Dell Data Protection | Endpoint Security Suite Enterprise for Mac

Administrator Guide v1.1

Remarques, précautions et avertissements

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

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

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

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

Administrator Guide

2017 - 05

Rev. A02

Contents

1

Introduction

L'Endpoint Security Suite Enterprise for Mac Administrator Guide (Guide de l'administrateur d'Enterprise Edition Endpoint Security Suite Enterprise pour Mac) fournit les informations nécessaires pour déployer et installer le logiciel client.

Sujets :

Présentation

Endpoint Security Suite Enterprise for Mac garantit une protection contre les menaces avancées au niveau du système d'exploitation et de la mémoire, ainsi qu'un cryptage, le tout géré de manière centralisée depuis Dell Data Protection 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 informatiques.

- Endpoint Security Suite Enterprise for Mac : suite de logiciels assurant le cryptage client des données (Client Encryption) et une prévention avancée contre les menaces (Advanced Threat Prevention).
- Proxy de règles : permet de distribuer des règles.
- Serveur de sécurité : assure les activations du logiciel de cryptage client
- Enterprise Server ou Dell Enterprise Server - VE : 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 « serveur Dell », sauf lorsqu'il est nécessaire de désigner une version spécifique (par exemple, une procédure varie en cas d'utilisation du serveur d'entreprise Dell - VE).

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

Endpoint Security Suite Enterprise for 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.

Dell Encryption Client et cryptage FileVault

Il est possible de gérer le cryptage FileVault, ainsi que Dell Encryption Client, avec Endpoint Security Suite Enterprise for Mac. L'option appropriée dépend des exigences de cryptage de l'entreprise. Pour plus d'informations sur les règles de cryptage, voir Cryptage Mac > Cryptage de volume Dell.

Contacter Dell ProSupport

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

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

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 :

Encryption Client

Matériel du client Encryption

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

REMARQUE : Le disque système doit être partitionné avec le schéma de partition GPT (GUID Partition Table) et avoir un format Mac OS X étendu (journalisé).

Matériel

- 30 Mo d'espace disque disponible
- Carte d'interface réseau 10/100/1000 ou Wi-Fi

Encryption Client Software

The following table details supported software.

NOTE: If you intend to perform a major operating system upgrade when using the Dell Encryption client (not FileVault encryption), a decrypt and uninstall operation will be needed followed by regular installation of the Encryption client for Mac on the new operating system.

Operating Systems (64-bit kernels)

- Mac OS X Yosemite 10.10.5
- Mac OS X El Capitan 10.11.6
- macOS Sierra 10.12.4 and 10.12.5

  NOTE: macOS Sierra is supported with the Advanced Threat Prevention Agent 1412 or later.

With Mac OS X El Capitan and higher, when using Dell Encryption Client (not FileVault encryption), you must disable Apple's System Integrity Protection (SIP).

NOTE: For information on disabling, see Interactive Installation/Upgrade and Activation, step 4. Before disabling, see Apple's help for how this impacts security.

NOTE: If you are using a network user account to authenticate, that account must be set up as a mobile account in order to fully configure FileVault 2 management.

The following table details the operating systems supported when accessing Dell-encrypted external media.

NOTE: External Media Shield supports FAT32, exFAT, or HFS Plus (Mac OS Extended) formatted media with Master Boot Record (MBR) or GUID Partition Table (GPT) partition schemes. See Enable HFS Plus.

NOTE: External media must have 55 MB available, plus open space on the media that is equal to the largest file to be encrypted, to host External Media Shield.

Encrypted Media

Windows Operating Systems (32- and 64-bit) Supported to Access Encrypted Media

- Microsoft Windows 7 SP0-SP1
  - Enterprise
  - Professional
  - Ultimate
  - Home Premium
- Microsoft Windows 8
  - Enterprise
  - Pro
  - Windows 8 (Consumer)
- Microsoft Windows 8.1 - Windows 8.1 Update 1
  - Enterprise
  - Pro
- Microsoft Windows 10
  - Enterprise
  - Pro

Mac Operating Systems (64-bit kernels) Supported to Access Encrypted Media

- Mac OS X Yosemite 10.10.5
- Mac OS X El Capitan 10.11.6
- macOS Sierra 10.12.4 and 10.12.5

  NOTE: macOS Sierra is supported with the Advanced Threat Prevention Agent 1412 or later.

With Mac OS X El Capitan and higher, when using Dell Encryption client (not FileVault encryption), you must disable Apple's System Integrity Protection (SIP).

NOTE: For information on disabling, see Interactive Installation/Upgrade and Activation, step 4. Before disabling, see Apple's help for how this impacts security.

Prévention des menaces avancées

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

Matériel 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
- 2 Go de RAM
- 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

REMARQUE : cette version s'applique uniquement à Advanced Threat Prevention, pas au client de cryptage.

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

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

Ports Advanced Threat Protection

- Les agents Advanced Threat Protection 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.

Utiliser	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

Tâches associées à 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 Client for Mac.

Il existe deux méthodes d'installation/de mise à niveau d'Encryption Client for 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, nous permettons la modification du fichier com.dell.ddp.plist pour prendre en charge ces cas. Dès qu'Apple publie une nouvelle version, nous la testons pour vérifier sa compatibilité avec Encryption Client for 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 le serveur Dell et ses composants sont déjà installés.

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

  Enterprise Server Installation and Migration Guide (Guide d'installation et de migration d'Enterprise Server)

  Enterprise Server - Guide de démarrage rapide et Guide d'installation de Virtual Edition
- Assurez-vous de disposer des URLs de serveur de sécurité et de proxy de règles. Vous en aurez 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 aurez 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 le serveur Dell. Le compte d'utilisateur de domaine sera utilisé pour l'activation du logiciel client. La configuration des points de terminaison Mac pour l'authentification de domaine (réseau) n'est pas nécessaire.
- Pour appliquer le cryptage sur l'ordinateur client, commencez par sélectionner l'option de cryptage appropriée pour votre entreprise.

Dell Encryption	Cryptage FileVault
Sélectionnez cette option pour faire ce qui suit : • Crypter toutes les partitions sur le disque de démarrage • Ignorer l'authentification avant démarrage • Utiliser un cryptage à 256 bits **REMARQUE : si vous utilisez Dell Encryption, vous devez désactiver la protection de l'intégrité du système (SIP). Voir Installation/mise à niveau et activation interactives, étape 4.**	Sélectionnez cette option pour faire ce qui suit : • Crypter les disques Fusion Drive • Utiliser l'authentification avant démarrage • Déployer une solution prise en charge par Apple **REMARQUE : si un Mac a un disque Fusion Drive, vous devez activer FileVault pour le crypter.**

Les paramètres de règles de cryptage doivent refléter l'option de cryptage que vous sélectionnez. Avant de définir des règles de cryptage, vérifiez que vous comprenez les règles *Crypter en utilisant FileVault pour Mac* et *Volumes ciblés pour le cryptage*. Pour utiliser Dell Encryption ou le cryptage FileVault, la règle *Cryptage de volume Dell* doit être *activée*.

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

Installation/mise à niveau et activation interactives

Pour installer/mettre à niveau et activer 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. L'ordinateur devra redémarrer tout de suite après l'installation.

1 À partir du support d'installation Dell, montez le fichier Dell-Data-Protection-<version>.dmg.

2 Double-cliquez sur le programme d'installation du package. Le message suivant est affiché :

Ce package va exécuter 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 examiné le contrat de licence, cliquez sur **Continuer**, puis sur **Accepter** pour accepter ses conditions.

Si vous utilisez Dell Encryption avec Mac OS X v10.11 ou version supérieure, la boîte de dialogue *La protection de l'intégrité du système Mac OS est activée* s'affiche. Vous devez désactiver la protection de l'intégrité du système (SIP).

Suivez ces étapes :

a Voir http://www.dell.com/support/Article/us/en/19/SLN299063 pour désactiver la SIP.

b Sur l'assistant, cliquez sur **OK** et poursuivez la *Configuration de Dell Data Protection*.

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 indiqué dans la boîte de dialogue *Authentification* des ordinateurs Windows gérés par un domaine.

8 Dans le champ **Serveur de sécurité :**, entrez le nom d'hôte du serveur de sécurité.

Si votre déploiement n'utilise pas une configuration par défaut, mettez à jour les champs de port et la case **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 de proxy de règles 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, entrez les identifiants de compte administrateur (exigés par l'application Mac OS X Installer), puis 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.**

14 Cliquez sur **Continuer l'installation**. L'installation commence.

15 Une fois l'installation terminée, cliquez sur **Redémarrer**.

16 Continuez pour Activer le client de cryptage pour Mac.

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.

> **REMARQUE : Si vous utilisez Dell Encryption sur Mac OS X v10.11.x, vous devez désactiver la SIP. Voir http://www.dell.com/support/Article/us/en/19/SLN299063.**

1 À partir du support d'installation Dell, montez le fichier Dell-Data-Protection-<version>.dmg.

2 Copiez le package **Install Dell Data Protection** et le fichier **com.dell.ddp.plist** sur le disque local.

3 Dans la console de gestion à distance, 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 à distance.

- **Mode Mot de passe du micrologiciel** : si vous avez l'intention d'utiliser Boot Camp sur des ordinateurs Mac cryptés ou une version d'un système d'exploitation que Dell ne prend pas encore entièrement en charge, vous **devez** définir cette règle sur *Facultative* pour **ne pas** utiliser la protection par mot de passe du micrologiciel. Pour plus d'informations, voir la section À propos de la protection par mot de passe du micrologiciel facultative.

  > **REMARQUE :**
  > Lorsque la règle FirmwarePasswordMode est définie sur **Facultative**, elle désactive uniquement l'application par le logiciel client de la protection par mot de passe du micrologiciel. Elle ne supprime **pas** la protection par mot de passe du programme interne existante. Après la fin de ces étapes, la fin de l'installation, et le redémarrage de l'ordinateur, 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.

- **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 le serveur Dell. Par exemple, dans un établissement scolaire, les enseignants seraient invités à activer leur ordinateur sur le serveur Dell, 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 n'est associé à chaque ordinateur Mac, tous les utilisateurs doivent activer par rapport au serveur Dell, de sorte que Enterprise ne sont donc pas modifier cette propriété. Cependant, si un utilisateur souhaite configurer un média EMS, il doit être authentifié par le serveur Dell.

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 pour 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 de cryptage 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/> [We recommend 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>FirmwarePasswordMode</key>
```

```
  <string>Required</string> [If using Boot Camp, this value must be Optional. For more
information, see About Optional Firmware Password Protection.]
  <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 Data Protection.pkg" -target /
```

8 Redémarrez l'ordinateur à l'aide de la ligne de commande suivante : `sudo shutdown -r now`

9 Continuez pour Activer le client de cryptage pour Mac.

Activation le client de cryptage

Le processus d'activation associe les comptes d'utilisateur réseau dans le serveur Dell 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 workflows 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.

REMARQUE : Pour obtenir des instructions sur l'activation d'un Mac sans domaine, voir l'article de la Base de connaissances SLN302497.

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, appuyez 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 le serveur Dell 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 de cryptage pour Mac est désormais totalement opérationnel et géré par le serveur Dell.

- 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 décrypter 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 demandera à l'utilisateur de permettre l'accès de l'administrateur et obligera 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 cryptage sur l'ordinateur local ou la console de gestion à distance.

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 Data Protection**.

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.

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

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

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

En fonction des exigences de cryptage de votre entreprise, vous pouvez définir des règles pour Dell Encryption ou le cryptage FileVault. Ce tableau répertorie les options de règles de chacun.

Mac Encryption (Cryptage Mac) > Dell Volume Encryption (Cryptage de volume Dell)

Dell Volume Encryption (Cryptage de volume Dell)	*Activation* ou *désactivation* 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. Lorsqu'elle est *activée*, cette règle active et lance le cryptage des volumes non cryptés, conformément à la règle *Volumes ciblés pour le cryptage* **ou** *Crypter en utilisant FileVault pour Mac*. Le paramètre par défaut est *Activé*. Sa désactivation désactive le cryptage et lance l'analyse de décryptage de tous les volumes complètement ou partiellement cryptés.
Cryptage utilisant FileVault pour Mac	Si vous pensez utiliser le cryptage FileVault, commencez par vérifier que Dell Volume Encryption est *activé*.

Assurez-vous que la règle *Crypter en utilisant FileVault pour Mac* est sélectionnée sur le serveur Dell.

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*.

REMARQUE : si vous utilisez Dell Encryption (plutôt que FileVault) et que cette règle est activée, un conflit de stratégies se produit.

REMARQUE :
Si vous avez l'intention d'effectuer une migration depuis le cryptage Dell vers le cryptage FileVault, reportez-vous à la section Effectuer une migration depuis le cryptage de volume Dell vers le cryptage FileVault.

Mac Encryption (Cryptage Mac) > Paramètres généraux Mac

Volumes choisis pour cryptage	*Volume système uniquement* ou *Tous les volumes fixes* Le paramètre *Volume système uniquement* protège uniquement le volume système actif. 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 à distance. Pour localiser une règle spécifique dans *AdminHelp* :

a Cliquez sur l'icône de recherche.

b Dans le champ Recherche, 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 cryptage...	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. 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 cryptage commencera 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 du serveur Dell...	Pour vous assurer que toutes les données cryptées sont récupérables, le logiciel client ne commence pas le processus de cryptage avant la mise en dépôt de toutes les clés de

État	Description
	cryptage auprès du serveur Dell. Le logiciel client interroge la connectivité du serveur de sécurité dans cet état jusqu'à la mise en dépôt des clés de cryptage.
Cryptage en cours...	Une analyse de cryptage est en cours.
Crypté	L'analyse de cryptage est terminée.
Décryptage en cours...	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 cryptage » pour l'analyse de décryptage.
Décrypté	L'analyse de décryptage est terminée.

Couleur	Description
Vert	Partie cryptée
Rouge	Partie non cryptée
Jaune	Partie recryptée 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. Dell Encryption n'est pas pris en charge avec la protection de l'intégrité du système (SIP). Si cette condition incompatible est spécifiée par la règle et que SIP est activée, une erreur apparaît à côté du disque sur l'onglet Volumes système. Pour désactiver SIP, voir installation/ mise à niveau et activation interactives, étape 4.
	Un volume configuré pour le cryptage. Ce badge représente une partition cryptée par Dell.
	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.

Badge	Type et état du volume
 	Plusieurs disques et aucun cryptage. **REMARQUE : l'icône de volume sans badge indique que rien n'a été fait sur le disque. Ce n'est pas un disque de démarrage.**
 	Plusieurs disques où seul le volume système est crypté. Cet exemple décrit une partition cryptée par Dell.

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	État
	Une icône de volume estompée indique un périphérique non monté. Raisons possibles : • L'utilisateur peut avoir choisi de ne pas le provisionner. • Le support peut être bloqué. **REMARQUE : 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 EMS aux supports non protégés est définie sur Lecture seule.
	Support crypté par EMS, désigné par un badge Dell.

Affichage de la règle et de l'état dans la console de gestion à distance

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

1 Connectez-vous à la console de gestion à distance 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 Nom d'hôte ou, si vous connaissez le nom d'hôte du point de terminaison, saisissez-le dans le champ de recherche. Vous pouvez également entrer 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. Vous pouvez entrer 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 Entrez une description des modifications dans la zone de commentaires, puis cliquez sur **Valider les 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

REMARQUE : Seuls les volumes Mac OS X étendu (journalisé) et les disques système qui sont partitionnés avec le schéma de partition GPT (GUID Partition Table) sont pris en charge pour le cryptage.

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 cryptage pour tous les ordinateurs Mac au niveau de la règle d'entreprise. Pour obtenir des instructions supplémentaires sur l'activation du cryptage au niveau de stratégie *Enterprise*, voir *AdminHelp*.

1 Connectez-vous à la Console de gestion à distance 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 la colonne Nom d'hôte ou, si vous connaissez le nom d'hôte du point de terminaison, entrez-le dans le champ de recherche. 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. Vous pouvez entrer 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 cryptage FileVault est activé, aucune autre stratégie du groupe ne sera appliquée. Voir Cryptage Mac > Cryptage de volume Dell.

7 Si le cryptage FileVault est désactivé, modifiez les autres règles comme vous le souhaitez.

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

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 le serveur Dell envoie la règle, dans le volet Stratégies des Préférences de Dell Data Protection, cliquez sur **Actualiser**.

Processus de cryptage

Le processus de cryptage varie en fonction des facteurs suivants :

- Le début du volume de démarrage lorsque le cryptage est activé.
- Le cryptage Dell Encryption ou FileVault est sélectionné.

> **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 Dell Encryption d'un lecteur non crypté
- Cryptage FileVault d'un volume non crypté
- Prise en charge de la gestion d'un volume crypté par FileVault

Cryptage Dell Encryption d'un lecteur non crypté

Après que le logiciel client reçoit la règle de cryptage, il effectue une validation par Utilitaire de disque des volumes ciblés pour le cryptage, puis configure ces volumes pour le cryptage.

1 La barre de progression indique l'état de la vérification. Lorsque la vérification est terminée, les volumes cibles sont configurés pour le cryptage.

Ce processus peut ralentir la réactivité de l'ordinateur pendant quelques minutes. Pour chaque volume en attente de cryptage, une boîte de dialogue indiquant que l'opération se déroule est affichée à l'utilisateur.

2 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 à distance, le logiciel client peut inviter l'utilisateur à redémarrer l'ordinateur.**

3 Après son redémarrage, l'ordinateur doit être connecté au réseau pour que le logiciel client mette en dépôt les informations de récupération auprès du serveur Dell.

Le logiciel client peut commencer et terminer le processus de cryptage, ainsi que signaler l'état de cryptage à la console de gestion à distance, 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.

Cryptage FileVault d'un volume non crypté

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**.

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**. Sélectionnez l'une des options suivantes :

- Faites du compte un compte mobile.
  OU
- Connectez-vous à un compte local et initialisez FileVault à partir de cet emplacement.

5 Cliquez sur **OK**.

6 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 à distance, le logiciel client peut inviter l'utilisateur à redémarrer l'ordinateur.

7 Après son redémarrage, l'ordinateur doit être connecté au réseau pour que le logiciel client mette en dépôt les informations de récupération auprès du serveur Dell.

Le logiciel client peut commencer et terminer le processus de cryptage, ainsi que signaler l'état de cryptage à la console de gestion à distance, 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 à distance 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 à distance, 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 *Protection de données Dell > 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 le serveur.

  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 finaux 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 Data Protection**.

2 Cliquez sur l'onglet **Volumes système**.

3 Sur le lecteur de volume système, effectuez Ctrl-clic, puis sélectionnez **Ajouter des utilisateurs FileVault au démarrage FileVault**.

4 Dans le champ Rechercher, saisissez 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 crypté par FileVault et que le cryptage FileVault est activé sur la console de gestion à distance, 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 Data Protection 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**.

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

  1 Entrez la clé.

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

  2 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.**

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

  2 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 sera accessible et crypté avec FileVault, mais le cryptage ne sera pas géré par Dell.

REMARQUE : Dans la console de gestion à distance, l'administrateur peut voir que le serveur Dell gère désormais le point de terminaison.

Recyclage des clés de récupération 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 récupération à partir de la console de gestion à distance et copiez-le sur le bureau de l'ordinateur.
2 Lancez les *Préférences système*, puis cliquez sur **Dell Data Protection**.
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 récupération à partir de la console de gestion à distance.

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 sera maintenu uniquement dans la mémoire. Par conséquent, l'ordinateur sera 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 blanche

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

1 Lancez les **Préférences système**, puis cliquez sur **Dell Data Protection**.

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 blanche** pour le support externe actuel. La règle de liste blanche est copiée dans le Presse-papiers.

5 Accédez au Presse-papiers, copiez la règle de liste blanche 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.

Si vous voulez exclure un périphérique ou un groupe de périphériques pour empêcher l'écriture de données cryptées sur le disque Thunderbolt ou le support EMS, vous pouvez utiliser cette règle de liste blanche pour modifier les valeurs.

Utilisez la règle complète pour spécifier un disque particulier pour l'ajout à la liste blanche. 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 EMS lors d'une connexion via Thunderbolt :

tbolt=1;bus=SATA

Vous pouvez également placer sur liste blanche ou exclure des supports dans EMS, en fonction des éléments suivants :

- **Taille du support**

  Règle de liste blanche permettant d'exclure les supports volumineux de la protection EMS :

  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'EMS 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 blanche :

  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 :

- Vous devez transférer les données cryptées d'un utilisateur vers un autre Mac dans le cadre d'un renouvellement du matériel.
- Vous devez accéder à un disque crypté en raison d'une défaillance du système d'exploitation qui empêche le démarrage du volume système, et vous oblige à exécuter divers utilitaires pour réparer le système d'exploitation.
- Vous devez accéder aux données cryptées d'un utilisateur, car celui-ci a fait un changement de configuration non autorisé, et vous devez remédier à la situation.

Dans cette section, vous découvrirez comment effectuer **l'une** des trois opérations de récupération disponibles.

Choisissez l'**une** des options ci-dessous :

- Montage du volume
- Acceptation de la nouvelle configuration du système
- Cryptage FileVault : uniquement en cas d'utilisation du cryptage FileVault sur le point de terminaison à récupérer. FileVault peut être utilisé avec Encryption Client s'exécutant sur Mac OS X 10.10.5 ou une version ultérieure. La récupération FileVault est également utilisée sur les disques Fusion Drive.

Montage du volume

Configuration requise

- Un volume de récupération externe non crypté ou un ordinateur qui exécutera l'utilitaire de récupération
- Un câble FireWire ou Thunderbolt, en fonction de votre matériel
- L'ID de périphérique/ID unique de l'ordinateur ciblé pour la récupération : dans la plupart des cas, vous pouvez trouver l'ordinateur ciblé pour la récupération dans la console de gestion à distance en recherchant le nom d'utilisateur de son propriétaire et en examinant les périphériques cryptés 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 à distance en tant qu'administrateur Dell.

2 Dans le volet de gauche, cliquez sur **Gestion > Récupérer le point de terminaison**.

3 Dans le champ de recherche, entrez le nom de domaine complet du point de terminaison et cliquez sur l'icône de recherche.

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 bundle clé 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.

REMARQUE : Si la protection par mot de passe du programme interne est activée sur cet ordinateur, vous serez invité à entrer le mot de passe du programme interne pour accéder au Gestionnaire de démarrage de pré-démarrage. Vous pouvez trouver le mot de passe du micrologiciel de cet ordinateur dans le bundle de récupération téléchargé à l'étape d'enregistrement du bundle de récupération. Voir la section Activation de Mac OS X Boot Camp pour plus d'informations.

7 Démarrez l'ordinateur cible à partir d'un volume de récupération 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.

Maintenant, connectez 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-Data-Protection-<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 Dans le dossier Utilitaires se trouvant sur le support d'installation Dell, lancez Dell Recovery Utility.

Un message s'affiche et indique : « Le texte du DDP [texte noyau] doit être chargé pour modifier les disques cryptés. Tapez votre mot de passe pour l'autoriser. »

10 Entrez le mot de passe de l'administrateur ou de l'utilisateur.

Un message s'affiche et indique : « Installation nécessaire : il faut installer la récupération. »

11 Cliquez sur **Installer**.

12 Sélectionnez le volume ou le disque à récupérer et cliquez sur **Continuer**.

Si vous sélectionnez le disque, tous les volumes du disque seront récupérés à la fois.

13 Sélectionnez le bundle de récupération (enregistré à l'étape 6), puis cliquez sur **Ouvrir**.

14 Sélectionnez l'option **Monter le volume**.

15 Cliquez sur **Continuer** pour confirmer l'option *Monter le volume*. Un message de confirmation s'affiche.

16 Cliquez sur **Fermer**.

Vous êtes maintenant en mesure d'ouvrir une fenêtre du Finder et d'accéder aux données du volume crypté comme vous le feriez avec un volume normal. Toutes les données seront cryptées et décryptées de manière transparente lors du transfert des fichiers entre les volumes.

Acceptation de la nouvelle configuration du système

Si un mot de passe du programme interne ou tout autre changement de configuration système a invalidé la clé de cryptage sur un ordinateur crypté, choisissez cette option pour accepter la configuration système mise à jour lors du prochain redémarrage et rétablir l'accès à l'ordinateur.

Étant donné que le cryptage est lié à la configuration spécifique de périphérique, les modifications de la configuration invalident la clé de cryptage du logiciel client. Lorsque vous choisissez d'accepter la nouvelle configuration système, vous demandez simplement au logiciel client de réinitialiser sa sécurité en fonction de la nouvelle configuration. Par exemple, vous pouvez avoir besoin de transférer le disque vers un autre Mac parce qu'un utilisateur a cassé l'écran. En utilisant cette méthode, vous demandez au logiciel client d'accepter la validité de cette « nouvelle » configuration.

Configuration requise

- Un volume de récupération externe non crypté ou un ordinateur qui exécutera l'utilitaire de récupération
- Un câble FireWire ou Thunderbolt, en fonction de votre matériel
- L'ID de périphérique/ID unique de l'ordinateur ciblé pour la récupération : dans la plupart des cas, vous pouvez trouver l'ordinateur ciblé pour la récupération dans la console de gestion à distance en recherchant le nom d'utilisateur de son propriétaire et en examinant les périphériques cryptés 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 à distance en tant qu'administrateur Dell.

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 récupération 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**.

> **REMARQUE : Si la protection par mot de passe du programme interne est activée sur cet ordinateur, vous serez invité à entrer le mot de passe du programme interne pour accéder au Gestionnaire de démarrage de pré-démarrage. Vous pouvez trouver le mot de passe du micrologiciel de cet ordinateur dans le bundle de récupération téléchargé à l'étape 7. Voir la section Activation de Mac OS X Boot Camp pour plus d'informations.**

8 Démarrez l'ordinateur cible à partir d'un volume d'installation externe pré-créé incluant un système d'installation complet. Pour ce faire, ouvrez le volet Disque de démarrage dans les Préférences système et sélectionnez le volume d'installation incluant un système d'installation complet, ou maintenez enfoncée la touche **Option** pendant le redémarrage de cet ordinateur, puis sélectionnez le volume d'installation externe 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.

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.**

9 Effectuez l'une des opérations suivantes :

- Connectez cet ordinateur à l'ordinateur hôte qui effectuera l'opération de récupération en utilisant un câble FireWire ou Thunderbolt, en fonction de votre matériel.

  ou

- Démarrez sur n'importe quel disque doté d'un système d'exploitation complet.

10 Montez l'image Dell-Data-Protection-<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.**

11 Dans le dossier Utilitaires se trouvant sur le support d'installation Dell, lancez Dell Recovery Utility.
Un message s'affiche et indique : « Le texte du DDP [texte noyau] doit être chargé pour modifier les disques cryptés. Tapez votre mot de passe pour l'autoriser. »

12 Entrez le mot de passe de l'administrateur ou de l'utilisateur.
Le message « Installation nécessaire : il faut installer la récupération. » s'affiche

13 Cliquez sur **Installer**.

14 Sélectionnez le volume ou le disque à récupérer et cliquez sur **Continuer**.
Si vous sélectionnez le disque, tous les volumes du disque seront récupérés à la fois.

La fenêtre de sélection de fichier apparaît.

15 Sélectionnez le bundle de récupération (enregistré à l'étape 7), puis cliquez sur **Ouvrir**.
La boîte de dialogue *Sélectionner l'opération de récupération* s'affiche.

16 Sélectionnez l'option **Accepter la nouvelle configuration du système**.

17 Cliquez sur **Continuer** pour confirmer l'option *Accepter la nouvelle configuration du système*.

18 Entrez votre mot de passe pour réinitialiser la propriété et accepter la nouvelle configuration système.

19 Cliquez sur **OK**.

Le message *Récupération terminée* s'affiche lors du démarrage vers le volume système interne d'origine. Ce message vous invite à redémarrer l'ordinateur. Le logiciel client a maintenant accepté la configuration système mise à jour, et vous pouvez accéder normalement à votre ordinateur.

Récupération FileVault

La récupération d'un volume géré crypté par FileVault est nettement différente de la récupération d'un volume crypté par Dell. Le processus de récupération est dicté par Apple et est autant que possible automatisé, mais 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. En général, utilisez d'abord la clé de récupération personnelle la plus récente. 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 serveur Dell. Il s'agit de la méthode recommandée.

  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 : 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 non de démarrage. La récupération du volume de démarrage corrigera généralement les problèmes concernant les volumes non de 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 récupération dans la console de gestion à distance en recherchant le nom d'utilisateur de son propriétaire et en examinant les périphériques cryptés 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 Ouvrez la console de gestion à distance.

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 récupération 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**.

9 Copiez le bundle de récupération ainsi que le fichier **Dell-Data-Protection-<version>.dmg** sur le disque USB amorçable.

10 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 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.

11 Montez l'image Dell-Data-Protection-<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.

12 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.

13 Sélectionnez le volume FileVault.

- Afin de décrypter et monter le disque, vous devez disposer d'une partition de démarrage de version 10.9.5 ou ultérieure. Sinon, vous ne pouvez obtenir que la clé de récupération personnelle.
- Si vous avez des volumes non de démarrage cryptés, en général, vous récupérerez la partition de démarrage en premier.

14 Cliquez sur **Continuer**.

La boîte de dialogue *Choisir le bundle de récupération* s'affiche.

15 Sélectionnez le bundle de reprise (enregistré à l'étape 9), puis cliquez sur **Ouvrir**.

La boîte de dialogue *Sélectionner l'enregistrement de récupération* s'affiche.

16 Dans 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.

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

- 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 récupération personnelle de l'authentification de pré-démarrage, qui peut varier en fonction du système d'exploitation.
- Pour les disques non de démarrage, seule la clé de récupération personnelle s'affiche. Pour monter un volume hors volume de démarrage, entrez la clé de récupération dans la boîte de dialogue d'invite du mot de passe du système d'exploitation. Si vous avez ignoré précédemment la boîte de dialogue, vous pouvez maintenant sélectionner Déverrouiller par Utilitaire de disque pour monter la partition cryptée.

17 Imprimez la clé ou notez-la.

18 Cliquez sur **Fermer**.

19 Démarrez sur le volume de démarrage externe en maintenant la touche **Option** au démarrage.

20 Au besoin, entrez le mot de passe du micrologiciel. Sélectionnez le volume de démarrage externe.

21 Après le redémarrage du système, cliquez sur **?** à l'écran d'ouverture de session.

22 Cliquez sur la flèche qui s'affiche.

23 Saisissez la clé de récupération et appuyez sur **Entrée**.

24 Dans la boîte de dialogue, entrez un nouveau mot de passe.

Trousseau de récupération

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

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 volume de démarrage externe en maintenant la touche **Option** au démarrage.

3 Au besoin, entrez le mot de passe du micrologiciel. Sélectionnez le volume de démarrage externe.

4 Montez le fichier .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 externe, 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 que vous devrez taper.

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

Dell Recovery Utility génère les fichiers à l'emplacement sélectionné, puis affiche les commandes exactes que vous devrez exécuter à partir du volume Recovery HD pour monter ou décrypter 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** (Commande-R) avant la sonnerie de démarrage/d'auto-test et pendant le démarrage de l'ordinateur.

  ou

- Appuyez sur la touche **Option** et utilisez le sélecteur de démarrage pour sélectionner la partition 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 pas en charge actuellement la gravure de CD/DVD pour EMS. 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 blanche pour autoriser 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 lecteur qui ne contient pas encore de sauvegardes, l'utilisateur doit copier sa règle de liste blanche et vous envoyer la règle pour vous indiquer son lecteur Time Machine à mettre sur la liste blanche. Voir Copier une règle de liste blanche.

EMS et mises à jour de règles

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

Exceptions de cryptage

Sur les supports externes, les attributs étendus ne sont pas cryptés.

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'EMS, et que vous le montez ensuite dans EMS, 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 :

  a Notez la quantité d'espace qui doit être libéré sur le périphérique. Le rapport affiche une liste des fichiers et leur taille.

  b Videz la corbeille. Lorsque vous libérez de l'espace, EMS crypte automatiquement des fichiers supplémentaires.

  c Si vous supprimez des fichiers ou des dossiers, veillez à vider à nouveau la corbeille.

Messages d'audit

Des messages d'audit sont envoyés au serveur Dell.

Pour Endpoint Security Suite Enterprise for Mac, accédez à la console de gestion à distance et sélectionnez **Populations > Entreprise ou Points de terminaison**. Ensuite, sélectionnez l'onglet **Événements de menaces avancées**. Pour en savoir plus, voir *AdminHelp*.

Collecte de fichiers journaux pour Endpoint Security Suite Enterprise

DellLogs.zip contient les journaux de Client Encryption 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 for Mac

Le logiciel client peut être désinstallé à l'aide de l'application **Désinstaller Dell Data Protection**. 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 crypté, définissez la règle **Cryptage de volume Dell** sur **Désactivé** dans la console de gestion à distance, 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 Data Protection** (se trouvant dans le dossier Utilitaires de l'image Dell-Data-Protection-<version>.dmg du support d'installation Dell).

  Les messages affichent l'état de la désinstallation.

  Encryption Client for 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 votre serveur Dell.

Configuration requise

- Encryption Client 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 Data Protection.

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 programme interne 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.

Si vous souhaitez que la protection par mot de passe 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, le système d'exploitation Windows ne peut pas être crypté.

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 et 8 Pro (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 et versions ultérieures est compatible 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 for Mac est installé, le volume système doit être crypté via Encryption Client for Mac à l'aide de Dell Client Encryption ou de FileVault2. Vous devez configurer votre installation client de sorte qu'elle n'utilise **pas** la protection par mot de passe du programme interne. Voir Installation/mise à niveau avec la ligne de commande pour obtenir des instructions.

REMARQUE :

Si votre partition Windows est un candidat EMS, assurez-vous de la placer sur la liste blanche sinon elle sera cryptée. Voir Copier une règle de liste blanche.

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

Configuration requise

- 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 récupération dans la console de gestion à distance en recherchant le nom d'utilisateur de son propriétaire et en examinant les périphériques cryptés pour cet utilisateur. Le format de l'ID unique/ID de périphérique 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 à distance, copiez le bundle de récupération 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 lecteur externe Boot Camp, appuyez sur la touche **Option** pendant que vous mettez l'ordinateur sous tension.

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 Data Protection Encryption, 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 cryptées...* - Si l'utilisateur ne peut pas accéder à certains fichiers cryptés 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 à ce 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 à distance 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 récupération 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\ Data\ Protection.prefPane/Contents/Helpers/**client -at** *domainAccount domainPassword*

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

/Library/PreferencePanes/Dell\ Data\ Protection.prefPane/Contents/Helpers/client

Tableau 1. Commandes de l'outil client

Commande	Objectif	Syntaxe	Résultats
Activer	Active un client Mac avec le serveur Dell sans passer par l'interface utilisateur. Pour l'activation, un nom d'utilisateur de domaine et un mot de passe valides doivent être entrés. Avec l'outil client, vous pouvez activer un autre utilisateur local que celui qui est connecté et lui affecter les informations d'identification du domaine.	-a ComptedeDomaine MotdepassedeDomaine -a CompteLocal* ComptedeDomaine MotdepassedeDomaine **ComptedeDomaine** est le compte utilisé pour l'activation à l'aide de l'outil client. **CompteLocal**, facultatif, correspond à l'utilisateur actuel lorsqu'aucun autre n'est spécifié. La commande d'activation est au format suivant : client -a <utilisateur à activer*> <UtilisateurdeDomaine> <MotdepassedeDomaine> Si vous utilisez la règle *No Auth User List* pour créer des classes d'utilisateurs ne s'activant pas sur le serveur Dell, 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.	0 = Réussite 2 = Échec de l'activation et raison de l'échec 6 = Utilisateur introuvable
Activer temporairement	Active un client Mac sans laisser d'empreinte.	-at ComptedeDomaine MotdepassedeDomaine -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.

Commande	Objectif	Syntaxe	Résultats
			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 -fc IDdePériphérique Cléde RécupérationPersonnelle -fc IDdePériphérique CheminversChaînedeclé MotdepassedeChaînedeclé -fc IDdePériphérique FichierdeRécupération **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 7= LVUUID introuvable 10 = Échec des identifiants 11 = Échec de dépôt
Stratégie	Demande les règles du client Mac	-P	Les règles s'affichent
Serveur	Interroge le serveur à propos des mises à jour de règles au nom du client Mac. **REMARQUE : L'interrogation peut prendre plusieurs minutes.**	-s	0 = Réussite Toute autre valeur indique que le serveur Dell 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 1 = Non activé 6 = Utilisateur introuvable
Utilisateur	Demander les informations de l'utilisateur	-u CompteLocal*	Les informations sur le compte utilisateur s'affichent : 0 (informations de compte) = Réussite 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\ Data\ Protection.prefPane/Contents/Helpers/**client -p -plist**

Pour récupérer les règles du client et les imprimer.

Library/PreferencePanes/Dell\ Data\ Protection.prefPane/Contents/Helpers/**client -at -plist** *CompteLocal ComptedeDomaine MotdepassedeDomaine*

Pour activer temporairement le client et imprimer le résultat.

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

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

Library/PreferencePanes/Dell\ Data\ Protection.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

Tâches d'Advanced Threat Prevention

Installation d'Advanced Threat Prevention pour Mac

Dans cette section, vous découvrirez comment installer 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.

Configuration requise

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 le serveur Dell et ses composants sont déjà installés.

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

  Enterprise Server Installation and Migration Guide (Guide d'installation et de migration d'Enterprise Server)

  Enterprise Server - Guide de démarrage rapide et Guide d'installation de Virtual Edition
- Assurez-vous d'avoir le nom d'hôte du serveur et le port. Vous en aurez besoin pour l'installation du logiciel client.
- Vérifiez que l'ordinateur cible dispose d'une connectivité réseau avec le serveur Dell.
- 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 for Mac s'ouvre.

2 Double-cliquez sur le programme d'installation d'**Endpoint Security Suite Enterprise**. Le message suivant est affiché :
Ce package va exécuter un programme pour déterminer si le logiciel peut être installé.

3 Cliquez sur **Continue** (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 serveur Dell 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, entrez les informations d'identification du compte d'administrateur (exigés par l'application Mac OS X Installer), puis cliquez sur **OK**.

10 Une fois l'installation terminée, cliquez sur **Fermer**.

Le client Advanced Threat Prevention for Mac est maintenant installé.

11 Voir Vérification de l'installation d'Advanced Threat Prevention.

Si l'installation échoue, vérifiez que vous disposez d'un certificat valide sur votre serveur Dell. Voir Désactivation du certificat SSL de confiance d'Advanced Threat Prevention.

Désinstallation interactive du client Advanced Threat Prevention

Pour désinstaller le logiciel client, lancez l'application **Uninstall 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 **Uninstall Endpoint Security Suite Enterprise**.

3 Cliquez sur **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 for 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 du serveur Dell 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>deviceserver.company.com</string>
  <key>ServerPort</key>
  <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 for 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 du package avec la ligne de commande, en exécutant 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 for Mac

Désactivation du certificat SSL de confiance 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.

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
```

Les paramètres par défaut sont indiqués ci-après :

```
Current Settings:

ServerHost = deviceserver.company.com

ServerPort = 8888

DisableSSLCertTrust = False

DumpXmlInventory = False

DumpPolicies = False
```

4 Saisissez **-help** pour répertorier les options.

5 Pour désactiver le certificat SSL de confiance sur le client, définissez `DisableSSLCertTrust` 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 de Dell 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 du serveur Dell.

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 Dell Advanced Threat Prevention est créé sous /Applications.

Collecte de fichiers journaux pour Endpoint Security Suite Enterprise

DellLogs.zip contient les journaux de Client Encryption 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 serveur Dell 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 sur la console de gestion à distance du serveur Dell.

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 serveur Dell 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 serveur Dell.
- **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 sur la console de gestion à distance du serveur Dell.

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'évènement 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

Menace en quarantaine

Menaces exonérées

Menaces modifiées

Configuration d'un locataire pour Advanced Threat Protection

Si votre entreprise utilise Advanced Threat Protection, un locataire doit être provisionné dans le serveur Dell avant que l'application des règles d'Advanced Threat Protection devienne active.

Configuration requise

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

Provisionner un service partagé

1. Connectez-vous à la console de gestion à distance et naviguez vers **Gestion des services**.
2. Cliquez sur **Configurer le service Advanced Threat Protection**. Importez vos licences ATP si un échec se produit à ce stade.
3. La configuration guidée débute une fois que les licences sont importées. Cliquez sur **Suivant** pour continuer.
4. Lisez et acceptez les termes du CLUF (la case est **désélectionnée** par défaut), puis cliquez sur **Suivant**.
5. Fournissez des identifiants d'authentification au serveur DDP pour le provisionnement du service partagé. Cliquez sur **Suivant**. *Un provisionnement de service partagé portant la marque Cylance n'est pas pris en charge.*
6. Téléchargez le certificat. C'est nécessaire à la récupération s'il existe un scénario de reprise après sinistre sur le serveur DDP. Ce certificat n'est pas automatiquement sauvegardé via le service « upgrader » de la v9.2. Sauvegardez le certificat en lieu sûr sur un autre ordinateur. Cochez la case pour confirmer que vous avez sauvegardé le certificat et cliquez sur **Suivant**.
7. La configuration est terminée. Cliquez sur **OK**.

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

Pour recevoir les mises à jour automatiques de l'agent Advanced Threat Prevention, vous pouvez vous inscrire dans la console de gestion à distance du serveur Dell. 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 serveur 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 v9.4.1 ou les versions ultérieures du serveur Dell.

Mises à jour automatique de l'agent de réception

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

1 Dans le volet de gauche de la console de gestion à distance, cliquez sur **Gestion** > **Gestion des services**.

2 Sur l'onglet **Menaces avancées**, sous Agent de mise à jour automatique, cliquez sur le bouton **Activé**, puis cliquez sur sur le bouton **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 :

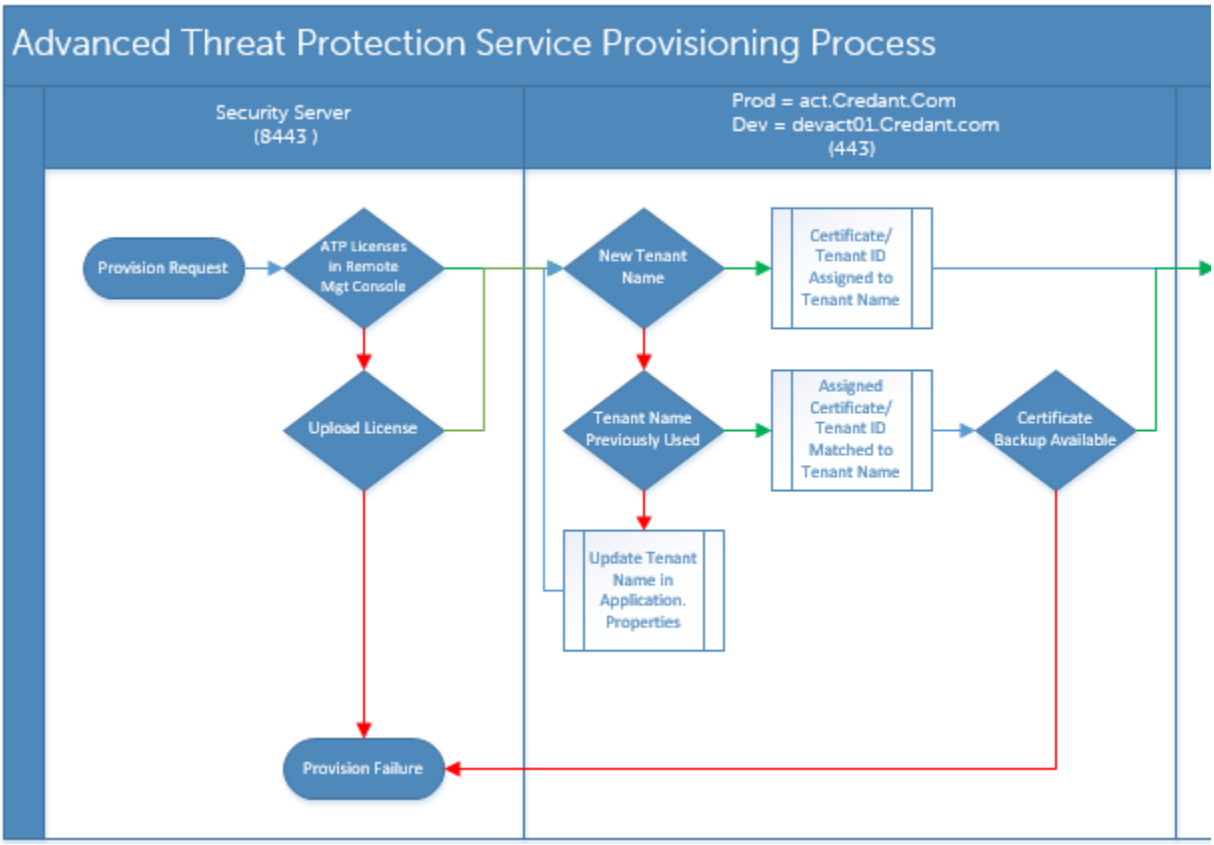
1 Dans le volet de gauche de la console de gestion à distance, cliquez sur **Gestion** > **Gestion des services**.

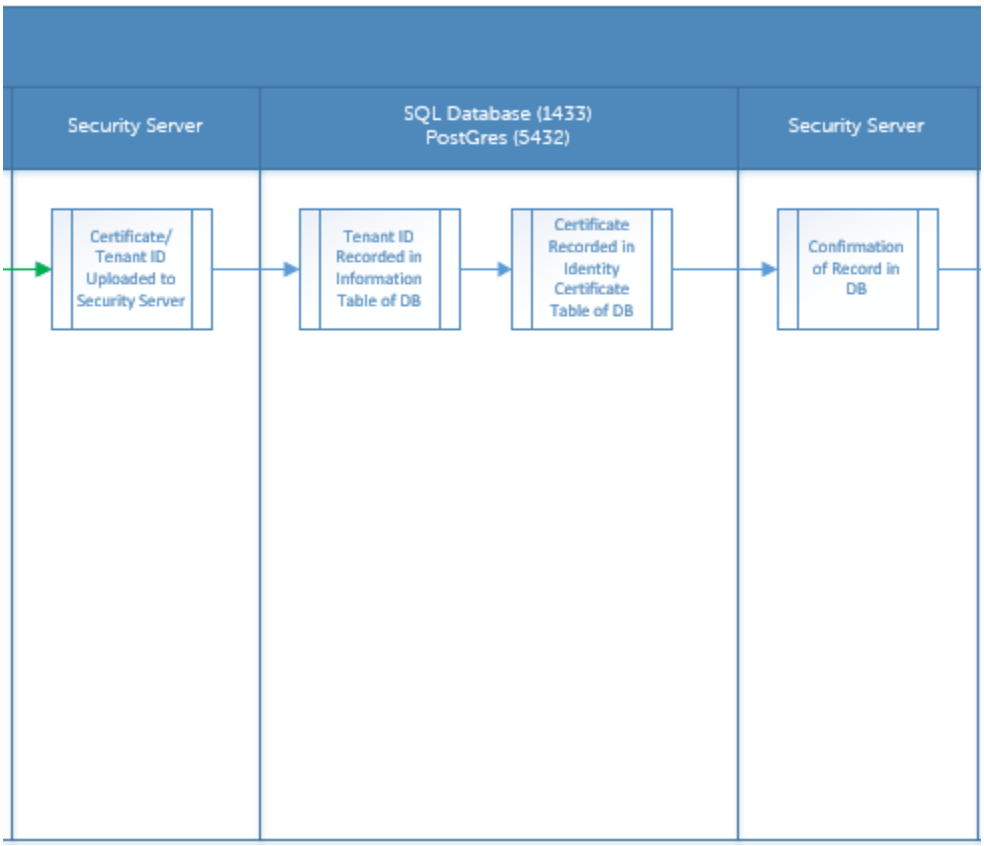
2 Dans l'onglet **Menaces avancées**, sous Mise à jour automatique de l'agent, cliquez sur le bouton **Désactivé**, puis cliquez sur le bouton **Enregistrer les préférences**.

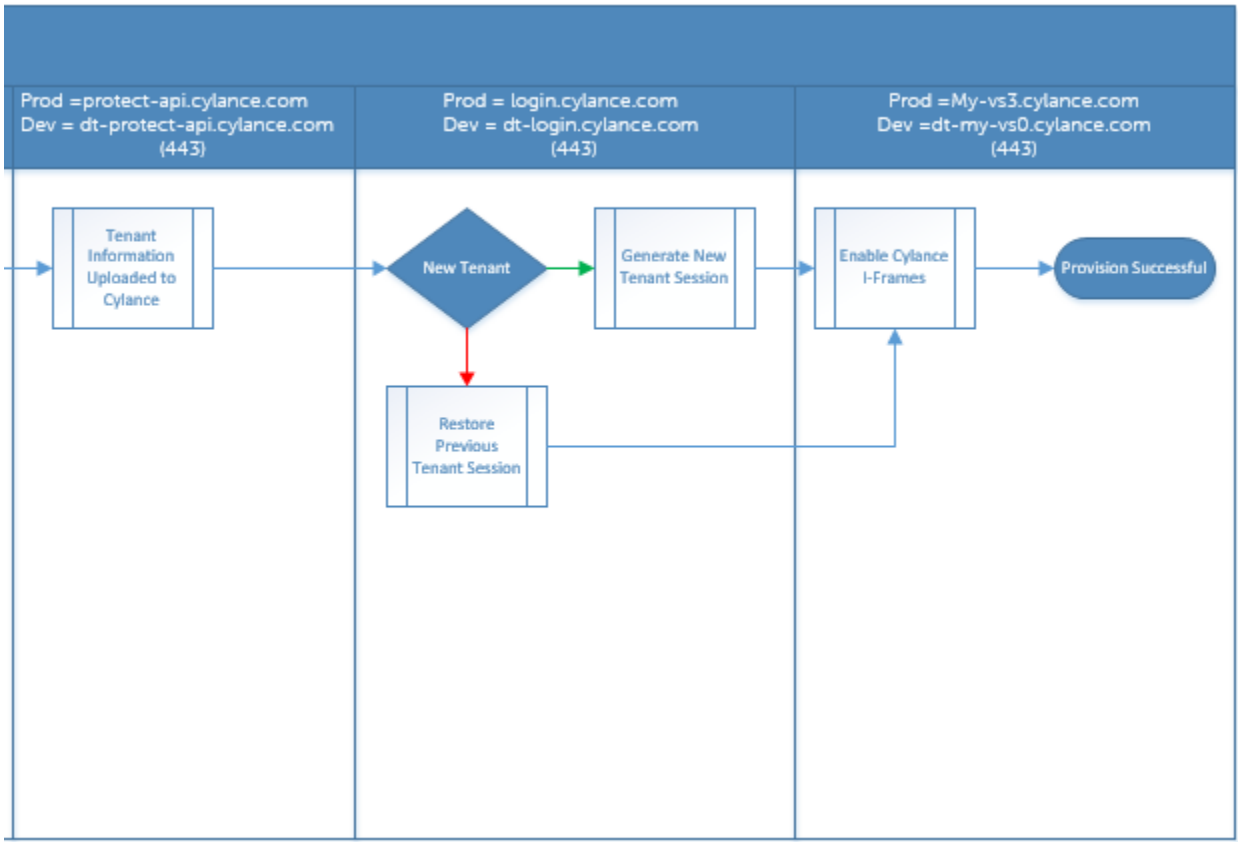
Dépannage du client Advanced Threat Protection

Provisionnement d'Advanced Threat Protection et communication agent

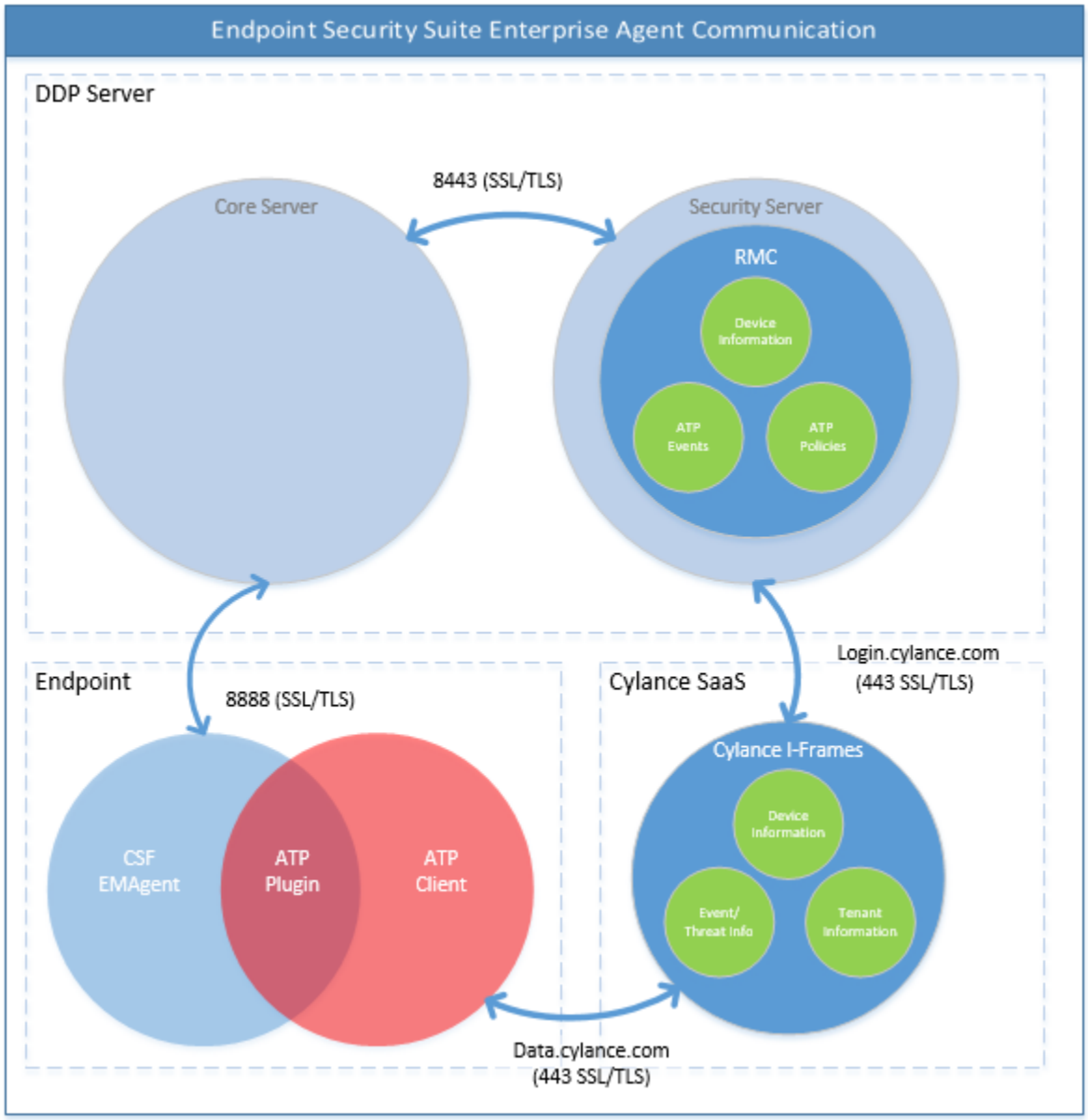
Les diagrammes suivants illustrent le processus de provisionnement du service Advanced Threat Protection.


Advanced Threat Protection Service Provisioning Process
Security Server
(8443)
Prod = act.Credant.Com
Dev = devact01.Credant.com
(443)
Provision Request
ATP Licenses in Remote Mgt Console
Upload License
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
Provision Failure


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 Protection.


Endpoint Security Suite Enterprise Agent Communication
DDP Server
8443 (SSL/TLS)
Core Server
Security Server
RMC
Device Information
ATP Events
ATP Policies
Endpoint
8888 (SSL/TLS)
CSF EMAgent
ATP Plugin
ATP Client
Cylance SaaS
Login.cylance.com
(443 SSL/TLS)
Cylance I-Frames
Device Information
Event/ Threat Info
Tenant Information
Data.cylance.com
(443 SSL/TLS)

5

Glossaire

Serveur de sécurité : assure les activations du cryptage client.

Proxy de règles : permet de distribuer des règles au logiciel client Endpoint Security Suite Enterprise pour Mac.

Console de gestion à distance : console administrateur pour tout le déploiement d'entreprise.

Bouclier : vous pourrez parfois rencontrer ce terme dans la documentation et dans l'interface utilisateur du client. Le terme « bouclier » est utilisé pour représenter le logiciel client.