# Dell Endpoint Security Suite Enterprise for Mac

Guide de l'administrateur v2.9

Mars 2021
Rév. A02

## Remarques, précautions et avertissements

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

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

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

**© 2012-2021 Dell Inc. All rights reserved.** Registered trademarks and trademarks used in the Dell Encryption and Endpoint Security Suite Enterprise suite of documents: Dell™ and the Dell logo, Dell Precision™, OptiPlex™, ControlVault™, Latitude™, XPS®, and KACE™ are trademarks of Dell Inc. Cylance®, CylancePROTECT, and the Cylance logo are registered trademarks of Cylance, Inc. in the U.S. and other countries. McAfee® and the McAfee logo are trademarks or registered trademarks of McAfee, Inc. in the US and other countries. Intel®, Pentium®, Intel Core Inside Duo®, Itanium®, and Xeon® are registered trademarks of Intel Corporation in the U.S. and other countries. Adobe®, Acrobat®, and Flash® are registered trademarks of Adobe Systems Incorporated. Authen tec® and Eikon® are registered trademarks of Authen tec. AMD® is a registered trademark of Advanced Micro Devices, Inc. Microsoft®, Windows®, and Windows Server®, Windows Vista®, Windows 7®, Windows 10®, Active Directory®, Access®, BitLocker®, BitLocker To Go®, Excel®, Hyper-V®, Outlook®, PowerPoint®, Word®, OneDrive®, SQL Server®, and Visual C++® are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. VMware® is a registered trademark or trademark of VMware, Inc. in the United States or other countries. Box® is a registered trademark of Box. Dropbox ℠ is a service mark of Dropbox, Inc. Google™, Android™, Google™ Chrome™, Gmail™, and Google™ Play are either trademarks or registered trademarks of Google Inc. in the United States and other countries. Apple®, App Store℠, Apple Remote Desktop™, Boot Camp™, FileVault™, iPad®, iPhone®, iPod®, iPod touch®, iPod shuffle®, and iPod nano®, Macintosh®, and Safari® are either servicemarks, trademarks, or registered trademarks of Apple, Inc. in the United States and/or other countries. EnCase™ and Guidance Software® are either trademarks or registered trademarks of Guidance Software. Entrust® is a registered trademark of Entrust®, Inc. in the United States and other countries. Mozilla® Firefox® is a registered trademark of Mozilla Foundation in the United States and/or other countries. iOS® is a trademark or registered trademark of Cisco Systems, Inc. in the United States and certain other countries and is used under license. Oracle® and Java® are registered trademarks of Oracle and/or its affiliates. Travelstar® is a registered trademark of HGST, Inc. in the United States and other countries. UNIX® is a registered trademark of The Open Group. VALIDITY™ is a trademark of Validity Sensors, Inc. in the United States and other countries. VeriSign® and other related marks are the trademarks or registered trademarks of VeriSign, Inc. or its affiliates or subsidiaries in the U.S. and other countries and licensed to Symantec Corporation. KVM on IP® is a registered trademark of Video Products. Yahoo!® is a registered trademark of Yahoo! Inc. Bing® is a registered trademark of Microsoft Inc. Ask® is a registered trademark of IAC Publishing, LLC. Other names may be trademarks of their respective owners.

# Table des matières

**Chapitre 1: Introduction** ..... **5**
Présentation ..... 5
Chiffrement FileVault ..... 5
Contacter Dell ProSupport ..... 5

**Chapitre 2: Configuration requise** ..... **6**
Client Encryption ..... 6
Matériel du client Encryption ..... 6
Logiciel client Encryption ..... 6
Advanced Threat Prevention ..... 7
Configuration matérielle requise pour Advanced Threat Prevention ..... 7
Logiciel Advanced Threat Prevention ..... 8
Ports Advanced Threat Prevention ..... 8
Compatibilité ..... 8

**Chapitre 3: Tâches associées à Encryption Client** ..... **12**
Installation/mise à niveau d'Encryption Client ..... 12
Installation ou mise à niveau interactive ..... 13
Installation/mise à niveau avec la ligne de commande ..... 14
Activation de l'accès intégral au disque pour les supports externes ..... 16
Activation de Encryption Client ..... 17
Affichage de la règle et de l'état de cryptage ..... 17
Affichage de la règle et de l'état dans la console de gestion ..... 20
Volumes système ..... 21
Activer le cryptage ..... 21
Processus de cryptage ..... 22
Recyclage des clés de restauration FileVault ..... 25
Expérience utilisateur ..... 25
Récupération ..... 26
Montage du volume ..... 27
Récupération FileVault ..... 28
Support amovible ..... 31
Formats pris en charge ..... 31
Encryption External Media et mises à jour de règles ..... 32
Exceptions de cryptage ..... 32
Erreurs sur l'onglet Support amovible ..... 32
Messages d'audit ..... 32
Collecte de fichiers journaux pour Endpoint Security Suite Enterprise ..... 33
Désinstallation d'Encryption Client pour Mac ..... 33
Activation en tant qu'administrateur ..... 33
Activer ..... 34
Activer temporairement ..... 34
Référence d'Encryption Client ..... 34
À propos de la protection par mot de passe du programme interne ..... 34

Utilisation de Boot Camp....35
Récupération d'un mot de passe du programme interne....37
Outil client....37

**Chapitre 4: Tâches....40**
Installation d'Advanced Threat Prevention pour Mac....40
Installation interactive d'Advanced Threat Prevention....40
Installation d'Advanced Threat Prevention avec la ligne de commande....43
Dépannage d'Advanced Threat Prevention pour Mac....44
Vérification de l'installation d'Advanced Threat Prevention....45
Collecte de fichiers journaux pour Endpoint Security Suite Enterprise....46
Affichage des détails d'Advanced Threat Prevention....46
Provision a Tenant....48
Provisionner un service partagé....49
Configuration de la mise à jour automatique de l'agent Advanced Threat Prevention....49
Dépannage d'Advanced Threat Prevention....49

**Chapitre 5: Glossaire....52**

# 1

# Introduction

Le Guide de l'administrateur d'Endpoint Security Suite Enterprise pour Mac fournit les informations nécessaires pour déployer et installer le logiciel client.

**Sujets :**


- Présentation
- Chiffrement FileVault
- Contacter Dell ProSupport


## Présentation

Endpoint Security Suite Enterprise pour Mac offre Advanced Threat Prevention au niveau du système d'exploitation et de la mémoire, ainsi qu'un chiffrement, le tout géré de manière centralisée depuis Dell Server. Grâce à la gestion centralisée, à la génération de rapports de conformité consolidés et aux alertes relatives aux menaces émises par la console, les entreprises peuvent atteindre leurs objectifs de conformité et fournir les justifications associées pour tous leurs points de terminaison. Des fonctionnalités comme les modèles de rapports et de règles prédéfinis bénéficient d'une expertise intégrée, aidant ainsi les entreprises à réduire leurs coûts de gestion et à simplifier leurs opérations IT.

- Endpoint Security Suite Enterprise for Mac : suite de logiciels assurant le chiffrement client des données ainsi que Advanced Threat Prevention.
- Proxy de règles : permet de distribuer des règles.
- Serveur de sécurité : assure les activations du logiciel de chiffrement client
- Security Management Server ou Security Management Server Virtual : fournit une administration centralisée des règles de sécurité, s'intègre avec les répertoires d'entreprise existants et crée des rapports. Dans ce document, les deux serveurs sont appelés Dell Server, sauf lorsqu'il est nécessaire de désigner une version spécifique (par exemple, une procédure varie en cas d'utilisation de Security Management Server Virtual).

  Ces composants Dell fonctionnent entre eux de façon transparente pour fournir un environnement mobile sécurisé sans dégrader l'expérience utilisateur.

Endpoint Security Suite Enterprise pour Mac comprend deux fichiers .dmg : l'un dédié à Encryption Client, l'autre à Advanced Threat Prevention. Vous pouvez installer un seul de ces fichiers ou les deux.

## Chiffrement FileVault

Dell Encryption peut gérer le chiffrement complet du disque FileVault pour Mac. La règle *Chiffrement de volume Dell* doit être **activée** pour que le chiffrement s'effectue et que les autres paramètres de règle fonctionnent. Pour plus d'informations sur d'autres règles, voir *AdminHelp*.

Seul le chiffrement FileVault est pris en charge et celui-ci sera géré par Endpoint Security Suite Enterprise. Si la règle *Cryptage de volume Dell* est **activée** et la règle *Crypter en utilisant FileVault pour Mac* est **désactivée** sur un ordinateur, un message de conflit de règles s'affiche sur le client Encryption. L'administrateur doit définir ces deux règles sur **Activée**.

## Contacter Dell ProSupport

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

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

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

2

# Configuration requise

Ce chapitre présente la configuration matérielle et logicielle requise pour le client. Avant d'effectuer toute opération de déploiement, assurez-vous que l'environnement de déploiement respecte les exigences suivantes.

**Sujets :**


- Client Encryption
- Advanced Threat Prevention


# Client Encryption

## Matériel du client Encryption

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

| Matériel |
| --- |
| • 30 Mo d'espace disque disponible |
| • Carte d'interface réseau 10/100/1000 ou Wi-Fi |
| • Le disque système doit être partitionné à l'aide du schéma de partition GPT (tableau de partition GUID) et peut être formaté avec l'un des éléments suivants :<br>○ Mac OS X étendu journalisé (HFS +) : conversion en Core Storage pour appliquer FileVault.<br>○ Apple File System (APFS) |

## Logiciel client Encryption

Le tableau suivant décrit les logiciels pris en charge.

| Systèmes d'exploitation (noyaux de 64 bits) |
| --- |
| • macOS High Sierra 10.13.6 |
| • macOS Mojave 10.14.5 - 10.14.6 |
| • macOS Catalina 10.15.5 - 10.15.6 |

**REMARQUE :** Dell Encryption ne prend pas en charge macOS Big sur.

**REMARQUE :**

Si vous utilisez un compte d'utilisateur réseau pour vous authentifier, ce compte doit être configuré comme un compte mobile afin de configurer entièrement la gestion de FileVault 2.

**Support Crypté**

Le tableau ci-dessous répertorie les systèmes d'exploitation pris en charge lors de l'accès aux supports externes cryptés par Dell.

**REMARQUE :**

Encryption External Media prend en charge :

- FAT32
- exFAT
- Les supports au format HFS Plus (MacOS étendu) dotés de schémas de partition MBR (Master Boot Record) ou GPT (tableau de partition GUID). Voir la section Activer HFS Plus.

**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 chiffrer, pour héberger Encryption External Media.

| **Systèmes d'exploitation Windows (32 et 64 bits) pris en charge pour accès aux supports cryptés** |
|---|
| • Microsoft Windows 7 SP1<br>- Entreprise<br>- Professionnel<br>- Ultimate |
| • Microsoft Windows 8.1 - Windows 8.1 Mise à jour 1<br>- Entreprise<br>- Professionnel |
| • Microsoft Windows 10<br>- Education<br>- Entreprise<br>- Pro v1607 (Mise à jour anniversaire/Redstone 1) jusqu'à v1909 (Mise à jour novembre 2019/19H2) |
| **Systèmes d'exploitation Mac (noyaux 64 bits) pris en charge pour accès aux supports cryptés** |
| • macOS High Sierra 10.13.6<br>**REMARQUE :**<br>Encryption External Media sur macOS High Sierra 10.14.x nécessite Encryption Enterprise v8.16 ou une version supérieure. |
| • macOS Mojave 10.14.5 - 10.14.6 |
| • macOS Catalina 10.15.5 - 10.15.6 |

# Advanced Threat Prevention

Désinstallez les applications antivirus, anti-programmes malveillants et anti-espions des autres fournisseurs avant d'installer le client Advanced Threat Prevention, afin d'éviter tout échec d'installation.

## Configuration matérielle requise pour Advanced Threat Prevention

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

| **Matériel** |
|---|
| • 500 Go d'espace disque disponible, selon le système d'exploitation<br>• 2 Go de RAM<br>• Carte d'interface réseau 10/100/1000 ou Wi-Fi |

# Logiciel Advanced Threat Prevention

Le tableau suivant décrit les logiciels pris en charge.

| Systèmes d'exploitation (noyaux de 64 bits) |
|---|
| • Mac OS X Mavericks 10.9.5<br>• Mac OS X Yosemite 10.10.5<br>• macOS Sierra 10.12.6<br>**REMARQUE :**<br>Les versions Mac OS X Mavericks 10.9.5, Mac OS X Yosemite 10.10.5 et macOS Sierra 10.12 sont prises en charge avec Advanced Threat Prevention uniquement, et pas avec le client Encryption. |
| • macOS High Sierra 10.13.6<br>**REMARQUE :**<br>Reportez-vous au logiciel client Encryption pour les versions macOS High Sierra spécifiques prises en charge avec le client Encryption. |
| • macOS Mojave 10.14.5 - 10.14.6<br>**REMARQUE :**<br>Vous pouvez installer l'agent ATP sur macOS Mojave, mais les fonctions de protection de la mémoire et contrôle des scripts sont automatiquement désactivées et ne sont pas actuellement prises en charge. |
| • macOS Catalina 10.15.3 - 10.15.4 |

**REMARQUE :**

les systèmes de fichiers sensibles à la casse ne sont pas pris en charge.

# Ports Advanced Threat Prevention

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

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

# Compatibilité

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

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

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

| Fonctionnalités | Stratégies | Windows | macOS | Linux | |
|---|---|---|---|---|---|
| **Actions de fichier** | | | | | |

| Fonctionnalités | Stratégies | Windows | macOS | Linux | |
|---|---|---|---|---|---|
| | Quarantaine automatique (Dangereux) | x | x | x | |
| | Quarantaine automatique (Anormal) | x | x | x | |
| | Téléchargement auto | x | x | x | |
| | Liste de confiance de la stratégie | x | x | x | |
| **Actions de mémoire** | | | | | |
| | Protection de la mémoire | x | x | x | |
| **Exploitation** | | | | | |
| | Zone dynamique d'empilement | x | x | x | |
| | Protection de l'empilement | x | x | x | |
| | Écraser le code | x | Sans objet | | |
| | Collecte de données stockées en RAM | x | Sans objet | | |
| | Charge malveillante | x | | | |
| **Injection de processus** | | | | | |
| | Attribution à distance de mémoire | x | x | Sans objet | |
| | Adressage à distance de mémoire | x | x | Sans objet | |
| | Écriture à distance dans la mémoire | x | x | Sans objet | |
| | Écriture à distance de PE dans la mémoire | x | Sans objet | Sans objet | |
| | Écraser le code à distance | x | Sans objet | | |
| | Suppression de l'adressage de la mémoire à distance | x | Sans objet | | |
| | Création de thread à distance | x | x | | |
| | Planification APC à distance | x | Sans objet | Sans objet | |
| | Injection de DYLD | | x | x | |
| **Escalade** | | | | | |
| | Lecture LSASS | x | Sans objet | Sans objet | |
| | Attribution nulle | x | x | | |
| **Paramètres de protection** | | | | | |
| | Contrôle de l'exécution | x | x | x | |
| | Interdire l'arrêt du service depuis le périphérique | x | x | | |

| Fonctionnalités | Stratégies | Windows | macOS | Linux | |
|---|---|---|---|---|---|
| | Arrêter les processus et sous-processus dangereux en cours d'exécution | x | x | x | |
| | Détection de menace d'arrière plan | x | x | x | |
| | recherche de nouveaux fichiers | x | x | x | |
| | Taille de fichier d'archive maximale à analyser | x | x | x | |
| | Exclure des dossiers spécifiques | x | x | x | |
| | Copier les fichiers exemples | x | | | |
| **Contrôle des applications** | | | | | |
| | Fenêtre de modification | x | | x | |
| | Exclusion de dossiers | x | | | |
| **Paramètres de l'agent** | | | | | |
| | Activer le téléchargement automatique des fichiers journaux | x | x | x | |
| | Activer les notifications sur le bureau | x | | | |
| **Contrôle des scripts** | | | | | |
| | Script actif | x | | | |
| | Powershell | x | | | |
| | Macros Office | x | | Sans objet | |
| | Bloquer l'utilisation de la console Powershell | x | | | |
| | Approuver les scripts dans ces dossiers (et leurs sous-dossiers) | x | | | |
| | Niveau de journalisation | x | | | |
| | Niveau d'auto-protection | x | | | |
| | Mise à jour automatique | x | | | |
| | Exécuter une détection (à partir de l'interface utilisateur de l'agent) | x | | | |
| | Supprimer les éléments mis en quarantaine (interface utilisateur de l'agent et interface utilisateur de la console) | x | | | |
| | Mode Déconnecté | x | | x | |
| | Données de menace détaillées | x | | | |

| Fonctionnalités | Stratégies | Windows | macOS | Linux | |
|---|---|---|---|---|---|
| | Liste de confiance des certificats | x | x | Sans objet | |
| | Copier les échantillons de programme malveillant | x | x | x | |
| | Paramètres de proxy | x | x | x | |
| | Vérification manuelle des stratégies (interface utilisateur de l'agent) | x | x | | |

3

# Tâches associées à Encryption Client

**Sujets :**


- Installation/mise à niveau d'Encryption Client
- Activation de Encryption Client
- Affichage de la règle et de l'état de cryptage
- Volumes système
- Récupération
- Support amovible
- Collecte de fichiers journaux pour Endpoint Security Suite Enterprise
- Désinstallation d'Encryption Client pour Mac
- Activation en tant qu'administrateur
- Référence d'Encryption Client


# Installation/mise à niveau d'Encryption Client

Cette section présente le processus d'installation/de mise à niveau et d'activation d'Encryption Cient pour Mac.

Il existe deux méthodes d'installation/de mise à niveau d'Encryption Client pour Mac. Sélectionnez l'**une** des opérations suivantes :

- Installation/mise à niveau et activation interactives : cette méthode constitue la méthode d'installation ou de mise à niveau du package du logiciel client la plus simple. Toutefois, cette méthode ne permet pas les personnalisations. Si vous avez l'intention d'utiliser Boot Camp ou une version d'un système d'exploitation que Dell ne prend pas encore entièrement en charge (via une modification .plist), vous devez utiliser la méthode d'installation/de mise à niveau avec la ligne de commande. Pour plus d'informations sur l'utilisation de Boot Camp, voir Utilisation de Boot Camp.
- Installation/mise à niveau avec la ligne de commande : cette méthode d'installation/de mise à niveau avancée est réservée aux administrateurs expérimentés en matière de syntaxe de ligne de commande. Si vous avez l'intention d'utiliser Boot Camp ou une version d'un système d'exploitation que Dell ne prend pas encore entièrement en charge (via une modification .plist), vous devez utiliser cette méthode pour installer ou mettre à niveau le package logiciel du client. Pour plus d'informations sur l'utilisation de Boot Camp, voir Utilisation de Boot Camp.

  Pour plus d'informations sur les options de commande du programme d'installation, voir la bibliothèque de référence Mac OS X sur http://developer.apple.com. Dell recommande fortement d'utiliser des outils de déploiement à distance comme Apple Remote Desktop, pour distribuer le package d'installation client.

  **REMARQUE :**

  Apple met souvent ses systèmes d'exploitation à jour entre les versions d'Endpoint Security Suite Enterprise For Mac. Pour prendre en charge autant de clients que possible, le fichier com.dell.ddp.plist peut être modifié. Le test de ces versions commence dès qu'Apple publie une nouvelle version pour garantir la compatibilité avec le client Encryption pour Mac.

## Pré-requis

Dell recommande de suivre les meilleures pratiques informatiques pendant le déploiement du logiciel client. Ceci inclut, sans s'y limiter, les environnements de test contrôlés pour les premiers tests et les déploiements échelonnés pour les utilisateurs.

Avant de démarrer ce processus, assurez-vous que les conditions préalables suivantes sont réunies :

- Assurez-vous que Dell Server et ses composants sont déjà installés.

  Si vous n'avez pas encore installé Dell Server, suivez les instructions figurant dans le guide approprié ci-dessous.

  *Security Management Server Installation and Migration Guide (Guide d'installation et de migration de Security Management Server)*

  *Security Management Server Virtual Quick Start Guide and Installation Guide (Guide de démarrage rapide et Guide d'installation de Security Management Server Virtual)*

- Assurez-vous de disposer des URLs de serveur de sécurité et de proxy de règles. Vous en avez besoin pour l'installation du logiciel client et l'activation.
- Si votre déploiement utilise une autre configuration que celle par défaut, vérifiez que vous connaissez le numéro de port du serveur de sécurité. Vous en avez besoin pour l'installation du logiciel client et l'activation.
- Vérifiez que l'ordinateur cible dispose d'une connectivité réseau vers le serveur de sécurité et le proxy de règles.
- Assurez-vous de disposer d'un compte d'utilisateur de domaine dans l'installation Active Directory configurée pour être utilisée avec Dell Server. Le compte d'utilisateur de domaine est utilisé pour l'activation du logiciel client. La configuration des points de terminaison Mac pour l'authentification de domaine (réseau) n'est pas nécessaire.

Avant de configurer les règles de chiffrement, la règle *Chiffrement de volume Dell* doit être *activée.* Vérifiez que vous comprenez les règles *Chiffrer en utilisant FileVault pour Mac* et *Volumes ciblés pour le chiffrement*.

Pour plus d'informations sur les règles de cryptage, voir Cryptage Mac > Cryptage de volume Dell.

# Installation ou mise à niveau interactive

Pour installer ou mettre à niveau et activer le logiciel client, suivez les étapes ci-dessous. Pour effectuer ces étapes, vous devez posséder un compte administrateur.

**Installation interactive**

**REMARQUE :**

Avant de commencer, enregistrez le travail de l'utilisateur et fermez les autres applications. L'ordinateur doit être redémarré tout de suite après l'installation.

1. À partir du support d'installation Dell, montez le fichier Dell-Encryption-Enterprise-<version>.dmg.
2. Double-cliquez sur le programme d'installation du package. Le message suivant est affiché :
   *Ce package exécute un programme pour déterminer si le logiciel peut être installé.*
3. Cliquez sur **Continuer** pour poursuivre.
4. Lisez le texte d'accueil et cliquez sur **Continuer**.
5. Après avoir lu le contrat de licence, cliquez sur **Continuer**, puis sur **Accepter** pour accepter ses conditions.
6. Dans le champ *Adresse de domaine*, entrez le nom de domaine complet pour les utilisateurs cibles, tel que *department.organization.com*.
7. Dans le champ *Nom d'affichage (facultatif)*, envisagez de définir le *Nom d'affichage* sur le nom de domaine NetBIOS (version antérieure à Windows 2000), qui est généralement en majuscules.

   S'il est configuré, ce champ est affiché à la place du champ Adresse de domaine dans la boîte de dialogue *Activation*, pour des raisons de cohérence avec le nom de domaine qui est indiqué dans la boîte de dialogue *Authentification* des ordinateurs Windows gérés par un domaine.

8. Dans le champ *Serveur de sécurité* entrez le hostname du serveur de sécurité.

   Si votre déploiement n'utilise pas une configuration par défaut, mettez à jour les ports et la case à cocher *Utiliser SSL*.

   Une fois qu'une connexion a été établie, l'indicateur de connectivité du serveur de sécurité passe du rouge au vert.

9. Dans le champ *Proxy de règles*, le nom d'hôte du proxy de règles est automatiquement rempli par un hôte qui correspond à l'hôte du serveur de sécurité. Cet hôte sert de proxy de règles si aucun hôte n'est spécifié dans la configuration des règles.

   Une fois qu'une connexion a été établie, l'indicateur de connectivité du proxy de règles passe du rouge au vert.

10. Une fois que la boîte de dialogue Configuration Dell est complétée et que la connexion a été établie sur le serveur de sécurité et le proxy de règles, cliquez sur **Continuer** pour afficher le type d'installation.
11. L'installation sur certains ordinateurs affiche une boîte de dialogue *Sélectionner une destination* avant l'affichage de la boîte de dialogue *Type d'installation*. Dans ce cas, sélectionnez le disque système actuel dans la liste des disques affichés. L'icône du disque système actuel affiche une flèche verte pointant vers le disque. Cliquez sur **Continuer**.
12. Une fois que le type d'installation s'est affiché, cliquez sur **Installer** pour poursuivre l'installation.
13. Lorsque vous y êtes invité, saisissez les informations d'identification du compte administrateur. (L'application MacOS X Installer les exige.)
14. Cliquez sur **OK**.

    **REMARQUE :**

Immédiatement après la fin de l'installation, vous devez redémarrer l'ordinateur. Si des fichiers sont ouverts dans d'autres applications et que vous n'êtes pas prêt à redémarrer, cliquez sur **Annuler,** enregistrez votre travail et fermez les autres applications.

15. Cliquez sur **Continuer l'installation**. L'installation commence.
16. Une fois l'installation terminée, cliquez sur **Redémarrer**.
17. Lors d'une nouvelle installation du logiciel Endpoint Security Suite Enterprise, la boîte de dialogue *Extension du système bloquée* s'affiche.

    Pour l'autorisation de l'extension de noyau, l'une et/ou l'autre de ces boîtes de dialogue s'affiche.

| **Extension du système bloquée** | **Extension du système bloquée** |
|---|---|
| a. Cliquez sur **OK**.<br>b. Cliquez sur **OK**.<br>c. Pour approuver ces extensions, sélectionnez **Préférences système > Sécurité et confidentialité**.<br>d. Cliquez sur **Autoriser** en regard *de System software du développeur Credant Technologies (Dell, Inc, anciennement Credant Technologies)*.<br>e. Cliquez sur **OK**. | Si l'extension du système destinée au montage des volumes FDEEM n'a pas pu être chargée, procédez comme suit :<br>a. Cliquez sur **Ouvrir les préférences système**.<br>b. Cliquez sur **OK**.<br>c. Sous l'onglet **Général**, cliquez sur **Autoriser** en regard de *System software du développeur Credant Technologies (Dell, Inc, anciennement Credant Technologies)*.<br>d. Cliquez sur **OK**. |

    Le bouton Autoriser peut être disponible 30 minutes maximum après l'installation. Si vous ignorez cette étape, la boîte de dialogue continue à s'afficher toutes les 25 minutes jusqu'à ce que vous ayez effectué l'opération.
18. Continuez pour Activer Encryption Client pour Mac.

**macOS 10.15 et versions ultérieures avec support amovible**

Si une entreprise utilise un support amovible avec macOS 10.15 ou une version ultérieure, les utilisateurs doivent activer l'accès intégral au disque pour les supports externes. Pour plus d'informations, reportez-vous à la section Activation de l'accès intégral au disque pour les supports amovibles.

# Installation/mise à niveau avec la ligne de commande

Pour installer le logiciel client en utilisant la ligne de commande, suivez les étapes ci-dessous.

**Installation par ligne de commande**

1. À partir du support d'installation Dell, montez le fichier Dell-Encryption-Enterprise-<version>.dmg.
2. Copiez le package **Install Dell Endpoint Security Suite Enterprise** et le fichier **com.dell.ddp.plist** sur le disque local.
3. Dans la console de gestion, modifiez si nécessaire les règles suivantes. Les paramètres de règle remplacent les paramètres du fichier .plist. Utilisez les paramètres .plist si les règles n'existent pas dans la console de gestion.
   - **Liste des utilisateurs sans authentification** : dans certains cas, vous devrez peut-être modifier cette règle afin que les utilisateurs ou les catégories d'utilisateurs spécifiés n'aient pas à être activés sur Dell Server. Par exemple, dans un établissement scolaire, les enseignants seraient invités à activer leur ordinateur sur Dell Server mais les élèves utilisant les ordinateurs du laboratoire n'auraient pas à le faire. L'administrateur du laboratoire pourrait utiliser cette règle et le compte exécutant l'outil client afin que les élèves puissent se connecter sans être invités à s'activer. Pour plus d'informations sur l'outil client, voir la section Outil client. Si une entreprise a besoin de savoir quel compte d'utilisateur est associé à chacun des ordinateurs Mac, tous les utilisateurs doivent s'activer sur Dell Server de sorte que l'entreprise ne modifie pas cette propriété. Cependant, si un utilisateur souhaite configurer Encryption External Media, il doit être authentifié sur Dell Server.
4. Ouvrez le fichier .plist et modifiez n'importe quelle valeur de l'espace réservé supplémentaire :

   **REMARQUE :**

   Apple met souvent ses systèmes d'exploitation à jour entre les versions d'Endpoint Security Suite Enterprise For Mac. Pour prendre en charge autant de clients que possible, Dell permet de modifier le fichier .plist. Dès qu'Apple publie une nouvelle version, Dell la teste pour vérifier sa compatibilité avec le client Encryption pour Mac.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/
PropertyList-1.0.dtd">
```

```
<plist version="1.0">
<dict>
  <key>NoAuthenticateUsers</key> [In this sample code, after one user activates the
computer against the Dell Server, other users can log in without being prompted to
activate.]
  <dict>
  <key>dsAttrTypeStandard:AuthenticationAuthority</key>
  <array>
  <string>*</string>
  </array>
  </dict>
  <key>NoAuthenticateUsers</key> [In this sample code, users from a specific domain name
can log in without being prompted to activate against the Dell Server.]
  <dict>
  <key>dsAttrTypeStandard:AuthenticationAuthority</key>
  <array>
  <string>;Kerberosv5;;*@domainName.com;domainName.com*</string>
  </array>
  </dict>
  <key>NoAuthenticateUsers</key> [In this sample code, specific users can log in without
being prompted to authenticate against the Dell Server.]
  <dict>
  <key>dsAttrTypeStandard:AuthenticationAuthority</key>
  <array>
  <string>;Kerberosv5;;username1@domainName.com;domainName.com*</string>
  <string>;Kerberosv5;;username2@domainName.com;domainName.com*</string>
  </array>
  </dict>
  <key>AllowedOSVersions</key> [AllowedOSVersions is not present in the default .plist
file, it must be added to the file. Add from <key> through </array> to allow a newer
version of operating system to be used. See Note above.]
  <array>
   <string>10.<x.x></string> [Operating system version]
  </array>
  <key>UseRecoveryKey</key>
  <false/> [This value is obsolete since current versions can use both personal and
institutional recovery keys for FileVault encryption.]
  <key>SecurityServers</key>
  <array>
   <dict>
      <key>Host</key>
      <string>securityserver.organization.com</string> [Replace this value with your
Security Server URL]
      <key>Port</key>
     <integer>8443</integer> [Beginning in v8.0, the default port number is 8443. However,
port number 8081 will still allow activations. In general, if your Dell Server is v8.0 or
later, use port 8443. If your Dell Server is pre-v8.0, use port 8081.]
      <key>UseSSL</key>
      <true/> [Dell recommends a true value]
   </dict>
  </array>
  <key>ReuseUniqueIdentifier</key>
  <false/> [When this value is set to true, the computer identifies itself to the Dell
Server by the same hostname it was activated with, regardless of changes to the computer
hostname.]
  <key>Domains</key>
  <array>
   <dict>
      <key>DisplayName</key>
      <string>COMPANY</string>
      <key>Domain</key>
      <string>department.organization.com</string> [Replace this value with the Domain URL
that users will activate against]
   </dict>
  </array>
  <key>PolicyProxies</key>
  <array>
   <dict>
      <key>Host</key>
      <string>policyproxy.organization.com</string> [Replace this value with your Policy
Proxy URL]
      <key>Port</key>
      <integer>8000</integer> [Leave as-is unless there is a conflict with an existing
```

```
port]
   </dict>
  </array>
  <key>Version</key>
  <integer>2</integer> [Do not modify]
  <key>MaxPasswordDelay</key>
  <integer>xxxx</integer> [Number of seconds to apply to the security policy, "Require
password XXXX after sleep or screen saver begins." The acceptable range is 0-32400.]
  <key>EMSTreatsUnsupportedFileSystemAs</key>
  <string>ignore</string> [For handling Mac OS Extended media. Possible values are
ignore, provisioningRejected, or unshieldable. ignore - the media is usable (default).
provisioningRejected - retains the value in the Dell Server policy, EMS Access to
unShielded Media. unshieldable - If the EMS Access to unShielded Media policy is set to
Block, the media is ejected. If the EMS Access to unShielded Media policy is not set to
Block, it is usable as provisioningRejected. The key and value are case sensitive.]
  <key>ClientActivationTimeout</key>
  <integer>120</integer> [Range: 5 to 300, inclusive. The default value is 30. The time in
seconds to give the Security Server time to respond to an activation attempt before giving
up. This plist value is valid for clients running v8.6.0.6627 or later.]
</dict>
</plist>
```

5. Enregistrez le fichier .plist, puis fermez-le.
6. Pour chaque ordinateur ciblé, copiez le package dans un dossier temporaire et le fichier com.dell.ddp.plist dans **/Bibliothèque/Préférences**.
7. Effectuez une installation par ligne de commande du package à l'aide de la commande **installer** :
   **`sudo installer -pkg "Install Dell Endpoint Security Suite Enterprise.pkg" -target /`**
8. Redémarrez l'ordinateur à l'aide de la ligne de commande suivante : **`sudo shutdown -r now`**

   **REMARQUE :**

   La protection de l'intégrité du système (SIP) a été renforcée dans macOS High Sierra (10.13) et les utilisateurs doivent désormais approuver la nouvelle extension de noyau tierce. Pour en savoir plus sur l'autorisation des extensions de noyau sur macOS High Sierra, consultez l'article SLN307814 de la base de connaissances.
9. Continuez pour Activer le client de cryptage pour Mac.

**macOS 10.15 et versions ultérieures avec support amovible**

Si une entreprise utilise un support amovible avec macOS 10.15 ou une version ultérieure, les utilisateurs doivent activer l'accès intégral au disque pour les supports externes. Pour plus d'informations, reportez-vous à la section Activation de l'accès intégral au disque pour les supports externes.

# Activation de l'accès intégral au disque pour les supports externes

Si une entreprise utilise un support amovible avec macOS 10.15 ou une version ultérieure, les utilisateurs doivent activer l'accès intégral au disque pour les supports externes. Les utilisateurs voient l'une des invites suivantes :

- Après l'installation du logiciel client, un message vous indique que vous devez fournir votre autorisation pour l'accès intégral au disque pour les supports externes. Cliquez sur le bouton **Accéder à Sécurité et confidentialité** et passez aux étapes ci-dessous.
- S'ils ne reçoivent pas ce message après l'installation, les utilisateurs sont invités à activer l'accès intégral au disque lors du premier montage du support amovible. Un message indique que Dell Encryption External Media ou EMS Explorer souhaite accéder aux fichiers sur un volume amovible. Cliquez sur **OK** et passez aux étapes ci-dessous.

Pour plus d'informations, reportez-vous à l'article de la base de connaissances SLN319972.

1. Dans *Préférences système* > *Sécurité et confidentialité*, cliquez sur l'onglet **Confidentialité**.
2. Dans le volet gauche, sélectionnez **Accès intégral au disque**.
   L'application *Dell Encryption External Media* ne s'affiche pas.
3. En bas, cliquez sur l'icône en forme de verrou et indiquez les informations d'identification d'un compte administrateur local.
   Dans le volet de gauche > **Fichiers et dossiers**, l'utilisateur peut vérifier les composants de support externe (EMS) pour lesquelles il souhaite fournir les autorisations requises.
4. Dans le volet gauche, sélectionnez **Accès intégral au disque**.

   L'application *Dell Encryption External Media* s'affiche désormais. Toutefois, lorsque la demande d'approbation est en attente, la case à cocher correspondant à cette application n'est pas sélectionnée.
5. Accordez l'autorisation en cochant la case.

Si l'application *Dell Encryption External Media* ne s'affiche pas :

a. Cliquez sur l'icône plus (+) dans le volet de droite.
b. Accédez à **/Library/Dell/EMS**, puis sélectionnez **Dell Encryption External Media**.
c. Cliquez sur **Ouvrir**.
d. Dans **Accès intégral au disque**, cochez la case *Dell Encryption External Media*.

6. Fermez **Sécurité et confidentialité**.

# Activation de Encryption Client

Le processus d'activation associe les comptes d'utilisateur réseau dans Dell Server à l'ordinateur Mac. Il récupère les stratégies de sécurité de chaque compte, envoie les mises à jour de l'inventaire et de l'état, active les flux de travail de récupération et fournit des rapports complets de conformité. Le logiciel client lance le processus d'activation pour chaque compte d'utilisateur qu'il trouve sur l'ordinateur lorsque chaque utilisateur se connecte à son compte d'utilisateur.

Après que le logiciel client a été installé et que le Mac a redémarré, l'utilisateur se connecte :

1. Entrez le nom d'utilisateur et le mot de passe gérés par Active Directory.

   Si la boîte de dialogue du mot de passe expire, cliquez sur **Actualiser** dans l'onglet Stratégies. Dans la section Afficher la stratégie et l'état de l'ordinateur local, voir l'étape 1.

2. Sélectionnez le domaine auquel vous connecter.

   Si Dell Server est configuré pour prendre en charge plusieurs domaines et qu'un domaine différent doit être utilisé pour l'activation, utilisez le nom principal d'utilisateur (UPN), qui est sous la forme *<username>@<domain>*.

3. Les options sont les suivantes :
   - Cliquez sur **Activer**.
     - Si l'activation réussit, un message s'affiche pour indiquer que l'activation a réussi. Le client Encryption pour Mac est désormais totalement opérationnel et géré par Dell Server.

       **REMARQUE :**

       Si une alerte s'affiche au sujet d'une ressource requise par Encryption External Media, cliquez sur le bouton **Accéder à Sécurité et confidentialité**, puis cliquez sur **Autoriser** pour l'extension de système requise par votre organisation. Vous devez autoriser cette extension afin qu'Encryption External Media fonctionne correctement.
     - Si l'activation échoue, le logiciel client permet trois tentatives pour entrer les identifiants de domaine corrects. Si les trois tentatives échouent, l'invite à entrer les identifiants de domaine s'affiche à nouveau lors de la prochaine connexion de l'utilisateur.
   - Cliquez sur **Pas maintenant** pour fermer la boîte de dialogue, qui s'affichera à nouveau à la prochaine ouverture de session d'utilisateur.

     **REMARQUE :**

     Lorsque l'administrateur a besoin de déchiffrer un disque sur un ordinateur Mac, que ce soit à partir d'un emplacement distant, en exécutant un script, ou en personne, le logiciel client demande à l'utilisateur de permettre l'accès de l'administrateur et oblige l'utilisateur à entrer son mot de passe.

     **REMARQUE :**

     Si vous configurez l'ordinateur pour le cryptage FileVault et que les fichiers sont cryptés, assurez-vous de vous connecter à un compte à partir duquel vous pouvez ensuite démarrer le système.

4. Effectuez l'une des opérations suivantes :
   - Si le cryptage n'était **pas** activé avant l'activation, passez au processus de cryptage.
   - Si le cryptage **était** activé avant l'activation, passez à la section Afficher la règle et l'état de cryptage.

# Affichage de la règle et de l'état de cryptage

Vous pouvez afficher la règle et l'état de chiffrement sur l'ordinateur local ou la console de gestion.

# Afficher la règle et l'état sur l'ordinateur local

Pour afficher la règle et l'état de cryptage sur l'ordinateur local, suivez les étapes ci-dessous.

1. Lancez les *Préférences système*, puis cliquez sur **Dell Encryption Enterprise**.
2. Cliquez sur l'onglet **Règles** pour afficher la règle actuellement définie pour cet ordinateur. Utilisez cette vue pour confirmer les règles de cryptage spécifiques en vigueur pour cet ordinateur.

   **REMARQUE :**

   cliquez sur **Actualiser** pour rechercher des mises à jour de règles.

   La console de gestion répertorie les règles Mac dans les groupes de technologie suivants :

   - **Cryptage Mac**
   - **Removable Media Encryption**

   Les règles que vous définissez dépendent des exigences de chiffrement de votre entreprise.

   Ce tableau répertorie les options de l'onglet de règles.

| | |
|---|---|
| **Cryptage Mac > Cryptage de volume Dell**<br>Pour High Sierra et les versions supérieures, les deux règles suivantes doivent être activées. Pour Sierra et les versions antérieures, reportez-vous aux versions précédentes de la documentation. | |
| Dell Volume Encryption (Cryptage de volume Dell) | *Activation* ou *désactivation*<br>Il s'agit de la « règle principale » de toutes les autres règles de Dell Volume Encryption. Cette règle doit être *activée* pour que d'autres règles de Dell Volume Encryption puissent être appliquées.<br>Lorsqu'elle est *activée*, cette règle active et lance le chiffrement des volumes non chiffrés, conformément à la règle *Volumes ciblés pour le chiffrement* **ou** *Chiffrement en utilisant FileVault pour Mac*. Le paramètre par défaut est *Activé*.<br>Sa désactivation désactive le chiffrement et lance l'analyse de déchiffrement de tous les volumes complètement ou partiellement chiffrés. |
| Cryptage utilisant FileVault pour Mac | Si vous pensez utiliser le cryptage FileVault, commencez par vérifier que Dell Volume Encryption est *activé*.<br>Assurez-vous que la règle *Chiffrer en utilisant FileVault pour Mac* est sélectionnée sur la console de gestion.<br>Lorsqu'elle est activée, FileVault est utilisé pour crypter le volume système incluant des disques Fusion Drives, en fonction de la configuration de la règle *Volumes ciblés pour le cryptage*. |
| **Cryptage Mac > Paramètres généraux Mac** | |
| Volumes choisis pour cryptage | *Volume système uniquement* ou *Tous les volumes fixes*<br>Le paramètre *Volume système uniquement* protège uniquement le volume système actif.<br>Le paramètre **Tous les volumes fixes** protège tous les volumes étendus Mac OS sur tous les disques fixes, ainsi que le volume système actif. |

3. Pour obtenir une description de toutes les règles, voir l'assistance *AdminHelp* disponible dans la console de gestion. Pour localiser une règle spécifique dans *AdminHelp* :
   a. Cliquez sur l'icône de recherche.
   b. Dans le champ *Rechercher*, entrez le nom de la règle entre guillemets.
   c. Cliquez sur le lien du sujet qui s'affiche. Le nom de règle que vous avez saisi entre guillemets est surligné dans le sujet.
4. Cliquez sur l'onglet **Volumes système** pour afficher l'état des volumes ciblés pour le cryptage.

| État | Description |
|---|---|
| Exclus | Le volume est exclu du cryptage. Cela s'applique aux volumes non cryptés lorsque le cryptage est désactivé, aux volumes externes, aux volumes ayant un autre format que Mac OS X étendu (journalisé) et aux volumes hors volume système lorsque la règle *Volumes ciblés pour le cryptage* est définie sur Volume système uniquement. |
| Préparation du volume pour le chiffrement | Le logiciel client est en train de lancer le processus de cryptage du volume, mais n'a pas encore commencé l'analyse du cryptage. |
| Le volume ne peut pas être redimensionné | Le logiciel client ne peut pas démarrer le cryptage, car le volume ne peut pas être redimensionné de manière appropriée. Une fois que vous avez reçu ce message, contactez Dell ProSupport et fournissez les fichiers journaux. |
| Doit être réparé avant de commencer le cryptage | La vérification du volume par Utilitaire de disque a échoué.<br>Pour réparer un volume, suivez les instructions de l'article HT1782 d'Apple Support (http://support.apple.com/kb/HT1782). |
| Préparation du cryptage terminée. En attente de redémarrage | Le chiffrement commence après le redémarrage. |
| Conflit de règles de cryptage | Le disque ne peut pas être mis en conformité avec la règle, car il est crypté avec des paramètres incorrects. Voir Cryptage utilisant FileVault pour Mac. |
| En attente de la mise en dépôt des clés auprès de Dell Server | Pour vous assurer que toutes les données chiffrées peuvent être restaurées, le logiciel client ne commence pas le processus de chiffrement avant la mise en dépôt de toutes les clés de chiffrement auprès de Dell Server. Le client interroge la connectivité du serveur de sécurité dans cet état jusqu'à la mise en dépôt des clés. |
| Crypter | Une analyse de cryptage est en cours. |
| Chiffré | L'analyse de cryptage est terminée. |
| Décrypter | Une analyse de décryptage est en cours. |
| Restauration à l'état d'origine en cours | Le logiciel client restaure le schéma de partition à son état d'origine à la fin du processus *Décryptage* en cours. Il s'agit de l'équivalent de l'état *Préparation du volume pour le chiffrement* pour l'analyse de déchiffrement. |
| Décrypté | L'analyse de décryptage est terminée. |

| Couleur | Description |
|---|---|
| Vert | Partie cryptée |
| Rouge | Partie non cryptée |
| Jaune | Partie recryptée<br>Par exemple, par une modification des algorithmes de cryptage. Les données sont toujours sécurisées. Cela consiste simplement à passer à un autre type de cryptage. |

L'onglet Volumes système affiche tous les volumes connectés à l'ordinateur résidant sur des disques au format GPT (GUID Partition Table). Le tableau ci-dessous présente des exemples de configurations de volume de disques internes.

**REMARQUE :**

Les badges et icônes peuvent varier légèrement en fonction de votre système d'exploitation.

| Badge | Type et état du volume |
|---|---|
|  | Le volume système Mac OS X démarré. Le badge Dossier X désigne la partition de démarrage actuelle. |
|  | Un volume configuré pour le cryptage. Le badge Sécurité et Confidentialité représente une partition protégée par FileVault. |
|  | Un volume non de démarrage configuré pour le cryptage. Le badge Sécurité et Confidentialité représente une partition protégée par FileVault. |
|  | Plusieurs disques et aucun cryptage.<br>**REMARQUE :**<br>l'icône de volume sans badge indique que rien n'a été fait sur le disque. Ce n'est pas un disque de démarrage. |

5. Cliquez sur l'onglet **Support amovible** pour afficher l'état des volumes ciblés pour le cryptage. Le tableau ci-dessous présente des exemples de configurations de volume de supports amovibles.

   Les badges et icônes peuvent varier légèrement en fonction de votre système d'exploitation.

| Badge | Statut |
|---|---|
|  | Une icône de volume estompée indique un périphérique non monté. Raisons possibles :<br>● L'utilisateur peut avoir choisi de ne pas le provisionner.<br>● Le support peut être bloqué.<br>**REMARQUE :**<br>un badge de cercle rouge/barre oblique sur cette icône indique une partition qui est exclue de la protection parce qu'elle n'est pas prise en charge. Cela comprend les volumes au format FAT32. |
|  | Une icône de volume saturée indique un périphérique monté. Le badge sans écriture indique qu'il est en lecture seule. Le cryptage est activé, mais le support n'est pas provisionné et la règle Accès Encryption External Media aux supports non protégés est définie sur Lecture seule. |
|  | Support crypté par Encryption External Media, désigné par un badge Dell. |

# Affichage de la règle et de l'état dans la console de gestion

Pour afficher la règle et l'état de chiffrement dans la console de gestion, suivez les étapes ci-dessous.

1. Connectez-vous à la console de gestion en tant qu'administrateur Dell.
2. Dans le volet gauche, cliquez sur **Populations > Points de terminaison**.

3. Pour Station de travail, cliquez sur une option dans le champ *Hostname* ou, si vous connaissez le hostname du point de terminaison, entrez-le dans le champ *Rechercher*. Vous pouvez également saisir un filtre pour rechercher le point de terminaison.

   **REMARQUE :**

   Le caractère générique (*) peut être utilisé mais n'est pas obligatoire au début ou à la fin du texte. Entrez le nom commun, le nom principal universel, ou sAMAccountName.
4. Cliquez sur le point de terminaison approprié :
5. Cliquez sur l'onglet **Détails et actions**.

   La zone de Détails du point de terminaison affiche des informations sur l'ordinateur Mac.

   La zone Détails de la protection affiche des informations sur le logiciel client, dont les heures de début et de fin de l'analyse de cryptage pour cet ordinateur.

   Pour afficher les règles effectives, dans la zone Actions, cliquez sur **Afficher les règles effectives**.
6. Cliquez sur l'onglet **Règles de sécurité**. Dans cet onglet, vous pouvez développer les types de règles et modifier des règles spécifiques.
   a. Une fois que vous avez terminé, cliquez sur **Terminé**.
   b. Dans le volet de gauche, cliquez sur **Gestion** > **Valider**.

      **REMARQUE :**

      Le nombre qui s'affiche en regard de Modifications de règles en attente est cumulatif. Il peut inclure les modifications apportées à d'autres points de terminaison ou par d'autres administrateurs utilisant le même compte.
   c. Saisissez une description des modifications dans la zone *Commentaires*, puis cliquez sur **Valider des règles**.
7. Cliquez sur l'onglet **Utilisateurs**. Cette zone affiche une liste d'utilisateurs activés sur cet ordinateur Mac. Cliquez sur le nom de l'utilisateur pour afficher les informations de tous les ordinateurs sur lesquels cet utilisateur est activé.
8. Cliquez sur l'onglet **Groupes de points de terminaison**. Cette zone affiche tous les groupes de points de terminaison auxquels cet ordinateur Mac appartient.

# Volumes système

## Activer le cryptage

Les éléments suivants sont pris en charge pour le cryptage :

- Les volumes du système de fichiers d'Apple (APFS) qui partagent des supports physiques avec le volume de démarrage.
- Les volumes Mac OS X étendu (journalisé) et les disques système qui sont partitionnés avec le schéma de partition GPT (GUID Partition Table)

Utilisez cette procédure pour activer le cryptage sur un ordinateur client si le cryptage n'était **pas** activé avant l'activation. Ce processus n'active le cryptage que pour un seul ordinateur. Vous pouvez, au besoin, choisir d'activer le chiffrement pour tous les ordinateurs Mac au niveau Enterprise. Pour obtenir des instructions supplémentaires sur l'activation du chiffrement au niveau *Enterprise*, voir AdminHelp.

1. Connectez-vous à la console de gestion en tant qu'administrateur Dell.
2. Dans le volet de gauche, cliquez sur **Populations** > **Points de terminaison**.
3. Pour Station de travail, cliquez sur une option dans la colonne Hostname ou, si vous connaissez le hostname du point de terminaison, entrez-le dans le champ *Rechercher*. Vous pouvez également saisir un filtre pour rechercher le point de terminaison.

   **REMARQUE :**

   Le caractère générique (*) peut être utilisé mais n'est pas obligatoire au début ou à la fin du texte. Entrez le nom commun, le nom principal universel, ou sAMAccountName.
4. Cliquez sur le point de terminaison approprié :
5. Sur la page *Stratégies de sécurité*, cliquez sur le groupe de technologies **Cryptage Mac**.

   Par défaut, la règle principale *Cryptage de volume Dell* est *activée*.
6. Si le Mac est doté de Fusion Drive, cochez la case *Crypter en utilisant FileVault* pour la stratégie Mac.

**REMARQUE :**

Cette stratégie exige que la règle *Cryptage de volume Dell* soit également *activée*. Cependant, lorsque le chiffrement FileVault est activé, aucune autre stratégie du groupe n'est appliquée. Voir Cryptage Mac > Cryptage de volume Dell.

7. Si FileVault est désélectionné (macOS Sierra et versions antérieures), modifiez les autres règles à votre convenance.

   Pour obtenir une description de toutes les règles, voir l'assistance *AdminHelp* disponible dans la console de gestion.

8. Une fois que vous avez terminé, cliquez sur **Terminé**.
9. Dans le volet de gauche, cliquez sur **Gestion** > **Valider**.

   Le nombre qui s'affiche en regard de Modifications de règles en attente est cumulatif. Il peut inclure les modifications apportées à d'autres points de terminaison ou par d'autres administrateurs utilisant le même compte.

10. Saisissez une description des modifications dans la zone de commentaires, puis cliquez sur **Valider des règles**.
11. Pour afficher la configuration de la règle sur l'ordinateur local après que Dell Server envoie la règle, dans le volet Stratégies des Préférences de Dell Encryption Enterprise Preferences, cliquez sur **Actualiser**.

# Processus de cryptage

Le processus de chiffrement varie en fonction de l'état du volume de démarrage lorsque le chiffrement est activé.

**REMARQUE :**

Pour maintenir l'intégrité des données de l'utilisateur, le logiciel client ne commence à crypter un volume qu'après la réussite du processus de vérification sur ce volume. Si la vérification du volume échoue, le logiciel client en informe l'utilisateur et signale l'échec dans Préférences de Dell Data Protection. Si vous avez besoin de réparer un volume, suivez les instructions de l'article HT1782 d'Apple Support (http://support.apple.com/kb/HT1782). Le logiciel client refait une tentative de vérification au prochain redémarrage de l'ordinateur.

Sélectionnez l'une de ces options :

- Cryptage FileVault d'un volume non crypté
- Prise en charge de la gestion d'un volume crypté par FileVault

## Chiffrement FileVault d'un volume non chiffré

Avec le chiffrement FileVault, un autre utilisateur sans nom s'affiche dans le PBA. Ne supprimez pas cet utilisateur, car il autorise le serveur Dell à appliquer la stratégie sur le périphérique. Si l'utilisateur PBA est supprimé, l'utilisateur doit prendre les mesures nécessaires pour commencer les déchiffrements imposés par la stratégie.

1. Après l'installation et l'activation, vous devez vous connecter au compte à partir duquel vous voulez démarrer après que le cryptage FileVault est activé.
2. Attendez la fin de la validation du disque et de la vérification du volume.
3. Saisissez le mot de passe du compte.

   **REMARQUE :**

   Si vous laissez expirer cette boîte de dialogue, vous devez redémarrer ou vous connecter pour que la boîte de dialogue de mot de passe s'affiche à nouveau.

4. Cliquez sur **OK**.
5. Assurez-vous que chaque utilisateur dispose d'un jeton sécurisé. Voir https://www.dell.com/support/article/us/en/19/sln309192/mobile-users-unable-to-activate-dell-encryption-enterprise-for-mac-on-macos-high-sierra?lang=en.

   Si le compte auquel l'utilisateur était connecté est un compte réseau non mobile, une boîte de dialogue apparaît. Après le disque de démarrage est crypté, le disque ne peut être démarré que par l'utilisateur qui était connecté lors de l'initialisation FileVault.

   Ce compte doit être un compte mobile local ou réseau. Pour changer les comptes réseau non mobiles en comptes mobiles, accédez à **Préférences système > Utilisateurs et groupes**. Effectuez l'une des opérations suivantes :

   - Faites du compte un compte mobile.

     OU

- Connectez-vous à un compte local et initialisez FileVault à partir de cet emplacement.

6. Cliquez sur **OK**.
7. À la fin de la préparation du cryptage, redémarrez l'ordinateur.

   **REMARQUE :**

   En fonction des stratégies d'expérience utilisateur définies dans la console de gestion, le logiciel client peut inviter l'utilisateur à redémarrer l'ordinateur.
8. Après son redémarrage, l'ordinateur doit être connecté au réseau pour que le logiciel client mette en dépôt les informations de récupération auprès de Dell Server.

   Le logiciel client peut commencer et terminer le processus de chiffrement, ainsi que signaler l'état de chiffrement à la console de gestion, avant la connexion de l'utilisateur. Cela vous permet d'assurer la conformité de tous les ordinateurs Mac sans nécessiter l'interaction de l'utilisateur.

## Modification de la règle pour ajouter des utilisateurs FileVault

FileVault sécurise les données sur un disque par cryptage automatique. Dans un volume de démarrage FileVault géré, vous pouvez modifier une règle dans la console de gestion pour permettre à plusieurs utilisateurs de déverrouiller le disque et utiliser votre dictionnaire des noms et valeurs enregistrés d'OpenDirectory pour autoriser ensuite les utilisateurs à s'ajouter eux-mêmes sur le disque FileVault.

1. Dans les règles avancées des *Paramètres globaux Mac* de la console de gestion, faites défiler la liste jusqu'à la règle *Liste d'utilisateurs FileVault 2 PBA*.
2. Dans le champ de la règle *Liste d'utilisateurs FileVault 2 PBA*, saisissez une règle qui correspond aux utilisateurs que vous souhaitez spécifier. Par exemple, `<string>*</string>` associé à n'importe quelle clé doit correspondre à tous les utilisateurs du serveur OpenDirectory lié.

   Les balises sont sensibles à la casse et la valeur entière doit être correctement formée en tant que dictionnaire et éléments de tableaux dans une liste de propriétés. Les clés du dictionnaire sont liées par AND. Les valeurs de tableaux sont liées par OR afin que la correspondance de n'importe quel élément dans un tableau corresponde à l'ensemble d'un tableau.

   **REMARQUE :**

   Si une règle est mal formée, une erreur s'affiche dans l'onglet *Dell Encryption Enterprise > Préférences*.

   Les valeurs <dict> suivantes répertorient des exemples pour deux clés :

```
<dict>
    <key>dsAttrTypeStandard:AuthenticationAuthority</key>
    <array>
     <string>;Kerberosv5;;user1@LKDC:*</string>
     <string>;Kerberosv5;;user2@LKDC:*</string>
     <string>;Kerberosv5;;user3@LKDC:*</string>
     <string>;Kerberosv5;;z*@LKDC:*</string>
    </array>
    <key>dsAttrTypeStandard:NFSHomeDirectory</key>
    <string>/Users/*</string>
</dict>
```

   - Les exemples d'entrées de clé *AuthenticationAuthority* spécifient un modèle *d'utilisateur1*, *utilisateur2* et *utilisateur3* ou de n'importe quel identifiant utilisateur commençant par *z*. Pour afficher la boîte de dialogue fournissant la syntaxe correcte pour chaque utilisateur, appuyez sur les touches **Contrôle-Option-Commande** sur le client. Copiez la syntaxe de l'utilisateur et collez-la sur la console de gestion.

     **REMARQUE :**

     Dans cet exemple, les astérisques en fin de ligne représentent la dernière partie des enregistrements d'autorité d'authentification. Pour éviter une sous-spécification, renseignez l'enregistrement complet et non l'astérisque en fin de ligne, car cet astérisque est associé à toutes les informations se trouvant après les deux points dans l'enregistrement OpenDirectory.
   - La clé NFSHomeDirectory exige que chaque utilisateur saisissant la première clé doit également disposer d'un dossier de travail dans */Utilisateurs/*.

     **REMARQUE :**

     Vous devez créer le dossier de travail s'il n'en existe pas pour un utilisateur.
3. Redémarrez les ordinateurs.

4. Demandez aux utilisateurs d'activer le démarrage FileVault pour leur compte d'utilisateur. L'utilisateur doit posséder un compte local ou mobile. les comptes réseau sont automatiquement convertis en comptes mobiles.

Pour qu'un utilisateur active son compte FileVault :

1. Lancez les **Préférences système**, puis cliquez sur **Dell Encryption Enterprise**.
2. Cliquez sur l'onglet **Volumes système**.
3. Sur le lecteur de volume système, appuyez sur la touche Ctrl et cliquez avec la souris, puis sélectionnez **Ajouter des utilisateurs FileVault au démarrage FileVault**.
4. Dans le champ *Rechercher*, entrez un nom d'utilisateur ou faites défiler vers le bas. Les comptes d'utilisateur s'affichent uniquement s'ils répondent aux critères définis par la stratégie.

   Pour les utilisateurs locaux et mobiles, un bouton *Activer l'utilisateur* s'affiche.

   Pour les utilisateurs réseau, un bouton *Convertir et activer l'utilisateur* s'affiche.

   **REMARQUE :**

   un voyant vert s'affiche en regard des comptes d'utilisateur qui peuvent démarrer FileVault.

5. Cliquez sur **Activer l'utilisateur** ou **Convertir et activer l'utilisateur**.
6. Saisissez le mot de passe du compte sélectionné, puis cliquez sur **OK**. Un indicateur de progression s'affiche.
7. Après une boîte de dialogue Réussite, cliquez sur **Terminé**.

## Prise en charge de la gestion d'un volume crypté par FileVault

Si l'ordinateur a déjà un volume chiffré par FileVault et que le chiffrage FileVault est activé sur la console de gestion, Dell Encryption peut assumer la gestion du volume.

Si Dell Encryption détecte que le volume de démarrage est déjà crypté, la boîte de dialogue Dell Encryption Enterprise s'affiche. Pour permettre à Dell Encryption d'assumer la gestion du volume, procédez comme suit.

1. Sélectionnez **Clé de récupération personnelle *ou* Informations d'identification de compte amorçable**.

   **REMARQUE :**

   Pour macOS High Sierra et Apple File System (APFS), vous devez sélectionner **Informations d'identification de compte amorçable**.

   - **Clé de récupération personnelle : si vous disposez de la clé de récupération personnelle que vous avez reçue lors du cryptage du disque par FileVault.**

     a. Entrez la clé.

        Si un utilisateur ne possède pas la clé existante, il peut en faire la demande auprès de l'administrateur.

     b. Cliquez sur **OK**.

     **REMARQUE :**

     Après la fin du processus de prise en charge, une nouvelle clé de récupération personnelle est générée et mise en dépôt. La clé de récupération précédente est invalidée et supprimée.

   - **Informations d'identification de compte amorçable : si vous avez le nom d'utilisateur et le mot de passe d'un compte qui est actuellement autorisé à démarrer à partir du volume.**

     a. Entrez un nom d'utilisateur et un mot de passe.

     b. Cliquez sur **OK**.

2. Quand une boîte de dialogue indiquant que Dell gère désormais le cryptage du volume s'affiche, cliquez sur **OK**.

   Si Dell Encryption détecte qu'un volume hors démarrage est déjà crypté, une invite de phrase de passe s'affiche.

3. (Volumes hors démarrage cryptés par FileVault uniquement) Pour permettre à Dell Encryption d'assumer la gestion du volume, entrez la phrase de passe d'accès au volume. Voici le mot de passe assigné au volume lors du cryptage initial de FileVault.

   Lorsque Dell gère le cryptage du volume, l'ancien mot de passe n'est plus valide. Votre administrateur Dell peut obtenir une clé de récupération de votre volume dans le cas où vous auriez besoin d'aide pour sa récupération.

   Si vous décidez de ne pas entrer le mot de passe, le contenu du volume est accessible et chiffré avec FileVault, mais le chiffrement n'est pas géré par Dell.

**REMARQUE :**

Dans la console de gestion, l'administrateur peut voir que Dell Server gère désormais le point de terminaison.

# Recyclage des clés de restauration FileVault

Si vous avez des problèmes de sécurité avec un bundle de récupération ou si un volume ou des clés sont compromis, vous pouvez recycler le matériel de clés de ce volume.

Vous pouvez recycler les clés des disques de démarrage et de non-démarrage sur Mac OS X.

Pour recycler le matériel de clés :

1. Téléchargez un bundle de restauration à partir de la console de gestion et copiez-le sur le bureau de l'ordinateur.
2. Lancez les *Préférences système*, puis cliquez sur **Dell Encryption Enterprise**.
3. Cliquez sur l'onglet **Volumes système**.
4. Faites glisser le bundle de récupération de l'étape 1 vers la partition appropriée.

   Une boîte de dialogue vous invite à changer les clés FileVault.

5. Cliquez sur **OK**.

   Une boîte de dialogue confirme le succès du changement des clés.

6. Cliquez sur **OK**.

   **REMARQUE :**

   Les clés du bundle de récupération pour ce disque sont désormais obsolètes. Vous devez télécharger un nouveau bundle de restauration à partir de la console de gestion.

# Expérience utilisateur

Pour plus de sécurité, le logiciel client désactive la fonction de *connexion automatique* des ordinateurs Mac OS X.

En outre, le logiciel client applique automatiquement la fonction *Exiger le mot de passe après la mise en veille ou l'activation de l'économiseur d'écran* de Mac OS X. En outre, une durée configurable est autorisée en mode veille/économiseur d'écran avant d'appliquer l'authentification. Le logiciel client permet à un utilisateur de configurer une valeur pouvant aller jusqu'à cinq minutes avant d'appliquer l'authentification.

Les utilisateurs peuvent utiliser l'ordinateur normalement pendant l'analyse de cryptage. Toutes les données du volume système actuellement démarré sont cryptées, y compris le système d'exploitation, pendant que le système d'exploitation continue de fonctionner.

Si l'ordinateur est redémarré ou entre en mode veille, l'analyse de cryptage s'interrompt, puis reprend automatiquement après le redémarrage ou la sortie du mode veille.

Le logiciel client ne prend pas en charge les images de mise en veille prolongée qu'utilise la fonction *Safe Sleep* pour activer l'ordinateur lorsque la batterie de l'ordinateur se décharge entièrement pendant la veille.

Pour réduire l'impact pour l'utilisateur, le logiciel client met à jour automatiquement le mode veille du système pour désactiver l'hibernation et applique cette configuration. L'ordinateur peut toujours entrer en veille, mais l'état du système actuel est maintenu uniquement dans la mémoire. Par conséquent, l'ordinateur est entièrement redémarré s'il est complètement arrêté en mode veille, ce qui pourrait se produire si la batterie se décharge ou est remplacée.

## Copier une règle de liste autorisée

Un élément de menu caché permet à un utilisateur de copier une règle de liste autorisée pour les supports amovibles.

1. Lancez les **Préférences système**, puis cliquez sur **Dell Encryption Enterprise**.
2. Sélectionnez l'onglet **Support amovible**.
3. Faites un clic droit sur la ligne d'un disque en appuyant simultanément sur la touche Commande.

   Un élément de menu caché s'affiche.

4. Cliquez sur **Copier une règle de liste autorisée** pour le support amovible actuel. La règle de liste autorisée est copiée dans le Presse-papiers.
5. Accédez au Presse-papiers, copiez la règle de liste autorisée et envoyez-la à votre administrateur.

Si la règle *Cryptage de support Mac* est **activée**, les données sont cryptées, y compris celles des disques Thunderbolt.

Pour exclure un appareil ou un groupe de périphériques pour empêcher l'écriture de données chiffrées sur le disque Thunderbolt ou sur Encryption External Media, utilisez cette règle de liste autorisée pour modifier les valeurs.

Utilisez la règle complète pour spécifier un disque particulier pour l'ajout à la liste autorisée. Par exemple :

bus=USB;fstype=HFS+;tbolt=0;size=4006608896;USBPRODUCTNUM=5669;USBPRODNAME=DT101 II;USBVENDORNAME=Kingston;USBVENDORNUM=2385;USBSERNUM=001CC0EC3447AA308699119F

**REMARQUE :**

Remplacez les valeurs de l'exemple par les informations de votre disque.

**REMARQUE :**

Vous devez activer HFS Plus. Voir la section Activer HFS Plus.

Pour exclure les périphériques SATA de l'application de la règle de Cryptage de support Mac lors d'une connexion via Thunderbolt :

tbolt=1;bus=SATA

Vous pouvez également placer sur liste autorisée ou exclure des supports dans Encryption External Media, en fonction des éléments suivants :

- **Taille du support**

  Règle de liste autorisée permettant d'exclure les supports volumineux de la protection Encryption External Media :

  size <op> <spécificateur de taille>

  <op> peut être =, <=, >=, <, >

  <spécificateur de taille> a la forme d'un entier décimal avec un suffixe facultatif de {K, M, G, T} aligné sur 1000 et non sur 1024. Par exemple, pour exclure d'Encryption External Media un support ou un disque faisant plus de 500 000 000 octets, utilisez l'une des formules suivantes :

  size >= 500000000

  size >= 500000K

  size >= 500M

- **Type de système de fichiers**

  Règle de liste autorisée :

  fstype=<fstype>

  <fstype> peut être ExFAT, FAT ou HFS+

Pour exclure les deux, voici un exemple pour un support HFS+ de 1 To ou plus :

size>=1T;fstype=HFS+

# Récupération

Vous pouvez occasionnellement avoir besoin d'accéder aux données sur les disques cryptés. En tant qu'administrateur Dell, vous pouvez accéder aux disques cryptés sans les décrypter, ce qui vous fera gagner un temps considérable.

Vous pourriez avoir besoin d'accéder aux données cryptées d'un utilisateur pour de nombreuses raisons, notamment dans les cas suivants :

- Une personne quitte l'entreprise et personne ne connaît son mot de passe.
- Un utilisateur ne se souvient pas de son mot de passe.

Dans cette section, vous découvrirez comment utiliser la récupération FileVault lorsque le chiffrement FileVault est appliqué au point de terminaison à restaurer. FileVault peut être utilisé avec le client Encryption s'exécutant sur macOS Sierra 10.12.6. La récupération FileVault est également utilisée sur les disques Fusion Drive.

# Montage du volume

**Pré-requis**

- Un volume de restauration externe non chiffré ou un ordinateur non chiffré qui exécute l'utilitaire de restauration
- Un câble FireWire ou Thunderbolt, en fonction de votre matériel
- L'ID de périphérique/ID unique de l'ordinateur ciblé pour la restauration : dans la plupart des cas, vous pouvez trouver l'ordinateur ciblé pour la restauration dans la console de gestion en recherchant le nom d'utilisateur de son propriétaire et en examinant les périphériques chiffrés pour cet utilisateur. Le format de l'ID unique/ID de périphérique est « MacBook.Z4291LK58RH de Pierre Dupont ».
- Le support d'installation Dell

## Processus

1. Connectez-vous à la console de gestion en tant qu'administrateur Dell.
2. Dans le volet de gauche, cliquez sur **Gestion > Récupérer le point de terminaison**.
3. Dans le champ *Rechercher*, entrez le nom de domaine complet du point de terminaison et cliquez sur l'icône Rechercher.
4. Cliquez sur le lien **Récupérer** du périphérique.
5. Si le point de terminaison requière une récupération avancée, une invite de mot de passe s'affiche. Attribuez un nouveau mot de passe au jeu de clés de cryptage que vous allez télécharger.

   **REMARQUE :**

   Vous devez vous souvenir de ce mot de passe pour accéder aux clés de récupération.
6. Pour enregistrer le bundle de récupération sur le volume de récupération externe ou l'ordinateur qui exécutera l'utilitaire de récupération pour effectuer l'opération de récupération, cliquez sur **Télécharger**, puis sur **Enregistrer**.

   Le fichier de récupération <machine_name.domain>.csv est téléchargé.
7. Démarrez l'ordinateur cible à partir d'un volume d'installation externe pré-créé. Pour ce faire, ouvrez le volet Disque de démarrage dans les Préférences système et sélectionnez le volume de récupération, ou maintenez enfoncée la touche **Option** pendant le redémarrage de cet ordinateur, puis sélectionnez le volume de récupération dans l'environnement préalable au démarrage du gestionnaire de démarrage.

   ou

   Démarrez l'ordinateur à récupérer en Mode de disque cible. Pour ce faire, ouvrez le volet Disque de démarrage dans les Préférences système et cliquez sur **Mode de disque cible**, ou maintenez enfoncée la touche **T** pendant que vous redémarrez cet ordinateur.

   **REMARQUE :**

   La protection par mot de passe du programme interne bloque la capacité d'utiliser la touche T au démarrage pour entrer en Mode de disque cible. Vous trouverez plus d'informations sur le Mode de disque cible auprès d'Apple sur http://support.apple.com/kb/HT1661.

   Connectez maintenant cet ordinateur à l'ordinateur hôte qui effectuera l'opération de récupération en utilisant un câble FireWire ou Thunderbolt, en fonction de votre matériel.
8. Montez l'image Dell-Encryption-Enterprise-<version>.dmg.

   **REMARQUE :**

   Recovery Utility doit être la même version ou une version plus récente que la version du logiciel client installé sur l'ordinateur à récupérer.
9. Sélectionnez le volume ou le disque à récupérer et cliquez sur **Continuer**.

   Si vous sélectionnez le disque, tous les volumes du disque seront restaurés à la fois.
10. Sélectionnez le bundle de récupération (enregistré à l'étape 6), puis cliquez sur **Ouvrir**.
11. Cliquez sur **Fermer**.

Vous pouvez maintenant ouvrir une fenêtre du Finder et accéder aux données du volume chiffré comme vous le feriez avec un volume normal. Toutes les données sont cryptées et décryptées de manière transparente lors du transfert des fichiers entre les volumes.

# Récupération FileVault

La récupération d'un volume géré chiffré par FileVault est dictée par Apple et automatisée dans la mesure du possible, mais elle nécessite quelques étapes supplémentaires.

Dell Recovery Utility simplifie l'utilisation des outils de récupération d'Apple avec des scripts pour aider à monter un volume ou, dans certains cas, à le décrypter. La fonctionnalité de la récupération FileVault est déterminée par le système d'exploitation installé sur la partition Recovery HD et la partition cible associée.

Un volume crypté par FileVault peut être récupéré uniquement à partir d'une partition Recovery HD qui est écrite sur tous les lecteurs de disque exécutant Mac OS X 10.9.5 ou version ultérieure. Cette exigence élimine la possibilité d'effectuer une opération de récupération directement depuis Dell Recovery Utility.

Deux méthodes de récupération existent, selon que la clé de récupération FileVault est une clé de récupération personnelle ou institutionnelle. Il existe toujours une clé de récupération valide. S'il existe une clé de récupération personnelle, Dell vous recommande d'utiliser l'entrée la plus récente pour cette clé. Si cette clé ne fonctionne pas, utilisez la chaîne de clés de récupération institutionnelle.

- Clé de récupération personnelle : le cryptage FileVault existant est géré par le Dell Server. si l'entrée la plus récente du bundle de récupération comprend une entrée RecoveryKey, suivez les étapes de la méthode Clé de récupération personnelle. RecoveryKey peut se présenter comme suit :

  ```
  RecoveryKey</key><string>C73W-CX2B-ANFY-HH3K-RLRE-LVAK</string>
  ```

- Trousseau de récupération (rarement utilisé) : cette méthode de récupération consiste à utiliser une clé de récupération institutionnelle FileVault.

  si l'entrée la plus récente du bundle de récupération comprend une entrée KeychainKey, suivez les étapes de la méthode Trousseau de récupération. RecoveryKey peut se présenter comme suit :

  ```
  KeychainKey</key><data>a3ljaAABAAAAA...
  ```

## Clé de récupération personnelle

Généralement, la meilleure pratique consiste à récupérer le volume de démarrage avant de récupérer les volumes hors démarrage, car cette opération monte tout autre volume qui a été crypté. La restauration du volume de démarrage corrige généralement les problèmes concernant les volumes hors démarrage.

**Pré-requis**

- Un disque de démarrage externe
- L'ID de périphérique/ID unique de l'ordinateur à récupérer. Dans la plupart des cas, vous pouvez trouver l'ordinateur ciblé pour la restauration dans la console de gestion en recherchant le nom d'utilisateur de son propriétaire et en examinant les périphériques chiffrés pour cet utilisateur. Le format de l'ID de périphérique/ID unique est « MacBook.Z4291LK58RH de Pierre Dupont ».
- Le support d'installation Dell

**Console de gestion : enregistrer le bundle de récupération**

1. Ouvrez la console de gestion.
2. Dans le volet gauche, cliquez sur **Populations > Points de terminaison**.
3. Recherchez le périphérique à récupérer.
4. Cliquez sur le périphérique pour ouvrir la page des détails du point de terminaison.
5. Cliquez sur l'onglet **Détails et actions**.
6. Sous *Détails de la protection*, cliquez sur le lien **Clés de restauration de périphérique**.
7. Pour enregistrer le bundle de récupération sur le volume de récupération externe ou l'ordinateur qui exécutera l'utilitaire de récupération pour effectuer l'opération de récupération, cliquez sur **Télécharger**, puis sur **Enregistrer**.
8. Entrez un emplacement pour le bundle de récupération, puis cliquez sur **Enregistrer**.

**Processus : monter le fichier .dmg**

1. Copiez le bundle de récupération ainsi que le fichier **Dell-Encryption-Enterprise-<version>.dmg** sur le disque USB amorçable.
2. Démarrez l'ordinateur cible à partir d'un volume d'installation externe incluant un système d'exploitation complet, créé au préalable. Pour ce faire, maintenez la touche **Option** pendant le redémarrage de cet ordinateur, puis sélectionnez le volume d'installation externe incluant un système d'exploitation complet dans l'environnement préalable au démarrage du gestionnaire de démarrage. Pour créer un volume amorçable, reportez-vous à la page https://support.apple.com/fr-fr/HT202796.
3. Montez l'image **Dell-Encryption-Enterprise-<version>.dmg**.

**Processus : lancer Dell Recovery Utility et restaurer le volume FileVault**

1. Dans le dossier Utilitaires se trouvant sur le support d'installation Dell, lancez Dell Recovery Utility.

   La boîte de dialogue *Dell Recovery Utility > Sélectionner des volumes* s'affiche.

   **REMARQUE :**

   Recovery Utility doit être la même version ou une version plus récente que la version du logiciel client installé sur l'ordinateur à récupérer.
2. Dans *Dell Recovery Utility > Sélectionner des volumes*, sélectionnez le volume FileVault.
   - Lorsque vous récupérez un système d'exploitation, les bonnes pratiques consistent à démarrer sur un ordinateur avec le même système d'exploitation ou une version supérieure.
   - Si vous avez des volumes non de démarrage cryptés, en général, vous récupérerez la partition de démarrage en premier.
3. Cliquez sur **Continuer**.
4. Identifiez et sélectionnez le bundle de récupération (enregistré précédemment) et cliquez sur **Ouvrir**.
5. Si la boîte de dialogue *Sélectionner l'enregistrement de récupération* s'affiche, consultez la colonne *Date de dépôt*, sélectionnez la date la plus récente pour le type Clé de récupération personnelle, puis cliquez sur **Continuer**.

   **REMARQUE :**

   avec une date de dépôt plus ancienne, il se peut que la clé ne soit plus valide.

   La boîte de dialogue *Résultat de l'opération de récupération* s'affiche.
   - Pour les disques de démarrage, l'outil de récupération fournit une clé de récupération personnelle qui vous permet de démarrer en utilisant la récupération FileVault Apple standard. Vous pouvez démarrer sur la partition cible et entrer la clé de restauration personnelle de l'authentification avant démarrage, qui peut varier en fonction du système d'exploitation.
   - Pour les disques non de démarrage, seule la clé de récupération personnelle s'affiche. Un bouton de déverrouillage permet de déverrouiller et de monter le volume.
6. Effectuez l'une des opérations suivantes :
   - Restauration du volume de démarrage (la plus courante)
   - Restauration d'un volume hors démarrage (rarement utilisée)

**Restauration du volume de démarrage (la plus courante)**

Dans la plupart des cas de restauration, utilisez cette option pour restaurer le volume de démarrage :

1. Notez la clé sur un pense-bête ou cliquez sur **Imprimer la clé de récupération**.
2. Cliquez sur **Fermer**.
3. Démarrez le volume que vous souhaitez restaurer en utilisant si nécessaire l'environnement préalable au démarrage du gestionnaire de démarrage.

   L'ordinateur affiche des icônes pour plusieurs utilisateurs ou demande un mot de passe.
4. Sélectionnez un utilisateur, le cas échéant, puis cliquez sur **?** à l'écran d'ouverture de session.
5. Cliquez sur la flèche qui s'affiche.
6. Saisissez la clé de récupération et appuyez sur **Entrée**.
7. Dans la boîte de dialogue, entrez un nouveau mot de passe pour l'utilisateur.

**Options de restauration de volume non amorçable** (rarement utilisées) : choisissez entre les options qui suivent.

**Restauration d'un volume non amorçable**

Si le volume de démarrage est endommagé ou effacé et qu'il existe des volumes secondaires, vous pouvez monter ces volumes hors démarrage.

1. Cliquez sur **Déverrouiller**. Le montage du volume s'exécute.
2. Cliquez sur **Fermer**.

**Déchiffrement du volume : cliquez sur le bouton**

1. Cliquez sur **Déchiffrer**. Une boîte de dialogue et une barre de progression indiquent le processus de déchiffrement.
2. Une fois ce processus terminé, cliquez sur **Fermer**.
3. Amorcez le système sur le volume déchiffré pour pouvoir l'utiliser.

**Déchiffrement du volume : exécutez la commande à partir du terminal**

1. Copiez la commande dans la zone *Déchiffrement du volume*.

2. Cliquez sur **Fermer**.
3. Exécutez la commande dans le terminal.

## Trousseau de récupération

Vous devez exécuter Dell Recovery Utility lorsqu'il est démarré à partir d'un volume de récupération non crypté.

**Pré-requis**

- Un volume de récupération externe ou un ordinateur qui exécutera l'utilitaire de récupération
- Un disque USB
- Un câble Firewire
- Le support d'installation Dell

**Console de gestion : enregistrer le bundle de récupération**

1. Ouvrez la console de gestion.
2. Dans le volet gauche, cliquez sur **Populations > Points de terminaison**.
3. Recherchez le périphérique à récupérer.
4. Cliquez sur le périphérique pour ouvrir la page des détails du point de terminaison.
5. Cliquez sur l'onglet **Détails et actions**.
6. Sous *Détails de la protection*, cliquez sur le lien **Clés de restauration de périphérique**.
7. Pour enregistrer le bundle de récupération sur le volume de récupération externe ou l'ordinateur qui exécutera l'utilitaire de récupération pour effectuer l'opération de récupération, cliquez sur **Télécharger**, puis sur **Enregistrer**.
8. Entrez un emplacement pour le bundle de récupération, puis cliquez sur **Enregistrer**.

**Processus**

1. Connectez un disque externe sur le système à récupérer.

   Le disque externe doit avoir un volume de démarrage Mac OS.
2. Démarrez sur le disque externe en appuyant sur la touche **Option** et en la maintenant enfoncée, et utilisez le sélecteur de démarrage pour sélectionner et démarrer à partir de ce volume.
3. Copiez le bundle de récupération depuis la Console de gestion.
4. Montez le fichier d'installation .dmg.
5. Dans le dossier Utilitaires, exécutez Dell Recovery Utility.

   La boîte de dialogue *Dell Recovery Utility > Sélectionner des volumes* s'affiche.
6. Sélectionnez le volume FileVault à récupérer et cliquez sur **Continuer**.

   La boîte de dialogue *Choisir le bundle de récupération* s'affiche.
7. Sélectionnez le bundle de récupération et cliquez sur **Ouvrir**.

   En présence de plusieurs clés de récupération pour ce disque, l'écran *Sélectionner l'enregistrement de récupération*.
8. Dans la colonne Date de dépôt, sélectionnez la date la plus récente pour le type de récupération Chaîne de clés, puis cliquez sur **Continuer**.

   **REMARQUE :**

   avec une date de dépôt plus ancienne, il se peut que la clé ne soit plus valide.

   La boîte de dialogue *Instructions de récupération FileVault* s'affiche.
9. Lisez les instructions et cliquez sur **Continuer**.

   La boîte de dialogue *Confirmer l'opération de récupération* s'affiche.
10. Mettez en surbrillance le volume FileVault à récupérer et cliquez sur **Continuer**.

    La boîte de dialogue *Choisir l'emplacement des fichiers de récupération* s'affiche, vous invitant à sélectionner un emplacement pour stocker les fichiers de récupération.

    Cet emplacement doit être celui que vous utiliserez pour la récupération puisque les scripts contiennent les chemins absolus des fichiers de données. Ne copiez **pas** ces fichiers sur la partition Recovery HD.

Dell vous recommande d'enregistrer ces fichiers à la racine d'un disque amovible, comme un disque USB.

**REMARQUE :**

veillez à ce que tous les utilisateurs aient un accès en lecture/écriture au disque USB ou autre que vous utilisez pour stocker la clé de récupération, et que le disque ait un espace suffisant. Si vous ne disposez pas des droits par rapport à un disque sélectionné ou si le disque n'a plus d'espace libre, une erreur indiquant que les clés de récupération n'ont pas été stockées s'affiche.

11. Sélectionnez un emplacement, puis cliquez sur **Enregistrer**.

    La boîte de dialogue *Résultat de l'opération de récupération* s'affiche pour indiquer que les fichiers ont été créés.

12. Cliquez sur **Fermer**.

13. Après le démarrage du volume Recovery HD, entrez le nom et le chemin du script.

    **REMARQUE :**

    Si vous stockez les fichiers à proximité de la racine d'un volume, cela raccourcit le chemin à saisir.

    Le Résultat de l'opération de récupération affiche la clé.

    L'utilitaire de restauration génère les fichiers à l'emplacement sélectionné, puis affiche les commandes exactes à exécuter à partir du volume Recovery HD pour monter ou déchiffrer le volume FileVault.

14. Une fois ces fichiers générés, copiez les chaînes de commande apparaissant surla boîte de dialogue *Résultat de l'opération de récupération*.

15. Redémarrez sur le volume Recovery HD de l'une des façons suivantes :

    - Appuyez de façon prolongée simultanément sur les touches **Commande** et **R** avant la sonnerie de démarrage/d'auto-test et pendant le démarrage de l'ordinateur.

      ou

    - Pour les versions antérieures d'Apple, appuyez sur la touche **Option** et utilisez le sélecteur de démarrage pour sélectionner le volume Recovery HD.

      La boîte de dialogue *Utilitaires Mac OS X* s'affiche.

16. Dans le menu Outils, sélectionnez **Utilitaires > Terminal**.

17. Pour monter le volume afin de pouvoir copier des fichiers à partir du terminal ou créer une image depuis Disk Utility : dans Terminal, saisissez le chemin d'accès complet et le nom du script **fv2mount.sh**. Par exemple :

    **/Volumes/recoveryFOB/fv2mount.sh**

18. Redémarrez l'ordinateur.

# Support amovible

## Formats pris en charge

Les supports au format FAT32, exFAT ou HFS Plus (Mac OS étendu) dotés de schémas de partition MBR (Master Boot Record) ou GPT (table de partition GUID) sont pris en charge. Vous devez activer HFS Plus.

**REMARQUE :**

Mac ne prend actuellement pas en charge la gravure de CD/DVD pour Encryption External Media. Cependant, l'accès aux lecteurs CD/DVD n'est pas bloqué, même si la règle *Accès bloqué d'EMS aux supports non protégeables* est sélectionnée.

### Activation de HFS Plus

Pour activer HFS Plus, ajoutez les éléments suivants au fichier .plist.

<key>EMSHFSPlusOptIn</key>

<true/>

**REMARQUE :**

Dell recommande de tester cette configuration avant de l'introduire dans l'environnement de production.

HFS Plus ne prend pas en charge les éléments suivants :

- Contrôle de version : les données de contrôle de version existantes sont supprimées du disque.
- Liens physiques : pendant l'analyse de cryptage du support amovible, le fichier n'est pas crypté. Une boîte de dialogue recommande d'éjecter le support.
- Supports contenant des sauvegardes Time machine :
  - Le support reconnu par les ordinateurs comme destination de sauvegarde Time Machine est automatiquement mis sur la liste autorisée pour permettre la poursuite des sauvegardes.
  - Tous les autres supports amovibles contenant des sauvegardes Time Machine sont basés sur la règle régissant les supports non provisionnés et les supports non protégés. Voir les règles *Accès EMS aux supports non protégés* et *Accès bloqué d'EMS aux supports non protégeables*.

    **REMARQUE :**

    Pour un nouveau disque qui ne contient pas encore de sauvegardes, l'utilisateur doit copier sa règle de liste autorisée et vous envoyer la règle pour vous indiquer son disque Time Machine à mettre sur la liste autorisée. Voir Copier une règle de liste autorisée.

# Encryption External Media et mises à jour de règles

Sur le système où le support amovible a été provisionné (ou récupéré), les règles sont mises à jour sur le support amovible au moment du montage.

# Exceptions de cryptage

Les attributs étendus ne sont pas cryptés sur des supports amovibles.

# Erreurs sur l'onglet Support amovible

- Sur un ordinateur non protégé, ne remplacez pas un fichier crypté par une version décryptée du fichier. Cela pourrait empêcher, plus tard, le décryptage. Cela peut également s'afficher comme une erreur sur l'onglet Support amovible.
- Si un marqueur de fin de fichier est invalidé, par exemple si un fichier est écrasé par un nouveau contenu hors du contrôle d'Encryption External Media, et que vous le montez ensuite dans Encryption External Media, une erreur de fin de fichier s'affiche sur l'onglet Support amovible.
- Lorsque vous convertissez des fichiers, les supports doivent disposer d'un espace libre supérieur à la taille du plus grand fichier à convertir. Si un triangle jaune apparaît dans la zone d'état de Support amovible, cliquez dessus. Si un message *Espace insuffisant* s'affiche, procédez comme suit :

  1. Notez la quantité d'espace qui doit être libéré sur le périphérique. Le rapport affiche une liste des fichiers et leur taille.
  2. Videz la corbeille. Lorsque vous libérez de l'espace, Encryption External Media chiffre automatiquement des fichiers supplémentaires.
  3. Si vous supprimez des fichiers ou des dossiers, veillez à vider à nouveau la corbeille.

# Messages d'audit

Des messages d'audit sont envoyés sur Dell Server.

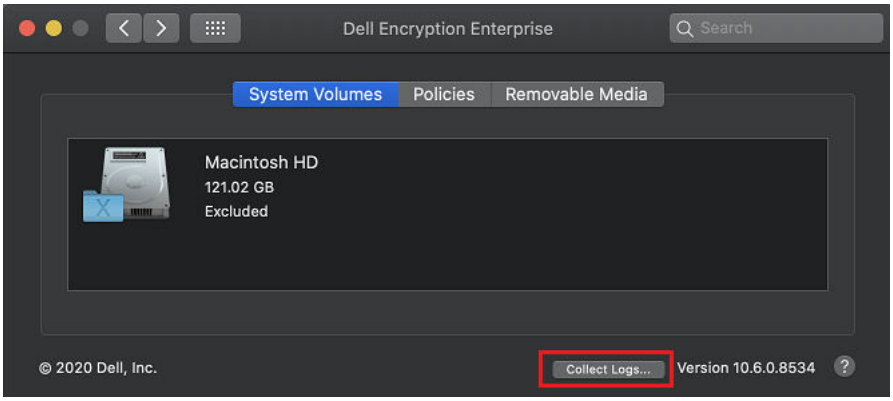
Pour afficher les messages d'audit de Endpoint Security Suite Enterprise For Mac :

1. Connectez-vous à la console de gestion en tant qu'administrateur Dell.
2. Dans le volet gauche, cliquez sur **Populations > Entreprise ou points de terminaison**.
3. Sélectionnez l'onglet **Événements de menaces avancées**.

Pour en savoir plus, voir *AdminHelp*.

# Collecte de fichiers journaux pour Endpoint Security Suite Enterprise

Dans *Préférences système* > *Dell Encryption Enterprise* > *Volumes système*, le bouton *collecter les journaux* en bas à droite permet à un administrateur de pré-générer des journaux pour le support. Cette action peut avoir un impact sur les performances lors de la collecte des fichiers log.




DellLogs.zip contient les journaux du logiciel Encryption Enterprise et Advanced Threat Prevention. Pour plus d'informations sur la collecte des journaux, voir http://www.dell.com/support/article/us/en/19/SLN303924.

# Désinstallation d'Encryption Client pour Mac

Le logiciel client peut être désinstallé à l'aide de l'application **Désinstaller Dell Encryption Enterprise**. Pour désinstaller le logiciel client, suivez les étapes ci-dessous.

**REMARQUE :**

avant d'exécuter l'application de désinstallation, le disque doit être entièrement décrypté.

1. Si le disque est actuellement chiffré, définissez la règle *Chiffrement de volume Dell* sur **Désactivé** dans la console de gestion, puis validez-la.

   Une boîte de dialogue s'affiche pour demander l'accès aux Préférences Système et le contrôle de l'ordinateur afin que le logiciel client puisse décrypter le disque.

   a. Cliquez sur **Ouvrir les préférences système**.

      Si **Refuser** est sélectionné, la désinstallation et le décryptage ne peuvent pas se poursuivre.

   b. Entrez le mot de passe administrateur.
2. Après que le disque est entièrement décrypté, redémarrez l'ordinateur (lorsque vous y êtes invité).
3. Une fois l'ordinateur redémarré, lancez l'application **Désinstaller Dell Encryption Enterprise** (se trouvant dans le dossier Utilitaires de l'image Dell-Encryption-Enterprise-<version>.dmg du support d'installation Dell).

   Les messages affichent l'état de la désinstallation.

   Encryption Client pour Mac est à présent désinstallé, et l'ordinateur peut être utilisé normalement.

# Activation en tant qu'administrateur

L'outil client offre à l'administrateur de nouvelles méthodes pour activer et examiner le logiciel client sur un ordinateur Mac. Deux méthodes d'activation sont disponibles :

- Activation à l'aide des informations d'identification d'administrateur
- Activation temporaire qui émule l'utilisateur sans laisser d'empreintes sur cet ordinateur.

Les deux méthodes peuvent être utilisées directement via un shell, ou dans un script.

**REMARQUE :**

ne pas activer le logiciel client sur plus de cinq ordinateurs ayant le même compte réseau. Cela pourrait entraîner des failles de sécurité graves et une dégradation des performances de Dell Server.

**Pré-requis**

- Le client Encryption for Mac doit être installé sur l'ordinateur distant.
- Ne pas activer via l'interface utilisateur client avant de tenter d'activer depuis un emplacement distant.

## Activer

Utilisez cette commande pour activer le client en tant qu'administrateur.

Exemple :

**client -a** *username@domain.com password admin admin*

## Activer temporairement

Utilisez cette commande pour activer le client sans laisser d'empreintes sur l'ordinateur.

1. Ouvrez un shell ou utiliser un script pour activer le logiciel client :

   ***client*** *-at username@domain.com password*

2. Utilisez l'outil client pour récupérer des informations sur le logiciel client, ses règles, l'état du disque, le compte d'utilisateur, etc. Pour en savoir plus sur l'outil client, voir la section Outil client.

   **REMARQUE :**

   Après l'activation, les informations sur le logiciel client, y compris les règles, l'état du disque et les informations de l'utilisateur, sont également disponibles dans Préférences Système dans les préférences Dell Encryption Enterprise.

# Référence d'Encryption Client

## À propos de la protection par mot de passe du programme interne

**REMARQUE :**

Les derniers ordinateurs Mac ne prennent pas en charges la protection par mot de passe du programme interne. La protection par mot de passe du programme interne est prise en charge pour les modèles suivants :

- iMac10.*
- iMac11.*
- Macmini4.*
- MacBook7.*
- MacBookAir2.*
- MacBookPro7.*
- MacPro5.*
- XServe3.*

Par exemple, iMac10.1, iMac11.1 et iMac11.2 prennent en charge la protection par mot de passe du micrologiciel facultative (comme l'indique le caractère *), mais pas iMac12.1 ni les versions ultérieures.

**REMARQUE :**

Lorsque l'option de clé FirmwarePasswordMode est définie sur **Facultative**, elle désactive uniquement l'application par le client de la protection par mot de passe du programme interne. Elle ne supprime **pas** la protection par mot de passe du programme interne

existante. Vous pouvez supprimer tout mot de passe du programme interne existant à l'aide de l'Utilitaire de mot de passe du programme interne Mac OS X.

Si vous avez l'intention d'utiliser Boot Camp (voir Activation de Mac OS X Boot Camp pour obtenir des instructions) sur des ordinateurs Mac cryptés, vous devez **impérativement** configurer le client de sorte qu'il n'utilise **pas** la protection par mot de passe du programme interne.

Les ordinateurs Mac utilisent la protection par mot de passe du programme interne pour améliorer la sécurité d'accès à l'ordinateur. Sur les ordinateurs Mac, la protection est *désactivée*. Pendant l'installation du client, qu'il s'agisse d'une nouvelle installation ou d'une mise à niveau à partir d'une version antérieure, vous pouvez modifier le fichier com.dell.ddp.plist existant pour que la clé *FirmwarePasswordMode* puisse être définie sur le paramètre *Requis* ou *Facultatif*. L'option *Requise* est le paramètre par défaut, tandis que lorsque le paramètre *Facultatif* est défini, la protection par mot de passe n'est pas appliquée. Après l'installation ou la mise à niveau, le client évalue le fichier com.dell.ddp.plist du programme d'installation modifié pendant le redémarrage.

**REMARQUE :**

Pour empêcher les utilisateurs de modifier la posture de l'ordinateur en matière de sécurité, le client n'accepte pas les modifications de la clé FirmwarePasswordMode après l'installation du logiciel client.

Vous pouvez modifier la valeur de cette clé après l'installation ou la mise à niveau en lançant un processus de décryptage du disque, suivi d'une réactivation du cryptage.

Pour que la protection par mot de passe de micrologiciel Mac OS X soit **requise**, suivez les procédures d'installation/de mise à niveau du client présentées dans Installation/mise à niveau d'Encryption Client for Mac.

# Utilisation de Boot Camp

## Prise en charge de Boot Camp pour Mac OS X

**REMARQUE :**

Lors de l'utilisation de Boot Camp, Dell Encryption Enterprise ne chiffre pas le système d'exploitation Windows. En outre, si l'appareil présente deux partitions macOS amorçables ou davantage, Encryption Enterprise chiffre uniquement le volume principal.

Boot Camp est un utilitaire fourni avec Mac OS X qui vous aide à installer Windows sur les ordinateurs Mac dans une configuration de double démarrage. Boot Camp est pris en charge par les systèmes d'exploitation Windows suivants :

- Windows 7 et 7 Home Premium, Professional et Ultimate (64 bits)
- Windows 8,1 et 8.1 Pro (64 bits)

**REMARQUE :**

Windows 7 est compatible avec Boot Camp 4 ou 5.1. Windows 8.1 et les versions ultérieures sont compatibles uniquement avec Boot Camp 5.1.

Pour utiliser Endpoint Security Suite Enterprise pour Windows dans Boot Camp sur un ordinateur sur lequel Endpoint Security Suite Enterprise pour Mac est installé, le volume système doit être chiffré via le client Encryption pour Mac à l'aide de FileVault2. Voir Installation/mise à niveau avec la ligne de commande pour obtenir des instructions.

**REMARQUE :**

Si votre partition Windows est un candidat pour Encryption External Media, assurez-vous de la placer sur la liste autorisée, sinon elle sera chiffrée. Voir Copier une règle de liste autorisée.

**REMARQUE :**

Vous devez vous assurer que Windows est installé avant de déployer des règles client permettant le cryptage. Après que le client commence le processus de cryptage, il rejette les opérations de partition de disque requises par Boot Camp.

## Récupération d'Endpoint Security Suite Enterprise pour Windows sur Boot Camp

Pour récupérerEndpoint Security Suite Enterprise pour Windows exécuté dans un volume Boot Camp, vous devez également créer un volume Boot Camp sur un disque externe.

**Pré-requis**

- Un disque de démarrage externe
- L'ID de périphérique/ID unique de l'ordinateur à récupérer. Dans la plupart des cas, vous pouvez trouver l'ordinateur ciblé pour la restauration dans la console de gestion en recherchant le nom d'utilisateur de son propriétaire et en examinant les périphériques chiffrés pour cet utilisateur. Le format de l'ID de périphérique/ID unique est « MacBook.Z4291LK58RH de Pierre Dupont ».

**Processus**

1. Sur un disque externe, créez un volume Boot Camp.

   Les étapes sont similaires à la création d'un volume Boot Camp sur votre système local. Voir http://www.apple.com/support/bootcamp/.

2. À partir de la console de gestion, copiez le bundle de restauration sur l'un des périphériques suivants :
   - Lecteur USB de démarrage

     ou

   - Partition FAT sur le volume Boot Camp externe
3. Arrêtez l'ordinateur doté du volume Boot Camp à récupérer.
4. Connectez le disque externe à l'ordinateur.

   Ce disque contient le volume Boot Camp créé à l'étape 1.

5. Pour démarrer l'ordinateur à partir du disque Boot Camp externe, effectuez l'une des opérations suivantes :
   - Appuyez de façon prolongée simultanément sur les touches **Commande** et **R** avant la sonnerie de démarrage/d'auto-test et pendant le démarrage de l'ordinateur.

     ou

   - Pour les versions antérieures d'Apple, appuyez sur la touche **Option** lors de la mise sous tension de l'ordinateur.

     La boîte de dialogue *Utilitaires Mac OS X* s'affiche.
6. Sélectionnez le volume Boot Camp (Windows) qui se trouve sur le disque externe.
7. Dans le lecteur USB ou la partition FAT, cliquez avec le bouton droit sur le bundle de récupération (à partir de l'étape 2) et sélectionnez **Exécuter en tant qu'administrateur**.
8. Cliquez sur **Oui**.
9. Dans la boîte de dialogue Dell Encryption Enterprise, sélectionnez une option :
   - *Mon système ne parvient pas à démarrer* - Si l'utilisateur ne peut pas démarrer le système, sélectionnez la première option

     ou

   - *Mon système ne me permet pas d'accéder à des données chiffrées* - Si l'utilisateur ne peut pas accéder à certains fichiers chiffrés lors de la connexion au système, sélectionnez la deuxième option.
10. Cliquez sur **Suivant** .

    L'écran Informations de sauvegarde et de récupération s'affiche.

11. Cliquez sur **Suivant** .
12. Sélectionnez le volume Boot Camp à récupérer.

    **REMARQUE :**

    Ce n'est **pas** le volume externe Boot Camp.
13. Cliquez sur **Suivant** .
14. Saisissez le mot de passe associé au fichier.
15. Cliquez sur **Suivant** .
16. Cliquez sur **Récupérer**.
17. Cliquez sur **Terminer**.
18. Lorsque vous êtes invité à redémarrer, cliquez sur **Oui**.
19. Le système redémarre, et vous pouvez vous connecter à Windows.

# Récupération d'un mot de passe du programme interne

Même si l'ordinateur client est configuré pour appliquer un mot de passe du programme interne, celui-ci n'est pas forcément nécessaire pour effectuer la récupération. Si l'ordinateur à récupérer peut être démarré, configurez la cible de démarrage dans le volet Disque de démarrage de Préférences Système.

Dans le cas où le mot de passe du programme interne est nécessaire pour accomplir la récupération (si l'ordinateur ne peut pas être démarré et la protection par mot de passe du programme interne est appliquée), suivez les étapes ci-dessous.

Pour récupérer le mot de passe du programme interne, vous devez d'abord récupérer le bundle de récupération contenant les clés de cryptage du disque.

1. Connectez-vous à la console de gestion en tant qu'administrateur Dell.
2. Dans le volet de gauche, cliquez sur **Populations > Points de terminaison**.
3. Recherchez le périphérique à récupérer.
4. Cliquez sur le périphérique pour ouvrir la page des détails du point de terminaison.
5. Cliquez sur l'onglet **Détails et actions**.
6. Sous *Détails de la protection*, cliquez sur le lien **Clés de restauration de périphérique**.
7. Pour enregistrer le bundle de récupération sur le volume de récupération externe ou sur l'ordinateur qui exécutera l'utilitaire de récupération pour effectuer l'opération de récupération, cliquez sur **Télécharger**, puis sur **Enregistrer**.
8. Ouvrez le bundle de récupération pour récupérer le mot de passe du programme interne de l'ordinateur cible à récupérer. Le mot de passe du programme interne se trouve dans les balises de chaîne qui suivent la clé **FirmwarePassword**.

   Par exemple :

   <key>FirmwarePassword</key>

   <string>Bo$vun8WDn</string>

# Outil client

L'outil client est une commande shell qui s'exécute sur un point de terminaison Mac. Il sert à activer le client à partir d'un emplacement distant ou à exécuter un script via un utilitaire de gestion à distance. En tant qu'administrateur, vous pouvez activer un client et faire ce qui suit :

- Activer en tant qu'administrateur
- Activer temporairement
- Récupérer des informations du client Mac

Pour utiliser l'outil client manuellement, ouvrez une session ssh et entrez la commande désirée sur la ligne de commande.

Exemple :

/Library/PreferencePanes/Dell\ Encryption\Enterprise.prefPane/Contents/Helpers/**client -at** *domainAccount domainPassword*

Entrez seulement **client** pour afficher les instructions d'utilisation.

/Library/PreferencePanes/Dell\ Encryption\Enterprise.prefPane/Contents/Helpers/client

### Tableau 1. Commandes de l'outil client

| Commande | Objectif | Syntaxe | Résultats |
|---|---|---|---|
| Activer | Active un client Mac avec Dell Server sans passer par l'interface utilisateur. Pour l'activation, un nom d'utilisateur de domaine et un mot de passe valides doivent être entrés.<br><br>Avec l'outil client, vous pouvez activer | -a ComptedeDomaine MotdepassedeDomaine<br><br>-a CompteLocal* ComptedeDomaine MotdepassedeDomaine<br><br>**ComptedeDomaine** est le compte utilisé pour l'activation à l'aide de l'outil client.<br><br>**CompteLocal**, facultatif, correspond à l'utilisateur actuel lorsqu'aucun autre n'est spécifié.<br><br>La commande d'activation est au format suivant : | 0 = Réussite<br><br>2 = Échec de l'activation et raison de l'échec<br><br>6 = Utilisateur introuvable |

**Tableau 1. Commandes de l'outil client (suite)**

| Commande | Objectif | Syntaxe | Résultats |
|---|---|---|---|
| | un autre utilisateur local que celui qui est connecté et lui affecter les informations d'identification du domaine. | client -a <utilisateur à activer*> <UtilisateurdeDomaine> <MotdepassedeDomaine><br>Si vous utilisez la règle *No Auth User List* pour créer des classes d'utilisateurs ne s'activant pas sur Dell Server, vous pouvez éventuellement utiliser l'outil client pour spécifier un autre compte local que celui qui est connecté. Voir Liste des utilisateurs sans authentification à l'étape 3. | |
| Activer temporairement | Active un client Mac sans laisser d'empreinte. | -at ComptedeDomaine MotdepassedeDomaine<br>-at CompteLocal* ComptedeDomaine MotdepassedeDomaine | |
| Disque | Demander l'état du disque | -d | L'état du disque s'affiche, y compris l'ID du disque, l'état du cryptage et les règles.<br>Si des accolades vides apparaissent, cela signifie qu'il n'y a pas de disques cryptés. |
| Changer les clés de récupération FileVault | Changer les clés de récupération des volumes FileVault | -fc IDdePériphérique PhrasedepassedeRécupération<br>-fc IDdePériphérique ClédeRécupérationPersonnelle<br>-fc IDdePériphérique CheminversChaînedeclé MotdepassedeChaînedeclé<br>-fc IDdePériphérique FichierdeRécupération<br>**REMARQUE :** IDdePériphérique doit être un UUID de volume logique ou résolu à exactement un LVUUID. Souvent, un point de montage ou devnode fera l'affaire. | 0 = Réussite<br>7= LVUUID introuvable<br>10 = Échec des identifiants<br>11 = Échec de dépôt |
| Stratégie | Demande les règles du client Mac | -P | Les règles s'affichent |
| Serveur | Interroge Dell Server à propos des mises à jour de règles au nom du client Mac<br>**REMARQUE :** L'interrogation peut prendre plusieurs minutes. | -s | 0 = Réussite<br>Toute autre valeur indique que Dell Server ou le logiciel client Mac était occupé ou ne répondait pas. |
| Test | Tester l'état d'activation du client Mac | -t CompteLocal* | 0 (ComptedeDomaine) = Réussite<br>1 = Non activé<br>6 = Utilisateur introuvable |

**Tableau 1. Commandes de l'outil client (suite)**

| Commande | Objectif | Syntaxe | Résultats |
|---|---|---|---|
| Utilisateur | Demander les informations de l'utilisateur | -u CompteLocal* | Les informations sur le compte utilisateur s'affichent :<br>0 (informations de compte) = Réussite<br>6 = Utilisateur introuvable |
| Version | Demander la version du client Mac | -v | La version du client Mac s'affiche. Par exemple : 8.x.x.xxxx |

* Le compte exécutant l'outil client est utilisé pour le CompteLocal, sauf spécification contraire.

**L'option Plist**

L'option -plist imprime les résultats de la commande avec laquelle elle est associée. Elle suit la commande et doit apparaître avant ses arguments pour faire imprimer les résultats sous forme de plist.

**Exemples**

Library/PreferencePanes/Dell\ Encryption\Enterprise.prefPane/Contents/Helpers/**client -p -plist**

Pour récupérer les règles du client et les imprimer.

Library/PreferencePanes/Dell\ Encryption\Enterprise.prefPane/Contents/Helpers/**client -at -plist** *localAccount domainAccount domainPassword*

Pour activer temporairement le client et imprimer le résultat.

Library/PreferencePanes/Dell\ Encryption\Enterprise.prefPane/Contents/Helpers/**client -s ; echo$?**

Pour interroger Dell Server à propos des mises à jour de règles au nom du client et les afficher à l'écran.

Library/PreferencePanes/Dell\ Encryption\Enterprise.prefPane/Contents/Helpers/**client -d -plist**

Pour récupérer l'état du disque du client et l'imprimer.

**Codes de retour généraux**

Aucune erreur 0

Erreur de paramètre 4

Commande non reconnue 5

Expiration de socket 8

Erreur interne 9

# 4

# Tâches

**Sujets :**


- Installation d'Advanced Threat Prevention pour Mac
- Vérification de l'installation d'Advanced Threat Prevention
- Collecte de fichiers journaux pour Endpoint Security Suite Enterprise
- Affichage des détails d'Advanced Threat Prevention
- Provision a Tenant
- Configuration de la mise à jour automatique de l'agent Advanced Threat Prevention
- Dépannage d'Advanced Threat Prevention


# Installation d'Advanced Threat Prevention pour Mac

Cette section vous guide dans l'installation de Advanced Threat Prevention.

Il existe deux méthodes d'installation d'Advanced Threat Prevention.

- Installation interactive : cette méthode d'installation est la plus facile. Toutefois, cette méthode ne permet pas les personnalisations.
- Installation par ligne de commande : cette méthode d'installation/de mise à niveau avancée doit être uniquement utilisée par les administrateurs expérimentés en matière de syntaxe de ligne de commande.

## Pré-requis

Dell recommande de suivre les meilleures pratiques informatiques pendant le déploiement du logiciel client. Ceci inclut, sans s'y limiter, les environnements de test contrôlés pour les premiers tests et les déploiements échelonnés pour les utilisateurs.

Avant de démarrer ce processus, assurez-vous que les conditions préalables suivantes sont réunies :

- Assurez-vous que Dell Server et ses composants sont déjà installés.

  Si vous n'avez pas encore installé Dell Server, suivez les instructions figurant dans le guide approprié ci-dessous.

  *Security Management Server Installation and Migration Guide (Guide d'installation et de migration de Security Management Server)*

  *Security Management Server Virtual Quick Start Guide and Installation Guide (Guide de démarrage rapide et Guide d'installation de Security Management Server Virtual)*
- Assurez-vous d'avoir le nom d'hôte du serveur et le port du Dell Server. Vous en aurez besoin pour l'installation du logiciel client.
- Vérifiez que l'ordinateur cible dispose d'une connectivité réseau à Dell Server.
- Si un certificat de serveur du client est manquant ou auto-signé, vous devez désactiver la confiance vis-à-vis du certificat SSL du côté du client uniquement.

# Installation interactive d'Advanced Threat Prevention

Cette section présente le processus d'installation d'Advanced Threat Prevention for Mac.

L'installation interactive constitue la méthode d'installation ou de mise à niveau du package logiciel du client la plus simple. Toutefois, cette méthode ne permet pas les personnalisations.

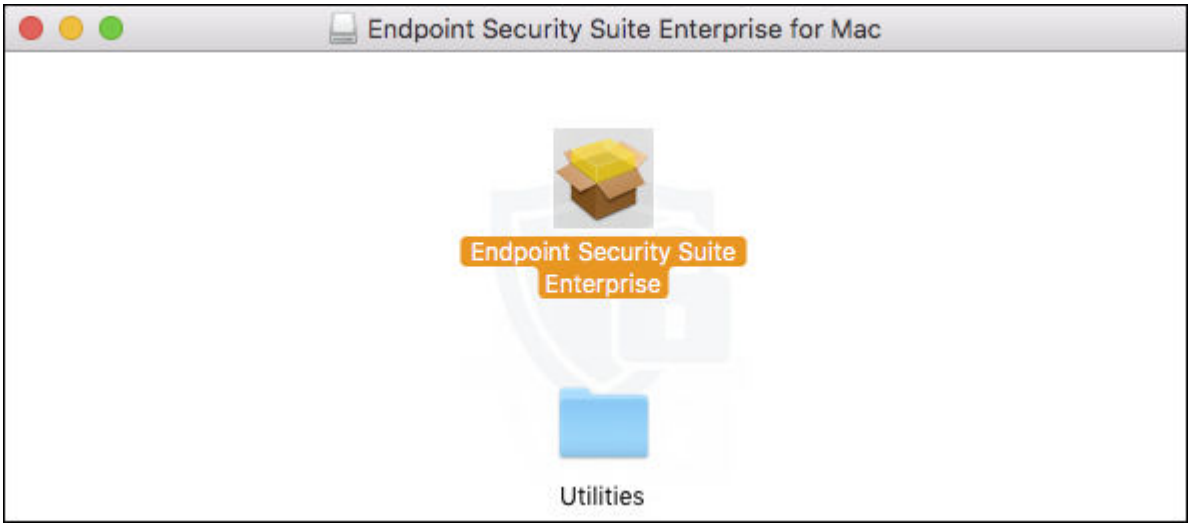
Pour désinstaller le logiciel client, suivez les étapes ci-dessous. Pour effectuer ces étapes, vous devez posséder un compte administrateur.

**REMARQUE :**

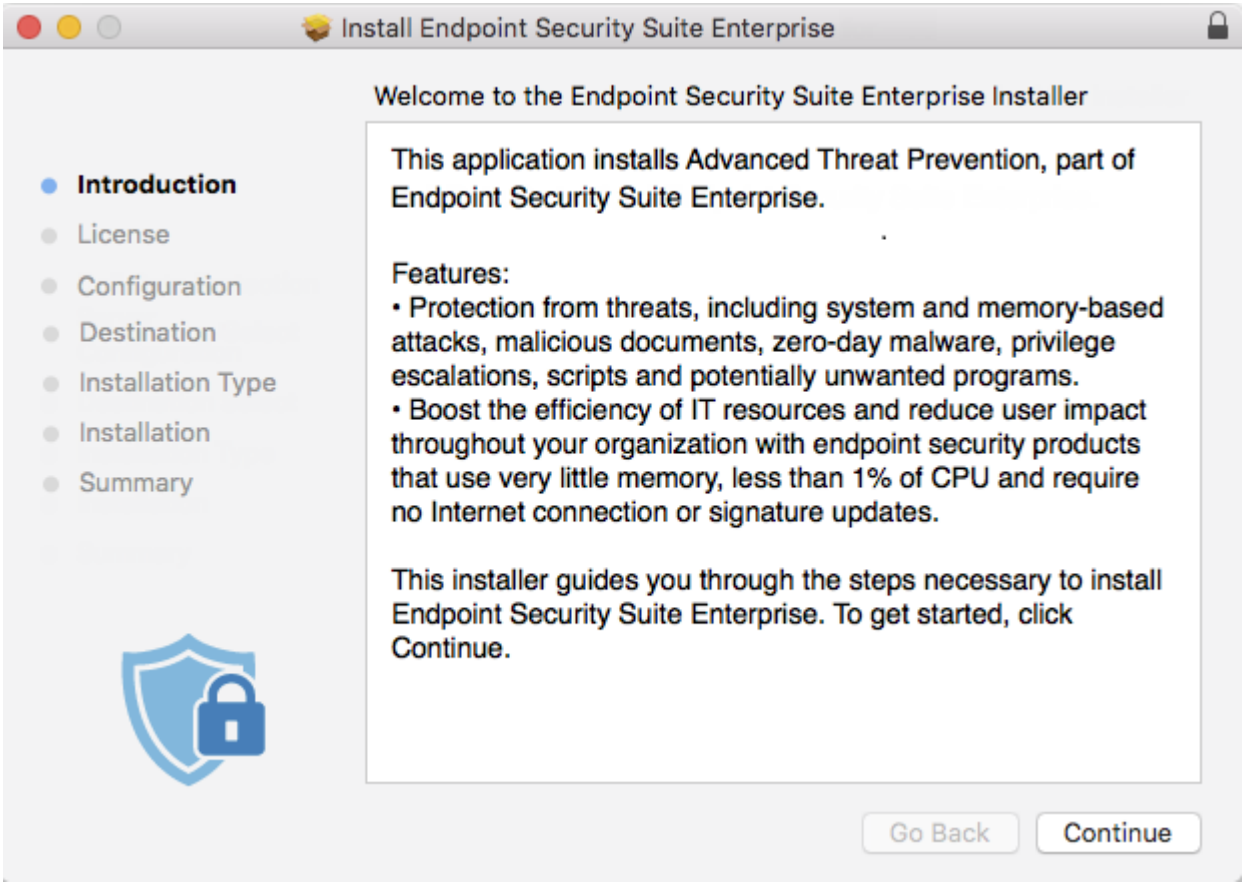
avant de commencer, enregistrez le travail de l'utilisateur et fermez les autres applications.

1. À partir du support d'installation Dell, montez le fichier **Endpoint-Security-Suite-Enterprise-<version>.dmg**.

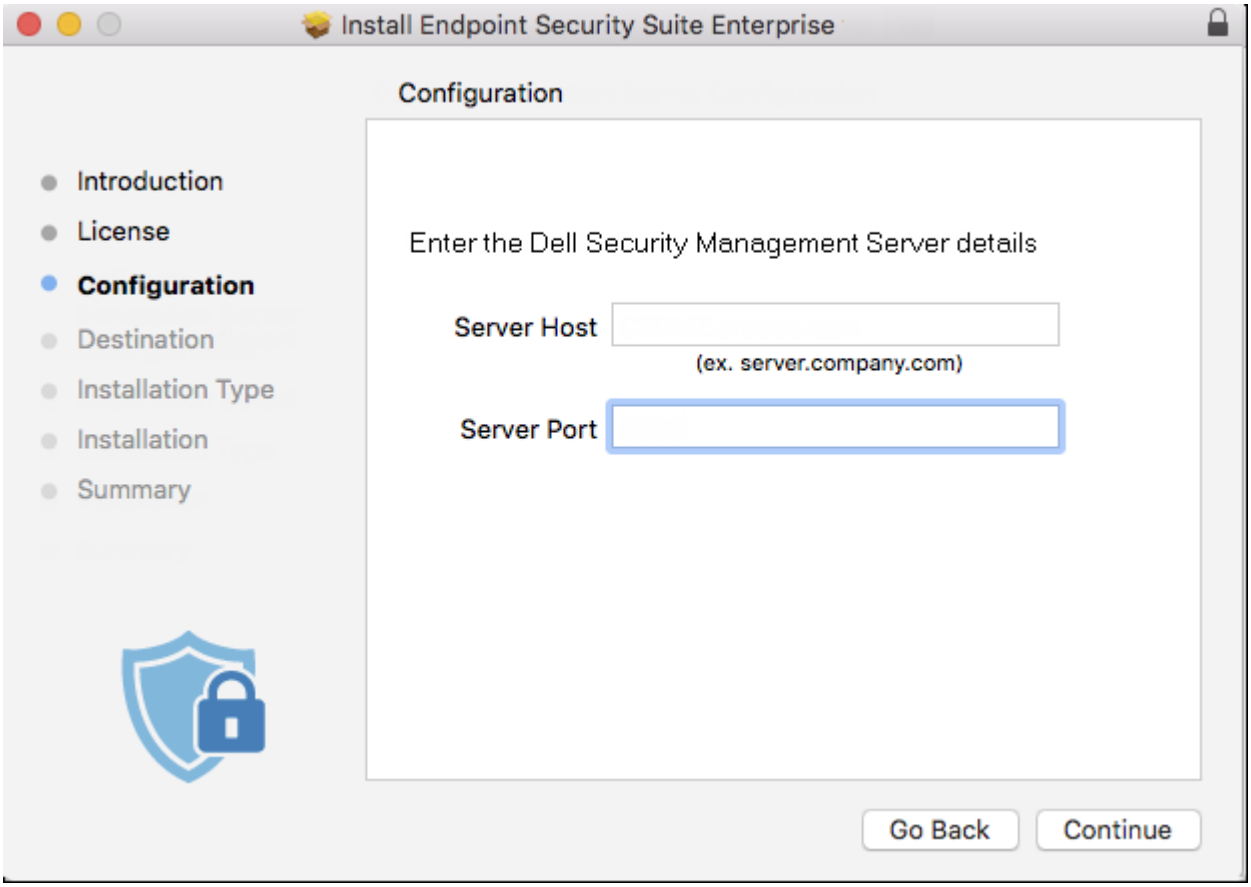
Le package Endpoint Security Suite Enterprise pour Mac s'ouvre.




2. Double-cliquez sur le programme d'installation d'**Endpoint Security Suite Enterprise**. Le message suivant est affiché : *Ce package exécute un programme pour déterminer si le logiciel peut être installé.*
3. Cliquez sur **Continuer**.
4. Lisez le texte d'accueil et cliquez sur **Continuer**.




5. Après avoir lu le contrat de licence, cliquez sur **Continuer**, puis sur **Accepter** pour accepter ses conditions.
6. Dans le champ *Hôte du serveur*, entrez le nom d'hôte complet du Dell Server qui va gérer l'utilisateur cible (par exemple, serveur.entreprise.com).




7. Dans le champ *Port du serveur*, entrez **8888** et cliquez sur **Continuer**.
   Une fois qu'une connexion a été établie, l'indicateur de connectivité passe du rouge au vert.

   **REMARQUE :**

   ce port correspond au port de service du serveur Core, lequel peut être configuré. Le numéro de port par défaut est 8888.
8. Sur l'écran d'installation, cliquez sur **Installer**.
9. Lorsque vous y êtes invité, saisissez les informations d'identification du compte d'administrateur (exigés par l'application Mac OS X Installer), puis cliquez sur **Installer le logiciel**.
10. Une fois l'installation terminée, cliquez sur **Fermer**.
    Le client Advanced Threat Prevention pour Mac est maintenant installé.
11. Fermez le package.
12. Voir Vérification de l'installation d'Advanced Threat Prevention.

Si le système n'est pas enregistré auprès de Dell Server, consultez les journaux pour déterminer si vous disposez d'un certificat valide sur votre Dell Server. Voir Désactivation du certificat SSL de confiance d'Advanced Threat Prevention.

## Désinstallation interactive du client Advanced Threat Prevention

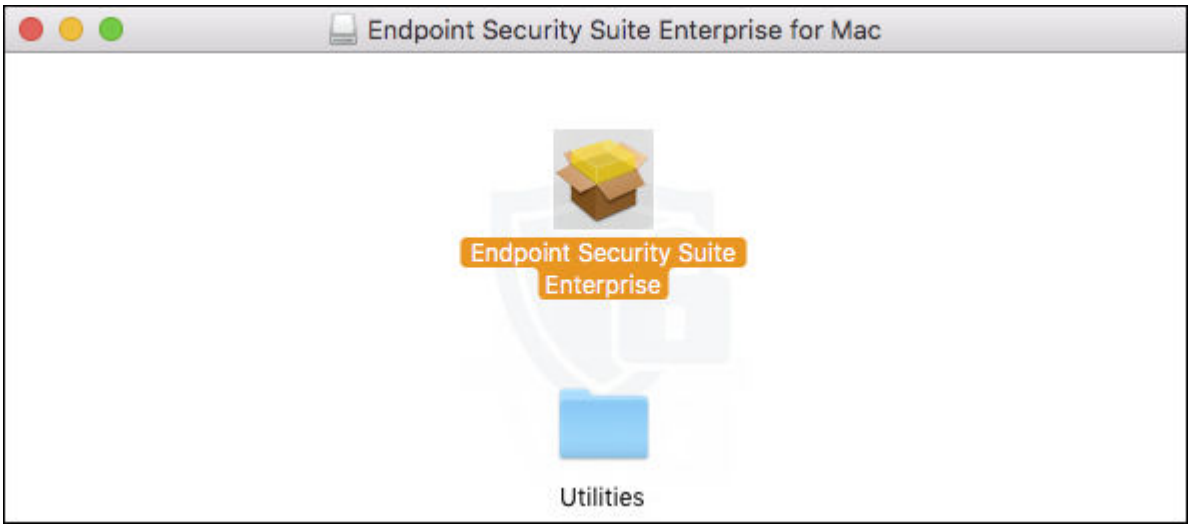
Il est possible de désinstaller le logiciel client en lançant l'application **Désinstaller Endpoint Security Suite Enterprise**. Pour désinstaller le logiciel client, suivez les étapes ci-dessous.

1. Montez le fichier Endpoint-Security-Suite-Enterprise-<version>.dmg.
2. Dans le dossier Utilitaires, lancez l'application **Désinstaller Endpoint Security Suite Enterprise**.
3. Cliquez sur **Uninstall** (Désinstaller).
4. Lorsque vous y êtes invité, entrez les informations d'identification du compte d'administrateur (exigés par l'application Mac OS X Installer), puis cliquez sur **OK**.
   Les messages affichent l'état de la désinstallation.
5. Lorsque la réussite de la désinstallation est confirmée, cliquez sur **OK**.
   Advanced Threat Prevention pour Mac est désormais désinstallé. Vous pouvez utiliser l'ordinateur normalement.

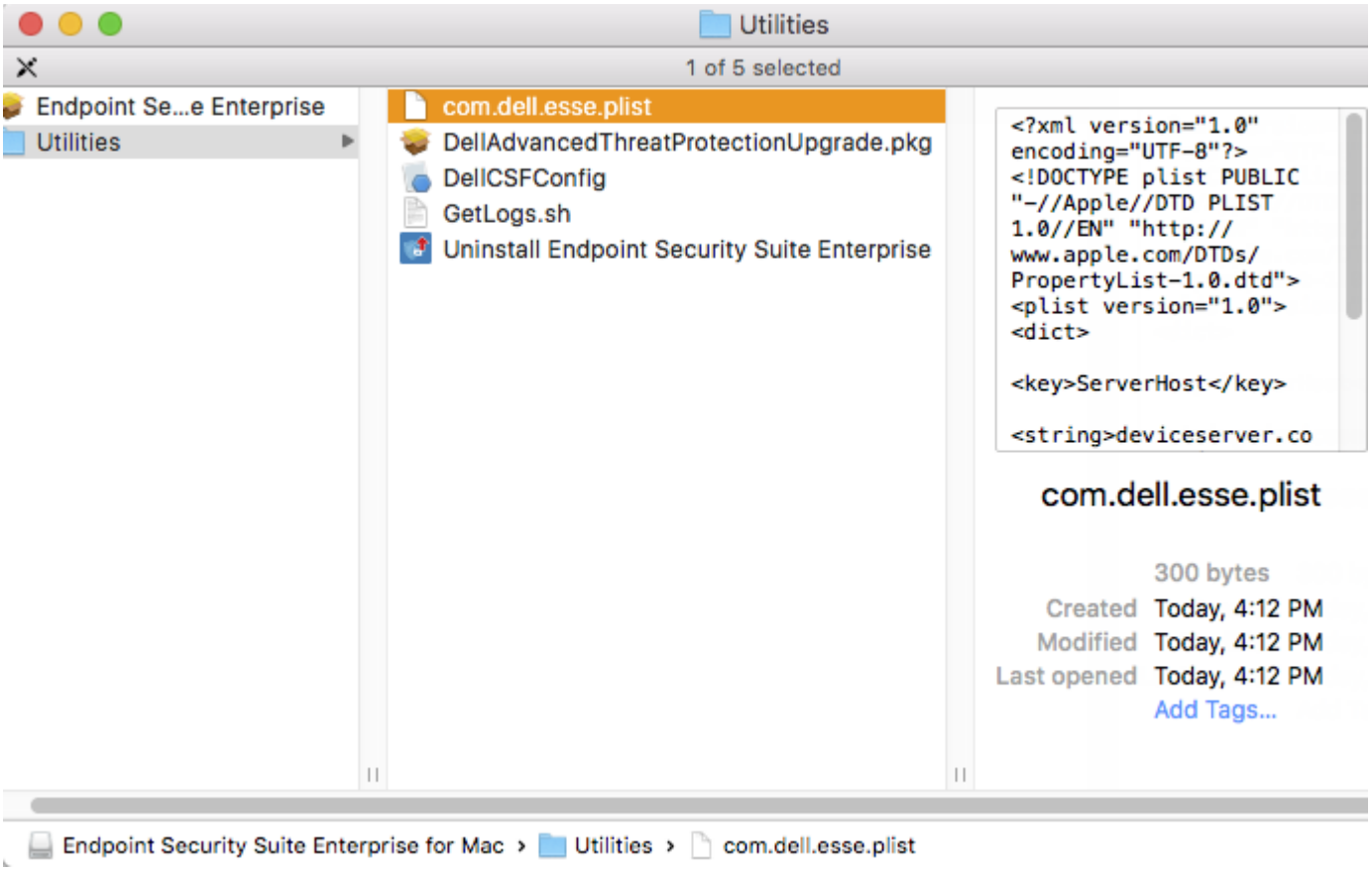
# Installation d'Advanced Threat Prevention avec la ligne de commande

Pour installer le client Advanced Threat Prevention à l'aide de la ligne de commande, suivez les étapes ci-dessous.

1. À partir du support d'installation Dell, montez le fichier Endpoint-Security-Suite-Enterprise-<version>.dmg. Le package Endpoint Security Suite Enterprise pour Mac s'ouvre.




2. Depuis le dossier Utilitaires, copiez le fichier **com.dell.esse.plist** sur le disque local.




3. Ouvrez le fichier .plist.
4. Remplacez les valeurs des espaces réservés par le nom d'hôte complet de Dell Server qui gèrera l'utilisateur cible, comme serveur.entreprise.com, et le numéro de port **8888** :

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/
PropertyList-1.0.dtd">
```

```
<plist version="1.0">
<dict>
  <key>ServerHost</key>
  <string>server.organization.com</string>
  <key>ServerPort</key>
  <string>8888</string>
  <array>
</dict>
</plist>
```

**REMARQUE :**

ce port correspond au port de service du serveur Core, lequel peut être configuré. Le numéro de port par défaut est 8888.

5. Enregistrez le fichier, puis fermez-le.
6. Pour chaque ordinateur ciblé, copiez le programme d'installation du package Endpoint Security Suite Enterprise **pour Mac** dans un dossier temporaire et le fichier **com.dell.esse.plist** modifié dans **/Library/Preferences**.
7. Si vous y êtes invité, entrez vos informations d'identification.
8. Lancez une fenêtre de terminal.
9. Effectuez une installation par ligne de commande du package à l'aide de la commande **installer** :
   **sudo installer -pkg /Volumes/Endpoint\ Security\ Suite\ Enterprise\ for\ Mac/Endpoint\ Security\ Suite\ Enterprise.pkg -target /**

   **REMARQUE :**

   le chemin -pkg correspond au chemin d'accès au programme d'installation inclus dans le fichier .dmg.
10. Appuyez sur **Entrée**.
11. Voir Vérification de l'installation d'ESSE Advanced Threat Prevention.

## Désinstallation d'Advanced Threat Prevention pour Mac avec la ligne de commande

Pour désinstaller le client Advanced Threat Prevention à l'aide de la ligne de commande, suivez les étapes ci-dessous.

1. Lancez une fenêtre de terminal.
2. Effectuez une installation du package à partir de la ligne de commande en utilisant la commande **uninstaller** :
   **sudo /Volumes/Endpoint\ Security\ Suite\ Enterprise\ for\ Mac/Utilities/Uninstall\ Endpoint\ Security\ Suite\ Enterprise.app/Contents/MacOS/Uninstall\ Endpoint\ Security\ Suite\ Enterprise --noui**

   **REMARQUE :** Assurez-vous que le commutateur --noui est inclus à la fin de la commande.
3. Appuyez sur **Entrée**.
   Advanced Threat Prevention pour Mac est désormais désinstallé. Vous pouvez utiliser l'ordinateur normalement.

# Dépannage d'Advanced Threat Prevention pour Mac

## Désactivation du certificat SSL de confiance ou de la vérification des stratégies d'Advanced Threat Prevention

Si un certificat de serveur du client est manquant ou auto-signé, vous devez désactiver la confiance vis-à-vis du certificat SSL du côté du client uniquement.

Si vous exécutez des certificats auto-signés dans votre environnement, désactivez la vérification des stratégies.

Si votre environnement contient des certificats auto-signés et si vous n'avez pas importé le certificat dans le trousseau de votre Mac, définissez les deux options DisableCertTrust et DisablePolicyCheck sur Faux.

1. Sur le client, lancez une fenêtre de terminal.
2. Entrez le chemin d'accès à DellCSFConfig.app :

   ```
   cd /Volumes/Endpoint\ Security\ Suite\ Enterprise\ for\ Mac/Utilities/DellCSFConfig.app/Contents/MacOS/
   ```
3. Exécutez DellCSFConfig.app :

```
sudo DellCSFConfig.app/Contents/MacOS/DellCSFConfig
```

Les paramètres par défaut sont indiqués ci-après :

```
Current Settings:
ServerHost = deviceserver.company.com
ServerPort = 8888
DisableCertTrust = False
DisablePolicyCheck = False
DumpXmlInventory = False
DumpPolicies = False
```

4. Saisissez **-help** pour répertorier les options.
5. Pour désactiver le certificat SSL de confiance sur le client, définissez `DisableCertTrust` sur **Vrai**.
6. Pour désactiver la vérification de la signature des stratégies sur le client, définissez `DisablePolicyCheck` sur **Vrai**.

## Ajout de modifications de règles et d'inventaire XML au dossier Journaux

Pour ajouter le fichier inventory.xml ou policies.xml au dossier Journaux :

1. Exécutez le fichier DellCSFConfig.app, comme indiqué ci-dessus.
2. Définissez DumpXmlInventory sur **Vrai**.
3. Définissez DumpPolicies sur **Vrai**.

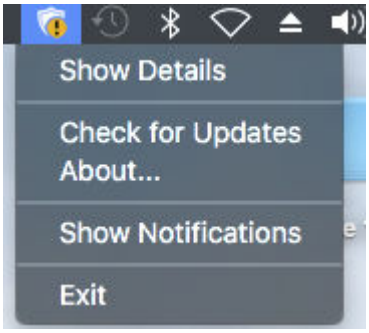
   Les fichiers de règles sont vidés uniquement en cas de modification de règle.

4. Pour afficher les journaux inventory.xml et policies.xml, accédez à **/Library/Application\ Support/Dell/Dell\ Data\ Protection/**.

# Vérification de l'installation d'Advanced Threat Prevention

Si vous le souhaitez, vous pouvez vérifier l'installation.

1. Assurez-vous que l'icône d'Advanced Threat Prevention s'accompagne d'un badge vert  dans la barre de commande.
2. Si un point d'exclamation s'affiche sur l'icône, faites un clic droit dessus, puis sélectionnez **Afficher les détails**). Ce problème peut indiquer que vous n'êtes pas enregistré.

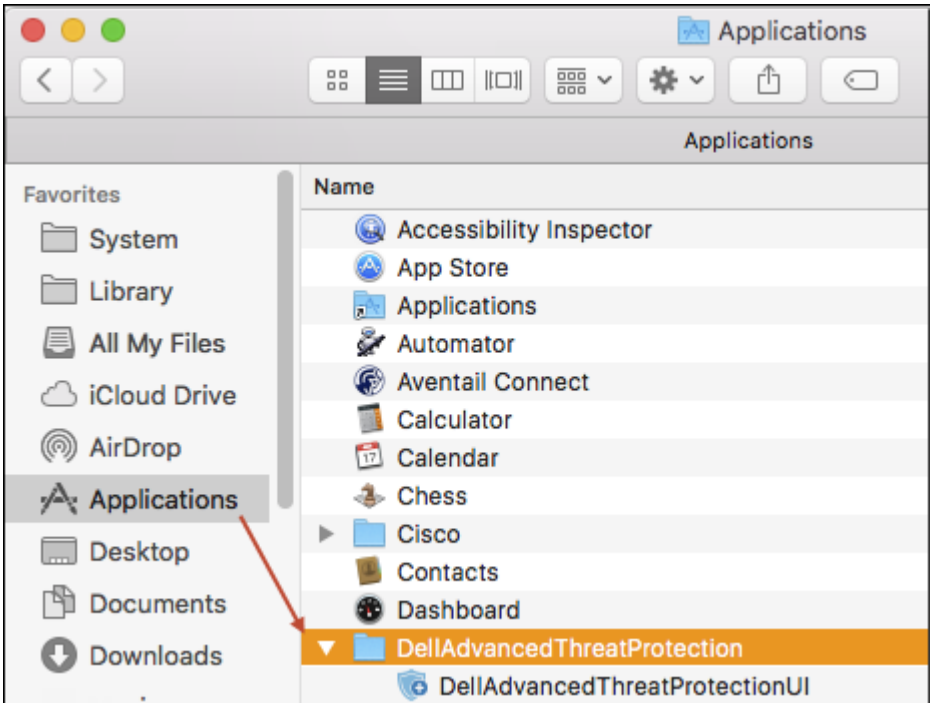



**Rechercher des mises à jour** : recherche des mises à jour du moteur Advanced Threat Prevention, mais pas des règles de Dell Server.

**À propos** : affiche les éléments suivants :

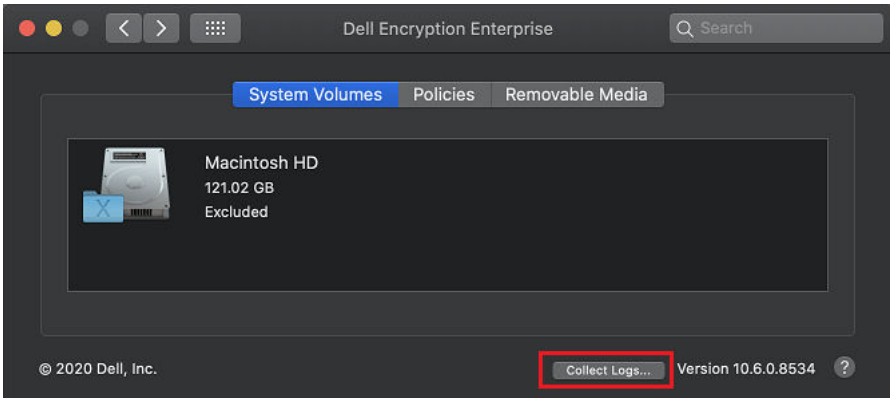
- Version
- Règle : [en ligne] indique une règle basée sur le serveur et [hors ligne] désigne une règle basée sur Airgap ou hors ligne.
- N° de série : à utiliser pour contacter le support. Il s'agit de l'identificateur unique de l'installation.

3. Le dossier Advanced Threat Prevention est créé sous /Applications.




# Collecte de fichiers journaux pour Endpoint Security Suite Enterprise

Dans *Préférences système* > *Dell Encryption Enterprise* > *Volumes système*, le bouton *collecter les journaux* en bas à droite permet à un administrateur de pré-générer des journaux pour le support. Cette action peut avoir un impact sur les performances lors de la collecte des fichiers log.




DellLogs.zip contient les journaux du logiciel Encryption Enterprise et Advanced Threat Prevention. Pour plus d'informations sur la collecte des journaux, voir http://www.dell.com/support/article/us/en/19/SLN303924.

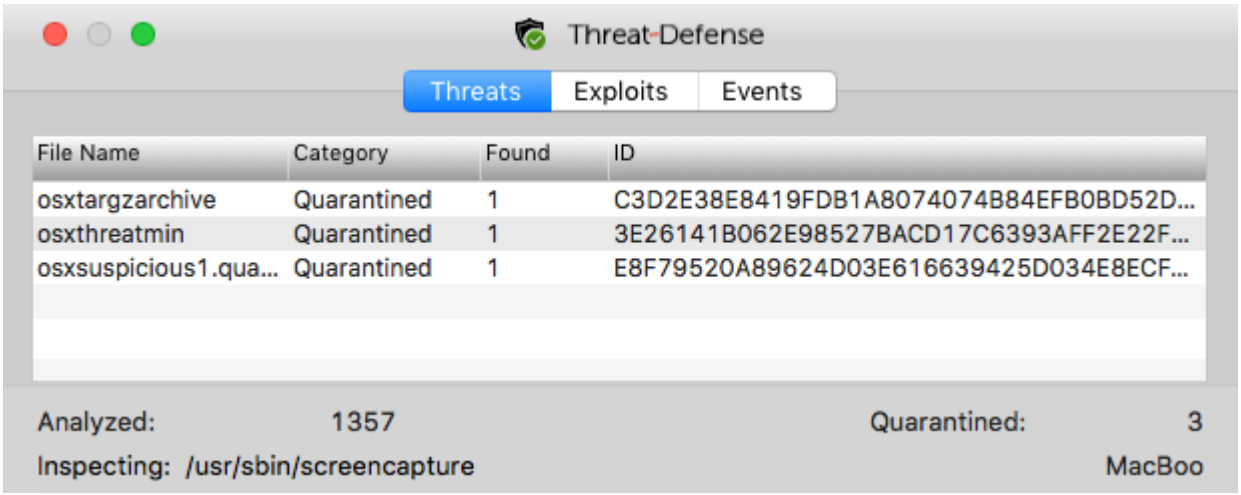
# Affichage des détails d'Advanced Threat Prevention

Une fois que le client Advanced Threat Prevention est installé sur un ordinateur de point de terminaison, il est reconnu par le Dell Server en tant qu'agent.

Cliquez avec le bouton droit sur l'icône Advanced Threat Prevention dans la barre de commande, puis sélectionnez **Afficher les détails**. L'écran Détails d'Advanced Threat Prevention comporte les onglets suivants.

## Onglet Menaces

L'onglet Menaces affiche toutes les menaces détectées sur le périphérique, ainsi que l'action appliquée. Les menaces sont une catégorie d'événements récemment détectés comme fichiers ou programmes potentiellement dangereux qui nécessitent une action corrective guidée.



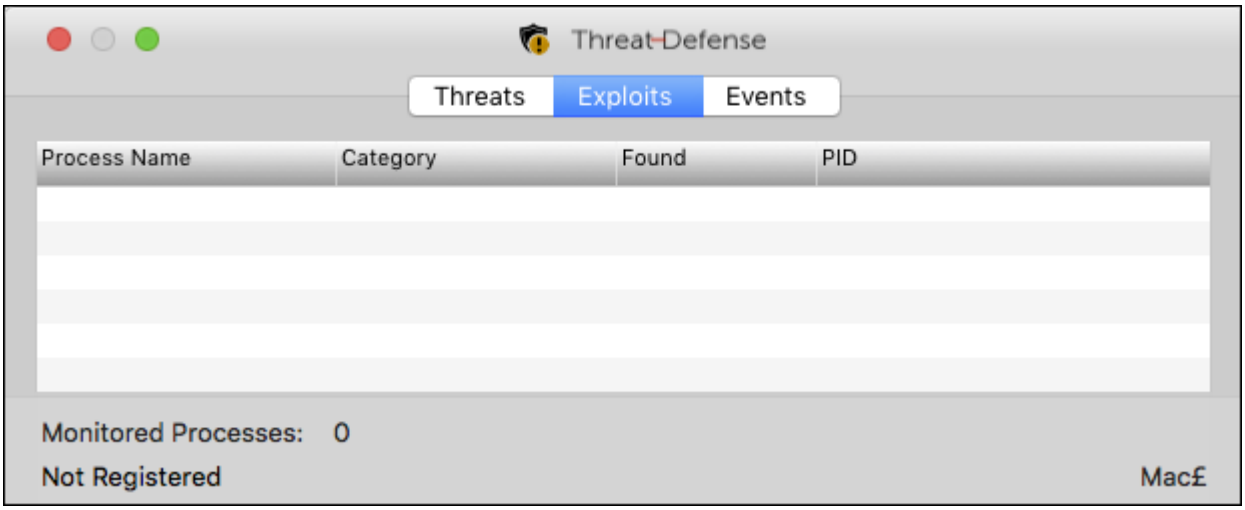

La colonne Catégorie peut inclure les éléments suivants.

- **Dangereux** : fichier suspect qui risque d'être un programme malveillant
- **Anormal** : fichier suspect qui pourrait être un programme malveillant
- **En quarantaine** : fichier déplacé de son emplacement d'origine, stocké dans le dossier de quarantaine et dont l'exécution sur le périphérique est bloquée.
- **Exonéré** : fichier dont l'exécution est autorisée sur le périphérique.
- **Effacé** : fichier effacé de l'organisation. Les fichiers autorisés comprennent des fichiers exonérés, ajoutés à la liste sécurisée et supprimés du dossier Quarantaine sur le périphérique.

Pour plus d'informations sur la classification des menaces d'Advanced Threat Prevention, voir la rubrique *AdminHelp*, disponible dans la console de gestion.

## Onglet Codes malveillants exploitant une faille de sécurité

Cet onglet répertorie les codes malveillants exploitant une faille de sécurité, qui sont considérés comme des menaces.




Les règles du Dell Server déterminent l'action appliquée lorsqu'un code malveillant exploitant une faille de sécurité est détecté :

- **Ignorer** : aucune action n'est appliquée pour les violations de mémoire identifiées.
- **Alerter** : la violation de mémoire est enregistrée et signalée au Dell Server.

- **Bloquer** : bloque l'appel de processus si une application tente d'appeler un processus qui constitue une violation de mémoire. L'application qui a émis l'appel est autorisée à continuer à s'exécuter.
- **Mettre fin** : bloque l'appel de processus si une application tente d'appeler un processus qui constitue une violation de mémoire. L'application qui a lancé l'appel est interrompue.

Les types de code malveillant exploitant une faille de sécurité suivants sont détectés :

- Zone dynamique d'empilement
- Protection de l'empilement
- Recherche dans la mémoire scanner
- Charge malveillante

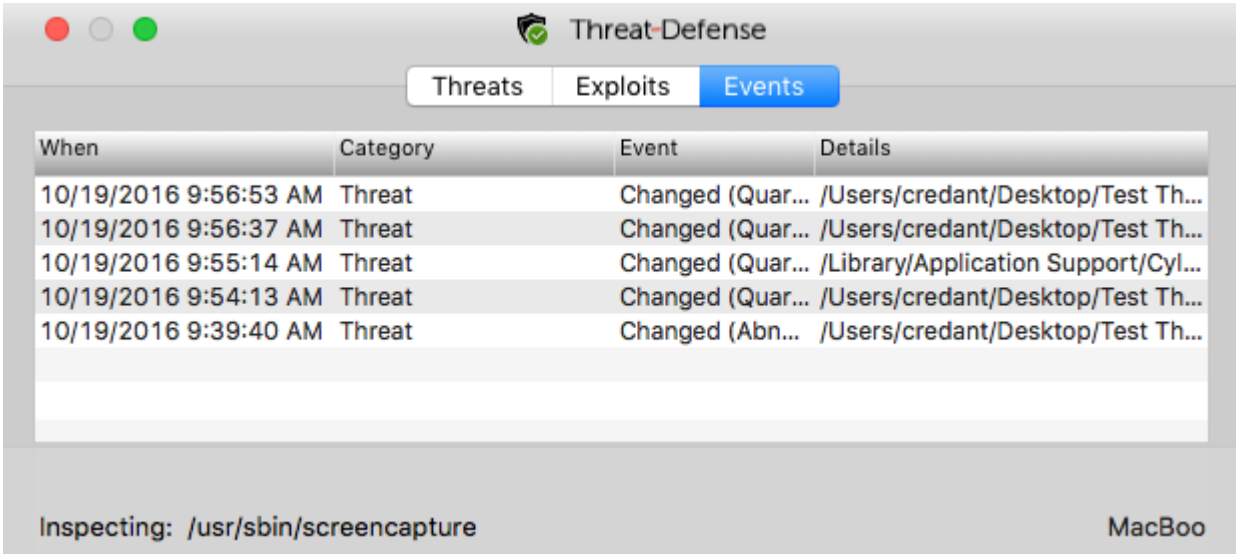
Pour plus d'informations sur les stratégies de code malveillant exploitant une faille de sécurité, voir la rubrique *AdminHelp*, disponible dans la console de gestion.

## Onglet Événements

**REMARQUE :**

Un événement n'est pas nécessairement une menace. Un événement est généré lorsqu'un fichier ou un programme reconnu est mis en quarantaine, placé dans la liste de sécurité ou exonéré.

L'onglet Événements affiche toutes les menaces qui se produisent sur le périphérique et les classe par type d'événement tel qu'attribué par Advanced Threat Prevention. Les données sont supprimées au redémarrage du système.




Les exemples de types d'événement incluent :

Menaces trouvées

Menaces supprimées

Menaces mises en quarantaine

Menaces exonérées

Menaces modifiées

# Provision a Tenant

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

**Pré-requis**

- Doit être effectué par un administrateur doté du rôle Administrateur système.
- Doit disposer d'une connexion à Internet pour provisionner sur Dell Server.
- Doit disposer d'une connexion à Internet sur le client pour afficher l'intégration de service en ligne Advanced Threat Prevention dans la console de gestion.

- Le provisionnement est basé sur un jeton qui est généré à partir d'un certificat pendant le provisionnement.
- Les licences Advanced Threat Prevention doivent être présentes sur Dell Server.

## Provisionner un service partagé

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

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

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

**REMARQUE :**

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

**Mises à jour automatique de l'agent de réception**

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

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

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

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

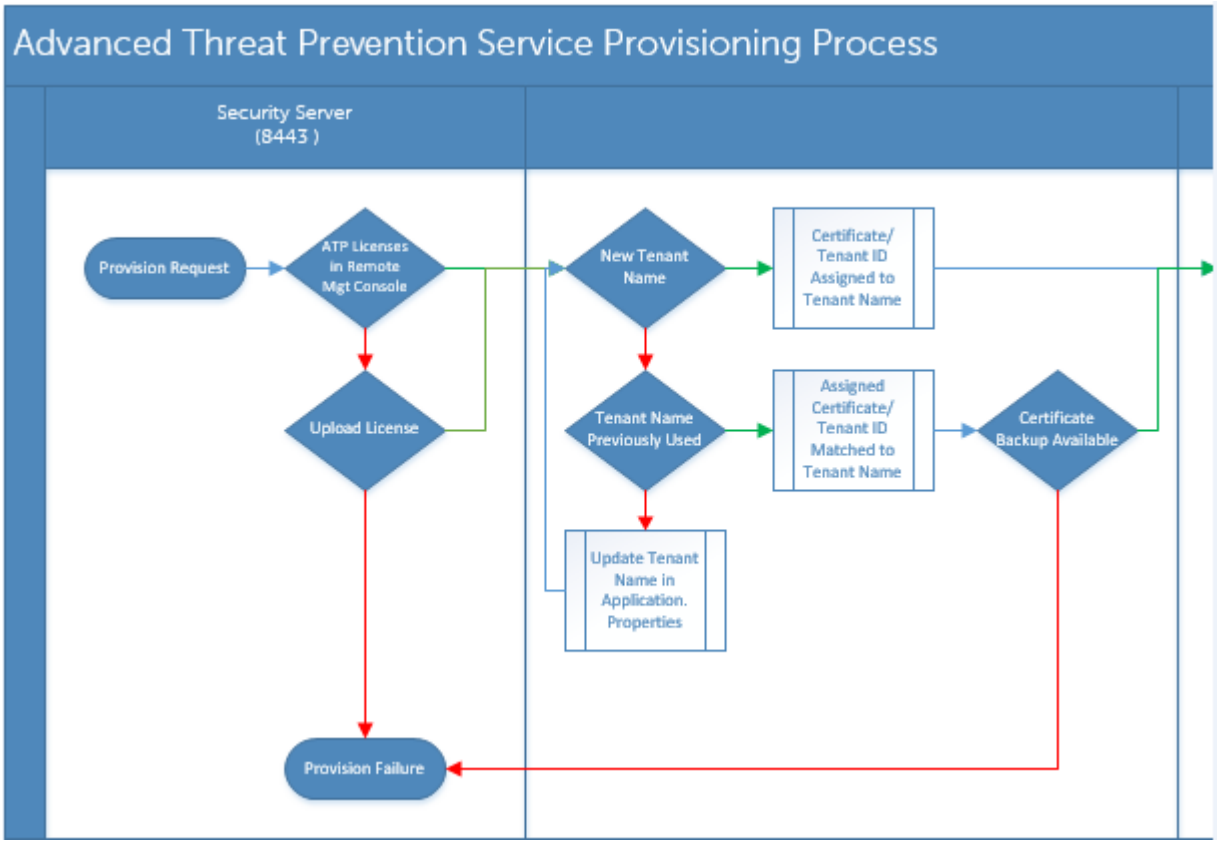
Pour ne plus recevoir les mises à jour automatiques de l'agent :

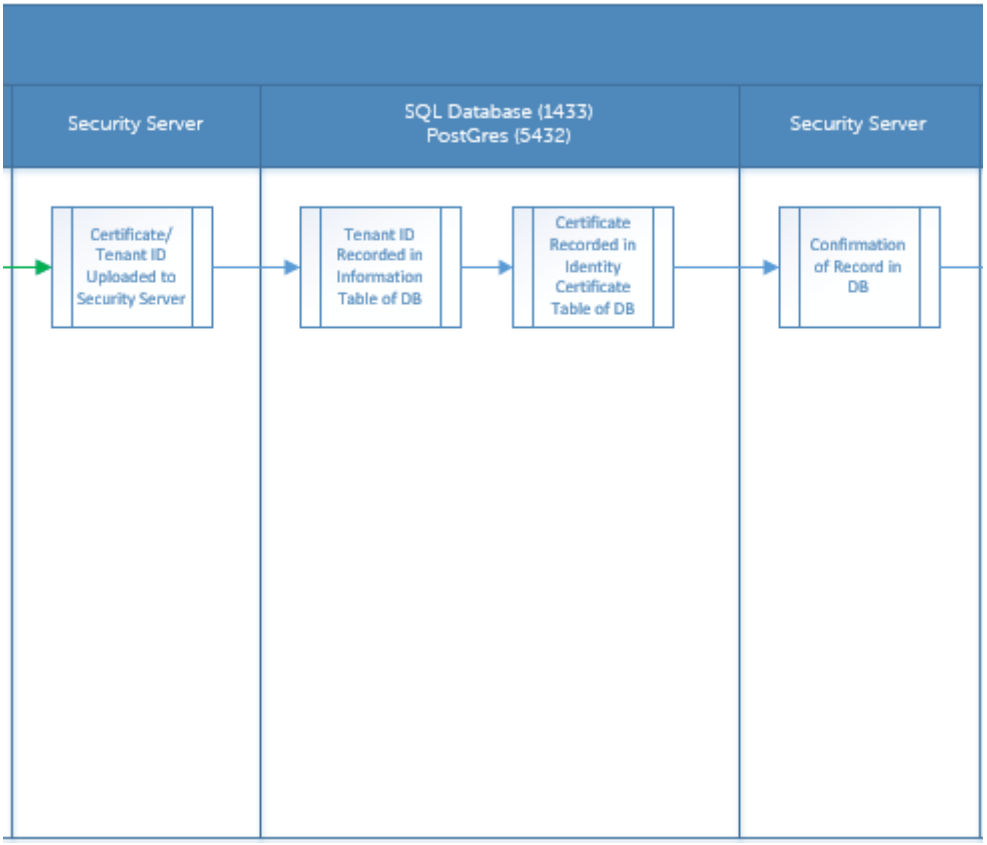
1. Dans le volet de gauche de la console de gestion, cliquez sur **Gestion** > **Services de gestion**.
2. Sur l'onglet *Menaces avancées*, sous *Mise à jour automatique de l'agent*, cliquez sur le bouton **Désactivé**, puis cliquez sur **Enregistrer les préférences**.

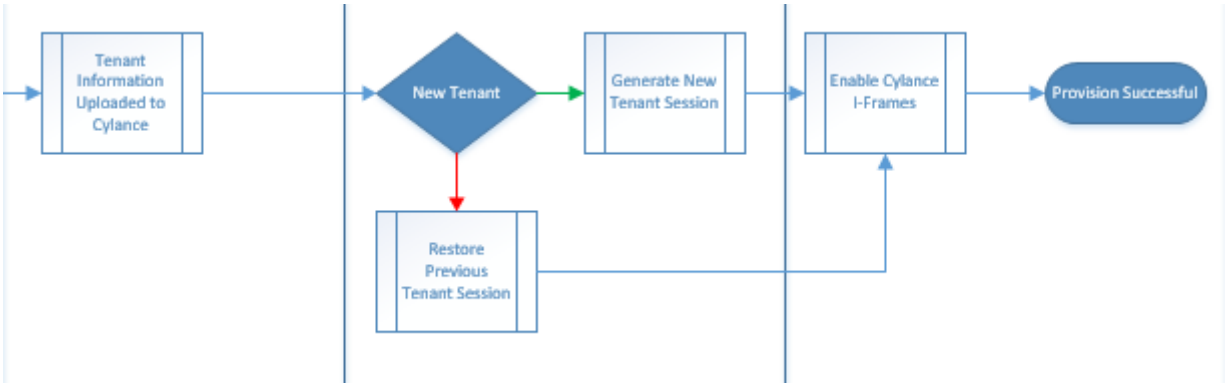
# Dépannage d'Advanced Threat Prevention

## Provisionnement d'Advanced Threat Prevention et communication agent

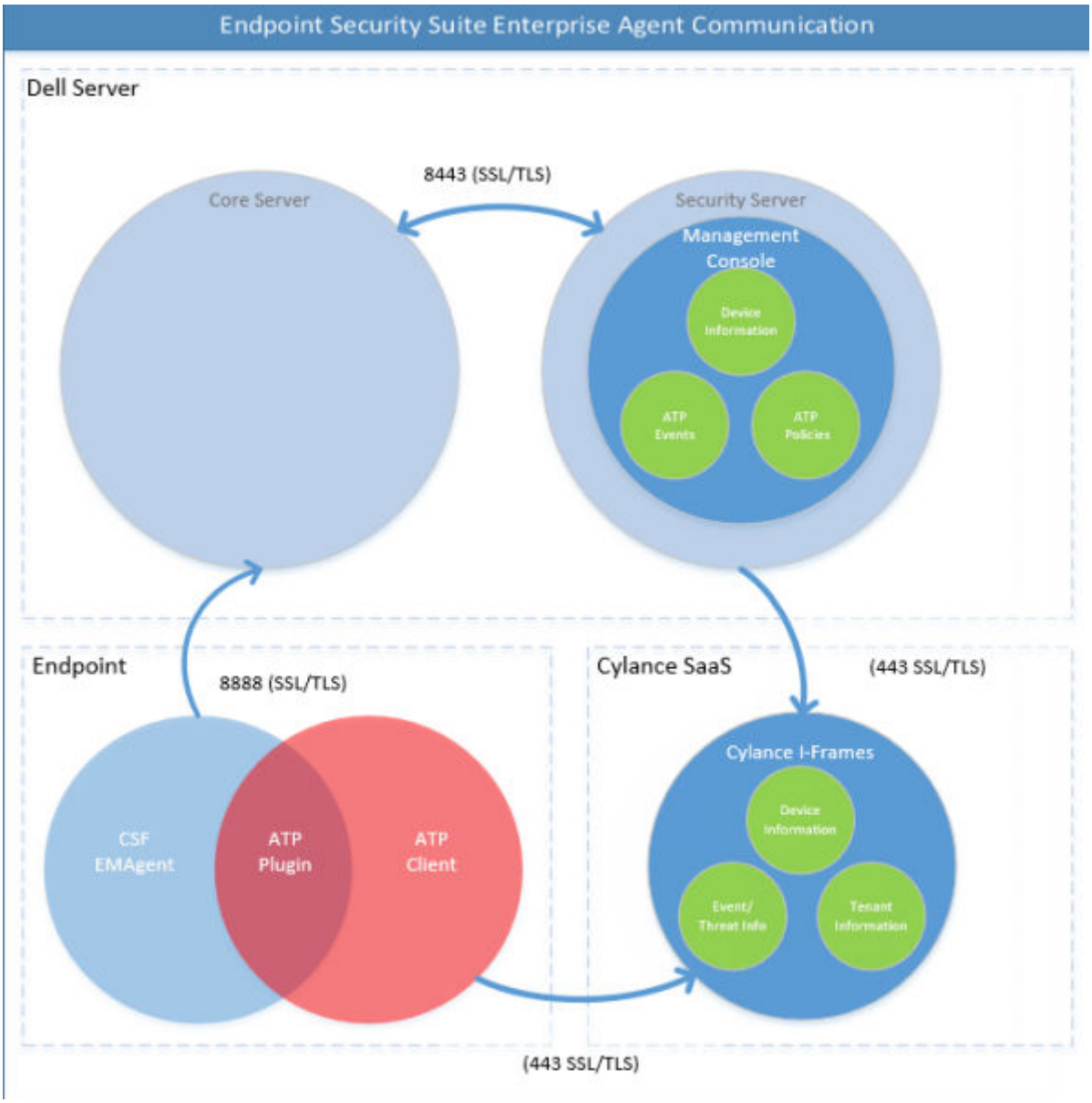
Les diagrammes suivants illustrent le processus de provisionnement du service Advanced Threat Prevention


Advanced Threat Prevention Service Provisioning Process
Security Server
(8443 )
Provision Request
ATP Licenses in Remote Mgt Console
Upload License
Provision Failure
New Tenant Name
Certificate/ Tenant ID Assigned to Tenant Name
Tenant Name Previously Used
Assigned Certificate/ Tenant ID Matched to Tenant Name
Certificate Backup Available
Update Tenant Name in Application. Properties


Security Server
SQL Database (1433)
PostGres (5432)
Security Server
Certificate/ Tenant ID Uploaded to Security Server
Tenant ID Recorded in Information Table of DB
Certificate Recorded in Identity Certificate Table of DB
Confirmation of Record in DB




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



# 5

# Glossaire

**Security Server** : utilisé pour les activations de Dell Encryption.

**Policy Proxy** : utilisé pour distribuer des règles au logiciel client.

**Console de gestion** : console d'administration de Dell Server pour tout le déploiement d'entreprise.

**Bouclier** : vous pourrez parfois rencontrer ce nom dans la documentation et dans les interfaces utilisateur. « Bouclier » est un nom utilisé pour désigner Dell Encryption.