise, Pro
- Windows 8.1 Mise à jour 0-1 : Enterprise Edition, Pro Edition
- Windows 10 : Education, Enterprise, Pro

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

Systèmes d'exploitation de périphériques mobiles

- Les systèmes d'exploitation mobiles suivants sont pris en charge avec la fonction de mot de passe à usage unique (OTP) de Security Tools.

Systèmes d'exploitation Android

- 4.0 - 4.0.4 Ice Cream Sandwich
- 4.1 - 4.3.1 Jelly Bean
- 4.4 - 4.4.4 KitKat
- 5.0 - 5.1.1 Lollipop

Systèmes d'exploitation iOS

- iOS 7.x
- iOS 8.x

Systèmes d'exploitation Windows Phone

- Windows Phone 8.1
- Windows 10 Mobile

Client BitLocker Manager

- Envisagez de revoir la Configuration requise de Microsoft BitLocker si BitLocker n'est pas encore déployé dans votre environnement,
- Assurez-vous que la partition d'authentification avant démarrage est déjà configurée. Si vous installez BitLocker Manager avant de configurer la partition PBA, vous ne pourrez pas activer BitLocker et BitLocker Manager ne sera pas opérationnel.
- Le clavier, la souris et les composants vidéo doivent être directement connectés à l'ordinateur. N'utilisez pas de commutateur KVM pour gérer les périphériques, car il risquerait de réduire la capacité de l'ordinateur à identifier le matériel.
- Lancez le TPM et activez-le. Le gestionnaire BitLocker s'appropriera le TPM sans nécessiter de redémarrage. Toutefois, si le TPM est déjà propriétaire, le 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.
- BitLocker Manager n'est pas pris en charge avec Server Encryption.

Configuration requise pour le client BitLocker Manager

- Le programme d'installation principal installe Microsoft Visual C++ 2010 SP1 **et** Microsoft Visual C++ 2012 Mise à jour 4 s'ils ne sont pas déjà installés sur l'ordinateur.

Pré-requis

- Visual C++ 2010 SP1 ou version ultérieure - Package redistribuable (x86 et x64)
- Visual C++ 2012 Redistributable Package (x86 and x64) Mise à jour 4 ou ultérieure

Systèmes d'exploitation du client BitLocker Manager

- 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 : Education, Enterprise, Pro
- Windows Server 2008 R2 : Standard Edition, Enterprise Edition (64 bits)
- Windows Server 2012
- Windows Server 2012 R2 : Standard Edition, Enterprise Edition (64 bits)
- Windows Server 2016

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 sont disponibles à l'adresse **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'External Media Shield (Bouclier de support externe), voir l'*Aide EMS*. Accédez à l'aide depuis **<Install dir>:\Program Files\Dell\Dell Data Protection\Encryption\EMS**.
  - Reportez-vous à l'*Aide de Security Tools, l'Aide de E*pour savoir comment utiliser les fonctions d'Advanced Authentication. Accédez à l'aide à partir de **<Install dir>:\Program Files\Dell\Dell Data Protection\Security Tools \Help**.
- Après l'installation, l'utilisateur devra mettre à jour ses règles en faisant un clic droit sur l'icône Dell Data Protection située dans la barre d'état système 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 de manière interactive à l'aide du programme d'installation principal

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

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

- Vous pouvez localiser le programme d'installation principal de la manière suivante :
  - **À partir de support.dell.com** - Si nécessaire, téléchargez le logiciel depuis support.dell.com puis Extrayez les programmes d'installation enfants depuis le programme d'installation principal .
  - **À partir de votre compte FTP de Dell** - Localisez le bundle d'installation à DDP-Enterprise-Edition-8.x.x.xxx.zip.
- Utilisez ces instructions pour installer Dell Enterprise Edition de manière interactive à l'aide du programme d'installation principal . Cette méthode peut être utilisée pour installer la suite de produits sur un ordinateur à la fois.

1. Localisez **DDPSetup.exe** sur le support d'installation Dell. Copiez-le sur l'ordinateur local.
2. Double-cliquez sur le fichier 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. Sélectionnez **Enterprise Edition**, puis cliquez sur **Suivant**.

   Cochez la case External Media Edition uniquement si vous avez l'intention d'installer uniquement External Media Edition
6. Dans le champ **Nom du serveur Enterprise**, saisissez le nom d'hôte complet du EE Server/VE Server qui va gérer l'utilisateur cible (par exemple, serveur.organisation.com).

Dans le champ **URL de Device Server**, saisissez l'URL du Device Server (Security Server) avec lequel le client communiquera.

Si votre EE Server est antérieur à v7.7, le format est https://server.organization.com:**8081**/xapi.

Si vous utilisez un serveur EE de version 7.7 ou ultérieureleformat est le suivant : https://serveur.organisation.com:**8443**/xapi**/** (barre oblique de fin incluse).

Cliquez sur **Suivant** .

7 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.

8 Sélectionnez les composants à installer.

Security Framework permet d'installer la structure de sécurité sous-jacente ainsi que Security Tools, le client d'Advanced Authentication qui gère plusieurs méthodes d'authentification, notamment PBA et les informations d'identification telles que les empreintes digitales et les mots de passe.

Advanced Authentication installe les fichiers et les services nécessaires pour l'authentification avancée. .

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.

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

Cliquez sur **Suivant** lorsque vos sélections sont terminées.

9 Cliquez sur **Installer** pour démarrer l'installation. L'installation peut prendre quelques minutes.

10 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 ligne de commande. D'autres paramètres figurent dans un argument transmis au commutateur /v.

Commutateurs

- Le tableau suivant décrit les commutateurs que vous pouvez utiliser avec le programme d'installation principal .

Commutateur	Description
-y -gm2	Extraction préalable du programme d'installation principal . Vous devez utiliser les commutateurs -y et -gm2 ensemble. Ne les séparez pas.
/S	Installation silencieuse
/z	Transmission des variables au fichier .msi dans DDPSetup.exe

Paramètres

- Le tableau suivant décrit les paramètres que vous pouvez utiliser avec le programme d'installation principal .

Paramètre	Description
SUPPRESSREBOOT	Supprime le redémarrage automatique une fois l'installation terminée. Peut être utilisé en mode SILENCIEUX.
SERVEUR	Spécifie l'URL de l'EE Server/VE Server.
InstallPath	Spécifie le chemin de l'installation. Peut être utilisé en mode SILENCIEUX.
FONCTIONS	Spécifie les composants qui peuvent être installés en mode SILENCIEUX : DE = Drive Encryption (Cryptage lecteur) EME = External Media Edition uniquement BLM = BitLocker Manager SED = gestion des disques durs à auto-cryptage (EMAgent/Manager, pilotes PBA/GPE)
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.
- Cet exemple installe tous les composants en utilisant le programme d'installation principal sur les ports standard, de façon silencieuse, à l'emplacement par défaut **C:\Program Files\Dell\Dell Data Protection** et le configure pour utiliser le EE Server/VE Server spécifié.

```
"DDPSetup.exe" -y -gm2 /S /z"\"SERVER=server.organization.com\""
```

- Cet exemple installe la gestion SED et External Media Edition avec le programme d'installation principal, sur les ports par défaut, de manière silencieuse, en supprimant le redémarrage, à l'emplacement par défaut **C:\Program Files\Dell\Dell Data Protection** et le configure pour utiliser le EE Server/VE Server spécifié.

```
"DDPSetup.exe" -y -gm2 /S /z"\"SERVER=server.organization.com, FEATURES=EME-SED,
SUPPRESSREBOOT=1\""
```

- Cet exemple installe la gestion SED avec le programme d'installation principal, sur les ports par défaut, de manière silencieuse, en supprimant le redémarrage, à l'emplacement par défaut **C:\Program Files\Dell\Dell Data Protection** et le configure pour utiliser le EE Server/VE Server spécifié.

```
"DDPSetup.exe" -y -gm2 /S /z"\"SERVER=server.organization.com, FEATURES=SED,
SUPPRESSREBOOT=1\""
```

- Cet exemple installe la gestion SED avec le programme d'installation principal, sur les ports par défaut, de manière silencieuse, à l'emplacement par défaut **C:\Program Files\Dell\Dell Data Protection** et le configure pour utiliser le EE Server/VE Server spécifié.

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

- Cet exemple installe Encryption client et BitLocker Manager (sans le plug-in SED Management), avec le programme d'installation principal ESSE, sur des ports standard, de manière silencieuse, à l'emplacement par défaut **C:\Program Files\Dell\Dell Data Protection** et le configure pour utiliser le EE Server/VE Server spécifié.

```
"DDPSetup.exe" -y -gm2 /S /z"\"SERVER=server.organization.com, FEATURES=DE-BLM, BLM_ONLY=1\""
```

- Cet exemple installe BitLocker Manager (sans le plug-in de gestion SED) avec le programme d'installation principal, sur les ports par défaut, de manière silencieuse, en supprimant le redémarrage, à l'emplacement par défaut **C:\Program Files\Dell\Dell Data Protection** et le configure pour utiliser le EE Server/VE Server spécifié.

```
"DDPSetup.exe" -y -gm2 /S /z"\"SERVER=server.organization.com, FEATURES=BLM-EME,
SUPPRESSREBOOT=1\""
```

- Cet exemple installe BitLocker Manager (avec le plug-in de gestion SED) avec le programme d'installation principal, sur les ports par défaut, de manière silencieuse, en supprimant le redémarrage, à l'emplacement par défaut **C:\Program Files\Dell\Dell Data Protection** et le configure pour utiliser le EE Server/VE Server spécifié.

```
"DDPSetup.exe" -y -gm2 /S /z"\"SERVER=server.organization.com, FEATURES=BLM-EME, BLM_ONLY=1,
SUPPRESSREBOOT=1\""
```

4

Désinstallation à l'aide du programme d'installation principal

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

  a Désinstallez le client Encryption.

  b Désinstallez les clients SED et Advanced Authentication.

  c Désinstallez le client BitLocker Manager.
- Passez à Désinstallez le programme d'installation principal .

Désinstaller le programme d'installation principal

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 désinstalle silencieusement le programme d'installation principal .

  ```
  "DDPSetup.exe" -y -gm2 /S /x
  ```

  Lorsque vous avez terminé, redémarrez l'ordinateur.

Désinstaller à l'aide des programme d'installation enfants

- Pour désinstaller chaque client individuellement, les fichiers exécutables enfants doivent d'abord être extraits du programme d'installation principal , tel qu'illustré dans Extraction des programmes d'installation enfants à partir 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:\<tout répertoire>\<tout nom de fichier journal>.log**. Dell recommande de ne pas utiliser la consignation détaillée « /l*v » dans une désinstallation avec ligne de commande, car le nom d'utilisateur/mot de passe est enregistré dans le fichier journal.
- Tous les programmes d'installation enfants utilisent les mêmes options d'affichage et commutateurs .msi de base, sauf lorsque cela est précisé, pour les désinstallations avec ligne de commande. Les commutateurs doivent être indiqués en premier. Le commutateur /v est requis et nécessite un argument. D'autres paramètres figurent dans un argument transmis au commutateur /v.

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

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

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

Option	Signification
/q	Boîte de dialogue Aucune progression, se réinitialise après la fin du processus
/qb	Boîte de dialogue de progression dotée du bouton **Annuler** : vous invite à effectuer un redémarrage

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

Désinstallation 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).
- Windows et les Boucliers EME actualisent le EE Server/VE Server pour modifier le statut en *Déprotégé* au début d'un processus de désinstallation du Bouclier. Toutefois, lorsque le client ne peut pas contacter le DDP EE Server/VE Server, quelle qu'en soit la raison, le statut ne peut pas être mis à jour. Dans ce cas, vous devez *supprimer le point final* manuellement dans la Console de gestion à distance. 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 à distance ou dans le Compliance Reporter.

Processus

- Le Key Server (et EE Server) doivent être configurés 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 par rapport à EE Server pour obtenir les instructions. Aucune action préalable n'est nécessaire si le client à désinstaller est activé par rapport à un VE Server, car le VE Server 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 , le programme d'installation du client Encryption est disponible sur **C:\extracted\Encryption\DDPE_XXbit_setup.exe**.
- Le tableau suivant indique les paramètres disponibles dans le cadre de la désinstallation.

Paramètre	Sélection
CMG_DECRYPT	propriété permettant de sélectionner le type d'installation d'Encryption Removal Agent :

Paramètre	Sélection
	3 - Utiliser le bundle LSARecovery 2 - Utiliser les clés d'analyse approfondie précédemment téléchargées 1 : télécharger les clés depuis le 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	Nom complet de l'hôte de l'EE Server hébergeant la session de négociation
DA_PORT	Port sur l'EE 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 l'EE Server
DA_RUNAS	Nom d'utilisateur dans un format compatible SAM, dans le contexte duquel la requête d'obtention de clé sera exécutée. Cet utilisateur doit être répertorié dans la liste des comptes Key Server, dans l'EE Server.
DA_RUNASPWD	Mot de passe de l'utilisateur d'exécution
FORENSIC_ADMIN	Compte administrateur d'analyse approfondie sur le serveur Dell, qui peut être utilisé pour des requêtes d'analyse approfondie, les désinstallations ou les clés.
FORENSIC_ADMIN_PWD	Mot de passe du compte de l'administrateur d'analyse approfondie.
Propriétés facultatives	
SVCLOGONUN	Nom d'utilisateur au format UPN pour le paramètre Connexion en tant que du 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 l'EE 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 à distance VE, 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"
```

Désinstaller External Media Edition

Après son extraction du programme d'installation principal, le programme d'installation du client Encryption est disponible sur C:\extracted \Encryption\DDPE_XXbit_setup.exe.

Désinstallation de ligne de commande

Exécutez une ligne de commande basée sur l'exemple suivant :

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

Lorsque vous avez terminé, redémarrez l'ordinateur.

Désinstaller les clients SED et Advanced Authentication

- La désactivation de l'authentification avant démarrage requiert une connexion réseau à EE Server/VE Server.

Processus

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

- Désinstallation du client Advanced Authentication.

Désactiver l'authentification avant démarrage

1 Connectez-vous à la Console de gestion à distance en tant qu'administrateur Dell.
2 Dans le volet de gauche, cliquez sur **Protection et gestion** > **Points finaux**.
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 l'icône **Détails** de l'ordinateur souhaité.
7 Cliquez sur **Règles de sécurité** sur le menu supérieur.
8 Sélectionnez **Disques à cryptage automatique** à partir du menu déroulant **Catégorie de règle**.
9 Développez la zone **Administration SED** et modifiez les règles **Activer la gestion SED** et **Activer l'authentification avant démarrage** de `True` (*Vrai*) à **`False`(*Faux*)**.
10 Cliquez sur **Enregistrer**.
11 Dans le menu de gauche, cliquez sur **Actions** > **Valider les règles**.
12 Cliquez sur **Appliquer les modifications**.

   Attendez que la règle se propage du EE Server/VE Server à l'ordinateur ciblé pour la désactivation.

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

Désinstallez le client SED et les clients Advanced Authentication

Désinstallation avec ligne de commande

- Après son extraction du programme d'installation principal , le programme d'installation du client SED est disponible sous C:\extracted \Security Tools\EMAgent_XXbit_setup.exe.
- Après son extraction du programme d'installation principal , le programme d'installation du client SED se trouve sous C:\extracted \Security Tools\Authentication\<x64/x86>\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.

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

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

  Après avoir terminé, éteignez et redémarrez l'ordinateur.

Désinstaller le client BitLocker Manager

Désinstallation avec ligne de commande

- Après son extraction du programme d'installation principal , le programme d'installation du client BitLocker est disponible sous **C:\extracted\Security Tools\EMAgent_XXbit_setup.exe**.
- L'exemple suivant correspond à la désinstallation silencieuse du BitLocker Manager.

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

  Lorsque vous avez terminé, redémarrez l'ordinateur.

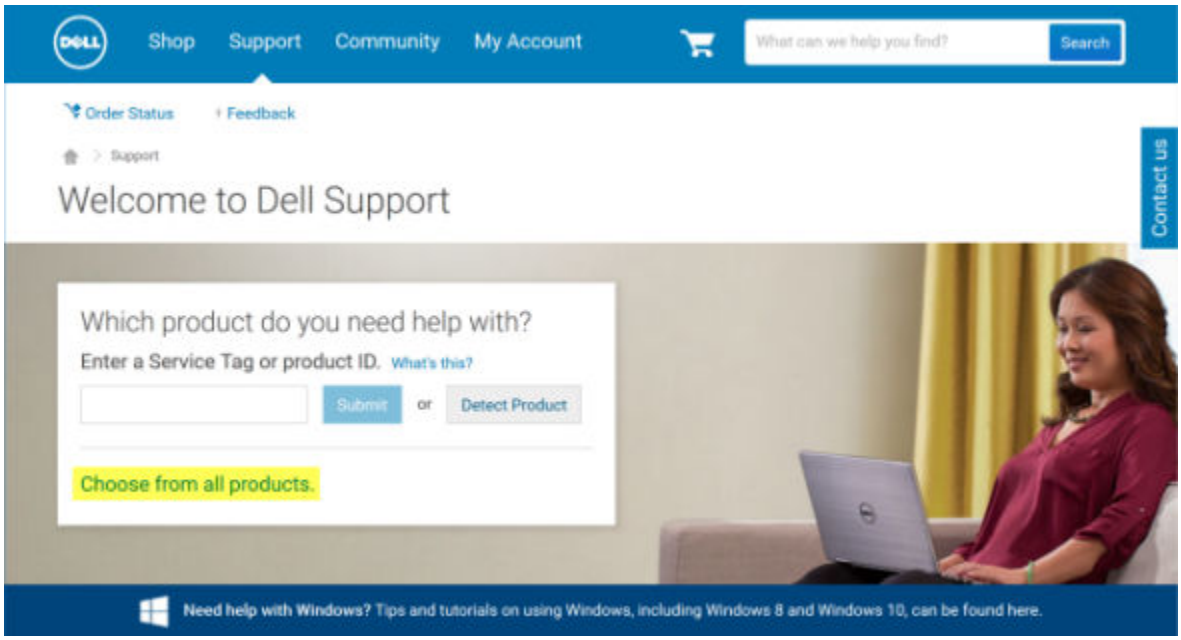
6

Télécharger le logiciel

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

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

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



2 Sélectionnez **Logiciel et sécurité** dans la liste des produits.

3 Sélectionnez **Solutions de sécurité des points finaux** dans la section *Logiciel et sécurité*.
Le site Web se rappellera la sélection initiale.

4 Sélectionnez le produit de protection des données Dell.
Exemples :

Dell Encryption

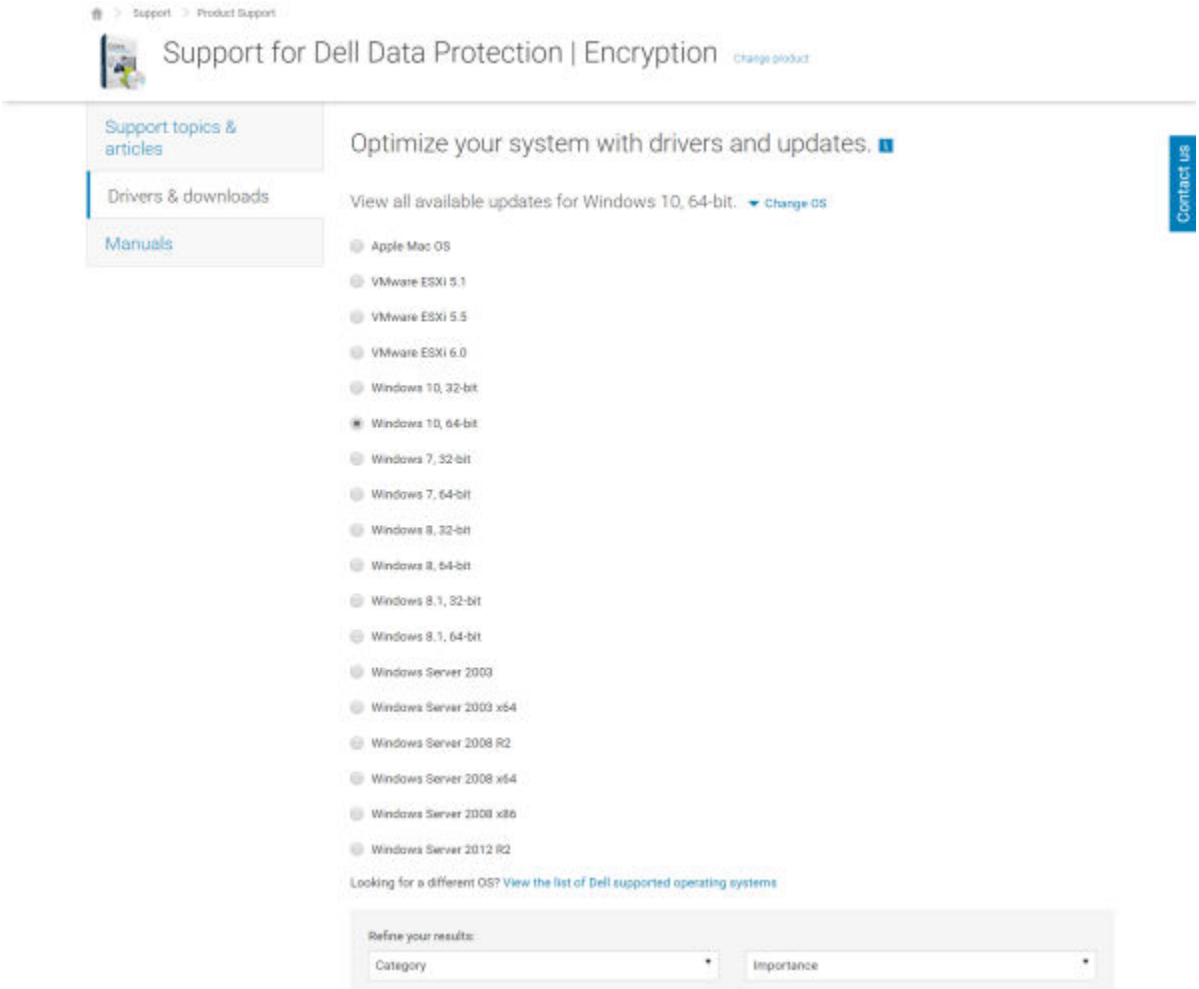
Dell Endpoint Security Suite

Dell Endpoint Security Suite Enterprise

5 Sélectionnez **Pilotes et téléchargements**.

6 Sélectionnez le type de système d'exploitation client souhaité.

7 Sélectionnez **Dell Data Protection (4 fichiers)** parmi les options correspondantes. Ceci n'étant qu'un exemple, elles pourront être légèrement différentes. Par exemple, il pourra ne pas exister 4 fichiers parmi lesquels choisir.



8 Sélectionnez **Télécharger le fichier** ou **Ajouter à ma liste de téléchargements #XX**.

Extraction des programmes d'installation enfants du programme d'installation principal

- Le programme d'installation principal n'est pas un *programme de désinstallation* principal. Chaque client doit être désinstallé individuellement, 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 **DDPSetup.exe** sur l'ordinateur local.

2 Ouvrez une invite de commande dans le même emplacement que le fichier **DDPSetup.exe** et saisissez :

```
DDPSetup.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\.**

Configurer le Key Server pour procéder à la désinstallation du client Encryption activé par rapport à EE Server

- Cette rubrique explique comment configurer les composants requis pour utiliser l'authentification/autorisation Kerberos avec un EE Server. Le VE Server n'utilise pas le 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 VE Server n'utilise pas le Key Server. Lors de la désinstallation d'un client Encryption activé par rapport à un VE Server, la récupération de la clé d'analyse approfondie standard s'effectue par le biais du Security Server plutôt que par la méthode Kerberos du Key Server. Voir Désinstallation avec ligne de commande pour plus d'informations.

Écran des services - Ajouter un utilisateur du compte de domaine

1 Dans le EE Server, naviguez vers le volet Services (Démarrer > Exécuter...> services.msc > OK).

2 Effectuez un clic droit sur Key Server, puis sélectionnez **Propriétés**.

3 Sélectionnez l'onglet Connexion, puis cochez 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 volet Services pour pouvoir y revenir ultérieurement).

5 Naviguez jusqu'au fichier log.txt qui se trouve dans le <rép. d'installation de Key Server> pour vérifier que le service a correctement démarré.

Fichier de configuration du Serveur de clés - Ajouter un utilisateur pour la communication avec l'EE Server

1 Naviguez jusqu'au <rép. d'installation de Key Server>.

2 Ouvrez le fichier ***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 de l'EE 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 - Redémarrer le service Key Server

1 Retournez au panneau des Services (Démarrer > Exécuter... > services.msc > OK).

2 Redémarrez le service Key Server.

3 Naviguez jusqu'au fichier log.txt qui se trouve dans le <rép. d'installation de Key Server> pour vérifier que le service a correctement démarré.

4 Fermez le volet Services.

Console de gestion à distance - Ajouter un administrateur d'analyse approfondie

1 Si nécessaire, connectez-vous à la Console de gestion à distance.

2 Cliquez sur **Populations** > **Domaines**.

3 Sélectionnez le Domaine pertinent.

4 Cliquez sur l'onglet **Key Server**.

5 Dans le champ Comptes, ajoutez l'utilisateur qui exécutera les opérations d'administration. 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** et cliquez sur **Mise à jour**.

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

Utiliser l'utilitaire Administrative Download (CMGAd)

- Cet utilitaire permet de télécharger un ensemble de matériel clé à l'utilisation d'un ordinateur non connecté à un EE Server/VE Server.
- 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 sont disponibles sous 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** (`oucmgad.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/. Si la version de votre EE Server est antérieure à v7.7, le format est https://deviceserver.domain.com:8081/xapi (numéro de port différent, sans barre oblique).

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 VE Server, car le VE Server n'utilise pas le Key Server. Utiliser le mode Analyse approfondie pour obtenir l'ensemble de clés si le client est activé par rapport à un VE Server.

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.

Dépannage

Tous les clients - Dépannage

- Les fichiers journaux du programme d'installation principal sont disponibles sous **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\<UserName>\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\<UserName>\AppData\Local\Temp. For example, C:\Users\<UserName>\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, consultez https://www.microsoft.com/en-us/download/details.aspx?id=30653.
- Reportez-vous à *Dell Data Protection | Security Tools - Compatibilité* 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.

Dépannage du client Encryption et Server Encryption

Mise à niveau vers la mise à jour Windows 10 Anniversary

Pour effectuer la mise à niveau vers la version Windows 10 Anniversary Update, suivez les instructions consignées 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 les références de l'administrateur du domaine.

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

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

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

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

Les informations d'identification utilisées pour l'activation ne sont pas dotées des privilèges 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, saisir les informations d'identification d'un administrateur de domaine et assurez-vous qu'ils sont au format UPN.

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 DDP Security 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 du DDP Server pour vous assurer qu'elle correspond à l'URL fournie par l'administrateur. L'adresse URL ainsi que d'autres données saisies par l'utilisateur dans le programme d'installation sont stockées dans le répertoire. Assurez-vous que les données sous [HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield] et [HKLM\SOFTWARE\Microsoft \Windows NT\CurrentVersion\Winlogon\CMGShield\Servlet] sont correctes.
- Déconnectez le serveur du réseau. Redémarrez le serveur et reconnectez-le au réseau.

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

Solutions possibles

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

Processus d'activation initiale

Le schéma suivant illustre une activation initiale réussie.

Le processus d'activation 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 de Server Encryption dans la barre d'état système 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 références de l'administrateur du 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 références de l'administrateur de domaine, reportez-vous à Avant de commencer.

6 DDP Server vérifie les informations d'identification dans le coffre de l'entreprise (Active Directory ou équivalent) afin de s'assurer que les identifiants appartiennent bien à un administrateur du domaine.

7 Un UPN est construit à l'aide des références.

8 Avec l'UPN, le DDP Server crée un nouveau compte utilisateur pour l'utilisateur du serveur virtuel et stocke ces identifiants dans le coffre du DDP Server.

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

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 partie de l'activation, 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 DDP Server virtuel, en demandant la clé d'ordinateur auprès de DDP Enterprise Server. 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 de bouclier est rouge, le cryptage n'a pas encore été activé.
- Dans la Console de gestion à distance, la version d'un serveur équipé de Server Encryption est répertoriée comme *Bouclier de serveur*.
- Si la récupération de la clé d'ordinateur échoue en raison d'une défaillance réseau, Server Encryption s'enregistre auprès du système d'exploitation pour les notifications du réseau.
- Si la récupération de la clé d'ordinateur échoue :
  - La connexion de l'utilisateur du serveur virtuel fonctionne malgré tout.
  - Définissez la règle d'*Intervalle entre les tentatives en cas d'échec du réseau* pour procéder à de nouvelles tentatives de récupération de la clé à intervalles définis.

    Pour 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 à distance.

Processus d'authentification et d'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 du serveur DDP :

- Si l'ordinateur n'a pas encore été activé par un périphérique, le serveur DDP attribue à l'ordinateur un MCID, un DCID et un certificat de confiance, et stocke toutes ces informations dans le coffre du serveur DDP.

- Si l'ordinateur avait été précédemment activé par un périphérique, le serveur DDP vérifie le certificat de confiance.

3 Une fois que le serveur DDP 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.

Interactions EMS et 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 protégés interagit avec le système de contrôle des ports - Classe 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 de la classe de stockage : 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 :

- Définissez EMS Encrypt External Media (Crypter le support externe EMS) = Vrai
- Définissez EMS Exclude CD/DVD Encryption (EMS ne prend pas en charge le cryptage de CD/DVD) = Faux
- 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 dans le menu déroulant : *Tous les lecteurs, Lecteurs fixes*, *Lecteurs amovibles*, ou *CD-ROM/ DVDROM*.

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

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 la liste déroulante est ignorée.

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

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

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

6 Choisissez le format de sortie :

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

7 Cliquez sur **Rechercher**.

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

Fichier cible WSScan

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

Exemple :

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

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

Sortie	Signification
	RIJNDAEL 256
	AES 128
	AES 256
	3DES

Vérification de l'état d'Encryption Removal Agent.

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

- **Attente de la désactivation SDE** - Le client Encryption est toujours installé, toujours configuré ou les deux. Le déchiffrement ne démarrera pas tant que le client Encryption ne sera pas désinstallé.
- **Balayage initial** - Le service procède à un premier balayage en calclant le nombre de fichiers cryptés et les octets. L'analyse initiale n'a lieu qu'une seule fois.
- **Balayage de décryptage** - Le service décrypte les fichiers et demande peut-être à décrypter des fichiers verrouillés.
- **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 décryptage.
- **Terminé** : l'analyse de déchiffrage est terminée. Le service, le fichier exécutable, le pilote et l'exécutable du pilote seront supprimés au prochain redémarrage.

Pilotes Dell ControlVault

Mettre à jour les pilotes et le micrologiciel Dell ControlVault

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

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

Télécharger les derniers pilotes

1 Rendez-vous sur le site support.dell.com.
2 Sélectionnez le modèle de votre ordinateur.

3 Sélectionnez **Pilotes et téléchargements**.
4 Sélectionnez le **système d'exploitation** de l'ordinateur cible.
5 Développez la catégorie **Sécurité**.
6 Téléchargez, puis enregistrez les pilotes Dell ControlVault.
7 Téléchargez, puis enregistrez le micrologiciel Dell ControlVault.
8 Copiez les pilotes et le micrologiciel sur les ordinateurs cibles, le cas échéant.

Installation du pilote Dell ControlVault

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

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

:

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

Cliquez sur **Continuer** pour commencer.

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

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

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

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

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

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

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

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

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

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

Vérifiez l'installation du pilote.

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

Installer le micrologiciel Dell ControlVault

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

:

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

Plusieurs messages d'état s'affichent.

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

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

Glossaire

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

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

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

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

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

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

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

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

Clé d'ordinateur : lorsque le cryptage est installé sur un serveur, la clé d'ordinateur protège le fichier de cryptage et les clés de règle d'un serveur. L'ensemble de clés d'ordinateur est stocké sur Dell Enterprise Server/VE. Le nouveau Server échange les certificats avec le DDP Server lors de l'activation et utilise le certificat lors d'événements d'authentification ultérieurs.

Mot de passe à usage unique (OTP – One-Time Password) : un mot de passe à usage unique est un mot de passe qui ne peut être utilisé qu'une seule fois et n'est valide que pendant une période limitée. OTP exige que le TPM soit présent, activé et détenu. Pour activer OTP, un terminal mobile doit être associé à l'ordinateur utilisant la Security Console et l'application Security Tools Mobile. L'application Security Tools Mobile génère le mot de passe sur le terminal mobile utilisé pour se connecter à l'ordinateur dans l'écran de connexion Windows. En fonction de cette règle, la fonction OTP peut être utilisée pour récupérer l'accès à l'ordinateur si un mot de passe a expiré ou été oublié, si OTP n'a pas été utilisé pour se connecter à l'ordinateur. La fonction OTP peut être utilisée pour l'authentification ou pour la récupération, mais pas pour les deux. La sécurité OTP est supérieure à celle de quelques autres méthodes d'authentification car le mot de passe généré ne peut être utilisé qu'une seule fois et expire rapidement.

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

Utilisateur du serveur : un compte d'utilisateur virtuel créé par Dell Server 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 à distance de Dell Enterprise Server/VE.