Encryption

Configuration requise v10.1

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 document présente la configuration requise pour Dell Encryption.

Pour accéder à la documentation de Dell Encryption, voir la page www.dell.com/support/home/us/en/04/product-support/product/dell-data-protection-encryption/manuals.

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

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

- 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 Security Management Server/Security Management Server Virtual 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. Le pilotes et le micrologiciel doivent être conservés à jour et peuvent être téléchargés à partir de http://www.dell.com/support en sélectionnant votre modèle d'ordinateur. Téléchargez les pilotes et le logiciel appropriés en fonction de votre matériel d'authentification.

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

Matériel pour tous les clients

- Le tableau suivant répertorie les matériels informatiques compatibles.

Matériel
– Processeur Intel Pentium ou AMD

Matériel

- 110 Mo d'espace disque disponible
- 512 Mo 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 et Gestionnaire BitLocker sont compatibles avec l'interface utilisateur multilingue (MUI) et sont localisés dans 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)

Client Encryption

- L'ordinateur client doit posséder une connexion active au réseau pour être activé.
- Pour réduire la durée du cryptage initial, lancez l'Assistant Nettoyage de disque Windows qui supprimera les fichiers temporaires et toute autre donnée inutile.
- Désactivez le mode Veille lors du balayage de cryptage initial pour prévenir la mise en veille d'un ordinateur lors des périodes d'inactivité. Le cryptage ne peut pas être exécuté sur un ordinateur en veille (le décryptage non plus).
- Le client Encryption ne prend pas en charge les configurations à double démarrage dans la mesure où il est possible de crypter les fichiers système de l'autre système d'exploitation, ce qui perturberait son fonctionnement.
- Le programme d'installation principal ne prend pas en charge les mises à niveau des composants antérieurs à la version v8.0. Extrayez les programmes d'installation enfants du programme d'installation principal et mettez à niveau le composant individuellement.
- Le client Encryption prend désormais en charge le mode Audit. Le mode Audit permet aux administrateurs de déployer le client Encryption dans le cadre de l'image d'entreprise, plutôt que d'utiliser un SCCM tiers ou des solutions similaires pour déployer le client Encryption. Pour obtenir des instructions relatives à l'installation du client Encryption dans une image d'entreprise, voir http://www.dell.com/support/article/us/en/19/SLN304039.
- Le 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, reportez-vous à l'article de la base de connaissances http://www.dell.com/support/article/us/en/19/SLN288353 ou contactez Dell ProSupport.
- Le module TPM (Trusted Platform Module) permet de sceller la clé GPK. Par conséquent, si vous exécutez le client Encryption, supprimez le module TPM du BIOS avant d'installer un nouveau système d'exploitation sur l'ordinateur client.
- 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. **Lors de l'utilisation du programme d'installation enfant**, vous devez installer ce composant avant d'installer le client Encryption.

Conditions requises

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

Matériel du client Encryption

- Le tableau suivant répertorie en détail le matériel compatible.

Matériel intégré en option

- TPM 1.2 ou 2.0

Systèmes d'exploitation du client Encryption

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

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

- Windows 7 SP1 : Entreprise, Professionnel, Ultimate
- Windows Embedded Standard 7 doté du modèle Compatibilité de l'application (le matériel de cryptage n'est pas pris en charge)
- Windows 8 : 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 : Éducation, Entreprise, Pro Version 1607 (Mise à jour anniversaire/Redstone 1) jusqu'à la version 1803 (Mise à jour avril 2018/Redstone 4)
- VMware Workstation 12.5 et versions ultérieures

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

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 8 : Enterprise, Pro, Grand public
- Windows 8.1 Mise à jour 0-1 : Enterprise Edition, Pro Edition
- 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 10.12.4 et 10.12.5
- macOS High Sierra 10.13.5 - 10.13.6
- macOS Mojave 10.14

Client Server Encryption

Server Encryption est conçu pour une utilisation sur des ordinateurs fonctionnant en mode Serveur, en particulier les serveurs de fichiers.

- Server Encryption est compatible uniquement avec Encryption Enterprise et Endpoint Security Suite Enterprise.
- Server Encryption offre les fonctions suivantes :
  - Le cryptage logiciel est
  - Removable Media Encryption
  - Contrôle de port

  REMARQUE :
  Le serveur doit prendre en charge les contrôles de port.

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

Server Encryption est conçu pour utilisation sur :

- les serveurs de fichier sur disque locaux
- les invités de la machine virtuelle (VM) s'exécutant sous un système d'exploitation serveur ou autre que serveur en tant que simple serveur de fichiers
- Configurations prises en charge :
  - les serveurs équipés de disques RAID 5 ou 10 ; RAID 0 (par bande) et RAID 1 (mis en miroir) sont pris en charge indépendamment l'un de l'autre.
  - les serveurs équipés de lecteurs RAID de plusieurs To
  - les serveurs équipés de lecteurs pouvant être remplacé sans avoir a mettre l'ordinateur hors tension.
  - Le cryptage du serveur est validé par les principaux fournisseurs d'antivirus du marché. Les exclusions codées en dur sont en place afin que ces fournisseurs d'antivirus puissent empêcher les incompatibilités entre le balayage et le cryptage des antivirus. Si votre entreprise utilise un fournisseur d'antivirus qui n'est pas répertorié, reportez-vous à l'article de base de connaissances SLN298707 ou contactez Dell ProSupport

Non pris en charge

Server Encryption n'est pas conçu pour les systèmes suivants :

- Security Management Servers/Security Management Server Virtuals ou les serveurs exécutant des bases de données pour Security Management Servers/Security Management Server Virtual.

- Server Encryption n'est pas compatible avec Encryption Personal.
- Server Encryption n'est pas pris en charge avec SED Management ou le client Gestionnaire BitLocker.
- Server Encryption n'est pas pris en charge sur des serveurs qui font partie de DFS (distributed file systems).
- La migration vers ou depuis Server Encryption n'est pas prise en charge. Les mises à niveau depuis Encryption External Media vers Server Encryption requièrent la désinstallation complète du ou des produits précédents avant l'installation de Server Encryption.
- les hôtes de machine virtuelle (un hôte de machine virtuelle contient généralement plusieurs invités de machine virtuelle.)
- Contrôleurs de domaine.
- Serveurs Exchange
- Serveurs hébergeant des bases de données (SQL, Sybase, SharePoint, Oracle, MySQL, Exchange etc.)
- Serveurs utilisant l'une des technologies suivantes :
  - Systèmes de fichiers résistants
  - Systèmes de fichiers fluides
  - Espace de stockage Microsoft
  - Solutions de stockage réseau SAN/NAS
  - Périphériques connectés iSCSI
  - Logiciel de déduplication
  - Matériel de déduplication
  - RAID fractionnés (plusieurs volumes sur un RAID unique)
  - Lecteurs SED (RAID et autre que NON RAID)
  - Connexion automatique (Windows 7, 8/8.1) des bornes
  - Microsoft Storage Server 2012
- Le client Server Encryption ne prend pas en charge les configurations à double amorçage, car 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 suivantes. Pour plus d'informations sur la récupération des données cryptées, reportez-vous au *Recovery Guide* (Guide de récupération).

Matériel du client Server Encryption

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

Systèmes d'exploitation du client Server Encryption

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

Systèmes d'exploitation (32 et 64 bits)

- Windows 7 SP1 : Entreprise, Professionnel, Ultimate
- Windows 8.0 : Enterprise, Professionnel
- 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)

Systèmes d'exploitation de serveur pris en charge

- Windows Server 2008 R2 SP1 : Édition Standard, Édition Datacenter, Édition Enterprise, Édition Webserver
- Windows Server 2012 : Édition Standard, Édition Essentials, Édition Datacenter (Server Core n'est pas pris en charge)
- Windows Server 2012 R2 : Édition Standard, Édition Essentials, Édition Datacenter (Server Core n'est pas pris en charge)

Systèmes d'exploitation de serveur pris en charge

- Windows Server 2016 : Édition Standard, Édition Essentials, Édition Datacenter (Server Core n'est pas pris en charge)

Systèmes d'exploitation pris en charge avec le mode UEFI

- 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)

REMARQUE :

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

Encryption External Media 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 8 : Enterprise, Pro, Grand public
- 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)

Systèmes d'exploitation de serveur pris en charge

- Windows Server 2012 R2

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
- macOS Mojave 10.14