Dell Encryption Enterprise for Mac

Guia do Administrador v10.9

Março de 2021
Rev. A02

Notas, avisos e advertências

NOTA: Uma NOTA fornece informações importantes para ajudar a utilizar melhor o produto.

AVISO: Um AVISO indica possíveis danos no hardware ou uma perda de dados e explica como pode evitar esse problema.

ADVERTÊNCIA: Uma ADVERTÊNCIA indica possíveis danos no equipamento, lesões corporais ou morte.

Índice

1

Introdução

O Guia do administrador do Encryption Enterprise para Mac fornece as informações necessárias para implementar e instalar o software cliente.

Tópicos

Descrição geral

O Encryption Enterprise for Mac é capaz de processar uma encriptação total do disco com FileVault.

- Encryption Enterprise for Mac - software cliente de encriptação que encripta todos os dados e aplica o controlo dos acessos
- Proxy de políticas - utilizado para distribuir as políticas
- Security Server - utilizado para as ativações do software de encriptação de cliente
- Security Management Server ou Security Management Server Virtual - proporciona uma administração centralizada de políticas de segurança, integra-se nos diretórios existentes na empresa e cria relatórios. Neste documento, ambos os servidores estão assinalados como Dell Server, a não ser que seja necessário indicar uma versão específica (por exemplo, um procedimento que seja diferente ao utilizar o Security Management Server Virtual).

  Estes componentes Dell interagem na perfeição para permitirem um ambiente de mobilidade segura sem reduzir a experiência do utilizador.

Encriptação FileVault

O Dell Encryption pode gerir a encriptação total do disco com FileVault para Mac. A política *Encriptação de Volumes Dell* deve ser definida como **Ativada** para que a encriptação ocorra e para que funcionem outras definições da política. Para obter informações sobre políticas adicionais, consulte *AdminHelp*.

Apenas é suportada a encriptação FileVault, que o Encryption Enterprise vai gerir. Se o computador tiver a política da *Encriptação de volume Dell* definida como **Ativada** e *Encriptar utilizando o FileVault para Mac* definida como **Desativada**, é apresentada uma mensagem de conflito de políticas no cliente de Encriptação. O administrador tem de selecionar ambas as políticas como **Ligado**.

Contacte o Dell ProSupport

Contacte o número 877-459-7304, extensão 4310039 para obter suporte telefónico permanente (24 x 7) para o seu produto Dell.

Adicionalmente, o suporte online para os produtos Dell encontra-se disponível em dell.com/support. O suporte online inclui controladores, manuais, conselhos técnicos, FAQ e problemas emergentes.

Para números de telefone fora dos Estados Unidos, consulte Números de telefone internacionais do Dell ProSupport.

2

Requisitos

Os requisitos de hardware e software do cliente são apresentados neste capítulo. Certifique-se de que o ambiente de implementação cumpre os requisitos antes de continuar as tarefas de implementação.

Tópicos

Hardware do Encryption Client

Os requisitos mínimos de hardware necessitam atender as especificações mínimas do sistema operativo.

Hardware
• 30 MB de espaço livre em disco
• Placa de rede 10/100/1000 ou Wi-Fi
• O disco do sistema tem de estar particionado com o esquema de partição GUID Partition Table (GPT) e pode ser formatado com qualquer um dos seguintes: ○ Mac OS X Extended Journaled (HFS+) – é convertido para CoreStorage para aplicar o FileVault. ○ Apple File System (APFS)

Software para o cliente de encriptação

A tabela seguinte lista os softwares suportados.

Sistemas operativos (kernels de 64 bits)
• macOS High Sierra 10.13.6
• macOS Mojave 10.14.5 - 10.14.6
• macOS Catalina 10.15.5 - 10.15.6

NOTA: O Dell Encryption não suporta o macOS Big Sur.

NOTA:

Se utiliza uma conta de utilizador da rede para efetuar a autenticação, essa conta tem de ser configurada como uma conta móvel para configurar totalmente a gestão do FileVault 2.

Suporte encriptado

A tabela seguinte indica os sistemas operativos compatíveis ao aceder a suportes multimédia externos com encriptação Dell.

NOTA:

O Encryption External Media suporta:

- FAT32
- exFAT

- São suportados suportes HFS Plus (MacOS Extended) formatados com esquemas de partição Registo de arranque principal (MBR) ou Tabela de partições GUID (GPT). Consulte Ativar HFS Plus.

NOTA:

O suporte externo tem de ter 55 MB disponíveis, bem como espaço livre no suporte igual ao maior ficheiro a encriptar para alojar o Encryption External Media.

Sistemas operativos Windows (32 e 64 bits) suportados para aceder a suportes multimédia encriptados
• Microsoft Windows 7 SP1 - Enterprise - Professional - Ultimate
• Microsoft Windows 8.1 - Windows 8.1 Update 1 - Enterprise - Pro
• Microsoft Windows 10 - Education - Enterprise – Pro v1607 (Atualização de Aniversário/Redstone 1) até à versão v1909 (Atualização de novembro de 2019/19H2)
Sistemas operativos Mac (kernels de 64 bits) suportados para aceder a suportes encriptados
• macOS High Sierra 10.13.6 **NOTA:** O Encryption External Media no macOS High Sierra 10.14.x requer o Encryption Enterprise v8.16 ou posterior.
• macOS Mojave 10.14.5 - 10.14.6
• macOS Catalina 10.15.5 - 10.15.6

3

Tarefas para o cliente de encriptação

Tópicos

Instalar/Atualizar o Encryption Enterprise for Mac

Esta secção vai guiá-lo através do processo de instalação/atualização e ativação do Encryption Enterprise para Mac.

Existem dois métodos para instalar/atualizar o Encryption Enterprise para Mac. Selecione **uma** das seguintes ações:

- Instalação/atualização e ativação interativas - Este é o método mais fácil para instalar ou atualizar o pacote de software cliente. No entanto, este método não permite quaisquer personalizações. Se pretender utilizar o Boot Camp ou uma versão do sistema operativo que ainda não seja totalmente suportada pela Dell (através de modificação do .plist), tem de utilizar o método de instalação/atualização através de linha de comandos. Para obter informações sobre a utilização do Boot Camp, consulte Utilizar o Boot Camp.
- Instalação/atualização através de linha de comandos - Este é um método avançado que só deve ser utilizado por administradores com experiência em sintaxe de linha de comandos. Se pretender utilizar o Boot Camp ou uma versão do sistema operativo que ainda não seja totalmente suportada pela Dell (através de modificação do .plist), tem de utilizar este método para instalar ou atualizar o pacote de software cliente. Para obter informações sobre a utilização do Boot Camp, consulte Utilizar o Boot Camp.

  Para obter mais informações sobre opções de comandos do instalador, consulte a Biblioteca de referências do Mac OS X em http://developer.apple.com. A Dell recomenda a utilização de ferramentas de implementação remota, como o Apple Remote Desktop, para distribuir o pacote de instalação do cliente.

  NOTA:

  A Apple lança frequentemente novas versões dos sistemas operativos entre os lançamentos do Encryption Enterprise for Mac. Para fornecer apoio ao máximo de clientes possível, permitimos a modificação do ficheiro com.dell.ddp.plist para apoiar estes casos. O teste destas versões começa assim que a Apple lança uma nova versão, certifique-se de que são compatíveis com Encryption Enterprise para Mac.

Pré-requisitos

A Dell recomenda que sejam seguidas as melhores práticas de TI durante a implementação do software cliente. Estas incluem, entre outras, ambientes de teste controlados para os testes iniciais e a implementação progressiva para os utilizadores.

Antes de iniciar este processo, certifique-se que são observados os seguintes pré-requisitos:

- Certifique-se de que o Dell Server e os seus componentes já estão instalados.

  Se ainda não tiver instalado o Dell Server, siga as instruções apresentadas no respetivo guia abaixo.

  Guia de instalação e migração do Security Management Server

  Guia de instalação e Guia de início rápido do Security Management Server Virtual

- Certifique-se de que tem os URL do Security Server e do proxy de políticas à mão. Ambos são necessários para a instalação e a ativação do software cliente.

- Se a sua implementação utilizar uma configuração não predefinida, certifique-se de que sabe o número de porta do Security Server. É necessário para a instalação e a ativação do software cliente.
- Certifique-se de que o computador de destino tem ligação por rede ao Security Server e ao proxy de políticas.
- Certifique-se de que tem uma conta de utilizador de domínio na instalação do Active Directory configurada para utilizar com o Dell Server. A conta de utilizador de domínio é utilizada para a ativação do software cliente. Não é necessária a configuração de endpoints Mac para a autenticação de domínio (rede).

Antes de definir as políticas de encriptação, a política de *Encriptação de Volume Dell* tem de estar *Ligada*. Certifique-se de que compreende as políticas *Encriptar Utilizando o FileVault para Mac* e *Volumes Visados para Encriptação*.

Para obter mais informações sobre as políticas de encriptação, consulte Mac Encryption > Encriptação de volume Dell.

Instalação ou Atualização Interativas

Para instalar ou atualizar e ativar o software cliente, siga os passos abaixo. Para realizar estes passos, tem de ter uma conta de administrador.

Instalação interativa

NOTA:

Antes de começar, guarde o trabalho do utilizador e feche as outras aplicações; logo após a conclusão da instalação, terá de reiniciar o computador.

1. A partir do suporte de instalação da Dell, instale o ficheiro Dell-Encryption-Enterprise-<version>.dmg.
2. Faça duplo clique no instalador do pacote. É apresentada a seguinte mensagem:
   Este pacote executa um programa que determinará se o software pode ser instalado.
3. Clique em **Continuar** para prosseguir.
4. Leia o texto de Boas-vindas e clique em **Continuar**.
5. Leia o acordo da licença, clique em **Continuar** e clique em **Aceito** para aceitar os termos do acordo da licença.
6. No campo *Endereço do domínio*, introduza o nome de domínio totalmente qualificado para os utilizadores alvo, como por exemplo *departamento.empresa.com*.
7. No campo *Nome apresentado (opcional)*, considere definir *Nome apresentado* para o nome NetBIOS (anterior ao Windows 2000) do domínio, que normalmente está em maiúsculas.

   Se definido, este campo é apresentado em vez do Endereço de domínio na caixa de diálogo *Ativação*. Este nome permite a coerência com o nome de domínio indicado nas caixas de diálogo *Autenticação* para computadores Windows geridos pelo domínio.
8. No campo *Security Server*, introduza o nome do anfitrião do Security Server.

   Se a sua implementação utiliza uma configuração não predefinida, atualize as portas e a caixa de verificação *Utilizar SSL*.

   Assim que uma ligação é estabelecida, o indicador de ligação ao Security Server muda de vermelho para verde.
9. No campo *Policy Proxy*, o nome do anfitrião do Policy Proxy é preenchido automaticamente com um anfitrião que corresponda ao anfitrião do Security Server. Este anfitrião é utilizado como proxy de políticas se não forem especificados anfitriões na configuração das políticas.

   Assim que a ligação tiver sido estabelecida, o indicador de ligação ao proxy de políticas muda de vermelho para verde.
10. Assim que a caixa de diálogo Configuração Dell estiver concluída e a ligação ao Security Server e ao proxy de políticas tiver sido estabelecida, clique em **Continuar** para ver o tipo de instalação.
11. Algumas instalações em computadores específicos apresentam uma caixa de diálogo *Selecionar um destino* antes de a caixa de diálogo *Tipo de instalação* ser apresentada. Nesse caso, desmarque o disco do sistema atual da lista de discos apresentada. O ícone do disco do sistema atual apresenta uma seta verde a apontar para o disco. Clique em **Continuar**.
12. Após o tipo de instalação ser apresentado, clique em **Instalar** para continuar a instalação.
13. Quando solicitado, introduza as credenciais da conta de administrador. (A aplicação de instalação para o MacOS X requer credenciais.)
14. Clique em **OK**.

    NOTA:

    Imediatamente após a instalação estar concluída, tem de reiniciar o computador. Se tiver ficheiros abertos noutras aplicações que não estão preparados para o reinício, clique em **Cancelar**, guarde o trabalho e feche as outras aplicações.
15. Clique em **Continuar a instalação**. A instalação é iniciada.

16. Quando a instalação estiver concluída, clique em **Reiniciar**.
17. Com uma nova instalação do Encryption Enterprise, é apresentada a caixa de diálogo *Extensão do sistema bloqueada* .

    Para consentimento por kext, é apresentada uma ou ambas as caixas de diálogo.

Extensão do Sistema Bloqueada	Extensão do Sistema Bloqueada
a. Clique em **OK**. b. Clique em **OK**. c. Para aprovar estas extensões, selecione **Preferências do sistema > Segurança e Privacidade**. d. Clique em **Permitir** junto de *Software do sistema do programador Credant Technologies (Dell, Inc, anteriormente Credant Technologies)*. e. Clique em **OK**.	Conclua estes passos se não for possível carregar a extensão do sistema para a montagem de volumes FDEEM. a. Clique em **Abrir preferências do sistema**. b. Clique em **OK**. c. No separador **Geral**, clique em **Permitir** junto de *Software do sistema do programador Credant Technologies (Dell, Inc, anteriormente Credant Technologies)*. d. Clique em **OK**.

    O botão Permitir pode estar disponível durante 30 minutos ou menos após a instalação. Se ignorar este passo, a caixa de diálogo continua a ser apresentada a cada vinte e cinco minutos até concluir esta ação.
18. Prossiga para Ativar o Encryption Enterprise for Mac.

macOS 10.15 e superior com suportes de dados amovíveis

Se uma empresa utilizar suportes de dados amovíveis com o macOS 10.15 e posterior, os utilizadores têm de ativar o acesso total ao disco para suportes de dados externos. Para obter mais informações, consulte Ativar Acesso Total ao Disco para Suportes de Dados Amovíveis.

Instalação/atualização através de linha de comandos

Para instalar o software de cliente através da linha de comandos, siga os passos abaixo.

Instalação com linha de comandos

1. A partir do suporte de instalação da Dell, instale o ficheiro Dell-Encryption-Enterprise-<version>.dmg.
2. Copie o pacote **Install Dell Encryption Enterprise** e o ficheiro **com.dell.ddp.plist** para a unidade de disco local.
3. Na Management Console, modifique as seguintes políticas, se necessário. As definições das políticas substituem as definições do ficheiro .plist. Utilize as definições .plist se não existirem políticas na Management Console.
   - **Sem Lista de utilizadores autenticados** - em alguns casos, poderá desejar editar esta política para que os utilizadores especificados ou as classes de utilizadores não tenham de proceder à ativação no Dell Server. Por exemplo, em instalações educacionais, os professores seriam instruídos a ativar o seu computador no Dell Server, mas cada aluno individual que utilizasse os computadores do laboratório não seria. O administrador do laboratório poderia utilizar esta política e a conta ativada no Client Tool para que os estudantes pudessem iniciar sessão sem lhes ser solicitada a ativação. Para obter informações sobre o Client Tool, consulte Client Tool. Se uma empresa precisar de saber que conta de utilizador está associada a cada computador Mac, todos os utilizadores têm de estar ativados no Dell Server, pelo que a empresa não editaria essa propriedade. No entanto, se um utilizador quiser fornecer suportes de dados Encryption External Media, este tem de ser autenticado no Dell Server.
4. Abra o ficheiro .plist e edite quaisquer valores de marcadores de posição adicionais:

   NOTA:

   A Apple lança frequentemente novas versões dos sistemas operativos entre os lançamentos do Encryption Enterprise for Mac. Para fornecer apoio ao máximo de clientes possível, permitimos a modificação do ficheiro .plist para apoiar estes casos. Assim que a Apple lança uma nova versão, a Dell começa a testá-la a fim de assegurar que é compatível com o Encryption Enterprise para Mac.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/
PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
  <key>NoAuthenticateUsers</key> [In this sample code, after one user activates the
computer against the Dell Server, other users can log in without being prompted to
activate.]
  <dict>
  <key>dsAttrTypeStandard:AuthenticationAuthority</key>
  <array>
```

```
  <string>*</string>
  </array>
  </dict>
  <key>NoAuthenticateUsers</key> [In this sample code, users from a specific domain name
can log in without being prompted to activate against the Dell Server.]
  <dict>
  <key>dsAttrTypeStandard:AuthenticationAuthority</key>
  <array>
  <string>;Kerberosv5;;*@domainName.com;domainName.com*</string>
  </array>
  </dict>
  <key>NoAuthenticateUsers</key> [In this sample code, specific users can log in without
being prompted to authenticate against the Dell Server.]
  <dict>
  <key>dsAttrTypeStandard:AuthenticationAuthority</key>
  <array>
  <string>;Kerberosv5;;username1@domainName.com;domainName.com*</string>
  <string>;Kerberosv5;;username2@domainName.com;domainName.com*</string>
  </array>
  </dict>
  <key>AllowedOSVersions</key> [AllowedOSVersions is not present in the default .plist
file, it must be added to the file. Add from <key> through </array> to allow a newer
version of operating system to be used. See Note above.]
  <array>
   <string>10.<x.x></string> [Operating system version]
  </array>
  <key>UseRecoveryKey</key>
  <false/> [This value is obsolete since current versions can use both personal and
institutional recovery keys for FileVault encryption.]
  <key>SecurityServers</key>
  <array>
   <dict>
      <key>Host</key>
      <string>securityserver.organization.com</string> [Replace this value with your
Security Server URL]
      <key>Port</key>
     <integer>8443</integer> [Beginning in v8.0, the default port number is 8443. However,
port number 8081 will still allow activations. In general, if your Dell Server is v8.0 or
later, use port 8443. If your Dell Server is pre-v8.0, use port 8081.]
      <key>UseSSL</key>
      <true/> [Dell recommends a true value]
   </dict>
  </array>
  <key>ReuseUniqueIdentifier</key>
  <false/> [When this value is set to true, the computer identifies itself to the Dell
Server by the same hostname it was activated with, regardless of changes to the computer
hostname.]
  <key>Domains</key>
  <array>
   <dict>
      <key>DisplayName</key>
      <string>COMPANY</string>
      <key>Domain</key>
      <string>department.organization.com</string> [Replace this value with the Domain URL
that users will activate against]
   </dict>
  </array>
  <key>PolicyProxies</key>
  <array>
   <dict>
      <key>Host</key>
      <string>policyproxy.organization.com</string> [Replace this value with your Policy
Proxy URL]
      <key>Port</key>
      <integer>8000</integer> [Leave as-is unless there is a conflict with an existing
port]
   </dict>
  </array>
  <key>Version</key>
  <integer>2</integer> [Do not modify]
  <key>MaxPasswordDelay</key>
  <integer>xxxx</integer> [Number of seconds to apply to the security policy, "Require
password XXXX after sleep or screen saver begins." The acceptable range is 0-32400.]
```

```
  <key>EMSTreatsUnsupportedFileSystemAs</key>
  <string>ignore</string> [For handling Mac OS Extended media. Possible values are
ignore, provisioningRejected, or unshieldable. ignore - the media is usable (default).
provisioningRejected - retains the value in the Dell Server policy, EMS Access to
unShielded Media. unshieldable - If the EMS Access to unShielded Media policy is set to
Block, the media is ejected. If the EMS Access to unShielded Media policy is not set to
Block, it is usable as provisioningRejected. The key and value are case sensitive.]
  <key>ClientActivationTimeout</key>
  <integer>120</integer> [Range: 5 to 300, inclusive. The default value is 30. The time in
seconds to give the Security Server time to respond to an activation attempt before giving
up. This plist value is valid for clients running v8.6.0.6627 or later.]
</dict>
</plist>
```

5. Guarde e feche o ficheiro .plist.
6. Para cada computador alvo, copie o pacote para uma pasta temporária e o ficheiro com.dell.ddp.plist para **/Library/Preferences**.
7. Execute a instalação do pacote a partir da linha de comandos através do comando **installer**:
   `sudo installer -pkg "Install Dell Encryption Enterprise.pkg" -target /`
8. Reinicie o computador através da seguinte linha de comandos: **`sudo shutdown -r now`**

   NOTA:

   A Proteção de integridade do sistema (SIP) foi reforçada no macOS High Sierra (10.13) de modo a que os utilizadores tenham de aprovar uma nova extensão kernel de terceiros. Para mais informações sobre a aprovação de extensões kernel no macOS High Sierra, consulte Artigo KB SLN307814.
9. Prossiga para Ativar o Enterprise Edition para Mac.

macOS 10.15 e superior com suportes de dados amovíveis

Se uma empresa utilizar suportes de dados amovíveis com o macOS 10.15 e posterior, os utilizadores têm de ativar o acesso total ao disco para suportes de dados externos. Para obter mais informações, consulte Ativar Acesso Total ao Disco para Suportes de Dados Amovíveis.

Ativar Acesso Total ao Disco para Suportes de Dados Amovíveis

Se uma empresa utilizar suportes de dados amovíveis com o macOS 10.15 e posterior, os utilizadores têm de ativar o acesso total ao disco para suportes de dados externos. Os utilizadores recebem uma das seguintes mensagens de confirmação:

- Após instalar o software cliente, é apresentada uma mensagem de confirmação a indicar que tem de fornecer consentimento para o Acesso Total ao Disco para suportes de dados externos. Clique no botão **Ir para Segurança e Privacidade** e siga os passos abaixo.
- Se não for apresentada uma mensagem após a instalação, é solicitado aos utilizadores que ativem o acesso total ao disco quando montarem o suporte de dados amovível pela primeira vez. É apresentada uma mensagem a indicar que o Dell Encryption External Media ou o EMS Explorer pretende aceder aos ficheiros num volume amovível. Clique em **OK** e siga os passos abaixo.

Para obter mais informações, consulte o artigo KB SLN319972.

1. Em *Preferências do Sistema > Segurança e Privacidade*, clique no separador **Privacidade**.
2. No painel esquerdo, selecione **Acesso Total ao Disco**.
   A aplicação *Dell Encryption External Media* não é apresentada.
3. Na parte inferior, clique no ícone de bloqueio e forneça credenciais para uma conta de administrador local.
   No painel esquerdo > **Ficheiros e pastas**, o utilizador pode verificar os componentes do External Media (EMS) para fornecer as permissões necessárias.
4. No painel esquerdo, selecione **Acesso Total ao Disco**.

   A aplicação *Dell Encryption External Media* é agora apresentada. No entanto, quando o pedido de aprovação estiver pendente, a caixa de verificação para essa aplicação não está selecionada.
5. Conceda permissão selecionando a caixa de verificação.

   Se a aplicação *Dell Encryption External Media* não for apresentada:

   a. Clique no ícone "mais" (+) no painel direito.
   b. Aceda a **/Biblioteca/Dell/EMS** e selecione **Dell Encryption External Media**.
   c. Clique em **Abrir**.
   d. Em **Acesso Total ao Disco**, selecione a caixa de verificação para *Dell Encryption External Media*.
6. Feche a janela **Segurança e Privacidade**.

Ativar o Encryption Enterprise for Mac

O processo de ativação associa as contas de utilizadores de rede do Dell Server ao computador Mac e obtém as políticas de segurança de cada conta, envia atualizações de inventário e de estado, ativa fluxos de trabalho de recuperação e comunicações de conformidade exaustivas. O software cliente executa o processo de ativação para cada conta de utilizador que encontrar no computador, à medida que cada utilizador iniciar sessão na sua conta.

Depois do software cliente ter sido instalado e do computador Mac ter sido reiniciado, o utilizador inicia sessão:

1. Introduza o nome de utilizador e a palavra-passe geridos pelo Active Directory.

   Se a caixa de diálogo da palavra-passe se fechar, clique em **Atualizar** no separador Políticas. Em Ver a política e o estado no computador local, consulte passo 1.

2. Selecione o domínio em que pretende iniciar sessão.

   Se o Dell Server estiver configurado para suporte multidomínio e um domínio diferente for utilizado para ativação, utilize o Nome principal do utilizador (UPN), que tem a forma *<username>@<domain>*.

3. As opções são:
   - Clique em **Ativar**.
     - Se a ativação for bem-sucedida, é apresentada uma mensagem a indicar o êxito da mesma. O Encryption Enterprise fica assim totalmente operacional e gerido pelo Dell Server.

       NOTA:

       Se for apresentado um alerta sobre um recurso de Encryption External Media necessário, clique no botão **Ir para Segurança e Privacidade** e, em seguida, em **Permitir** para qualquer extensão de sistema requerida pela sua organização. Tem de permitir esta extensão para que o Encryption External Media funcione corretamente.
     - Se a ativação falhar, o software cliente permite três tentativas para introduzir as credenciais de domínio corretas. Se as três tentativas fracassarem, é novamente apresentada uma mensagem a solicitar as credenciais de domínio quando o próximo utilizador iniciar sessão.
   - Clique em **Agora não** para ignorar a caixa de diálogo, que será apresentada novamente no próximo início de sessão do utilizador.

     NOTA:

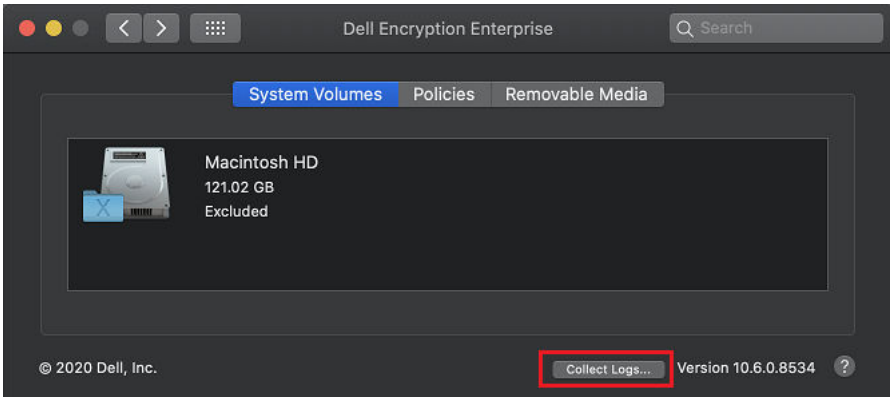
     Quando o administrador precisar de desencriptar uma unidade de um computador Mac, quer seja a partir de uma localização remota, executando um script, ou pessoalmente, o software cliente solicita ao utilizador que permita o acesso de administrador e que introduza a sua palavra-passe.

     NOTA:

     Se configurar o computador para a encriptação FileVault e os ficheiros estiverem encriptados, certifique-se de que inicia sessão numa conta a partir da qual mais tarde pode reiniciar o sistema.
4. Proceda da seguinte forma:
   - Se a encriptação **não** tiver sido ativada antes da ativação, prossiga para Processo de encriptação.
   - Se a encriptação **tiver** sido ativada antes da ativação, prossiga para Ver o estado e a política de encriptação.

Recolher ficheiros de registo para o Encryption Enterprise

Em *Preferências do sistema > Dell Encryption Enterprise > Volumes do sistema* , um botão *Recolher de registos* no canto inferior direito permite que um administrador pré-gere registos para suporte. Esta ação pode afetar o desempenho enquanto os registos são recolhidos.



Os ficheiros DellLogs.zip contêm os registos da Mac Encryption Enterprise. Para mais informações sobre como recolher os registos, consulte http://www.dell.com/support/article/us/en/19/SLN303924.

Ver o estado e a política de encriptação

Pode ver a política de encriptação e o estado no computador encriptado ou na Management Console.

Ver a política e o estado no computador local

Para ver a política de encriptação e o estado de encriptação no computador local, siga os passos abaixo.

1. Inicie *Preferências do sistema* e clique em **Dell Encryption Enterprise**.
2. Clique no separador **Políticas** para ver a política que se encontra definida para este computador. Utilize esta vista para confirmar políticas de encriptação específicas aplicadas neste computador.

   NOTA:

   Clique em **Atualizar** para verificar as atualizações de políticas.

   A Management Console lista as políticas Mac nos seguintes grupos de tecnologia:

   - **Encriptação Mac**
   - **Encriptação de suportes amovíveis**

   As políticas que definir dependem dos requisitos de encriptação da sua empresa.

   Esta tabela indica as opções de política.

Encriptação Mac > Encriptação de volume Dell Para High Sierra e versões superiores, ambas as políticas têm de estar ativadas. Para Sierra e versões anteriores, consulte as versões anteriores da documentação.	
Encriptação de volume Dell	*Ativado* ou *Desativado* Esta é a "política principal" para todas as restantes políticas de Encriptação de volume Dell. Esta política deve ser definida como *Ativada* para que quaisquer outras políticas de Encriptação de volume Dell sejam aplicadas. *Ativado* ativa a encriptação e inicia a encriptação de volumes desencriptados, com base na política *Volumes visados para encriptação* **ou** *Encriptar utilizando o FileVault para Mac*. A predefinição é *Ativado*. A opção "Desativado" desativa a encriptação e inicia o varrimento de desencriptação para quaisquer volumes totalmente ou parcialmente encriptados.
Encriptar utilizando o FileVault para Mac	Se planear utilizar a encriptação do FileVault, certifique-se de que primeiro define a Encriptação de volume Dell para *Ativado*.

	Certifique-se de que a política *Encriptar utilizando o FileVault para Mac* está selecionada na Management Console. Quando ativado, o FileVault é utilizado para encriptar volumes do sistema, incluindo unidades Fusion, com base na definição de política *Volumes visados para encriptação*.
Encriptação Mac > Definições Globais Mac	
Volumes visados para encriptação	*Apenas volume do sistema* ou *Todas as unidades fixas* A definição *Apenas volume do sistema* protege apenas o volume do sistema em execução no momento. A definição **Todas as unidades fixas** protege todos os Volumes expandidos do Mac OS em todos os discos fixos, juntamente com o volume do sistema em execução no momento.

3. Para obter descrições de todas as políticas, consulte *AdminHelp* que está disponível a partir da Management Console. Para localizar uma política especifica em *AdminHelp*:
   a. Clique no ícone de Procura.
   b. Em *Procurar*, introduza o nome da política entre aspas.
   c. Clique na ligação ao tópico que é apresentado. O nome da política que introduziu entre aspas é destacado no tópico.
4. Clique no separador **Volumes do sistema** para ver o estado dos volumes definidos para encriptação.

"Distrito",	**Descrição**
Excluído	O volume é excluído da encriptação. Isto aplica-se a volumes desencriptados quando a encriptação está desativada, volumes externos, volumes com formatos além do Mac OS X Extended (Journaled) e volumes não pertencentes ao sistema quando a política *Volumes visados para encriptação* está definida para Apenas volume do sistema.
A preparar volume para encriptação	O software cliente está atualmente a iniciar o processo de encriptação para o volume, mas ainda não começou o varrimento da encriptação.
O volume não pode ser redimensionado	O software cliente não pode iniciar a encriptação, pois o volume não pode ser redimensionado adequadamente. Depois de receber esta mensagem, contacte o Dell ProSupport e forneça os ficheiros de registo.
Reparação necessária antes do início da encriptação	O volume não conseguiu verificar o Utilitário do disco. Para reparar um volume, siga as instruções no artigo do Suporte Apple HT1782 (http://support.apple.com/kb/HT1782).
Preparação da encriptação concluída. Reinício pendente	A encriptação inicia após o reinício.
Conflito da política de encriptação	A política não pode ser aplicada ao disco pois este está encriptado com uma definição incorreta. Consulte Encriptar utilizando o FileVault para Mac.
A aguardar que chaves de caução estejam na posse do Dell Server	Para garantir que todos os dados encriptados podem ser recuperados, o cliente não inicia o processo de encriptação até que todas as chaves de encriptação tenham sido depositadas com sucesso no Dell Server. O cliente mantém a conectividade com o servidor de segurança enquanto permanecer neste estado até que as chaves sejam caucionadas.
Encriptação	Está em curso um varrimento da encriptação.
Encriptado	O varrimento da encriptação está concluído.
Desencriptação	Está em curso um varrimento da desencriptação.
A restaurar para o estado original	O software cliente está a restaurar o esquema de partição para o seu estado original no final do processo *A desencriptar*. Este é o varrimento de desencriptação equivalente ao estado *A preparar o volume para a encriptação*.

"Distrito",	Descrição
Desencriptado	O varrimento da desencriptação está concluído.

Cor	Descrição
Verde	Porção encriptada
Vermelho	Porção desencriptada
Amarelo	A porção está a ser reencriptada Por exemplo, através de uma alteração nos algoritmos de encriptação. Os dados continuam seguros. Estão apenas a mudar para um tipo de encriptação diferente.

O separador Volumes do sistema apresenta todos os volumes anexados ao computador residentes nos discos formatados Tabela de partições GUID (GPT). A tabela seguinte lista exemplos de configurações do volume para unidades internas.

NOTA:

Os distintivos e os ícones podem variar ligeiramente consoante o sistema operativo.

Distintivo	Tipo de volume e estado
	O volume do sistema Mac OS X atualmente iniciado. O distintivo X-folder indica a partição de arranque atual.
	Um volume configurado para encriptação. O distintivo Segurança e Privacidade indica uma partição protegida pelo FileVault.
	Um volume que não é de arranque configurado para encriptação. O distintivo Segurança e Privacidade indica uma partição protegida pelo FileVault.
	Várias unidades e nenhuma encriptação. **NOTA:** O ícone do volume sem um distintivo indica que nada foi feito ao disco. Este não é um disco de arranque.

5. Clique no separador **Suporte amovível** para ver o estado dos volumes definidos para encriptação. A tabela seguinte lista exemplos de configurações do volume para suportes multimédia amovíveis.

   Os distintivos e os ícones podem variar ligeiramente consoante o sistema operativo.

Distintivo	Estado
	Um ícone de volume mais esbatido indica que o dispositivo não foi montado. As razões incluem: • O utilizador pode ter decidido não fornecê-lo. • O suporte multimédia pode estar bloqueado. **NOTA:**

Distintivo	Estado
	Um distintivo com um círculo/barra vermelha indica uma partição que foi excluída da proteção porque não é suportada. Isto inclui volumes formatados FAT32.
	Um ícone de volume mais escuro indica que o dispositivo foi montado. O distintivo sem escrita indica que é apenas de leitura. A encriptação está ativada, mas o suporte não está aprovisionado e a política Acesso Encryption External Media a suporte de dados não encriptados está definida como Só de leitura.
	Suporte de dados encriptados através de Encryption External Media, indicado por um distintivo Dell.

Ver a política e o estado na Management Console

Para ver a política de encriptação e o estado de encriptação na Management Console, siga os passos abaixo.

1. Como administrador Dell, inicie sessão na Management Console.
2. No painel esquerdo, clique em **Populações > Endpoints**.
3. Para Estação de trabalho, clique numa opção no campo *Nome do anfitrião* ou, se souber o nome do anfitrião do ponto terminal, introduza-o em *Procurar*. Pode também introduzir um filtro para procurar o endpoint.

   NOTA:

   O caráter universal (*) pode ser utilizado, mas não é necessário no início ou fim do texto. Introduza Nome comum, Nome principal universal ou sAMAccountName.
4. Clique no endpoint apropriado.
5. Clique no separador **Detalhes e ações**.

   A secção Detalhes do endpoint apresenta informações sobre o computador Mac.

   A área de detalhes Shield apresenta informações sobre o software cliente, incluindo as horas de início e fim do varrimento de encriptação neste computador.

   Para ver as políticas aplicadas, na secção Ações, clique em **Ver políticas aplicadas**.
6. Clique no separador **Políticas de segurança**. Neste separador, pode expandir os tipos de políticas e alterar cada uma das políticas.
   a. Quando terminar, clique em **Guardar**.
   b. No painel da esquerda, clique em **Gestão** > **Consolidar**.

      NOTA:

      O número apresentado em Alterações às políticas pendentes é cumulativo. Pode incluir as alterações efetuadas noutros endpoints ou efetuadas por outros administradores que estão a utilizar a mesma conta.
   c. Introduza uma descrição das alterações na caixa *Comentário* e clique em **Consolidar políticas**.
7. Clique no separador **Utilizadores**. Esta secção apresenta uma lista de utilizadores ativados neste computador Mac. Clique no nome do utilizador para apresentar informações sobre todos os computadores no qual este utilizador efetuou a ativação.
8. Clique no separador **Grupos de endpoints**. Esta secção apresenta todos os grupos de endpoints aos quais este computador Mac pertence.

Volumes do sistema

Activar encriptação

Os seguintes itens são suportados para encriptação:

- Os volumes do Apple File System (APFS) que partilham suportes físicos com o volume de arranque.
- Os volumes Mac OS X Extended (Journaled) e discos do sistema que são particionados com o esquema de partição Tabela de partições GUID (GPT)

Utilize este processo para ativar a encriptação num computador cliente no qual a encriptação **não** foi ativada antes da ativação. Este processo ativa a encriptação apenas para um único computador. Pode escolher ativar a encriptação para todos os computadores Mac ao nível Enterprise, se desejar. Para obter mais instruções sobre como ativar a encriptação ao nível *Enterprise*, consulte AdminHelp.

1. Como administrador Dell, inicie sessão na Management Console.
2. No painel esquerdo, clique em **Populações** > **Endpoints**.
3. Para estação de trabalho, clique numa opção na coluna hostname ou, se souber o hostname do endpoint, introduza-o no campo *Procurar*. Pode também introduzir um filtro para procurar o endpoint.

   NOTA:

   O caráter universal (*) pode ser utilizado, mas não é necessário no início ou fim do texto. Introduza Nome comum, Nome principal universal ou sAMAccountName.

4. Clique no endpoint apropriado.
5. Na página *Políticas de segurança*, clique no grupo de tecnologia **Encriptação Mac**.

   Por predefinição, a política principal *Encriptação de volume Dell* está definida como *Ligada*.

6. Se um Mac tiver uma unidade Fusion, marque a caixa de verificação da política *Encriptar utilizando o FileVault* para Mac.

   NOTA:

   Esta política requer que a política *Encriptação de volume Dell* também seja definida como *Ligada*. Contudo, quando a encriptação FileVault é ativada, nenhuma das restantes políticas do grupo se encontra aplicada. Consulte Encriptação Mac > Encriptação de volume Dell.

7. Se o FileVault for desativado (macOS Sierra e anteriores), altere as outras políticas conforme pretender.

   Para obter descrições de todas as políticas, consulte *AdminHelp* que está disponível a partir da Management Console.

8. Quando terminar, clique em **Guardar**.
9. No painel da esquerda, clique em **Gestão** > **Consolidar**.

   O número apresentado em Alterações às políticas pendentes é cumulativo. Pode incluir as alterações efetuadas noutros endpoints ou efetuadas por outros administradores que estão a utilizar a mesma conta.

10. Introduza uma descrição das alterações na caixa Comentário e clique em **Consolidar políticas**.
11. Para ver a definição da política no computador local depois de o Dell Server enviar a política, no painel Políticas das Preferências do Dell Encryption Enterprise, clique em **Atualizar**.

Processo de encriptação

O processo de encriptação varia consoante o estado do volume de arranque quando a encriptação está ativada.

NOTA:

Para manter a integridade dos dados do utilizador, o software cliente não começa a encriptar o volume antes de o processo de verificação ter sido concluído com êxito nesse volume. Se um volume não for verificado, o software cliente notifica o utilizador e comunica a falha nas Preferências do Dell Data Protection. Se precisar de reparar um volume, siga as instruções no artigo do Suporte Apple HT1782 (http://support.apple.com/kb/HT1782). O software cliente volta a tentar a verificação no próximo reinício do computador.

Selecione um dos seguintes:

- Encriptação FileVault de um volume não encriptado
- Assumir a gestão de um volume com encriptação FileVault já existente

Encriptação FileVault de um volume não encriptado

Com encriptação FileVault, é apresentado um utilizador adicional sem nome na PBA. Não elimine este utilizador, pois permite que o Dell Server implemente a política no dispositivo. Se o utilizador da PBA for removido, o utilizador terá de efetuar uma ação para iniciar desencriptações autorizadas pela política.

1. Após a instalação e a ativação, deve iniciar sessão na conta que quer reiniciar depois da encriptação do FileVault estar ativa.
2. Aguarde até que a validação da unidade e a verificação do volume sejam concluídas.
3. Introduza a palavra-passe da conta.

   NOTA:

   Se deixar esta caixa de diálogo expirar, terá de reiniciar o computador ou iniciar sessão para que a caixa de diálogo da palavra--passe seja apresentada novamente.
4. Clique em **OK**.
5. Certifique-se de que cada utilizador tem um token seguro. Consulte https://www.dell.com/support/article/us/en/19/sln309192/mobile-users-unable-to-activate-dell-encryption-enterprise-for-mac-on-macos-high-sierra?lang=en.

   Se a conta em que o utilizador tinha sessão iniciada era uma conta de rede não móvel, é apresentada uma caixa de diálogo. Depois da unidade de arranque ser encriptada, a unidade só pode ser reiniciada pelo utilizador que tinha sessão iniciada durante a inicialização do FileVault.

   Esta conta tem de ser uma conta móvel local ou de rede. Para alterar contas sem rede móvel para contas móveis, vá a **Preferências do sistema > Utilizadores e grupos**. Realize um dos seguintes procedimentos:

   - Torne a conta uma conta móvel.

     OU

   - Inicie sessão numa conta local e inicialize o FileVault a partir dessa localização.
6. Clique em **OK**.
7. Após a preparação da encriptação estar concluída, reinicie o computador.

   NOTA:

   Consoante as políticas de experiência do utilizador definidas na Management Console, o software cliente pode solicitar ao utilizador que reinicie o computador.
8. Após o reinício do computador, este deve ser ligado a uma rede para que o software cliente deposite as informações de recuperação no Dell Server.

   O software cliente pode iniciar e concluir o processo de encriptação, bem como comunicar o estado de encriptação à Management Console antes de o utilizador iniciar a sessão. Isto permite-lhe garantir conformidade em todos os computadores Mac sem necessitar da interação do utilizador.

Modificar a política para adicionar utilizadores do FileVault

O FileVault protege os dados num disco, encriptando-o automaticamente. Para permitir que vários utilizadores desbloqueiem o disco num volume de arranque gerido do FileVault, pode modificar uma política na Management Console e utilizar o seu dicionário de nomes e valores de registo do OpenDirectory para permitir que os utilizadores se adicionem ao disco do FileVault.

1. Nas políticas avançadas de *Definições globais Mac* da Management Console, percorra até à política *Lista de utilizadores do FileVault 2 PBA*.
2. No campo da política da *Lista de utilizadores do FileVault 2 PBA*, introduza uma regra que corresponda aos utilizadores que pretende especificar. Por exemplo, ao criar correspondência entre `<string>*</string>` e qualquer tecla, tal deverá fazer correspondência com todos os utilizadores que estão presentes no servidor vinculado do OpenDirectory.

   As etiquetas são sensíveis a maiúsculas e minúsculas, e o valor completo tem de ser formado adequadamente como elementos de dicionário e de matriz numa lista de propriedades. As teclas de dicionário são agrupadas com AND. Os valores de matriz são agrupados com OR. Por conseguinte, ao criar correspondência com qualquer elemento numa matriz, tal fará correspondência com toda a matriz.

NOTA:

Se uma regra for formada incorretamente, é apresentada uma mensagem de erro no separador *Dell Encryption Enterprise* > *Preferências*.

O seguinte <dict> lista exemplos de duas teclas:

```
<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>
```

- As entradas exemplo da tecla *AuthenticationAuthority* especificam um padrão de *user1*, *user2* e *user3* ou qualquer id de utilizador que comece por *z*. Para ver a caixa de diálogo que fornece a sintaxe correta de cada utilizador, prima as teclas **Control-Option--Command** no cliente. Copie a sintaxe do utilizador e cole-a na Management Console.

  NOTA:

  Neste exemplo, os asteriscos à direita representam a última parte dos registos de autoridade de autenticação. Normalmente, e para evitar subespecificações, inclua o registo completo em vez de um asterisco à direita, uma vez que o asterisco corresponde a qualquer informação depois de dois pontos no registo do OpenDirectory.
- A tecla NFSHomeDirectory requer que qualquer utilizador que passe pela primeira tecla tenha também de ter um diretório raiz em */Users/*.

  NOTA:

  Tem de criar a pasta raiz se os utilizadores não tiverem nenhuma.

3. Reinicie os computadores.
4. Notifique os utilizadores para ativarem o arranque do FileVault nas respetivas contas de utilizador. O utilizador tem de ter uma conta local ou móvel. As contas de rede são convertidas automaticamente em contas móveis.

Para que um utilizador ative a sua conta do FileVault:

1. Inicie **Preferências do sistema** e clique em **Dell Encryption Enterprise**.
2. Clique no separador **Volumes do sistema**.
3. Prima a tecla Control e clique na unidade Volume do sistema e selecione **Adicionar utilizadores do FileVault ao arranque do FileVault**.
4. Em *Procurar*, introduza o nome de um utilizador ou percorra para baixo. As contas de utilizador só serão apresentadas se reunirem os critérios definidos pela política.

   É apresentado um botão *Ativar utilizador* aos utilizadores locais e móveis.

   É apresentado um botão *Converter e ativar utilizador* aos utilizadores de rede.

   NOTA:

   É apresentado um indicador verde junto às contas de utilizador que conseguem efetuar o arranque do FileVault.

5. Clique em **Ativar utilizador** ou **Converter e ativar utilizador**.
6. Introduza a palavra-passe da conta selecionada e clique em **OK**. É apresentado um indicador de progresso.
7. Depois de a caixa de diálogo de êxito ter sido apresentada, clique em **Concluído**.

Assumir a gestão de um volume com encriptação FileVault já existente

Se o computador já tiver um volume encriptado pelo FileVault e a encriptação do FileVault estiver ativada na Management Console, o Dell Encryption pode assumir a gestão do volume.

Se a Encriptação Dell detetar que o volume de arranque já está encriptado, é apresentada a caixa de diálogo do Dell Encryption Enterprise. Para permitir que a Encriptação Dell assuma a gestão do volume, siga estes passos.

1. Selecione **Chave de recuperação pessoal *ou* Credenciais de conta de arranque**.

   NOTA:

Para o macOS High Sierra e o Apple File System (APFS), tem de selecionar **Credenciais de conta de arranque**.

- **Chave de recuperação pessoal - Se tem a chave de recuperação pessoal que recebeu quando a unidade foi encriptada pelo FileVault:**
  a. Introduza a chave.

     Se um utilizador não tiver a chave existente, pode solicitá-la ao administrador.

  b. Clique em **OK**.

  NOTA:

  Depois do processo de assunção estar concluído, é gerada e depositada uma nova chave de recuperação pessoal. A chave de recuperação anterior é invalidada e removida.
- **Credenciais de conta de arranque - Se tem o nome de utilizador e a palavra-passe de uma conta atualmente autorizada a arrancar a partir do volume:**
  a. Introduza o nome de utilizador e a palavra-passe.

  b. Clique em **OK**.

2. Quando for apresentada uma caixa de diálogo a indicar que a Dell está agora a gerir a encriptação do volume, clique em **OK**.

   Se a Encriptação Dell detetar que um volume de não arranque já está encriptado, é apresentada uma frase de acesso.

3. (Apenas para volumes de não arranque com encriptação FileVault) Para permitir que a Encriptação da Dell assuma a gestão do volume, introduza a frase de acesso ao volume. Esta é a palavra-passe que foi atribuída ao volume quando foi este foi inicialmente encriptado por FileVault.

   Assim que a Dell passar a gerir a encriptação do volume, a palavra-passe anterior deixará de ser válida. O seu administrador Dell poderá obter uma chave de recuperação para o seu volume no caso de necessitar assistência na recuperação.

   Se optar por não introduzir a palavra-passe, os conteúdos do volume ficam acessíveis e são encriptados com FileVault, mas a encriptação não é gerida pela Dell.

NOTA:

Na Management Console, o administrador pode ver que agora o Dell Server gere o endpoint.

Reciclar chaves de recuperação do FileVault

Se tem problemas de segurança com um pacote de recuperação ou se um volume ou chaves estão comprometidas, pode reciclar o material de chave desse volume.

Pode reciclar chaves para unidades de arranque e de não arranque no Mac OS X.

Para reciclar o material de chave:

1. Transfira um pacote de recuperação da Management Console e copie-o para o ambiente de trabalho do computador.
2. Inicie *Preferências do sistema* e clique em **Dell Encryption Enterprise**.
3. Clique no separador **Volumes do sistema**.
4. Arraste o pacote de recuperação do passo 1 para a partição adequada.

   É apresentada uma caixa de diálogo a solicitar que troque as chaves do FileVault.

5. Clique em **OK**.

   É apresentada uma caixa de diálogo a confirmar o êxito da troca de chaves.

6. Clique em **OK**.

   NOTA:

   As chaves presentes no pacote de recuperação desta unidade são agora obsoletas. Tem de transferir um novo pacote de recuperação da Management Console.

Experiência do utilizador

Para máxima segurança, o software cliente desativa a funcionalidade de *Início de sessão automático* dos computadores com Mac OS X.

Além disso, o software cliente adota automaticamente a funcionalidade de *solicitar palavra-passe após suspensão ou início da proteção de ecrã* do Mac OS X. Além disso, no modo de suspensão/proteção de ecrã, é possível configurar o período de tempo antes de aplicar a autenticação. O software cliente permite a um utilizador definir um valor até cinco minutos antes de a autenticação ser forçada.

Os utilizadores podem utilizar normalmente o computador à medida que o varrimento da encriptação é efetuado. Todos os dados no volume de sistema em arranque estão a ser encriptados, incluindo o sistema operativo, enquanto o sistema operativo continua a funcionar.

Se o computador for reiniciado ou entrar no modo de hibernação, o varrimento da encriptação é interrompido e retomado automaticamente quando o computador for ligado ou reiniciado.

O software cliente não suporta a utilização de imagens de hibernação, algo que a função de *Safe Sleep* do Mac OS X utiliza para acordar o computador caso a bateria descarregue completamente durante a suspensão.

Para reduzir impacto para o utilizador, o software cliente atualiza automaticamente o modo de suspensão do sistema para desativar a suspensão e força a aplicação desta definição. O computador continua a poder entrar em hibernação, mas o estado atual do sistema é mantido apenas na memória. Portanto, o computador é totalmente reiniciado caso se desligue completamente durante a hibernação, que pode ocorrer se a bateria ficar sem carga ou for substituída.

Copiar regra de lista de permissões

Um item oculto do menu permite a um utilizador copiar uma regra de lista de permissões para um suporte de dados amovível.

1. Inicie **Preferências do sistema** e clique em **Dell Encryption Enterprise**.
2. Selecione o separador **Suporte amovível**.
3. Clique com o botão direito na linha de uma unidade e, ao mesmo tempo, prima a tecla de comando.

   É apresentado o item de menu oculto.
4. Clique na opção **Copiar regra de lista de permissões** relativa ao suporte de dados amovível atual. A regra de lista de permissões é copiada para a Área de transferência.
5. Aceda à Área de transferência, copie a regra de lista de permissões aprovada e envie-a ao seu administrador.

Se a política *Encriptação de suporte Mac* estiver definida para **Ligado**, os dados são encriptados, inclusive em unidades Thunderbolt.

Para excluir um dispositivo ou um grupo de dispositivos para evitar a escrita de dados encriptados na unidade Thunderbolt ou em suportes Encryption External Media, utilize a regra da lista de permissões para modificar os valores.

Utilize a regra completa para especificar uma unidade particular para colocação na lista de permissões, como por exemplo:

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

NOTA:

Certifique-se de que substitui os valores de exemplo com as informações da sua unidade.

NOTA:

Tem de ativar HFS Plus. Consulte Ativar HFS Plus.

Para excluir dispositivos SATA da aplicação de política da encriptação de suporte de dados para Mac quando ligado através do Thunderbolt:

tbolt=1;bus=SATA

Também pode colocar na lista de permissões ou excluir suportes de Encryption External Media com base no seguinte:

- **Tamanho do suporte**

  Crie uma regra na lista de permissões para excluir suportes grandes da proteção Encryption External Media:

  size <op> <size specifier>

  <op> pode ser =, <=, >=, <, >

<size specifier> tem uma forma de número inteiro decimal com um sufixo opcional de {K, M, G, T} alinhado a 1000, não 1024. Por exemplo, para excluir suportes ou uma unidade maiores do que 500.000.000 bytes do Encryption External Media, utilize um dos seguintes:

size >= 500000000

size >= 500000K

size >= 500M

- **Tipo de sistema de ficheiros**

  Regra de lista de permissões:

  fstype=<fstype>

  <fstype> pode ser ExFAT, FAT ou HFS+

Para excluir ambos, aqui está um exemplo para suportes HFS+ com 1TB e mais:

size>=1T;fstype=HFS+

Recuperação

Ocasionalmente, pode precisar de aceder a dados em discos encriptados. Como um administrador da Dell, pode aceder aos discos encriptados sem desencriptá-los, poupando tempo precioso.

São vários os motivos que o poderão levar a ter de aceder aos dados encriptados de um utilizador, mas eis alguns casos comuns abaixo:

- Alguém sai da empresa e ninguém sabe a palavra-passe.
- Um utilizador não se lembra da palavra-passe.

Esta secção vai guiá-lo através do processo de utilizar a Recuperação FileVault quando a encriptação FileVault está no ponto terminal a recuperar. O FileVault pode ser utilizado com o Encryption Enterprise for Mac v8.11 ou posterior executado em macOS Sierra 10.12.6. A recuperação do FileVault também é utilizada em unidades Fusion.

Recuperação do FileVault

A recuperação de um volume gerido encriptado pelo FileVault é ditada pela Apple e é automatizada sempre que possível, mas requer mais alguns passos.

O utilitário Dell Recovery simplifica a operação das ferramentas de recuperação da Apple com scripts para assistir na montagem de um volume ou, em alguns casos, na sua desencriptação. A funcionalidade de recuperação do FileVault é determinada pelo sistema operativo instalado na partição de destino emparelhada e Recovery HD.

Um volume encriptado pelo FileVault pode ser recuperado apenas a partir de uma partição Recovery HD que está escrita em todas as unidades de disco executadas no Mac OS X 10.9.5 ou posterior. Este requisito elimina a possibilidade de executar uma operação de recuperação diretamente a partir do utilitário Dell Recovery.

Existem dois métodos de recuperação, dependendo do facto de a chave de recuperação do FileVault ser uma chave de recuperação pessoal ou institucional. Existe sempre uma chave de recuperação válida. Se existir uma chave de recuperação pessoal, a Dell recomenda que utilize a entrada mais recente para essa chave. Se essa chave não funcionar, utilize a keychain de recuperação institucional.

- Chave de recuperação pessoal - a encriptação FileVault existente é gerida pelo Dell Server. Se a entrada mais recente no pacote de recuperação contém uma entrada RecoveryKey, siga os passos de Chave de recuperação pessoal. Segue-se um exemplo de RecoveryKey:

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

- Keychain de Recuperação (raramente utilizada) – Este método de recuperação baseia-se na utilização de uma chave de recuperação institucional do FileVault.

  Se a entrada mais recente no pacote de recuperação contém uma entrada KeychainKey, siga os passos de Keychain de recuperação. Segue-se um exemplo de KeychainKey:

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

Chave de recuperação pessoal

Normalmente, a melhor prática é recuperar o volume de arranque antes de recuperar volumes de não arranque, uma vez que esta ação monta qualquer outro volume que tenha sido encriptado. A recuperação do volume de arranque normalmente corrige os problemas dos volumes não relacionados com o arranque.

Pré-requisitos

- Uma unidade externa de arranque
- O ID do dispositivo/ID único do computador visado para recuperação. Na maioria dos casos, pode encontrar o computador visado para recuperação na Management Console ao pesquisar o nome de utilizador do proprietário e visualizar os dispositivos encriptados para esse utilizador. O formato do ID do dispositivo/ID único é "MacBook.Z4291LK58RH de Fulano de Tal".
- O suporte multimédia de instalação da Dell

Management Console - Guardar o pacote de recuperação

1. Abra a Management Console.
2. No painel esquerdo, clique em **Populações > Endpoints**.
3. Procure o dispositivo a recuperar.
4. Clique no nome do dispositivo para abrir a página Detalhe do Endpoint.
5. Clique no separador **Detalhes e ações**.
6. Em *Detalhe de proteção*, clique na ligação **Chaves de recuperação de dispositivos**.
7. Para guardar o pacote de recuperação no volume de recuperação externo ou no computador que executará o utilitário de recuperação para realizar a operação de recuperação, clique em **Transferir** e clique em **Guardar**.
8. Introduza uma localização para o pacote de recuperação e clique em **Guardar**.

Processo - Instalar .dmg

1. Copie o pacote de recuperação e o ficheiro **Dell-Encryption-Enterprise-<version>.dmg** para a unidade USB de arranque.
2. Arranque o computador de destino a partir de um volume de instalação externo pré-criado do sistema operativo completo premindo a tecla **Opção** enquanto reinicia este computador e, em seguida, selecione o volume de instalação externo pré-criado do sistema operativo completo no Gestor de arranque em modo pré-arranque. Para criar um volume de arranque, consulte https://support.apple.com/en-us/HT202796.
3. Monte o ficheiro **Dell-Encryption-Enterprise-<version>.dmg**.

Processo - Iniciar o Utilitário de recuperação Dell e recuperar o volume FileVault

1. Na pasta Utilitários localizada no suporte de instalação da Dell, inicie o Utilitário de recuperação Dell.

   É apresentada a caixa de diálogo *Utilitário de recuperação Dell > Selecionar volumes*.

   NOTA:

   O Utilitário de recuperação deverá ser o mesmo ou uma versão mais recente do que a versão do software cliente instalado no computador visado para recuperação.
2. Em *Utilitário de recuperação Dell > Selecionar volumes*, selecione o volume FileVault.
   - Ao recuperar um sistema operativo, a melhor prática é iniciar um computador com o mesmo sistema operativo ou posterior.
   - Se tem volumes de não arranque encriptados, por norma, terá de recuperar a partição de arranque primeiro.
3. Clique em **Continuar**.
4. Localize e selecione o pacote de recuperação (guardado anteriormente) e clique em **Abrir**.
5. Se a caixa de diálogo *Selecionar registo de recuperação* for apresentada, consulte a coluna *Data de depósito*, selecione a data mais recente para o tipo de chave de recuperação pessoal e clique em **Continuar.**

   NOTA:

   Com uma data de depósito mais antiga, a chave pode já não ser válida.

   A caixa de diálogo *Resultado da operação de recuperação* é apresentada.
   - Para unidades de arranque, a ferramenta de recuperação oferece uma chave de recuperação pessoal que lhe permite efetuar o arranque através do método normal de recuperação do FileVault da Apple. Pode efetuar o arranque na partição de destino e introduzir a chave de recuperação pessoal para a Autenticação de pré-arranque, que pode variar consoante o sistema operativo.
   - Para unidades de não arranque, é apenas apresentada a chave de recuperação pessoal. É fornecido um botão de Desbloquear para desbloquear e montar o volume.
6. Proceda da seguinte forma:

- Recuperar o volume de arranque (mais comum)
- Recuperar um volume de não arranque (raramente utilizada)

Recuperar o volume de arranque (mais comum)

Para a maioria dos casos de recuperação, utilize esta opção para recuperar o volume de arranque:

1. Anote a chave ou clique em **Imprimir chave de recuperação**.
2. Clique em **Fechar**.
3. Efetue o arranque do volume que pretende recuperar, utilizando o Gestor de Arranque em pré-arranque, se necessário.

   O computador apresenta ícones para vários utilizadores ou solicita uma palavra-passe.
4. Selecione um utilizador, se aplicável, e clique em **?** no ecrã de início de sessão.
5. Clique na seta apresentada.
6. Escreva a chave de recuperação e prima **Enter**.
7. Na caixa de diálogo, introduza uma nova palavra-passe para o utilizador.

Opções para recuperar volumes de não arranque (raramente utilizada) – Efetue uma das seguintes ações:

Recuperar um volume de não arranque

Se o volume de arranque estiver danificado ou tiver sido apagado e existirem volumes secundários, pode montar estes volumes de não arranque.

1. Clique em **Desbloquear**. O volume é montado.
2. Clique em **Fechar**.

Desencriptar volume - clique no botão

1. Clique em **Desencriptar**. O processo de desencriptação é indicado por uma caixa de diálogo e uma barra de progresso.
2. Quando estiver concluído, clique em **Fechar**.
3. Inicie com o volume desencriptado para o utilizar.

Desencriptar volume - execute o comando a partir de Terminal

1. Copie o comando na área *Desencriptar volume*.
2. Clique em **Fechar**.
3. Execute o comando em Terminal.

Keychain de recuperação

Tem de executar o Dell Recovery Utility enquanto este é iniciado num volume de recuperação não encriptado.

Pré-requisitos

- Um volume de recuperação externo ou computador que irá executar o utilitário de recuperação
- Uma unidade USB
- Um cabo Firewire
- O suporte multimédia de instalação da Dell

Management Console - Guardar o pacote de recuperação

1. Abra a Management Console.
2. No painel esquerdo, clique em **Populações > Endpoints**.
3. Procure o dispositivo a recuperar.
4. Clique no nome do dispositivo para abrir a página Detalhe do Endpoint.
5. Clique no separador **Detalhes e ações**.
6. Em *Detalhe de proteção*, clique na ligação **Chaves de recuperação de dispositivos**.
7. Para guardar o pacote de recuperação no volume de recuperação externo ou no computador que executará o utilitário de recuperação para realizar a operação de recuperação, clique em **Transferir** e clique em **Guardar**.
8. Introduza uma localização para o pacote de recuperação e clique em **Guardar**.

Processo

1. Ligue um disco externo ao sistema a recuperar.

O disco externo tem de conter um volume de arranque Mac OS.

2. Efetue o arranque na unidade externa mantendo premida a tecla **Opção** e utilize o seletor de arranque para efetuar a seleção e o arranque a partir deste volume.
3. Copie o pacote de recuperação a partir da Management Console.
4. Monte o ficheiro de instalação .dmg.
5. Na pasta Utilitários, execute o Utilitário de recuperação Dell.

   É apresentada a caixa de diálogo *Utilitário de recuperação Dell > Selecionar volumes*.
6. Selecione o volume FileVault a recuperar e clique em **Continuar**.

   É apresentada a caixa de diálogo *Escolher pacote de recuperação*.
7. Selecione o pacote de recuperação e clique em **Abrir**.

   Se houver mais do que uma chave de recuperação para esse disco, é apresentado o ecrã *Selecionar registo de recuperação*.
8. Na coluna Data de depósito, selecione a data mais recente para o tipo de recuperação de Keychain e clique em **Continuar**.

   NOTA:

   Com uma data de depósito mais antiga, a chave pode já não ser válida.

   É apresentada a caixa de diálogo *Instruções de recuperação FileVault*.
9. Leia as instruções e clique em **Continuar**.

   É apresentada a caixa de diálogo *Confirmar operação de recuperação*.
10. Destaque o volume FileVault a recuperar e clique em **Continuar**.

    É apresentada a caixa de diálogo *Escolher localização para os ficheiros de recuperação*, solicitando que escolha uma localização para os ficheiros de recuperação.

    Esta localização tem de ser a localização que irá utilizar para a recuperação, uma vez que os scripts contêm caminhos absolutos para os ficheiros de dados. **Não** copie estes ficheiros para o Recovery HD.

    A Dell recomenda que guarde estes ficheiros na raiz de uma unidade amovível, como uma unidade USB.

    NOTA:

    Certifique-se de que todos os utilizadores têm acesso de leitura/escrita ao USB ou outro disco que utiliza para armazenar a chave de recuperação e que o disco tem espaço suficiente. Se não tem direitos para aceder a um disco selecionado ou se o disco não tem espaço, é apresentado um erro a indicar que as chaves de recuperação não foram armazenadas.
11. Selecione uma localização e clique em **Guardar**.

    É apresentada a caixa de diálogo *Resultado da operação de recuperação*, que indica os ficheiros que foram criados.
12. Clique em **Fechar**.
13. Depois do volume do Recovery HD reiniciar, introduza o nome e o caminho do script.

    NOTA:

    Armazenar os ficheiros perto da raiz de um volume encurta o caminho que precisará de introduzir.

    O Resultado da Operação de Recuperação apresenta a chave.

    O utilitário Recovery envia os ficheiros para a localização selecionada e, em seguida, apresenta os comandos exatos que precisa de executar a partir do volume Recovery HD para montar ou desencriptar o volume FileVault.
14. Depois destes ficheiros serem gerados, copie as strings de comandos apresentadas na caixa de diálogo *Resultado da operação de recuperação*.
15. Reinicie o disco rígido de recuperação de uma das seguintes formas:
    - Prima em simultâneo as teclas **Command-R** antes do sinal sonoro de Power-On/Self-Test e durante o arranque do computador.

      ou em
    - Para versões anteriores da Apple, prima a tecla **Opção** e utilize o seletor de arranque para selecionar o Recovery HD.

      É apresentada a caixa de diálogo *Mac OS X Utilities*.

16. No menu Ferramentas, selecione **Utilitários > Terminal**.
17. Para montar o volume de forma a poder copiar ficheiros do Terminal ou a criar uma imagem do disco a partir do Utilitário do disco: no Terminal, digite o caminho completo e o nome de script **fv2mount.sh**, por exemplo:

    /Volumes/recoveryFOB/fv2mount.sh
18. Reinicie o computador.

Suporte multimédia amovível

Formatos suportados

São suportados suportes multimédia FAT32, exFAT ou HFS Plus (Mac OS Extended) formatados com esquemas de partição Registo de arranque principal (MBR) ou Tabela de partições GUID (GPT). Tem de ativar HFS Plus.

NOTA:

De momento, o Mac não suporta a gravação de CD/DVD para Encryption External Media. No entanto, o acesso às unidades CD/DVD não é bloqueado, mesmo que a política *Bloqueio EMS a acesso a suporte UnShieldable* seja selecionada.

Ativar o HFS Plus

Para ativar o HFS Plus, adicione o seguinte ao ficheiro .plist.

<key>EMSHFSPlusOptIn</key>

<true/>

NOTA:

A Dell recomenda o teste desta configuração antes de ser introduzida no ambiente de produção.

O HFS Plus não suporta:

- Versões - Os dados de versões existentes são removidos do disco.
- Ligações físicas - Durante um varrimento de encriptação dos suportes de dados amovíveis, o ficheiro não é encriptado. Uma caixa de diálogo recomenda que o suporte de dados seja ejetado.
- Suportes com cópias de segurança Time Machine:
  - Os suportes que sejam reconhecidamente utilizados pelo computador como destino de cópias de segurança Time Machine são colocados automaticamente na lista de permissões, a fim de permitir que as cópias de segurança continuem a ser realizadas.
  - Todos os outros suportes amovíveis com cópias de segurança Time Machine baseiam-se em políticas que regem os suportes de dados não indicados e os suportes de dados não protegidos. Consulte as políticas *Acesso EMS a suporte UnShieldable* e *Bloqueio EMS a suporte UnShieldable*.

    NOTA:

    Para uma nova unidade que ainda não tenha cópias de segurança, o utilizador deve copiar a respetiva regra de lista branca e enviar-lhe a regra para especificar a sua unidade Time Machine para integrar a lista de permissões. Consulte Copiar regra de lista de permissões.

Atualizações de políticas e de Encryption External Media

No sistema onde o suporte de dados amovível foi fornecido (ou recuperado), as políticas são atualizadas no suporte de dados amovível durante a montagem.

Exceções de encriptação

Os atributos expandidos não são encriptados no suporte de dados amovível.

Erros no separador Suporte multimédia amovível

- Num computador desprotegido, não substitua um ficheiro encriptado por uma versão desencriptada do ficheiro. Mais tarde, isto poderá impedir a desencriptação. Isto também pode ser apresentado como um erro no separador Suporte multimédia amovível.
- Se um marcador no fim do ficheiro for invalidado, por exemplo, se um ficheiro for substituído por novo conteúdo fora do controlo do Encryption External Media e, em seguida, o montar no Encryption External Media, é apresentado um erro no fim do ficheiro no separador Suporte de dados amovível.
- Quando converte ficheiros, o suporte multimédia tem de ter mais espaço livre do que o tamanho do maior ficheiro a converter. Se for apresentado um triângulo de aviso amarelo na área de estado do Suporte multimédia amovível, clique no mesmo. Se uma mensagem indicar *Espaço insuficiente*, faça o seguinte:

  1. Tenha em atenção a quantidade de espaço que deve ser libertada no dispositivo. O relatório apresenta uma lista de ficheiros e o tamanho.
  2. Esvazie o lixo. À medida que for libertando espaço, o Encryption External Media encripta automaticamente ficheiros adicionais.
  3. Se eliminar algum ficheiro ou pasta, certifique-se de que esvazia o lixo novamente.

Mensagens de auditoria

As mensagens de auditoria são enviadas para o Dell Server.

Desinstalar o Encryption Enterprise para Mac

O software cliente pode ser desinstalado através da execução da aplicação **Uninstall Dell Encryption Enterprise**. Para desinstalar o software cliente, siga os passos abaixo.

NOTA:

Antes de executar a aplicação de desinstalação, o disco tem de estar totalmente desencriptado.

1. Se o disco estiver encriptado, defina a política *Encriptação de volume Dell* do computador para **Desativado** na Management Console e consolide a política.

   É apresentada uma caixa de diálogo que solicita o acesso às Preferências do sistema e o controlo do computador, de forma a que o software cliente possa desencriptar o disco.

   a. Clique em **Abrir preferências do sistema**.

      Se **Recusar** for selecionado, não é possível prosseguir com a desinstalação e a encriptação.

   b. Introduza a palavra-passe de administrador.
2. Depois do disco estar totalmente desencriptado, reinicie o computador (quando solicitado).
3. Após o reinício do computador, inicie a aplicação **Uninstall Dell Encryption Enterprise** (localizada na pasta Utilities, em Dell--Encryption-Enterprise-<version>.dmg no suporte de instalação da Dell).

   As mensagens apresentam o estado da desinstalação.

   O Encryption Enterprise para Mac fica assim desinstalado e o computador pode ser utilizado normalmente.

Desinstaslar o Encryption External Media

Para desinstalar o Encryption External Media:

1. Navegue até **Biblioteca > Dell > EMS** e selecione a aplicação **Uninstall EMS**.
2. Na página Uninstall Dell EMS, clique em **Desinstalar**.
3. Introduza o seu nome de utilizador e palavra-passe, e clique em **OK**.
4. No ecrã de confirmação da desinstalação, clique em **OK**.

4

Ativação como administrador

O Client Tool oferece ao administrador novos métodos para ativar o software cliente num computador Mac e para analisar o software cliente. Estão disponíveis dois métodos de ativação:

- Ativação com as credenciais de administrador
- Uma ativação temporária que emula o utilizador sem deixar rastro nesse computador.

Ambos os métodos podem ser utilizados diretamente através de uma shell ou de um script.

NOTA:

Não ative o software cliente em mais de cinco computadores com a mesma conta de rede. Tal poderá resultar em graves vulnerabilidades em termos de segurança e num desempenho degradado do seu Dell Server.

Pré-requisitos

- O Encryption Enterprise for Mac v8.1.3 ou posterior tem de ser instalado no computador remoto.
- Não efetue a ativação através da interface do utilizador do cliente antes de tentar efetuá-la a partir de uma localização remota.

Tópicos

Ativar

Utilize este comando para ativar o cliente como administrador.

Exemplo:

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

Ativar temporariamente

Utilize este comando para ativar o cliente sem deixar rastro no computador.

1. Abra uma shell ou utilize um script para ativar o software cliente:

   client *-at username@domain.com password*

2. Utilize o Client Tool para obter informações sobre o software cliente, as suas políticas, o estado do disco, a conta de utilizador e mais. Para obter mais informações sobre o Client Tool, consulte Client Tool.

   NOTA:

   Após a ativação, as informações sobre o software cliente, incluindo as políticas, o estado do disco e as informações sobre o utilizador também estão disponíveis em Preferências do sistema nas Preferências do Dell Encryption Enterprise.

5

Utilizar o Boot Camp

Tópicos

- Assistência Mac OS X Boot Camp
- Recuperação de Encryption Enterprise for Windows no Boot Camp

Assistência Mac OS X Boot Camp

NOTA:

Ao utilizar o Boot Camp, o Dell Encryption Enterprise não encripta o sistema operativo Windows. Além disso, se existirem duas ou mais partições macOS de arranque no dispositivo, o Encryption Enterprise encripta apenas o volume principal.

O Boot Camp é um utilitário incluído no Mac OS X que o ajuda a instalar o Windows em computadores Mac através de uma configuração de arranque duplo. O Boot Camp é compatível com os seguintes sistemas operativos Windows:

- Windows 7 e 7 Home Premium, Professional e Ultimate (64 bits)
- Windows 8.1 e 8.1 Pro (64 bits)

NOTA:

Windows 7 para o Boot Camp 4 ou 5.1. Windows 8,1 e posterior apenas para o Boot Camp 5.1.

Para utilizar o Encryption Enterprise para Windows no Boot Camp de um computador com Encryption Enterprise para Mac, o volume do sistema tem de ser encriptado pelo Encryption Enterprise com o FileVault2. Consulte Instalação/atualização através de linha de comandos para mais instruções.

NOTA:

Se a sua partição Windows for candidata para Encryption External Media, certifique-se de que a coloca na lista de permissões ou esta será encriptada. Consulte Copiar regra de lista de permissões.

NOTA:

Deve certificar-se de que o Windows está instalado antes de implementar as políticas do cliente ativando a encriptação. Depois do cliente iniciar o processo de encriptação, este proíbe as operação de partição de disco exigida pelo Boot Camp.

Recuperação de Encryption Enterprise for Windows no Boot Camp

Para recuperar o Encryption Enterprise for Windows num volume Boot Camp, tem também de criar um volume Boot Camp numa unidade externa.

Pré-requisitos

- Uma unidade externa de arranque
- O ID do dispositivo/ID único do computador visado para recuperação. Na maioria dos casos, pode encontrar o computador visado para recuperação na Management Console ao pesquisar o nome de utilizador do proprietário e visualizar os dispositivos encriptados para esse utilizador. O formato do ID do dispositivo/ID único é "MacBook.Z4291LK58RH de Fulano de Tal".

Processo

1. Numa unidade externa, crie um volume Boot Camp.

   Os passos são semelhantes à criação de um volume Boot Camp no seu sistema local. Consulte http://www.apple.com/support/bootcamp/.

2. Na Management Console, copie o pacote de recuperação para uma das seguintes:

- Unidade USB de arranque

  ou em

- Partição FAT no volume Boot Camp externo

3. Desligue o computador com o volume Boot Camp para efetuar a recuperação.
4. Ligue a unidade externa ao computador.

   Esta unidade contém o volume Boot Camp criado no passo 1.

5. Para arrancar o computador a partir de uma unidade Boot Camp externa, efetue um destes passos:
   - Prima em simultâneo as teclas **Command-R** antes do sinal sonoro de Power-On/Self-Test e durante o arranque do computador.

     ou em

   - Para versões anteriores da Apple, prima a tecla **Opção** enquanto liga o computador.

     É apresentada a caixa de diálogo *Mac OS X Utilities*.

6. Selecione o volume Boot Camp (Windows) que se encontra na unidade externa.
7. Na unidade USB ou na partição FAT, clique com o botão direito no pacote de recuperação (do passo 2) e selecione **Executar como administrador**.
8. Clique em **Sim.**
9. Na caixa de diálogo do Dell Encryption Enterprise, selecione uma opção:
   - *O meu sistema não arranca* - Se o utilizador não consegue arrancar o sistema, selecione a primeira opção

     ou em

   - *O meu sistema não permite me permite aceder a dados encriptados* - Se o utilizador não conseguir aceder a alguns ficheiros encriptados ao iniciar sessão no sistema, selecione a segunda opção.
10. Clique em **Seguinte**.

    É apresentado o ecrã Informações de cópia de segurança e de recuperação.

11. Clique em **Seguinte**.
12. Selecione o volume Boot Camp a recuperar.

    NOTA:

    Não é o volume Boot Camp externo.

13. Clique em **Seguinte**.
14. Introduza a palavra-passe associada a este ficheiro.
15. Clique em **Seguinte**.
16. Clique em **Recuperar**.
17. Clique em **Concluir**.
18. Quando o reinício for solicitado, clique em **Sim.**
19. O sistema reinicia e pode iniciar sessão no Windows.

6

Client Tool

O Client Tool é um comando shell executado num endpoint Mac. É utilizado para ativar o cliente a partir de uma localização remota ou para executar um script através de um utilitário de gestão remota. Enquanto administrador, pode ativar um cliente e fazer o seguinte:

- Ativar como administrador
- Ativar temporariamente
- Obter informações do cliente Mac

Para utilizar o Client Tool manualmente, abra uma sessão ssh e introduza o comando pretendido na linha de comandos.

Exemplo:

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

Introduza apenas **client** para ver as instruções de utilização.

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

Tabela 1. Comandos do Client Tool

Comando	Propósito	Sintaxe	Resultados
Ativar	Ativa um cliente Mac com o Dell Server, mas sem passar pela interface de utilizador. Para ativar, é preciso introduzir um domínio, um nome de utilizador e uma palavra-passe válidos. Com o Client Tool, pode ativar um utilizador local diferente daquele que iniciou sessão e associar as credenciais de domínio a esse utilizador.	-a domainAccount domainPassword -a localAccount* domainAccount domainPassword **domainAccount** é a conta utilizada para ativar através do Client Tool. **localAccount** é opcional e é o utilizador atual, caso não seja especificado nenhum outro. O comando de ativação tem o seguinte formato: client -a <user to activate*> <domainUser> <domainPassword> Se utilizar a política *Sem Lista de utilizadores autenticados* para criar classes de utilizadores que não sejam ativadas no Dell Server, pode, opcionalmente, utilizar o Client Tool para especificar uma conta local diferente daquela em que iniciou sessão. Consulte a política Sem Lista de utilizadores autenticados no passo 3.	0 = Sucesso 2 = Falha na ativação e a razão da falha 6 = Utilizador não encontrado
Ativar temporariamente	Ativa um cliente Mac sem deixar rastro.	-at domainAccount domainPassword -at localAccount* domainAccount domainPassword	
Disco	Solicita o estado do disco	-d	É apresentado o estado do disco, incluindo o ID do disco, o estado da encriptação e as políticas Se forem apresentadas chavetas vazias, significa que não existem discos encriptados.

Tabela 1. Comandos do Client Tool (continuação)

Comando	Propósito	Sintaxe	Resultados
Recuperação de alterações do FileVault	Troca chaves de recuperação para volumes FileVault	-fc deviceId recoveryPassphrase -fc deviceId personalRecoveryKey -fc deviceId pathToKeychain keychainPassword -fc deviceId recoveryFile **NOTA:** O ID do dispositivo tem de ser um UUID de volume lógico ou resolvido para exatamente um LVUUID. Muitas vezes, um ponto de montagem ou devnode funciona.	0 = Sucesso 7= LVUUID não encontrado 10 = Falha nas credenciais 11 = Falha na caução
Política	Solicita as políticas do cliente Mac	-p	São apresentadas as políticas
Servidor	Consulta o Dell Server para obter políticas atualizadas em nome do cliente Mac **NOTA:** A consulta pode demorar vários minutos a ser concluída.	-s	0 = Sucesso Qualquer outro valor indica que o Dell Server ou o software cliente do Mac estava ocupado ou não respondeu.
Teste	Testar o estado de ativação do cliente Mac	-t localAccount*	0 (domainAccount) = Sucesso 1 = Desativado 6 = Utilizador não encontrado
Utilizador	Solicita informações sobre o utilizador	-u localAccount*	São apresentadas informações sobre a conta do utilizador: 0 (informações da conta) = Sucesso 6 = Utilizador não encontrado
Versão	Solicita a versão do cliente Mac	-v	É apresentada a versão do cliente Mac: Exemplo: 8.x.x.xxxx

* A conta que está a executar o Client Tool é utilizada para localAccount, exceto se for especificada outra.

A opção Plist

A opção -plist imprime os resultados do comando com o qual é combinada. Segue o comando e deve aparecer antes dos argumentos para fazer com que os resultados sejam imprimidos como uma plist.

Exemplos

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

Para obter as políticas do cliente e imprimi-las.

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

Para ativar o cliente temporariamente e imprimir o resultado.

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

Para consultar o Dell Server para atualizar as políticas em nome do cliente e apresentá-las no ecrã.

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

Para obter o estado do disco do cliente e imprimi-lo.

Códigos de retorno globais

Sem erros 0

Erro do parâmetro 4

Comando não reconhecido 5

Socket expirado 8

Erro interno 9

7

Glossário

Security Server - Utilizado para ativações do Dell Encryption.

Policy Proxy - Utilizado para distribuir políticas para o software cliente.

Management Console - A consola de administração do Dell Server para implementação em toda a empresa.

Shield - Ocasionalmente, poderá ver este nome na documentação e nas interfaces do utilizador. "Shield" é um nome utilizado para representar o Dell Encryption.