Dell Data Protection | Endpoint Security Suite Enterprise for Mac

Administrator Guide v1.1

Notas, avisos e advertências

NOTA: Uma NOTA indica informações importantes que ajudam você a usar melhor o seu produto.

CUIDADO: Um AVISO indica possíveis danos ao hardware ou perda de dados e ensina como evitar o problema.

ATENÇÃO: Uma ADVERTÊNCIA indica possíveis danos à propriedade, risco de lesões corporais ou mesmo risco de vida.

Administrator Guide

2017 - 05

Rev. A02

Contents

1

Introdução

O Guia do administrador do Endpoint Security Suite Enterprise para Mac fornece as informações necessárias para implantar e instalar o software cliente.

Tópicos:

Visão geral

O Endpoint Security Suite Enterprise para Mac oferece prevenção avançada contra ameaças no sistema operacional, nas camadas de memória e na criptografia, com gerenciamento centralizado pelo Dell Data Protection Server. Com gerenciamento centralizado, relatórios de conformidade consolidados e alertas de ameaças ao console, as empresas podem facilmente reforçar e comprovar a conformidade em todos os seus pontos de extremidade. A experiência em segurança está integrada a recursos, como modelos predefinidos de políticas e relatórios, para ajudar as empresas a reduzirem os custos de gerenciamento e a complexidade de TI.

- Endpoint Security Suite Enterprise para Mac - um pacote de software para criptografia de dados e prevenção avançada contra ameaças para o cliente.
- Proxy de política - usada para distribuir políticas
- Servidor de segurança - usado para ativações do software Client Encryption
- Enterprise Server ou Dell Enterprise Server - VE - fornece administração centralizada da política de segurança, integra-se a diretórios existentes da empresa e cria relatórios. Para a finalidade deste documento, ambos os servidores são citados como Dell Server, a menos que uma versão específica precise ser citada (por exemplo, um procedimento é diferente ao ser usado o Dell Enterprise Server - VE).

  Esses componentes Dell interoperam diretamente para fornecer um ambiente móvel seguro sem desprezar a experiência do usuário.

O Endpoint Security Suite Enterprise para Mac possui dois arquivos .dmg - um para o Encryption client e outro para Advanced Threat Prevention. Você pode instalar apenas um ou ambos.

Dell Encryption Client e criptografia FileVault

A opção de gerenciar a criptografia FileVault, juntamente com o Dell Encryption client, está disponível com o Endpoint Security Suite Enterprise para Mac. A opção mais adequada depende dos requisitos de criptografia da empresa. Para obter mais informações sobre políticas de criptografia, consulte Criptografia para Mac > Dell Volume Encryption.

Entre em contato com o Dell ProSupport

Ligue para 877-459-7304, extensão 4310039 para obter suporte por telefone, 24 horas por dia, 7 dias na semana, para o seu produto Dell Data Protection.

Há também disponível o serviço de suporte on-line para os produtos Dell Data Protection no site dell.com/support. O suporte on-line inclui drivers, manuais, orientações técnicas, perguntas frequentes e problemas emergentes.

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

2

Requisitos

Os requisitos de hardware e software de cliente são apresentados neste capítulo. Verifique se o ambiente de implementação atende aos requisitos antes de continuar com as tarefas de implementação.

Tópicos:

Encryption Client

Hardware do Encryption Client

Os requisitos mínimos de hardware precisam atender às especificações mínimas do sistema operacional.

NOTA: O disco do sistema precisa ser particionado com o esquema de partição da Tabela de Partição GUID (GPT) e ter um formato Mac OS X Extended (Journaled).

Hardware

- 30 MB de espaço livre em disco
- Placa de interface de rede 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.

Advanced Threat Prevention

- Desinstale os aplicativos antivírus, antimalware e antispyware de outros fornecedores antes de instalar o cliente Advanced Threat Prevention para evitar falhas na instalação.

Hardware do Advanced Threat Protection

Os requisitos mínimos de hardware precisam atender às especificações mínimas do sistema operacional.

Hardware

- 500 MB de espaço livre em disco, dependendo do sistema operacional
- 2 GB de RAM
- Placa de interface de rede 10/100/1000 ou Wi-Fi

Hardware do Advanced Threat Prevention

A tabela a seguir detalha os softwares suportados.

Sistemas operacionais (kernels de 64 bits)

- Mac OS X Mavericks 10.9.5

NOTA: Essa versão se aplica somente ao Advanced Threat Prevention, não ao cliente de criptografia.

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

NOTA: Não há suporte para sistemas de arquivos que diferenciam maiúsculas de minúsculas.

Portas do Advanced Threat Prevention

- Os agentes do Advanced Threat Prevention são gerenciados pela plataforma SaaS do console de gerenciamento e se comunicam com ela. A porta 443 (https) é usada para a comunicação e precisa estar aberta no firewall para que os agentes consigam se comunicar com o console. O console é hospedado pelo Amazon Web Services e não possui IP fixo. Se a porta 443 estiver bloqueada por algum motivo, não será possível fazer o download das atualizações, de modo que os computadores podem não ter a proteção mais atual. Certifique-se de que os computadores cliente possam acessar os URLs da seguinte forma.

Uso	Protocolo de aplicativo	Protocolo de transporte	Número da porta	Destino	Direção
Toda a comunicação	HTTPS	TCP	443	Permitir todo o tráfego https para *.cylance.com	Saída

Tarefas para o Encryption Client

Instalar/Fazer upgrade do Encryption Client

Esta seção ajudará você na instalação/upgrade e no processo de ativação do Encryption Client para Mac.

Existem dois métodos para instalação/upgrade do Encryption Client para Mac. Selecione **uma** das seguintes opções:

- Instalação/Upgrade interativos e ativação - Este é o método mais fácil para instalar ou fazer upgrade do pacote de software cliente. Entretanto, não permite quaisquer personalizações. Se você pretender usar o Boot Camp ou uma versão de sistema operacional que ainda não seja totalmente suportada pela Dell (por modificação do .plist), precisará usar o método de instalação/upgrade por linha de comando. Para obter informações sobre como usar o Boot Camp, consulte Como usar o Boot Camp.
- Instalação/upgrade por linha de comando - Este é um método avançado de instalação/upgrade que só deve ser usado por administradores com experiência na sintaxe da linha de comando. Se você pretender usar o Boot Camp ou uma versão de sistema operacional que ainda não seja totalmente suportada pela Dell (por modificação do .plist), precisará usar este método para instalar/fazer upgrade do pacote de software cliente. Para obter informações sobre como usar o Boot Camp, consulte Como usar o Boot Camp.

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

> **NOTA: A Apple frequentemente lança novas versões de sistemas operacionais entre liberações do Endpoint Security Suite Enterprise para Mac. Para que essas versões de sistemas operacionais sejam compatíveis com o máximo de clientes possível, é permitido modificar o arquivo com.dell.ddp.plist. Assim que a Apple lança uma nova versão, começamos a testar essa versão para garantir que ela é compatível com o Encryption client para Mac.**

Pré-requisitos

A Dell recomenda que as boas práticas de TI sejam seguidas durante a implantação do software cliente. Isso inclui, entre outros, ambientes de teste controlados para testes iniciais e implantações escalonadas para os usuários

Antes de iniciar este processo, confirme que os seguintes pré-requisitos sejam atendidos:

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

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

  Enterprise Server Installation and Migration Guide (Guia de Instalação e Migração do Enterprise Server)

  Guia de Instalação e de Início Rápido do Enterprise Server - Virtual Edition
- Certifique-se de que você tenha à mão os URLs do Servidor de segurança e do Proxy de política. Os dois serão necessários para a instalação e a configuração do software cliente.
- Se a implantação usar uma configuração que não é a padrão, certifique-se de conhecer o número da porta do Servidor de segurança. Ele será necessário para a instalação e a configuração do software cliente.
- Certifique-se de que o computador de destino tenha conectividade de rede com o Servidor de segurança e com o Proxy de política.
- Certifique-se de que haja uma conta de usuário de domínio configurada na instalação do Active Directory para ser usada com o Dell Server. A conta de usuário de domínio será usada para a ativação do software cliente. Não é necessário configurar pontos de extremidade Mac para autenticação de domínio (rede).
- Para impor criptografia no computador cliente, primeiramente selecione a opção de criptografia adequada para sua organização.

Dell Encryption	Criptografia FileVault
Selecione essa opção para fazer o seguinte:	Selecione essa opção para fazer o seguinte:
• Criptografar todas as partições na unidade de inicialização • Ignorar a autenticação de pré-inicialização • Usar criptografia de 256 bits	• Criptografar Fusion Drives • Usar a autenticação de pré-inicialização • Implementar uma solução que seja suportada pela Apple
NOTA: Se o Dell Encryption for usado, é preciso desativar a Proteção de integridade do sistema (SIP - System Integrity Protection). Consulte Instalação/Upgrade interativos e ativação, etapa 4.	**NOTA: Se um Mac tem um Fusion Drive, é necessário ativar o FileVault para criptografar a unidade.**

As configurações das políticas de criptografia precisam refletir a opção de criptografia selecionada. Antes de definir políticas de criptografia, certifique-se de que você entenda as políticas *Criptografar usando FileVault para Mac* e *Volumes direcionados para criptografia*. Para usar Dell Encryption ou criptografia FileVault, a política *Dell Volume Encryption* precisa estar *Ativada*.

Para obter mais informações sobre políticas de criptografia, consulte Criptografia para Mac > Dell Volume Encryption.

Instalação/Upgrade interativos e ativação

Para instalar/fazer upgrade e ativar o software cliente, siga o procedimento abaixo. Você precisa ter uma conta de administrador para executar este procedimento.

NOTA: Antes de começar, salve o trabalho do usuário e feche os outros aplicativos; imediatamente após a conclusão da instalação, será necessário reiniciar o computador.

1 Na mídia de instalação da Dell, monte o arquivo Dell-Data-Protection-<version>.dmg.

2 Clique duas vezes no instalador do pacote. A seguinte mensagem será mostrada:

Este pacote executará um programa para determinar se o software pode ser instalado.

3 Clique em **Continuar** para avançar.

4 Leia o texto de boas-vindas e clique em **Continuar**.

5 Analise o contrato de licença, clique em **Continuar** e, em seguida, clique em **Concordar** para aceitar os termos do contrato de licença.

Se você usar Dell Encryption com Mac OS X v10.11 ou superior, a seguinte caixa de diálogo será exibida: *A Proteção de integridade do sistema Mac OS está ativada*. Você precisa desativar a Proteção de integridade do sistema (SIP).

Execute este procedimento:

a Consulte http://www.dell.com/support/Article/us/en/19/SLN299063 para desativar a SIP.

b No assistente, clique em **OK** e continue com a *Configuração do Dell Data Protection*.

6 No campo `Endereço do domínio:`, digite o domínio totalmente qualificado para os usuários de destino, como *department.organization.com*.

7 No campo **Nome de exibição (opcional):**, considere configurar o *Nome de exibição* para o nome do domínio NetBIOS (antes do Windows 2000), que é normalmente em maiúsculas.

Se configurado, esse campo será mostrado na caixa de diálogo *Ativação* em vez do Endereço do domínio. Isso é consistente com o nome do domínio mostrado nas caixas de diálogo *Autenticação* para computadores Windows gerenciados por domínio.

8 No campo **Servidor de segurança**: digite o nome de host do Servidor de segurança.

Se a implantação usar uma configuração que não é a padrão, atualize os campos de porta e a caixa de seleção **Usar SSL**.

Depois que for estabelecida uma conexão, o indicador de conectividade do Servidor de segurança mudará de vermelho para verde.

9 No campo **Proxy de política:** o nome de host do Proxy de política é automaticamente preenchido com um host de Proxy de política que corresponde ao host do Servidor de segurança. Esse host será usado como Proxy de política se nenhum host for especificado na configuração da política.

Depois que for estabelecida uma conexão, o indicador de conectividade do Proxy de política mudará de vermelho para verde.

10 Depois que a caixa de diálogo Configuração Dell estiver preenchida e a conectividade tiver sido estabelecida para o Servidor de segurança e o Proxy de política, clique em **Continuar** para mostrar o tipo de instalação.

11 Algumas instalações em computadores específicos exibem uma caixa de diálogo *Selecione um destino* antes de exibir a caixa de diálogo *Tipo de instalação*. Nesse caso, selecione o disco de sistema atual fora da lista de discos mostrados. O ícone do disco de sistema atual mostra uma seta verde apontando para o disco. Clique em **Continuar**.

12 Depois que o tipo de instalação for exibido, clique em **Instalar** para continuar a instalação.

13 Quando solicitado, digite as credenciais da conta de administrador (exigidas pelo aplicativo do instalador do Mac OS X) e clique em **OK**.

> **NOTA: É necessário reiniciar o computador logo após a instalação. Se você tiver arquivos abertos em outros aplicativos e não estiver pronto para reiniciar, clique em Cancelar, salve o trabalho e feche os outros aplicativos.**

14 Clique em **Continuar a instalação**. A instalação começa.

15 Ao concluir a instalação, clique em **Reiniciar**.

16 Vá para Ativar o Encryption Client para Mac.

Instalação/Upgrade por linha de comando

Para instalar o software cliente usando a linha de comando, siga as etapas abaixo.

> **NOTA: Se você usar o Dell Encryption no Mac OS X v10.11.x, precisará desativar a SIP. Consulte http://www.dell.com/support/Article/us/en/19/SLN299063.**

1 Na mídia de instalação da Dell, monte o arquivo Dell-Data-Protection-<version>.dmg.

2 Copie o pacote **Instalar o Dell Data Protection** e o arquivo **com.dell.ddp.plist** para a unidade local.

3 No Console de Gerenciamento Remoto, modifique as seguintes políticas, se necessário. As configurações da política substituem as configurações do arquivo .plist. Use as configurações do .plist se as políticas não existirem no Console de Gerenciamento Remoto.

- **Modo de senha do firmware** - Se você pretende usar o Boot Camp em computadores Mac criptografados ou usar uma versão do sistema operacional ainda não totalmente suportada pela Dell, você **precisa** definir essa política como *Opcional* para **não** usar a proteção de senha do firmware. Para obter mais informações, consulte Sobre a proteção de senha do firmware opcional.

  > **NOTA:**
  > Quando a política FirmwarePasswordMode estiver definida como **Opcional**, ela desativará somente a imposição da proteção por senha de firmware do software do cliente. Ela **não** remove qualquer proteção por senha de firmware existente. Depois de concluir esse procedimento, a instalação é finalizada e o computador é reiniciado; você pode remover qualquer senha de firmware existente usando o Utilitário de senha de firmware do Mac OS X.

- **Nenhuma lista de usuários aut** - Em alguns casos, você pode editar essa política para que usuários ou classes de usuários especificados não tenham que ativar o Dell Server. Por exemplo, em uma instituição educativa, os professores seriam solicitados a ativar seus computadores no Dell Server, mas estudantes individuais usando computadores do laboratório, não. O administrador do laboratório poderia usar essa política e a conta executando a ferramenta do cliente para que os usuários estudantes pudessem fazer login sem serem solicitados a ativar. Para obter informações sobre a Client Tool, consulte Client Tool. Se uma empresa precisar saber que conta de usuário está associada a cada computador Mac, todos os usuários precisarão ser ativados no Dell Server para que a empresa não edite esta propriedade. No entanto, se um usuário quiser fornecer mídia EMS, ele deverá ser autenticado no servidor Dell.

4 Abra o arquivo .plist e edite quaisquer valores de espaço reservado adicionais:

> **NOTA:**
> A Apple frequentemente lança novas versões de sistemas operacionais entre liberações do Endpoint Security Suite Enterprise para Mac. Para oferecer suporte ao máximo de clientes possível, a Dell permite modificar o arquivo .plist. Assim que a Apple lança uma nova versão, a Dell começa a testar essa versão para garantir que ela é compatível com o Encryption client 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/> [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 Salve e feche o arquivo .plist.

6 Para cada computador de destino, copie o pacote para uma pasta temporária e o arquivo com.dell.ddp.plist para **/Library/Preferences**.

7 Execute a instalação do pacote por linha de comando usando o comando **instalador**:

```
sudo installer -pkg "Install Dell Data Protection.pkg" -target /
```

8 Reinicie o computador usando a seguinte linha de comando: `sudo shutdown -r now`

9 Vá para Ativar o Encryption Client para Mac.

Ativar o Encryption Client

O processo de ativação associa contas de usuário de rede do Dell Server ao computador Mac, recupera todas as políticas de segurança da conta, envia atualizações de inventário e de status, ativa fluxos de trabalho de recuperação e fornece relatórios de conformidade abrangentes. O software cliente executa o processo de ativação de cada conta de usuário que encontra no computador à medida que cada usuário faz login na sua conta de usuário.

NOTA: Para obter instruções sobre a ativação de um Mac sem domínio, consulte o Artigo da base de dados SLN302497.

Depois de o software cliente ter sido instalado e o Mac ter reiniciado, o usuário faz o login:

1 Digite o nome de usuário e a senha gerenciados pelo Active Directory.

Se o tempo de espera da caixa de diálogo da senha expirar, pressione **Atualizar** na guia Políticas. Em Visualizar a política e o status no computador local, consulte a etapa 1.

2 Selecione o domínio no qual quer fazer login.

Se o Dell Server estiver configurado para suporte a múltiplos domínios e um domínio diferente tiver de ser usado para ativação, use o Nome principal do usuário (UPN), que tem o formato *<username>@<domain>*.

3 As opções são:

- Clique em **Ativar**.
  - Se a ativação for bem-sucedida, uma mensagem será mostrada para indicar que a ativação foi satisfatória. O O Encryption client para Mac agora está totalmente operacional e gerenciado pelo Dell Server.
  - Se a ativação falhar, o software cliente permite três tentativas para você digitar corretamente as credenciais do domínio. Se todas as três tentativas forem malsucedidas, a mensagem solicitando as credencias de domínio será mostrada novamente no próximo login do usuário.
- Clique em **Não agora** para ignorar a caixa de diálogo, que será exibida novamente no próximo login de usuário.

NOTA: Quando o administrador precisar descriptografar uma unidade em um computador Mac a partir de um local remoto, executando um script ou pessoalmente, o software cliente solicitará ao usuário acesso de administrador e exigirá que o usuário digite a sua senha.

NOTA: Caso você tenha configurado o computador para criptografia FileVault e os arquivos estejam criptografados, faça login em uma conta a partir da qual você poderá posteriormente reinicializar o sistema.

4 Execute um destes processos:

- Se a criptografia **não** tiver sido habilitada antes da ativação, vá para Processo de criptografia.
- Se a criptografia **tiver sido** habilitada antes de ativação, vá para Visualizar a política e o status da criptografia.

Visualizar a política e o status da criptografia

Você pode visualizar a política e o status da criptografia no computador local ou no Remote Management Console.

Ver a política e o status no computador local

Para ver a política e o status da criptografia no computador local, siga o procedimento abaixo.

1 Abra *Preferências do sistema* e clique em **Dell Data Protection**.

2 Clique na guia **Políticas** para visualizar a política atual definida para esse computador. Use essa exibição para confirmar as políticas de criptografia específicas que estão em vigor nesse computador.

DICA: Clique em Atualizar para verificar se há atualizações nas políticas.

O Remote Management Console mostra em uma lista as políticas de Mac nesses grupos de tecnologia:

- **Criptografia para Mac**
- **Criptografia de mídia removível**

Dependendo dos requisitos de criptografia da sua empresa, você pode definir políticas para o Dell Encryption ou a criptografia FileVault. Esta tabela mostra em uma lista as opções de política para cada um.

Criptografia para Mac > Dell Volume Encryption

Dell Volume Encryption	*Ativada* ou *Desativada* Essa é a "política mestre" de todas as outras políticas de Dell Volume Encryption. Essa política precisa estar definida como *Ativada* para que qualquer outra política do Dell Volume Encryption seja aplicada. A definição como *Ativada* habilitará a criptografia e iniciará a criptografia dos volumes descriptografados de acordo com a política *Volumes direcionados para criptografia* **ou** *Criptografar usando FileVault para Mac*. A configuração padrão é *Ativada*. A definição como Desativada desabilita a criptografia e iniciará uma varredura de descriptografia em todos os volumes totalmente ou parcialmente criptografados.
Criptografar usando FileVault para Mac	Se você planeja usar a criptografia FileVault, defina primeiro o Dell Volume Encryption como *Ativado*. Certifique-se de que a política *Criptografar usando o FileVault para Mac* esteja selecionada no Dell Server. Quando ativado, o FileVault é usado para criptografar o volume do sistema, incluindo unidades Fusion, com base na configuração de política *Volumes direcionados para criptografia*. **NOTA: Se você usa o Dell Encryption (e não o FileVault) e esta política estiver ativada, haverá um conflito de políticas.**

NOTA:
Se você planeja migrar da Criptografia da Dell para a criptografia do FileVault, consulte Migrar da criptografia de volume da Dell para a criptografia do FileVault.

Criptografia para Mac > Configurações globais do Mac

Volumes direcionados para criptografia	*Somente volume do sistema* ou *Todos os volumes fixos* A configuração de *Somente volume do sistema* protege apenas o volume do sistema atualmente em execução. A configuração de **Todos os volumes fixos** protege todos os volumes do Mac OS Exended em todos os discos fixos juntamente com o volume do sistema atualmente em execução.

3 Para obter as descrições de todas as políticas, consulte *AdminHelp*, que está disponível por meio do Remote Management Console. Para encontrar uma política específica no *AdminHelp*:

a Clique no ícone Pesquisar.

b No campo Pesquisar, insira o nome da política entre aspas.

c Clique no link de tópico que é exibido. O nome da política que você inseriu entre aspas é realçado no tópico.

4 Clique na guia **Volumes do sistema** para exibir o status dos volumes direcionados para criptografia.

Estado	Descrição
Excluído	O volume está excluído da criptografia. Isso se aplica a volumes descriptografados quando a criptografia está desativada, volumes externos, volumes com formatos diferentes de Mac OS X Extended (Journaled) e volumes que não são de sistema quando a política *Volumes direcionados para criptografia* é definida como Somente volume do sistema.
Preparando o volume para criptografia...	O software cliente está iniciando no momento o processo de criptografia do volume, mas não começou a varredura de criptografia.
O volume não pode ser redimensionado	O software cliente não pode iniciar a criptografia porque o volume não pode ser redimensionado adequadamente. Depois de receber esta mensagem, entre em contato com o Dell ProSupport e forneça os arquivos de log.
Reparo necessário antes de iniciar a criptografia	O volume falhou durante a verificação do Utilitário de disco. Para reparar um volume, siga as instruções descritas no artigo HT1782 do Suporte Apple (http://support.apple.com/kb/HT1782).
Preparação para criptografia concluída. Reinicialização pendente...	A criptografia começará depois da reinicialização.
Conflito de política de criptografia	O disco não pode ser colocado conforme a política porque ele está criptografado com uma configuração incorreta. Consulte Criptografar usando FileVault para Mac.
Aguardando o depósito das chaves no Dell Server...	Para garantir que é possível recuperar todos os dados criptografados, o software cliente não começará o processo de criptografia até que todas as chaves de criptografia estejam depositadas satisfatoriamente no Dell Server. O software cliente sondará a conectividade do Servidor de segurança enquanto estiver neste estado até que as chaves sejam depositadas.
Criptografando...	Uma varredura de criptografia está em andamento.
Criptografado	A varredura de criptografia está concluída.
Descriptografando...	Uma varredura de descriptografia está em andamento.

Estado	Descrição
Restaurando para o estado original...	O software cliente está restaurando o esquema de partição para seu estado original no final do processo "Descriptografando...". É a varredura de descriptografia equivalente ao estado "Preparando o volume para criptografia".
Descriptografado	A varredura de descriptografia está concluída.

Cor	Descrição
Verde	Parte criptografada
Vermelho	Parte não criptografada
Amarelo	Parte sendo criptografada novamente Por exemplo, devido a uma mudança nos algoritmos de criptografia. Os dados continuam seguros. É apenas uma transição para outro tipo de criptografia.

A guia Volumes de sistema mostra todos os volumes conectados ao computador contidos nos discos formatados da Tabela de Partição GUID (GPT). A tabela a seguir apresenta uma lista de exemplos de configurações de volume para unidades internas.

NOTA: Os emblemas e ícones podem ser um pouco diferentes, dependendo do seu sistema operacional.

Emblema	Tipo de volume e status
	O volume do sistema Mac OS X atualmente inicializado. O emblema da pasta X indica a partição de inicialização atual. O Dell Encryption não é compatível com a Proteção de integridade do sistema (SIP). Se essa condição de incompatibilidade for especificada pela política e a SIP estiver ativada, um erro será mostrado ao lado da unidade na guia Volumes de sistema. Para desativar a SIP, consulte Instalação/Upgrade interativos e ativação, etapa 4.
	Um volume configurado para criptografia. Esse emblema denota uma partição criptografada pela Dell.
	Um volume configurado para criptografia. O emblema Segurança e privacidade indica uma partição protegida pelo FileVault.
	Um volume de não inicialização configurado para criptografia. O emblema Segurança e privacidade indica uma partição protegida pelo FileVault.
 	Múltiplas unidades e nenhuma criptografia. **NOTA: O ícone de volume sem um emblema indica que nada foi feito para o disco. Não é um disco de inicialização.**

Emblema	Tipo de volume e status
	Múltiplas unidades e apenas o volume de sistema está criptografado. Esse exemplo é uma partição criptografada pela Dell.

5 Clique na guia **Mídia removível** para exibir o status de volumes direcionados para criptografia. A tabela a seguir apresenta uma lista de exemplos de configurações de volume para mídia removível.

Os emblemas e ícones podem ser um pouco diferentes, dependendo do seu sistema operacional.

Emblema	Status
	Um ícone de volume esmaecido indica um dispositivo desmontado. Os motivos são: • O usuário pode ter escolhido não o provisionar. • A mídia pode estar bloqueada. **NOTA: Um emblema de barra/círculo vermelho neste ícone indica uma partição excluída da proteção por não ser compatível. Abrange volumes com formatação FAT32.**
	Um ícone de volume cheio indica um dispositivo montado. O emblema "Sem gravação" indica que é somente leitura. A criptografia é ativada, mas a mídia não está provisionada e o Acesso do EMS a mídias não blindáveis está definido como Somente leitura.
	Mídia criptografada usando o EMS, indicada por um emblema Dell.

Visualizar a política e o status no Remote Management Console

Para visualizar a política e o status da criptografia no Remote Management Console, siga o procedimento abaixo.

1 Como um administrador Dell, faça login no Remote Management Console.

2 No painel esquerdo, clique em **Populações > Pontos de extremidade**.

3 Para Estação de trabalho, clique em uma opção no campo Nome de host ou, se você souber o Nome de host do endpoint, insira-o no campo Pesquisar. Você também pode inserir um filtro para pesquisar pelo endpoint.

NOTA: O caractere curinga (*) pode ser usado, mas não é obrigatório no início nem no fim do texto. Você pode digitar um nome comum, um nome principal universal ou sAMAccountName.

4 Clique no endpoint adequado

5 Clique na guia **Detalhes e ações**.

A área Detalhes do endpoint mostra as informações sobre o computador Mac.

A área do detalhe do Shield mostra informações sobre o software cliente, incluindo o horário de início e fim da varredura da criptografia para este computador.

Para visualizar as políticas em vigor, clique em **Visualizar políticas em vigor** na área Ações.

6 Clique na guia **Políticas de segurança**. Nesta guia, você pode expandir os tipos de políticas e alterar políticas individuais.

a Quando concluído, clique em **Salvar**.

b No painel à esquerda, clique em **Gerenciamento > Confirmar**.

> **NOTA: O número exibido por Alterações de política pendentes é cumulativo. Ele pode incluir alterações feitas em outros endpoints, ou feitas por outros administradores que estão usando a mesma conta.**

c Digite uma descrição das alterações na caixa Comentário e clique em **Confirmar políticas**.

7 Clique na guia **Usuários**. Essa área mostra uma lista de usuários ativados nesse computador Mac. Clique no nome do usuário para mostrar as informações sobre todos os computadores em que esse usuário está ativado.

8 Clique na guia **Grupos de pontos de extremidade**. Essa área mostra todos os grupos de endpoint aos quais esse computador Mac pertence.

Volumes do sistema

Ativar criptografia

> **NOTA: Apenas volumes Mac OS X Extended (Journaled) e discos de sistema particionados com o esquema de partição da Tabela de Partição GUID (GPT) podem ser criptografados.**

Use esse processo para ativar a criptografia em um computador cliente se a criptografia **não** tiver sido habilitada antes da ativação. Esse processo ativa a criptografia apenas para um único computador. Se você quiser pode escolher ativar a criptografia para todos os computadores Mac no nível de política Enterprise. Para obter instruções adicionais sobre a habilitação da criptografia no nível de políticas do *Enterprise*, consulte o *AdminHelp*.

1 Como um administrador Dell, faça login no Remote Management Console.

2 No painel esquerdo, clique em **Populações** > **Pontos de extremidade**.

3 Para Estação de trabalho, clique em uma opção na coluna Nome de host ou, se você souber o Nome de host do endpoint, insira-o no campo Pesquisar. Você também pode inserir um filtro para pesquisar pelo endpoint.

> **NOTA: O caractere curinga (*) pode ser usado, mas não é obrigatório no início nem no fim do texto. Você pode digitar um nome comum, um nome principal universal ou sAMAccountName.**

4 Clique no endpoint adequado

5 Na página *Políticas de segurança*, clique no grupo de tecnologia **Criptografia para Mac**.

Por padrão, a política mestre do *Dell Volume Encryption* está definida como *Ativada*.

6 Se o Mac possuir uma unidade Fusion, marque a caixa de seleção da política *Criptografar usando FileVault* para Mac.

> **NOTA: Essa política exige que a política do *Dell Volume Encryption* também seja definida como *Ativada*. Entretanto, quando a criptografia FileVault estiver ativada, nenhuma das outras políticas no grupo estarão em vigor. Consulte Criptografia para Mac > Dell Volume Encryption.**

7 Se FileVault estiver desmarcado, altere as outras políticas conforme desejado.

Para obter as descrições de todas as políticas, consulte *AdminHelp*, que está disponível por meio do Remote Management Console.

8 Quando concluído, clique em **Salvar**.

9 No painel à esquerda, clique em **Gerenciamento > Confirmar**.

O número exibido por Alterações de política pendentes é cumulativo. Ele pode incluir alterações feitas em outros endpoints, ou feitas por outros administradores que estão usando a mesma conta.

10 Digite uma descrição das alterações na caixa Comentário e clique em **Confirmar políticas**.

11 Para ver a configuração de política no computador local depois que o Dell Server enviar a política, clique em **Atualizar** no painel de Políticas das preferências do Dell Data Protection.

Processo de criptografia

O processo de criptografia varia dependendo desses fatores:

- O início do volume de inicialização quando a criptografia está ativada.
- Se a Dell Encryption ou a criptografia FileVault está selecionada.

> **NOTA: Para manter a integridade dos dados do usuário, o software cliente não começa a criptografia de um volume até que o processo de verificação seja bem-sucedido nesse volume. Se um volume falhar durante a verificação, o software cliente notificará o usuário e reportará a falha em Preferências do Dell Data Protection. Se for necessário reparar um volume, siga as instruções descritas no artigo HT1782 do Suporte Apple (http://support.apple.com/kb/HT1782). O software cliente tentará executar a verificação novamente na próxima reinicialização do computador.**

Selecione uma dessas opções:

- Dell Encryption de uma unidade não criptografada
- Criptografia FileVault de um volume não criptografado
- Assumir o Gerenciamento de um volume existente criptografado por FileVault

Dell Encryption de uma unidade não criptografada

Depois de o software cliente receber a política de criptografia, ele realiza uma validação dos volumes direcionados para criptografia usando o Utilitário de disco e, em seguida, configura esses volumes para criptografia.

1 A barra de andamento indica o status da verificação. Quando a verificação terminar, os volumes de destino serão configurados para criptografia.

   Esse processo pode diminuir a velocidade de resposta do computador por alguns minutos. Para cada volume com a criptografia pendente, uma caixa de diálogo é mostrada ao usuário indicando que a operação está em andamento.

2 Depois de concluir a preparação para a criptografia, reinicie o computador.

> **NOTA: Dependendo das políticas de experiência do usuário definidas no Remote Management Console, o software cliente pode solicitar que o usuário reinicie o computador.**

3 Depois que o computador reiniciar, ele precisa estar conectado à rede para que o software cliente deposite as informações de recuperação no Dell Server.

O software cliente pode começar e concluir o processo de criptografia, além de relatar o status da criptografia ao Remote Management Console antes do login do usuário. Isso permite garantir a conformidade de todos os computadores Mac sem exigir a interação do usuário.

Criptografia FileVault de um volume não criptografado

1 Após a instalação e ativação, você precisa fazer login na conta a partir da qual você quer inicializar após a criptografia FileVault estar ativa.

2 Aguarde a conclusão da validação da unidade e da verificação do volume.

3 Digite a senha da conta.

> **NOTA: Se você deixar o tempo de espera dessa caixa de diálogo expirar, você precisará reinicializar ou fazer login para que a caixa de diálogo de senha seja mostrada novamente.**

4 Clique em **OK**.

   Se a conta em que o usuário fez login for uma conta de rede não móvel, uma caixa de diálogo será mostrada. Após a unidade de inicialização ser criptografada, a unidade poderá ser inicializada apenas pelo usuário que estava conectado durante a inicialização do FileVault.

Essa conta precisa ser uma conta móvel local ou de rede. Para transformar contas de rede não móveis em contas móveis, vá para **Preferências do sistema > Usuários e grupos**. Execute uma das seguintes ações:

- Torne a conta uma conta móvel.
  OU
- Faça login em uma conta local e inicialize o FileVault desse local.

5 Clique em **OK**.

6 Depois de concluir a preparação para a criptografia, reinicie o computador.

> **NOTA: Dependendo das políticas de experiência do usuário definidas no Remote Management Console, o software cliente pode solicitar que o usuário reinicie o computador.**

7 Depois que o computador reiniciar, ele precisa estar conectado à rede para que o software cliente deposite as informações de recuperação no Dell Server.

O software cliente pode começar e concluir o processo de criptografia, além de relatar o status da criptografia ao Remote Management Console antes do login do usuário. Isso permite garantir a conformidade de todos os computadores Mac sem exigir a interação do usuário.

Modificar a política para adicionar usuários do FileVault

O FileVault protege os dados de um disco automaticamente, por meio da criptografia. Em um volume de boot gerenciado do FileVault, para permitir que vários usuários desbloqueiem o disco, você pode modificar uma diretiva no Console de Gerenciamento Remoto e usar o dicionário de nomes e valores de registro do OpenDirectory para permitir que os usuários se adicionem ao disco FileVault.

1 Nas políticas avançadas de *Configurações globais do Mac* do Console de Gerenciamento Remoto, role para baixo até a diretiva *Lista de Usuários do PBA do FileVault 2*.

2 No campo da política *Lista de Usuários do PBA do FileVault 2*, insira uma regra que corresponda aos usuários que você planeja especificar. Por exemplo, a correspondência `<string>*</string>` para qualquer chave deve corresponder a todos os usuários do servidor OpenDirectory vinculado.

As tags diferenciam maiúsculas de minúsculas e o valor inteiro deve ser corretamente formado como elementos de dicionário e matriz em uma lista de propriedades. As chaves de dicionário são AND'd juntos. Os valores de matriz são or'd juntos, combinando qualquer elemento de uma matriz com a matriz inteira.

> **NOTA:**
> Se uma regra for formada incorretamente, um erro será exibido na guia *Dell Data Protection > Preferências*.

O seguinte <dict> lista exemplos para duas chaves:

```
<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 de chave de exemplo *AuthenticationAuthority* especificam um padrão de *user1*, *user2* e *user3* ou qualquer ID de usuário que começar com *z*. Para visualizar a caixa de diálogo que fornece a sintaxe correta para cada usuário, pressione as teclas **Control-Option-Command** no cliente. Copie a sintaxe para o usuário e cole-a no servidor.

NOTA:
Para esse exemplo, os asteriscos à direita representam a última parte dos registros da autoridade de autenticação. Normalmente, para evitar a subespecificação, inclua o registro completo em vez de um asterisco à direita porque o asterisco corresponde a qualquer informação após o dois-pontos no registro do OpenDirectory.

- A chave NFSHomeDirectory requer que qualquer usuário passando a primeira chave também tenha um diretório inicial em */Users/*.

NOTA:
Você deverá criar a pasta inicial se ela não existir para um usuário.

3 Reinicie os computadores.

4 Notifique aos usuários finais para ativarem o boot do FileVault para suas contas de usuário. O usuário precisa ter uma conta local ou móvel. As contas de rede são automaticamente convertidas para contas móveis.

Para um usuário para ativar sua conta do FileVault:

1 Execute as **Preferências do sistema** e clique em **Dell Data Protection**.

2 Clique na guia **Volumes do sistema**.

3 Clique com o botão direito na unidade Volume do sistema, e selecione **Adicionar usuários do FileVault à inicialização do FileVault**.

4 No campo de pesquisa, digite o nome do usuário ou role para baixo. As contas de usuário são exibidas somente se atenderem aos critérios definidos pela política.

Para usuários locais e móveis, um botão *Ativar usuário* é exibido.

Para usuários da rede, um botão *Converter e ativar usuário* é exibido.

NOTA:
Um indicador verde é exibido ao lado de contas de usuário que podem inicializar o FileVault.

5 Clique em **Ativar usuário** ou **Converter e ativar usuário**.

6 Digite a senha para a conta selecionada e clique em **OK**. Uma barra de progresso é exibida.

7 Assim que uma caixa diálogo for exibida, clique em **Concluído**.

Assumir o Gerenciamento de um volume existente criptografado por FileVault

Se o computador já tiver um volume criptografado por FileVault e a criptografia FileVault estiver ativada no Remote Management Console, o Dell Encryption pode assumir o gerenciamento do volume.

Se o Dell Encryption detectar que o volume de inicialização já está criptografado, a caixa de diálogo do Dell Data Protection é exibida. Para permitir que o Dell Encryption assuma o gerenciamento do volume, execute este procedimento.

1 Selecionar **Chave de recuperação pessoal *ou* Credenciais de contas inicializáveis.**

- **Chave de recuperação pessoal - se você tem a chave de recuperação pessoal que você recebeu quando a unidade foi criptografada usando o FileVault.**

  1 Digite a chave.

  Caso um usuário não tenha a chave existente, é possível solicitá-la a um administrador.

  2 Clique em **OK**.

  NOTA: Após a conclusão do processo em que o gerenciamento é assumido, uma nova chave de recuperação pessoal é gerada e depositada. A chave de recuperação anterior é invalidada e removida.

- **Credenciais de contas inicializáveis - se você tem o nome de usuário e a senha de uma conta com autorização para inicializar a partir do volume.**

1. Digite o nome de usuário e a senha.
2. Clique em **OK**.

2 Quando for exibida uma caixa de diálogo indicando que a Dell agora gerencia a criptografia do volume, clique em **OK**.

Se o Dell Encryption detectar que um volume de não inicialização já está criptografado, um prompt de senha será exibido.

3 (Somente volumes de não inicialização criptografados pelo FileVault) Para permitir que o Dell Encryption assuma o gerenciamento do volume, insira a senha para acessar o volume. Essa é a senha que foi atribuída ao volume no momento em que ele foi originalmente criptografado com FileVault.

Assim que o Dell assumir o gerenciamento da criptografia do volume, a senha antiga não será mais válida. O administrador Dell poderá recuperar uma chave de recuperação para seu volume, caso você precise de assistência na recuperação.

Se você optar por não inserir a senha, o conteúdo do volume ficará acessível e será criptografado com o FileVault, mas a criptografia não será gerenciada pelo Dell.

NOTA: No Remote Management Console, o administrador pode ver que o Dell Server agora gerencia o ponto de extremidade.

Reciclar as chaves de recuperação do FileVault

Caso surjam problemas de segurança com um pacote de recuperação ou se houver um volume ou chaves comprometidos, é possível reciclar o material de chave desse volume.

Você pode reciclar chaves de unidades de inicialização e de não inicialização no Mac OS X.

Para reciclar o material de chave:

1. Faça download de um pacote de recuperação do Remote Management Console e copie-o na área de trabalho do computador.
2. Abra *Preferências do sistema* e clique em **Dell Data Protection**.
3. Clique na guia **Volumes do sistema**.
4. Arraste o pacote de recuperação da etapa 1 para a partição adequada.
   Uma caixa de diálogo solicitará que você troque as chaves do FileVault.
5. Clique em **OK**.
   Uma caixa de diálogo confirmará a troca das chaves.
6. Clique em **OK**.

NOTA: As chaves dessa unidade contidas nesse pacote de recuperação estão agora obsoletas. Você precisa fazer download de um novo pacote de recuperação do Remote Management Console.

Experiência do usuário

Para a máxima segurança, o software cliente desativa o recurso *Login automático* dos computadores Mac OS X.

Além disso, o software cliente automaticamente impõe o recurso *exigir senha após o início da suspensão ou da proteção de tela* do Mac OS X. Um período de tempo configurável também é permitido no modo repouso/proteção de tela antes de impor a autenticação. O software cliente permite que um usuário configure um período de até cinco minutos antes de a autenticação ser imposta.

Os usuários podem usar o computador normalmente durante a varredura de criptografia. Todos os dados no volume do sistema atualmente inicializado estão sendo criptografados, incluindo o sistema operacional, enquanto o sistema operacional continua em execução.

Se o computador for reinicializado ou entrar no estado de suspensão do sistema, a varredura de criptografia é pausada e, depois, retoma automaticamente após a reinicialização ou a ativação.

O software cliente não suporta o uso de imagens de hibernação que o recurso *Suspensão segura* do Mac OS X usa para acordar o computador se a bateria estiver totalmente descarregada durante a suspensão.

Para reduzir o impacto sobre o usuário, o software cliente atualiza automaticamente o estado de suspensão do sistema para desativar a hibernação e impõe essa configuração. O computador ainda pode entrar no estado de suspensão, mas o estado atual do sistema será mantido apenas na memória. Portanto, o computador será totalmente reinicializado se ele se desligar completamente durante o estado de suspensão, o que pode ocorrer caso a bateria esgote ou seja substituída.

Copiar regra de lista branca

Um item de menu oculto permite que um usuário copie uma regra de lista branca para uma mídia externa.

1 Abra **Preferências do sistema** e clique em **Dell Data Protection**.
2 Selecione a guia **Mídia removível**.
3 Clique com o botão direito na linha de uma unidade e, ao mesmo tempo, pressione a tecla command.

   Um item de menu oculto é mostrado.
4 Clique em **Copiar regra de lista branca** para a mídia externa atual. A regra de lista branca é copiada para a área de transferência.
5 Acesse a área de transferência, copie a regra de lista branca e envie-a ao seu administrador.

Se a política *Criptografia de mídia Mac* estiver **Ativada**, os dados serão criptografados, incluindo unidades Thunderbolt.

Se você quiser excluir um dispositivo ou um grupo de dispositivos para impedir a gravação de dados criptografados na unidade Thunderbolt ou na mídia EMS, você pode usar a regra de lista branca para modificar os valores.

Use a regra completa para especificar uma unidade específica a ser inserida na lista branca, por exemplo:

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

NOTA: Substitua os valores do exemplo pelas informações da unidade.

NOTA: É preciso ativar o HFS Plus. Consulte Ativar o HFS Plus.

Para excluir dispositivos SATA da aplicação da política do EMS quando conectados via Thunderbolt:

tbolt=1;bus=SATA

Você também pode incluir ou excluir a mídia do EMS com base em:

- **Tamanho da mídia**

  Regra de lista branca para excluir mídias grandes da proteção do EMS:

  size <op> <especificador de tamanho>

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

  <especificador de tamanho> tem a forma de um número inteiro decimal com um sufixo opcional de {K, M, G, T} alinhado em 1000, e não 1024. Por exemplo, para excluir mídias ou uma unidade com mais de 500000000 bytes do EMS, use uma dessas opções:

  size >= 500000000

  size >= 500000K

  size >= 500M
- **Tipo de sistema de arquivos**

Regra de lista branca:

fstype=<fstype>

<fstype> pode ser ExFAT, FAT ou HFS+

Para excluir ambos, existe um exemplo para 1TB e mídia HFS+ maior:

size>=1T;fstype=HFS+

Recuperação

Ocasionalmente, pode ser necessário acessar dados em discos criptografados. Como administrador Dell, você pode acessar discos criptografados sem descriptografá-los, economizando tempo valioso.

Por muitos motivos, talvez você precise acessar dados criptografados de um usuário; porém, os casos de uso mais comuns são os seguintes:

- Pode ser necessário mover dados criptografados de um usuário para outro Mac como parte de uma atualização de hardware.
- Pode ser necessário acessar um disco criptografado devido a uma falha no sistema operacional que faz com que o volume do sistema não inicialize mais, e você precise executar vários utilitários para reparar o sistema operacional.
- Pode ser necessário acessar os dados criptografados de um usuário porque ele fez uma alteração de configuração não autorizada e você precisa corrigir a situação.

Esta seção ajudará você no processo de usar **uma** das três operações de recuperação disponíveis.

Escolha **uma** opção abaixo:

- Montar volume
- Aceitar a nova configuração do sistema
- FileVault Recovery - use somente se estiver usando a criptografia FileVault no ponto de extremidade a ser recuperado. O FileVault pode ser usado com o Encryption client em execução no Mac OS X 10.10.5 ou posterior. A recuperação do FileVault é também usada em Fusion Drives.

Montar volume

Pré-requisitos

- Um computador ou um volume de recuperação externo descriptografado com o utilitário de recuperação instalado
- Um cabo FireWire ou Thunderbolt, dependendo do hardware
- O ID do dispositivo/ID único do computador que você pretende recuperar - na maioria dos casos, você pode encontrar o computador que você pretende recuperar no Remote Management Console, procurando pelo nome de usuário do proprietário e mostrando os dispositivos criptografados para esse usuário. O formato de ID do dispositivo/ID único é "John Doe's MacBook.Z4291LK58RH".
- A mídia de instalação Dell

Processo

1 Como um administrador Dell, faça login no Remote Management Console.

2 No painel esquerdo, clique em **Gerenciamento > Recuperar ponto de extremidade**.

3 No campo Pesquisar, digite o nome de domínio totalmente qualificado do endpoint a ser recuperado e clique no ícone Pesquisar.

4 Clique no link de **Recuperação** do dispositivo.

5 Se o endpoint exigir recuperação avançada, uma senha será solicitada. Atribua uma nova senha ao pacote principal do qual você está prestes a fazer o download.

NOTA: Você precisa memorizar essa senha para acessar as chaves de recuperação.

6 Para salvar o pacote de recuperação no volume de recuperação externo ou no computador que estará executando o utilitário de recuperação para realizar a operação de recuperação, clique em **Download** e clique em **Salvar**.

O arquivo de recuperação <nome_da_máquina.domínio>.csv é obtido por download.

> **NOTA: Se a proteção por senha de firmware estiver habilitada nesse computador, a senha de firmware será solicitada para acessar o Gerenciador de Inicialização de pré-inicialização. Você pode encontrar a senha de firmware desse computador no pacote de recuperação obtido por download em salvar o pacote de recuperação. Consulte Como ativar o Boot Camp do Mac OS X para obter mais informações.**

7 Inicialize o computador de destino a partir de um volume de recuperação externo pré-criado. Você pode executar essa ação iniciando o painel do Disco de inicialização em Preferências do sistema e selecionando o volume de recuperação, ou mantendo pressionada a tecla **Opção** enquanto reinicia o computador e selecionando o volume de recuperação no Gerenciador de Inicialização de pré-inicialização.

ou

Inicialize o computador que você pretende recuperar no modo de disco de destino. Você pode executar essa ação iniciando o painel do Disco de inicialização em Preferências do sistema e clicando em **Modo de disco de destino**, ou mantendo pressionada a tecla **T** enquanto reinicia o computador.

> **NOTA: A proteção por senha de firmware impede o uso da tecla T para colocar o computador no modo de disco de destino durante a inicialização. Mais informações sobre o modo de disco de destino estão disponíveis no site da Apple em http://support.apple.com/kb/HT1661.**

Conecte agora esse computador ao computador host que realizará a operação de recuperação usando um cabo FireWire ou Thunderbolt, dependendo do hardware.

8 Monte o arquivo Dell-Data-Protection-<version>.dmg.

> **NOTA: A versão do utilitário de recuperação precisa ser a mesma ou uma mais recente do que a versão do software cliente instalado no computador que você pretende recuperar.**

9 Na pasta Utilitários localizada na mídia de instalação Dell, abra o Dell Recovery Utility.

Uma mensagem será mostrada informando que "O kext [texto do kernel] do DDP precisa ser carregado para que seja possível modificar os discos criptografados. Digite a sua senha para que isso seja permitido."

10 Digite a senha do administrador ou do usuário.

É exibida uma mensagem informando "Instalação necessária: é necessário instalar o Recovery."

11 Clique em **Instalar**.

12 Selecione o volume ou a unidade que precisa ser recuperada e clique em **Continuar**.

Selecionar a unidade recuperará todos os volumes nesta unidade de uma só vez.

13 Selecione o pacote de recuperação (salvo na etapa 6) e clique em **Abrir**.

14 Selecione a opção **Montar volume**.

15 Clique em **Continuar** para confirmar a opção *Montar volume*. Uma mensagem de êxito será exibida.

16 Clique em **Fechar**.

Agora é possível abrir uma janela do Finder e acessar os dados do volume criptografado como se fosse um volume normal. Todos os dados serão criptografados e descriptografados de modo transparente conforme os arquivos forem transferidos entre os volumes.

Aceitar a nova configuração do sistema

Se uma senha de firmware ou outra alteração de configuração do sistema invalidou a chave de criptografia em um computador criptografado, escolha esta opção para aceitar a configuração do sistema atualizado na próxima reinicialização e restaurar o acesso ao computador.

Como a criptografia é ligada a uma configuração de dispositivo específica, as alterações na configuração invalidam a chave de criptografia do software cliente. Quando você aceitar a nova configuração do sistema, simplesmente instrua o software cliente a redefinir a sua segurança com base na nova configuração. Por exemplo, pode ser necessário mover a unidade para outro Mac porque um usuário quebrou a tela. Usando esse método, você instrui o software cliente a aceitar essa "nova" configuração como válida.

Pré-requisitos

- Um computador ou um volume de recuperação externo descriptografado com o utilitário de recuperação instalado
- Um cabo FireWire ou Thunderbolt, dependendo do hardware
- O ID do dispositivo/ID único do computador que você pretende recuperar - na maioria dos casos, você pode encontrar o computador que você pretende recuperar no Remote Management Console, procurando pelo nome de usuário do proprietário e mostrando os dispositivos criptografados para esse usuário. O formato de ID do dispositivo/ID único é "John Doe's MacBook.Z4291LK58RH".
- A mídia de instalação Dell

Processo

1 Como um administrador Dell, faça login no Remote Management Console.

2 No painel esquerdo, clique em **Populações > Pontos de extremidade**.

3 Pesquise pelo dispositivo a ser recuperado.

4 Clique no nome do dispositivo para abrir a página Detalhe do endpoint.

5 Clique na guia **Detalhes e ações**.

6 Em Detalhe do Shield, clique no link **Chaves de recuperação do dispositivo**.

7 Para salvar o pacote de recuperação no volume de recuperação externo ou no computador que estará executando o utilitário de recuperação para realizar a operação de recuperação, clique em **Download** e clique em **Salvar**.

> **NOTA: Se a proteção por senha de firmware estiver habilitada nesse computador, a senha de firmware será solicitada para acessar o Gerenciador de Inicialização de pré-inicialização. Você pode encontrar a senha de firmware desse computador no pacote de recuperação obtido por download na etapa 7. Consulte Como ativar o Boot Camp do Mac OS X para obter mais informações.**

8 Inicialize o computador de destino a partir de um volume de instalação do SO completo externo pré-criado. Você pode executar essa ação iniciando o painel do Disco de inicialização em Preferências do sistema e selecionando o volume de instalação do SO completo ou mantendo pressionada a tecla **Opção** enquanto reinicia o computador e selecionando o volume de instalação do SO completo externo no Gerenciador de inicialização de pré-inicialização. Para criar um volume inicializável, consulte https://support.apple.com/en-us/HT202796.

ou

Inicialize o computador que você pretende recuperar no modo de disco de destino. Você pode executar essa ação iniciando o painel do Disco de inicialização em Preferências do sistema e clicando em **Modo de disco de destino**, ou mantendo pressionada a tecla **T** enquanto reinicia o computador.

> **NOTA: A proteção por senha de firmware impede o uso da tecla T para colocar o computador no modo de disco de destino durante a inicialização. Mais informações sobre o modo de disco de destino estão disponíveis no site da Apple em http://support.apple.com/kb/HT1661.**

9 Execute um destes processos:

- Conecte esse computador ao computador host que realizará a operação de recuperação usando um cabo FireWire ou Thunderbolt, dependendo do hardware.

  ou

- Alterne a inicialização para qualquer disco com uma instalação do SO completo nele.

10 Monte o arquivo Dell-Data-Protection-<version>.dmg.

> **NOTA: A versão do utilitário de recuperação precisa ser a mesma ou uma mais recente do que a versão do software cliente instalado no computador que você pretende recuperar.**

11 Na pasta Utilitários localizada na mídia de instalação Dell, abra o Dell Recovery Utility.

Uma mensagem será mostrada informando que "O kext [texto do kernel] do DDP precisa ser carregado para que seja possível modificar os discos criptografados. Digite a sua senha para que isso seja permitido."

12 Digite a senha do administrador ou do usuário.

É exibida uma mensagem informando "Instalação necessária: é necessário instalar o Recovery."

13 Clique em **Instalar**.

14 Selecione o volume ou a unidade que precisa ser recuperada e clique em **Continuar**.

Selecionar a unidade recuperará todos os volumes nesta unidade de uma só vez.

A janela de seleção de arquivos é mostrada.

15 Selecione o pacote de recuperação (salvo na etapa 7) e clique em **Abrir**.
A caixa de diálogo *Selecionar operação de recuperação* é exibida.

16 Selecione a opção **Aceitar nova configuração do sistema**.

17 Clique em **Continuar** para confirmar *Aceitar nova configuração do sistema*.

18 Digite a sua senha para redefinir a posse e aceitar a nova configuração do sistema.

19 Clique em **OK**.

A mensagem *Recuperação concluída* será exibida quando for feita a inicialização no volume do sistema interno original. Essa mensagem solicitará que você reinicialize o computador novamente. O software cliente agora aceitou a configuração do sistema atualizado, e você pode acessar o seu computador normalmente.

Recuperação do FileVault

A recuperação de um volume gerenciado criptografado usando o FileVault é significativamente diferente de uma recuperação de um volume criptografado pela Dell. O processo de recuperação é definido pela Apple e é automatizado quando possível, mas exige mais algumas etapas.

O Dell Recovery Utility simplifica a operação das ferramentas de recuperação da Apple com scripts que auxiliam a montagem de um volume ou, em alguns casos, sua descriptografia. A funcionalidade de recuperação do FileVault é determinada pelo sistema operacional instalado no Recovery HD e na partição de destino emparelhada.

Um volume criptografado usando o FileVault pode ser recuperado apenas a partir de uma partição Recovery HD que é gravada em todas as unidades de disco com o Mac OS X 10.9.5 ou posterior em execução. Esse requisito descarta a possibilidade de realizar uma operação de recuperação diretamente do Dell Recovery Utility.

Existem dois métodos de recuperação: baseado em se a chave de recuperação do FileVault é uma chave de recuperação pessoal ou institucional. Sempre existe uma chave de recuperação válida. Normalmente, use a chave de recuperação pessoal mais recente primeiro. Se essa chave não funcionar, use a cadeia de chaves de recuperação institucional.

- Chave de recuperação pessoal - A criptografia usando o FileVault é gerenciada pelo Dell Server. Este é o método preferido.

  Se a entrada mais recente no pacote de recuperação contiver uma entrada RecoveryKey, siga as etapas da Chave de recuperação pessoal. Eis um exemplo de RecoveryKey:

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

- Cadeia de chaves de recuperação - este método de recuperação é baseado no uso de uma chave de recuperação institucional do FileVault.

  Se a entrada mais recente no pacote de recuperação contiver uma entrada KeychainKey, siga as etapas da Cadeia de chaves de recuperação. Eis um exemplo de KeychainKey:

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

Chave de recuperação pessoal

Geralmente, a boa prática é recuperar o volume de inicialização antes de recuperar os volumes que não são de inicialização. A recuperação do volume de inicialização normalmente corrigirá os problemas com os volumes que não são de inicialização.

Pré-requisitos

- Uma unidade inicializável externa
- O ID do dispositivo/ID único do computador que você pretende recuperar. Na maioria dos casos, é possível encontrar o computador a ser recuperado no Remote Management Console procurando pelo nome de usuário do proprietário e exibindo os dispositivos criptografados para esse usuário. O formato de ID do dispositivo/ID único é "John Doe's MacBook.Z4291LK58RH".

- A mídia de instalação Dell

Processo

1 Abra o Remote Management Console.

2 No painel esquerdo, clique em **Populações > Pontos de extremidade**.

3 Pesquise pelo dispositivo a ser recuperado.

4 Clique no nome do dispositivo para abrir a página Detalhe do endpoint.

5 Clique na guia **Detalhes e ações**.

6 Em Detalhe do Shield, clique no link **Chaves de recuperação do dispositivo**.

7 Para salvar o pacote de recuperação no volume de recuperação externo ou no computador que estará executando o utilitário de recuperação para realizar a operação de recuperação, clique em **Download** e clique em **Salvar**.

8 Digite um local para o pacote de recuperação e clique em **Salvar**.

9 Copie o pacote para recuperação e o arquivo **Dell-Data-Protection-<version>.dmg** para a unidade USB inicializável.

10 Inicialize o computador de destino a partir de um volume de instalação do SO completo externo pré-criado mantendo pressionada a tecla **Opção** tecla enquanto reinicia o computador e, em seguida, selecionando o volume de instalação do SO completo externo no Gerenciador de inicialização de pré-inicialização. Para criar um volume inicializável, consulte https://support.apple.com/en-us/HT202796.

11 Monte o arquivo Dell-Data-Protection-<version>.dmg.

> **NOTA:**
> A versão do utilitário de recuperação precisa ser a mesma ou uma mais recente do que a versão do software cliente instalado no computador que você pretende recuperar.

12 Na pasta Utilitários localizada na mídia de instalação Dell, abra o Dell Recovery Utility.

A caixa de diálogo *Dell Recovery Utility > Selecionar Volumes* é exibida.

13 Selecione o volume do FileVault.

- Para descriptografar e montar a unidade, você precisa ter uma partição de inicialização com a versão 10.9.5 ou superior. Caso contrário, será possível apenas obter a chave de recuperação pessoal.
- Se você tiver volumes de não inicialização criptografados, você normalmente recuperará a partição de inicialização primeiro.

14 Clique em **Continuar.**

A caixa de diálogo *Escolher pacote de recuperação* é exibida.

15 Selecione o pacote de recuperação (salvo na etapa 9) e clique em **Abrir**.

A caixa de diálogo *Selecionar registro de recuperação* é exibida.

16 Na coluna Data do 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 não ser mais válida.

A caixa de diálogo Resultado da operação de recuperação mostra a chave.

- Para unidades de inicialização, a ferramenta de recuperação fornece uma chave de recuperação pessoal que permite a inicialização usando a recuperação padrão do FileVault da Apple. Você pode inicializar na partição de destino e digitar a chave de recuperação pessoal para executar a Autenticação de pré-inicialização, o que pode variar dependendo do SO.
- Para unidades que não são de inicialização, apenas a chave de recuperação pessoal é mostrada. Para montar um volume que não é de inicialização, digite a chave de recuperação na caixa de diálogo de solicitação da senha do sistema operacional. Caso a caixa de diálogo tenha sido fechada anteriormente, você pode selecionar Desbloquear no utilitário de disco para montar a partição criptografada.

17 Imprima ou anote a chave.

18 Clique em **Fechar**.

19 Inicialize no volume de inicialização externo mantendo pressionada a tecla **Opção** na inicialização.

20 Se necessário, digite a senha de firmware. Selecione o volume de inicialização externo.

21 Depois que o sistema reiniciar, clique em **?** na tela de login.

22 Clique na seta mostrada.

23 Digite a chave de recuperação e pressione **Enter**.

24 Na caixa de diálogo, digite uma senha nova.

Cadeia de chaves de recuperação

Você precisa executar o Dell Recovery Utility enquanto ele é inicializado em um volume de recuperação não criptografado. Não execute o Dell Recovery Utility a partir de um volume de inicialização externo criptografado.

Pré-requisitos

- Um computador ou um volume de recuperação externo com o utilitário de recuperação instalado
- Uma unidade USB
- Um cabo Firewire
- A mídia de instalação Dell

Processo

1 Conecte uma unidade externa ao sistema a ser recuperado.

A unidade externa precisa ter um volume de inicialização do Mac OS.

2 Inicialize no volume de inicialização externo mantendo pressionada a tecla **Opção** na inicialização.

3 Se necessário, digite a senha de firmware. Selecione o volume de inicialização externo.

4 Monte o arquivo .dmg.

5 Na pasta Utilities, execute o Dell Recovery Utility.

A caixa de diálogo *Dell Recovery Utility > Selecionar Volumes* é exibida.

6 Selecione o volume do FileVault a ser recuperado e clique em **Continuar.**

A caixa de diálogo *Escolher pacote de recuperação* é exibida.

7 Selecione o pacote de recuperação e clique em **Abrir**.

Se houver mais de uma chave de recuperação para esse disco, a mensagem *Selecionar registro de recuperação* é exibida.

8 Na coluna Data do depósito, selecione a data mais recente para o tipo de recuperação Cadeia de chaves e clique em **Continuar.**

> **NOTA:**
> Com uma data de depósito mais antiga, a chave pode não ser mais válida.

A caixa de diálogo *Instruções de recuperação do FileVault* é exibida.

9 Leia as instruções e clique em **Continuar**.

A caixa de diálogo *Confirmar operação de recuperação* é exibida.

10 Destaque o volume do FileVault a ser recuperado e clique em **Continuar.**

A caixa de diálogo *Escolher local para arquivos de recuperação* é mostrada, solicitando que você selecione um local para armazenar os arquivos de recuperação.

Esse local precisa ser o local que você usará para a recuperação, pois os scripts contêm caminhos absolutos para os arquivos de dados. **Não** copie esses arquivos para o Recovery HD.

A Dell recomenda que você salve esses arquivos na raiz de uma unidade externa, como de uma unidade USB.

> **NOTA:**
> Confirme que todos os usuários têm acesso de leitura/gravação à unidade USB ou ao disco que você usa para armazenar a chave de recuperação, e que o disco tem espaço suficiente. Se você não tem direitos a um disco selecionado ou se o disco está sem espaço, um erro será mostrado indicando que as chaves de recuperação não foram armazenadas.

11 Selecione um local e clique em **Salvar**.

A caixa de diálogo *Resultado da operação de recuperação* é exibida, indicando que os arquivos foram criados.

12 Clique em **Fechar.**

13 Após a inicialização do volume Recovery HD, digite o nome e o caminho do script.

> **NOTA:**
> Armazenar os arquivos perto da raiz de um volume encurta o caminho que você precisará digitar.

A caixa de diálogo Resultado da operação de recuperação mostra a chave.

O Dell Recovery Utility gera os arquivos no local selecionado e, em seguida, mostra os comandos exatos que você precisará executar a partir do volume Recovery HD para montar ou descriptografar o volume do FileVault.

14 Depois que esses arquivos forem gerados, copie as cadeias de caracteres de comando mostradas na caixa de diálogo final *Resultado da operação de recuperação*.

15 Reinicialize no Recovery HD de uma das maneiras a seguir:

- Ao mesmo tempo, pressione e mantenha pressionadas as teclas **Comando** e **R** (Comando-R) antes do sinal sonoro de computador ligado/autoteste e durante a inicialização.

  ou
- Pressione a tecla **Opção** e use o seletor de inicialização para selecionar o Recovery HD.

  A caixa de diálogo *Utilitários do Mac OS X* é exibida.

16 No menu Ferramentas, selecione **Utilitários > Terminal**.

17 Para montar o volume para copiar arquivos do Terminal ou criar uma imagem de disco partir do Utilitário de disco: em Terminal, digite o caminho completo e o nome do script **fv2mount.sh**, por exemplo:

/Volumes/recoveryFOB/fv2mount.sh

18 Reinicie o computador.

Mídia removível

Formatos suportados

Mídias formatadas FAT32, exFAT ou HFS Plus (Mac OS Extended) com esquemas de partição MBR (Master Boot Record [registro da inicialização mestre]) ou GPT (Tabela de partição GUID) são suportadas. É preciso ativar o HFS Plus.

> **NOTA: Mac atualmente não oferece suporte para gravação de CD/DVD no EMS. Entretanto, o acesso às unidades de CD/DVD não está bloqueado, mesmo se a política *Bloquear acesso do EMS a mídias não blindáveis* estiver selecionada.**

Ativar o HFS Plus

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

<key>EMSHFSPlusOptIn</key>

<true/>

NOTA: A Dell recomenda testar essa configuração antes de introduzi-la no ambiente de produção.

O HFS Plus não suporta:

- Controle de versão - dados de controle de versão existentes são removidos do disco.
- Links físicos - durante uma varredura de criptografia da mídia removível, o arquivo não é criptografado. Uma caixa de diálogo recomenda ejetar a mídia.
- Mídia contendo backups do Time Machine:
  - Mídias usadas pelo computador de uma maneira reconhecível como destino de backup do Time Machine são automaticamente adicionadas à lista branca para permitir a continuação dos backups.
  - Todas as outras mídias removíveis com backups do Time Machine são baseadas na política que rege mídias não provisionadas e mídias desprotegidas. Consulte as políticas *Acesso do EMS a mídias não blindáveis* e *Bloquear acesso do EMS a mídias não blindáveis*.

    NOTA: Para uma nova unidade que ainda não tem backups, o usuário precisará copiar sua regra de lista branca para especificar a unidade da Time Machine para adição à lista branca. Consulte Copiar regra de lista branca.

EMS e atualizações de política

No sistema em que a mídia foi provisionada (ou recuperada), as políticas são atualizadas em relação à mídia no momento da montagem.

Exceções de criptografia

Em uma mídia externa, os atributos estendidos não são criptografados.

Erros na guia Mídia removível

- Em um computador desprotegido, não substitua um arquivo criptografado por uma versão descriptografada do arquivo. Posteriormente, isso pode impedir a descriptografia. Pode também ser mostrado como um erro na guia Mídia removível.
- Se houver um marcador de fim de arquivo invalidado, por exemplo, se um arquivo for substituído por um novo conteúdo fora do controle do EMS e depois montado no EMS, um erro de fim de arquivo será mostrado na guia Mídia removível.
- Quando você converte arquivos, o espaço livre disponível na mídia precisa ser maior do que o tamanho do maior arquivo a ser convertido. Se um triângulo de advertência amarelo for mostrado na área de status da Mídia removível, clique nele. Se uma mensagem indicar *Espaço insuficiente*, faça o seguinte:

  a Observe o espaço que que precisa ser liberado no dispositivo. O relatório mostra uma lista de arquivos e o tamanho.

  b Esvazie a lixeira. À medida que você liberar espaço, o EMS criptografará automaticamente arquivos adicionais.

  c Se você apagar arquivos ou pastas, lembre-se de apagá-los da lixeira novamente.

Mensagens de auditoria

Mensagens de auditoria são enviadas ao Dell Server.

Para o Endpoint Security Suite Enterprise para Mac, consulte o Remote Management Console e selecione **Populações > Enterprise ou Pontos de extremidade**. Em seguida, selecione a guia **Eventos de ameaça avançada**. Para obter mais informações, consulte *AdminHelp*.

Coletar arquivos de log para Endpoint Security Suite Enterprise

O DellLogs.zip contém os logs para o Client Encryption e Advanced Threat Prevention.

Para obter informações sobre como coletar os logs, consulte http://www.dell.com/support/article/us/en/19/SLN303924.

Desinstalar o Encryption client para Mac

O software cliente pode ser desinstalado por meio do aplicativo **Uninstall Dell Data Protection**. Para desinstalar o software cliente, siga o procedimento abaixo.

NOTA: Antes de executar o aplicativo de desinstalação, o disco precisa ser totalmente descriptografado.

1 Se o disco estiver atualmente criptografado, configure a política **Dell Volume Encryption** do computador em **Desativada** no Remote Management Console e confirme a política.

Uma caixa de diálogo é mostrada para pedir acesso às Preferências do sistema e ao controle do computador, de modo que o software cliente possa descriptografar o disco.

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

   Se a opção **Negar** estiver selecionada, a desinstalação e a descriptografia serão incapazes de prosseguir.

   b Digite a senha de administrador.

2 Após o disco ser totalmente descriptografado, reinicie o computador (quando solicitado).

3 Após a reinicialização do computador, abra o aplicativo **Uninstall Dell Data Protection** (localizado na pasta Utilitários no Dell-Data-Protection-<version>.dmg na mídia de instalação da Dell).

As mensagens mostram o status do processo de desinstalação.

O Encryption client para Mac agora está desinstalado e o computador pode ser usado normalmente.

Ativação como administrador

A Client Tool oferece ao administrador novos métodos para a ativação do software cliente em um computador Mac e a análise do software cliente. Há dois métodos de ativação disponíveis:

- Ativação usando as credenciais do Administrador
- Ativação temporária que emula o usuário sem deixar rastros nesse computador.

Os dois métodos podem ser usados diretamente através de um shell ou em um script.

NOTA: Não ative o software cliente em mais de cinco computadores com a mesma conta de rede. Isso poderia deixar o Enterprise Server/Enterprise Server - VE com graves vulnerabilidades de segurança e desempenho degradado.

Pré-requisitos

- O Encryption client para Mac precisa ser instalado no computador remoto.
- Não o ative através da interface do usuário do cliente sem antes tentar ativá-lo a partir de um local remoto.

Ativar

Use este comando para ativar o cliente como administrador.

Exemplo:

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

Ativar temporariamente

Use este comando para ativar o cliente sem deixar rastros no computador.

1 Abra um shell ou use um script para ativar o software cliente:

client *-em username@domain.com password*

2 Use a Client Tool para recuperar as informações sobre o software cliente, suas políticas, status do disco, conta de usuário dentre outros. Para obter mais informações sobre a Client Tool, consulte Client Tool.

> **NOTA: Após a ativação, as informações sobre o software cliente, incluindo suas políticas, status do disco e informações do usuário, estão também disponíveis em Preferências do sistema, nas preferências do Dell Data Protection.**

Referência do Encryption Client

Sobre proteção adicional por senha de firmware

> **NOTA: Os computadores Mac mais recentes não oferecem suporte para Proteção por senha de firmware. A Proteção por senha de firmware é suportada pelos modelos a seguir:**
>
> - iMac10.*
> - iMac11.*
> - Macmini4.*
> - MacBook7.*
> - MacBookAir2.*
> - MacBookPro7.*
> - MacPro5.*
> - XServe3.*
>
> Por exemplo, iMac10.1, iMac11.1 e iMac11.2 suportarão a proteção adicional por senha de firmware (conforme indicado pelo *), ao contrário do iMac12.1 ou posterior.

> **NOTA: Quando a opção da chave FirmwarePasswordMode estiver definida como Opcional, ela desativará somente a imposição da proteção por senha de firmware do cliente. Ela não remove qualquer proteção por senha de firmware existente. Você pode remover qualquer senha de firmware existente usando o Utilitário de senha de firmware do Mac OS X.**

Se você planejar usar o Boot Camp (consulte Como Ativar o Boot Camp do Mac OS X para obter instruções) em computadores Mac criptografados, você **precisará** configurar o cliente para **não** usar proteção por senha de firmware.

Os computadores Mac usam a proteção por senha de firmware para melhorar a segurança de acesso do computador. Por padrão, nos computadores Mac, a proteção é *DESATIVADA*. Durante a instalação do cliente, seja uma nova instalação ou um upgrade de uma versão anterior do cliente, é possível editar o arquivo com.dell.ddp.plist existente para permitir que a chave *FirmwarePasswordMode* seja definida como *Obrigatória* ou *Opcional*. A opção *Obrigatória* é a configuração padrão, que impõe a proteção por senha de firmware, enquanto a configuração *Opcional* faz com que a senha de firmware não seja imposta. Após a instalação ou upgrade, o cliente avaliará o arquivo instalador modificado com.dell.ddp.plist durante a reinicialização.

> **NOTA: Para impedir que os usuários alterem o estado de segurança do computador, o cliente não aceita alterações na chave FirmwarePasswordMode após a instalação do software cliente.**
>
> É possível alterar o valor dessa chave após a instalação ou upgrade iniciando um processo de descriptografia de disco e, em seguida, reativando a criptografia.

Se você quiser que a proteção por senha de firmware do Mac OS X seja **obrigatória**, siga os procedimentos normais de instalação/atualização do cliente descritos em Instalação/Upgrade do Encryption Client para Mac.

Como usar o Boot Camp

Suporte ao Boot Camp do Mac OS X

NOTA: Quando o Boot Camp for usado, o sistema operacional Windows não poderá ser criptografado.

O Boot Camp é um utilitário contido no Mac OS X que auxilia você na instalação do Windows em computadores Mac, em uma configuração de inicialização dupla. O Boot Camp é compatível com os seguintes sistemas operacionais Windows:

- Windows 7 e 7 Home Premium, Professional e Ultimate (64 bits)
- Windows 8 e 8 Pro (64 bits)
- Windows 8.1 e 8.1 Pro (64-bit)

NOTA: Para Windows 7, deve-se usar o Boot Camp 4 ou 5.1. A partir do Windows 8, deve-se usar apenas o Boot Camp 5.1.

Para usar o Endpoint Security Suite Enterprise para Windows no Boot Camp em um computador com o Endpoint Security Suite Enterprise para Mac, o volume do sistema precisa ser criptografado por meio do Encryption client para Mac com o Dell Client Encryption ou o FileVault2. É preciso configurar sua instalação de cliente para **não** usar a proteção por senha de firmware. Consulte Instalação/Atualização de linha de comando para obter instruções.

NOTA:
Se sua partição do Windows for uma candidata do EMS, certifique-se de adicioná-la à lista branca, ou ela será criptografada. Consulte Copiar regra de lista branca.

NOTA:
Você precisa confirmar que o Windows está instalado antes de implementar as políticas de cliente que ativam a criptografia. Após o cliente começar o processo de criptografia, ele desativa as operações de partição de disco exigidas pelo Boot Camp.

Recuperação do Endpoint Security Suite Enterprise para Windows no Boot Camp

Para recuperar o Endpoint Security Suite Enterprise para Windows sendo executado em um volume Boot Camp, será preciso criar um volume Boot Camp em uma unidade externa.

Pré-requisitos

- Uma unidade inicializável externa
- O ID do dispositivo/ID único do computador que você pretende recuperar. Na maioria dos casos, é possível encontrar o computador a ser recuperado no Remote Management Console procurando pelo nome de usuário do proprietário e exibindo os dispositivos criptografados para esse usuário. O formato de ID do dispositivo/ID único é "John Doe's MacBook.Z4291LK58RH".

Processo

1 Em uma unidade externa, crie um volume Boot Camp.

O procedimento é semelhante à criação de um volume Boot Camp no seu sistema local. Consulte http://www.apple.com/support/bootcamp/.

2 No Remote Management Console, copie o pacote de recuperação para uma das seguintes opções:

- Uma unidade USB inicializável

ou

- Uma partição FAT no volume Boot Camp externo

3 Desligue o computador com o volume Boot Camp a ser recuperado.

4 Conecte a unidade externa ao computador.

Essa unidade contém o volume Boot Camp criado na etapa 1.

5 Para iniciar o computador a partir da unidade de Boot Camp externa, pressione a tecla **Opção** ao mesmo tempo em que liga o computador.

6 Selecione o volume Boot Camp (Windows) que está na unidade externa.

7 Na unidade USB ou partição FAT, clique com o botão direito do mouse no pacote de recuperação (da etapa 2) e selecione **Executar como administrador**.

8 Clique em **Sim.**

9 Na caixa de diálogo do Dell Data Protection Encryption, selecione uma opção:

- *Meu sistema não inicializa....* - Se o usuário não puder inicializar no sistema, selecione a primeira opção

ou

- *Meu sistema não permite que eu acesse dados criptografados....* - Se o usuário não puder acessar alguns arquivos criptografados ao fazer login no sistema, selecione a segunda opção.

10 Clique em **Avançar**.

A tela Informações de backup e recuperação é mostrada.

11 Clique em **Avançar**.

12 Selecione o volume Boot Camp a ser recuperado.

NOTA: Esse não é o volume Boot Camp externo.

13 Clique em **Avançar**.

14 Informe a senha associada a este arquivo.

15 Clique em **Avançar**.

16 Clique em **Recuperar.**

17 Clique em **Concluir**.

18 Quando for solicitado a reinicializar, clique em **Sim.**

19 O sistema reinicializa e você pode fazer login no Windows.

Como recuperar uma senha de firmware

Mesmo que o computador cliente esteja configurado para imposição de senha de firmware, pode ser que ela não seja necessária para recuperação. Se o computador a ser recuperado for inicializável, defina o destino da inicialização no painel de preferências do sistema Disco de inicialização.

Nos casos em que a senha de firmware for necessária para fazer a recuperação (se o computador não for inicializável e a proteção por senha de firmware for imposta), siga o procedimento abaixo.

Para recuperar uma senha de firmware, primeiro você precisa recuperar o pacote de recuperação que contém as chaves de criptografia do disco.

1 Como um administrador Dell, faça login no Remote Management Console.

2 No painel esquerdo, clique em **Populações > Pontos de extremidade**

3 Pesquise pelo dispositivo a ser recuperado.

4 Clique no nome do dispositivo para abrir a página Detalhe do endpoint.

5 Clique na guia **Detalhes e ações**.

6 Em Detalhe do Shield, clique no link *Chaves de recuperação do dispositivo*.

7 Para salvar o pacote de recuperação no volume de recuperação externo ou no computador que estará executando o utilitário de recuperação para realizar a operação de recuperação, clique em **Download** e clique em **Salvar**.

8 Abra o pacote de recuperação para recuperar a senha de firmware do computador que você pretende recuperar. A senha de firmware está localizada dentro das tags string após a chave **Senha de firmware**.

Por exemplo:

<key>FirmwarePassword</key>

<string>Bo$vun8WDn</string>

Client Tool

A Client Tool é um comando shell executado em um endpoint Mac. É usada para ativar o cliente a partir de um local remoto ou para executar um script através de um utilitário de gerenciamento remoto. Como administrador, você pode ativar um cliente e fazer o seguinte:

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

Para usar a Client Tool manualmente, abra uma sessão ssh e digite o comando desejado na linha de comando.

Exemplo:

/Library/PreferencePanes/Dell\ Data\ Protection.prefPane/Contents/Helpers/**client -at** *domainAccount domainPassword*

Digite **cliente** isoladamente para mostrar as instruções de uso.

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

Tabela 1. Comandos da Client Tool

Comando	Finalidade	Sintaxe	Resultados
Ativar	Ativa um cliente Mac com o Dell Server, mas sem passar pela interface do usuário. Para ativar, um nome de usuário e senha do domínio válidos precisam ser inseridos. Com a Client Tool, você pode ativar um usuário local diferente do usuário conectado e associar as credenciais do domínio a ele.	-a contaDomínio senhaDomínio -a contaLocal* contaDomínio senhaDomínio **domainAccount** é a conta usada para ativar por meio da Client Tool. **localAccount** é opcional e será o usuário atual se nenhum for especificado. O comando de ativação tem este formato: client -a <usuário a ser ativado*> <usuárioDomínio> <senhaDomínio> Se você usar a política *Nenhuma lista de usuários aut* para criar classes de usuários que não são ativados para o Dell Server, opcionalmente você poderá usar a ferramenta do cliente para especificar uma conta	0 = Bem-sucedido 2 = Falha na ativação e motivo da falha 6 = Usuário não encontrado

Comando	Finalidade	Sintaxe	Resultados
		local diferente da registrada no login. Consulte a política Nenhuma lista de usuários aut na etapa 3.	
Ativar temporariamente	Ativa um cliente Mac sem deixar rastros.	-at contaDomínio senhaDomínio -at contaLocal* contaDomínio senhaDomínio	
Disk	Solicita o status do disco	-d	O status do disco é mostrado, incluindo o ID, o status da criptografia e as políticas do disco Se o comando retornar chaves vazias, não há discos criptografados.
Alterar recuperação do FileVault	Recicla as chaves de recuperação de volumes do FileVault	-fc IdDispositivo senhaDeRecuperação -fc IdDispositivo chaveDeRecuperaçãoPessoal -fc IdDispositivo caminhoParaCadeiaDeChaves senhaDaCadeiaDeChaves -fc IdDispositivo arquivoDeRecuperação **NOTA: O IdDispositivo precisa ser um UUID de volume lógico ou resolvido para exatamente um LVUUID. Um ponto de montagem ou um devnode frequentemente funciona.**	0 = Bem-sucedido 7= LVUUID não encontrado 10 = Falha na credencial 11 = Falha no depósito
Política	Solicita as políticas do cliente Mac	-p	As políticas são mostradas
Servidor	Sonda o Dell Server em busca de políticas atualizadas em nome do cliente Mac **NOTA: A sondagem pode levar vários minutos para terminar.**	-s	0 = Bem-sucedido Qualquer outro valor indica que o Dell Server ou o software cliente Mac estava ocupado ou não estava respondendo.
Teste	Testa o status de ativação do cliente Mac	-t contaLocal*	0 (contaDomínio) = Bem-sucedido 1 = Não ativado 6 = Usuário não encontrado
Usuário	Solicita informações do usuário	-u contaLocal*	As informações da conta do usuário são mostradas: 0 (informações da conta) = Bem-sucedido 6 = Usuário não encontrado

Comando	Finalidade	Sintaxe	Resultados
Versão	Solicita a versão do cliente Mac	-v	A versão do cliente Mac é mostrada: exemplo: 8.x.x.xxxx

* A conta que está executando a Client Tool é usada para a contaLocal, ao menos que outra seja especificada.

A opção Plist

A opção -plist imprime os resultados do comando com o qual ele for combinado. Segue o comando e precisa ser colocado antes dos seus argumentos para fazer com que os resultados sejam impressos como uma plist.

Exemplos

Library/PreferencePanes/Dell\ Data\ Protection.prefPane/Contents/Helpers/**client -p -plist**

Para recuperar as políticas do cliente e imprimi-las.

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

Para ativar temporariamente o cliente e imprimir o resultado.

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

Para sondar o Dell Server quanto a políticas atualizadas em nome do cliente e exibi-las na tela.

Library/PreferencePanes/Dell\ Data\ Protection.prefPane/Contents/Helpers/**client -d -plist**

Para recuperar e imprimir o status do disco do cliente.

Códigos de retorno globais

Sem erros 0

Erro de parâmetro 4

Comando não reconhecido 5

O soquete esgotou o tempo limite 8

Erro interno 9

Tarefas para o Advanced Threat Prevention

Instalar o Advanced Threat Prevention para Mac

Esta seção ajudará você na instalação do Advanced Threat Prevention.

Há dois métodos para instalar o Advanced Threat Prevention.

- Instalação interativa - este método é o mais fácil. Entretanto, não permite quaisquer personalizações.
- Instalação por linha de comando - este é um método avançado de instalação/upgrade que só deve ser usado por administradores com experiência na sintaxe da linha de comando.

Pré-requisitos

A Dell recomenda que as boas práticas de TI sejam seguidas durante a implantação do software cliente. Isso inclui, entre outros, ambientes de teste controlados para testes iniciais e implantações escalonadas para os usuários

Antes de iniciar este processo, confirme que os seguintes pré-requisitos sejam atendidos:

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

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

  Enterprise Server Installation and Migration Guide (Guia de Instalação e Migração do Enterprise Server)

  Guia de Instalação e de Início Rápido do Enterprise Server - Virtual Edition
- Certifique-se de que você tenha o nome do host e a porta do servidor. Os dois serão necessários para a instalação do software cliente.
- Confirme se o computador de destino tem conectividade de rede com o Dell Server.
- Se um certificado do servidor do cliente estiver faltando ou for autoassinado, será preciso desativar o certificado de confiança SSL apenas no lado do cliente.

Instalação interativa do Advanced Threat Prevention

Esta seção ajudará você no processo de instalação do Advanced Threat Prevention para Mac.

Instalação interativa é o método mais fácil para instalar ou fazer upgrade do pacote de software cliente. Entretanto, não permite quaisquer personalizações.

Para instalar o software cliente, siga o procedimento abaixo. Você precisa ter uma conta de administrador para executar este procedimento.

NOTA: Antes de começar, salve o trabalho do usuário e feche outros aplicativos.

1 Na mídia de instalação da Dell, monte o arquivo **Endpoint-Security-Suite-Enterprise-<version>.dmg**.
O pacote Endpoint Security Suite Enterprise para Mac é aberto.

2 Clique duas vezes no pacote do instalador do **Endpoint Security Suite Enterprise**. A seguinte mensagem será mostrada:
Este pacote executará um programa para determinar se o software pode ser instalado.

3 Clique em **Continuar**.

4 Leia o texto de boas-vindas e clique em **Continuar**.

5 Analise o contrato de licença, clique em **Continuar** e, em seguida, clique em **Concordar** para aceitar os termos do contrato de licença.

6 No campo **Host do servidor**, digite o nome de host totalmente qualificado do Dell Server que gerenciará o usuário de destino, como server.organization.com.

7 No campo **Porta do servidor**, digite **8888** e clique em **Continuar**.

Depois que for estabelecida uma conexão, o indicador de conectividade mudará de vermelho para verde.

NOTA: A porta é a porta de serviço Servidor principal, que é configurável. O número da porta padrão é 8888.

8 Na tela de instalação, clique em **Instalar**.

9 Quando solicitado, digite as credenciais da conta de administrador (exigidas pelo aplicativo do instalador do Mac OS X) e clique em **OK**.

10 Quando a instalação estiver concluída, clique em **Fechar**.

O cliente do Advanced Threat Prevention para Mac está instalado.

11 Consulte Verificar a instalação do Advanced Threat Prevention.

Se a instalação falhar, verifique se você tem um certificado válido no seu Dell Server. Consulte Desativar o Certificado de confiança SSL do Advanced Threat Prevention.

Desinstalação interativa do cliente do Advanced Threat Prevention

O software cliente pode ser desinstalado por meio do aplicativo **Uninstall Endpoint Security Suite Enterprise**. Para desinstalar o software cliente, siga o procedimento abaixo.

1 Monte o arquivo Endpoint-Security-Suite-Enterprise-<version>.dmg.

2 Na pasta Utilitários, inicie o aplicativo **Uninstall Endpoint Security Suite Enterprise**.

3 Clique em **Desinstalar**.

4 Quando solicitado, digite as credenciais da conta de administrador (exigidas pelo aplicativo do instalador do Mac OS X) e clique em **OK**.

As mensagens mostram o status do processo de desinstalação.

5 Com a confirmação de sucesso, clique em **OK**.

O Advanced Threat Prevention para Mac agora está desinstalado e o computador pode ser usado normalmente.

Instalação do Advanced Threat Prevention por linha de comando

Para instalar o cliente do Advanced Threat Prevention usando a linha de comando, siga o procedimento a seguir.

1 Na mídia de instalação da Dell, monte o arquivo Endpoint-Security-Suite-Enterprise-<version>.dmg. O pacote Endpoint Security Suite Enterprise para Mac é aberto.

2 Da pasta utilitários, copie o arquivo **com.dell.esse.plist** para a unidade local.

3 Abra o arquivo .plist.

4 Edite os valores do espaço reservado com o nome do host totalmente qualificado que gerenciará o usuário de destino, como server.organization.com, e o número da porta **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>
```

NOTA: A porta é a porta de serviço Servidor principal, que é configurável. O número da porta padrão é 8888.

5 Salve e feche o arquivo.

6 Para cada computador de destino, copie o instalador do pacote **Endpoint Security Suite Enterprise para Mac** para uma pasta temporária e o arquivo modificado **com.dell.esse.plist** para **/Library/Preferences**.

7 Se for solicitado, digite suas credenciais.

8 Abra uma janela Terminal.

9 Execute a instalação do pacote por linha de comando usando o comando **instalador**:

```
sudo installer -pkg /Volumes/Endpoint\ Security\ Suite\ Enterprise\ for\ Mac/Endpoint\ Security\ Suite\ Enterprise.pkg -target /
```

NOTA: O -pkg path é o caminho para o instalador .pkg encontrado no arquivo .dmg.

10 Pressione **Enter**.

11 Consulte Verificar a instalação do ESSE Advanced Threat Prevention.

Linha de comando Desinstalar do Advanced Threat Prevention para Mac

Para desinstalar o cliente do Advanced Threat Prevention usando a linha de comando, siga o procedimento a seguir.

1 Abra uma janela Terminal.

2 Execute a desinstalação do pacote por linha de comando usando o comando **desinstalador**:

```
sudo /Volumes/Endpoint\ Security\ Suite\ Enterprise\ for\ Mac/Utilities/Uninstall\ Endpoint\ Security\ Suite\ Enterprise.app/Contents/MacOS/Uninstall\ Endpoint\ Security\ Suite\ Enterprise --noui
```

NOTA: Certifique-se de que o comutador --noui esteja incluído no final do comando.

3 Pressione **Enter**.

O Advanced Threat Prevention para Mac agora está desinstalado e o computador pode ser usado normalmente.

Como solucionar problemas no Advanced Threat Prevention para Mac

Desativar o Certificado de confiança SSL do Advanced Threat Prevention

Se um certificado do servidor do cliente estiver faltando ou for autoassinado, será preciso desativar o certificado de confiança SSL apenas no lado do cliente.

1 No cliente, abra uma janela Terminal.

2 Digite o caminho do DellCSFConfig.app:

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

3 Execute o DellCSFConfig.app:

```
sudo ./DellCSFConfig
```

O seguinte é exibido com as configurações padrão:

```
Current Settings:

ServerHost = deviceserver.company.com

ServerPort = 8888

DisableSSLCertTrust = False

DumpXmlInventory = False

DumpPolicies = False
```

4 Digite **-help** para listar as opções.

5 Para desativar o Certificado de confiança SSL no cliente, altere `DisableSSLCertTrust`para **Verdadeiro**.

Adicionar Inventário de XML e Alterações nas políticas à pasta Logs

Para adicionar os arquivos inventory.xml ou policies.xml à pasta Logs:

1 Execute o DellCSFConfig.app conforme descrito acima.

2 Altere o DumpXmlInventory para **Verdadeiro**.

3 Altere o DumpPolicies para **Verdadeiro**.

Arquivos de políticas só serão despejados se tiver ocorrido uma alteração na política.

4 Para visualizar os arquivos de log inventory.xml e policies.xml, acesse **/Biblioteca/Aplicativo\Suporte/Dell/Dell\Dados\Proteção/**.

Verificar a instalação do Advanced Threat Prevention

Opcionalmente, é possível verificar a instalação.

1 Confirme se o ícone Dell Advanced Threat Prevention possui um emblema verde  na barra de comando.

2 Se houver um ponto de exclamação sobre o ícone, clique com o botão direito do mouse e selecione **Mostrar detalhes**. Isso pode indicar que você não está registrado.

Verificar atualizações - verifica atualizações do mecanismo Advanced Threat Prevention e não atualizações das políticas do Dell Server.

Sobre - inclui o seguinte:

- Verison
- Política - [online] indica política baseada no servidor e [offline] indica política baseada em Airgap ou offline
- Nº de série - use quando entrar em contato com o serviço de suporte. Esse é o identificador exclusivo da instalação.

3 Em /Aplicativos, é criada a pasta Dell Advanced Threat Prevention

Coletar arquivos de log para Endpoint Security Suite Enterprise

O DellLogs.zip contém os logs para o Client Encryption e Advanced Threat Prevention.

Para obter informações sobre como coletar os logs, consulte http://www.dell.com/support/article/us/en/19/SLN303924.

Visualizar detalhes do Advanced Threat Protection

Após um cliente do Advanced Threat Prevention ser instalado em um computador de ponto de extremidade, ele será reconhecido pelo Dell Server como um agente.

Clique com o botão direito do mouse no ícone do Advanced Threat Prevention  na barra de comandos e selecione **Mostrar detalhes**. A tela Detalhes do Advanced Threat Protection tem as seguintes guias.

Guia Ameaças

A guia Ameaças mostra todas as ameaças descobertas no dispositivo e a ação executada. Ameaças são uma categoria de eventos recém-detectados como arquivos ou programas potencialmente inseguros e exigem correção orientada.

A coluna Categoria pode incluir o seguinte.

- **Não seguro** - um arquivo suspeito que provavelmente é malware
- **Anormal** - um arquivo suspeito que pode ser malware
- **Em quarentena** - um arquivo movido do seu local original, armazenado na pasta Quarentena e impedido de ser executado no dispositivo.
- **Dispensado** - um arquivo que pode ser executado no dispositivo.
- **Limpo** - Um arquivo que foi limpo dentro da organização. Dentre os arquivos limpos, estão arquivos dispensados, adicionados à lista Segura e excluídos da pasta Quarentena do dispositivo.

Para obter mais informações sobre as classificações de ameaças do Advanced Threat Prevention, consulte *AdminHelp*, disponível no Remote Management Console do Dell Server.

Guia Exploits

A guia Exploits lista exploits, que são considerados ameaças.

As políticas do Dell Server determinam a ação executada quando um exploit é detectado:

- **Ignorar** - nenhuma ação é realizada contra as violações de memória identificadas.
- **Alerta** - a violação de memória é registrada e informada ao Dell Server.
- **Bloquear** - a chamada de processo é bloqueada se um aplicativo tenta chamar um processo de violação de memória. O aplicativo que fez a chamada tem autorização para continuar a executar.
- **Encerrar** - a chamada de processo é bloqueada se um aplicativo tenta chamar um processo de violação de memória. O aplicativo que fez a chamada é encerrado.

Os seguintes tipos de exploit são detectados:

- Stack Pivot
- Proteção de pilha
- Pesquisa de memória de scanner
- Carga mal-intencionada

Para obter mais informações sobre políticas de Exploits, consulte *AdminHelp*, disponível no Remote Management Console do Dell Server.

Guia Eventos

NOTA: Um evento não é necessariamente uma ameaça. Um evento é gerado quando um arquivo ou programa reconhecido é colocado em quarentena, indicado como seguro ou ignorado.

A guia Eventos exibe todos os eventos de ameaça que ocorrem no dispositivo e os exibe por tipo de evento conforme designado pelo Advanced Threat Prevention. Os dados são removidos quando o sistema é reiniciado.

Os exemplos de tipos de evento incluem:

Ameaça encontrada

Ameaça removida

Ameaça em quarentena

Ameaça dispensada

Ameaça alterada

Provisionar um locatário para o Advanced Threat Prevention

Se sua organização está usando o Advanced Threat Prevention, um locatário precisa ser provisionado no Dell Server antes que o modo de imposição das políticas do Advanced Threat Prevention se torne ativa.

Pré-requisitos

- Precisa ser realizado por um administrador com a função Administrador de sistema.
- É necessária conectividade com a Internet para provisionar no Dell Server.
- É necessária conectividade do cliente com a Internet para exibir a integração do serviço online do Advanced Threat Prevention no Remote Management Console.
- O provisionamento é baseado em um token gerado a partir de um certificado durante o provisionamento.
- As licenças do Advanced Threat Prevention precisam estar presentes no Dell Server.

Fazer o provisionamento de um locatário

1. Faça login no Remote Management Console e vá até **Gerenciamento de serviços**.
2. Clique em **Configurar serviço Advanced Threat Protection**. Importe as suas licenças do ATP se ocorrer uma falha neste ponto.
3. A configuração guiada começa após as licenças serem importadas. Clique em **Avançar** para começar.
4. Leia e concorde com o Contrato de licença do usuário final (a caixa de seleção está **desmarcada** por padrão) e clique em **Avançar**.
5. Forneça as credenciais de identificação ao DDP Server para o provisionamento do locatário. Clique em **Avançar**. *Não é suportado fazer o provisionamento de um locatário existente da marca Cylance.*
6. Faça download do certificado. Ele será necessário para fazer a recuperação em cenários de desastre com o DDP Server. O backup desse certificado não é feito automaticamente através do utilitário de upgrade v9.2. Faça backup do certificado em um local seguro disponível em outro computador. Marque a caixa de seleção para confirmar que você fez o backup do certificado e clique em **Avançar**.
7. A configuração foi concluída. Clique em **OK**.

Configurar Atualização automática do agente do Advanced Threat Prevention

No Remote Management Console do Dell Server, você pode se inscrever para receber atualizações automáticas do agente do Advanced Threat Prevention. A inscrição para receber atualizações do agente automáticas permite aos clientes fazer download automaticamente das atualizações e aplicá-las a partir do servidor do Advanced Threat Prevention. As atualizações são liberadas mensalmente.

NOTA: Atualizações automáticas do agente são suportadas com o Dell Server v9.4.1 ou posterior.

Receber atualizações automáticas do agente

Para se inscrever para receber atualizações automáticas do agente:

1. No painel esquerdo do Remote Management Console, clique em **Gerenciamento** > **Gerenciamento de serviços**.
2. Na guia **Ameaças avançadas**, em Atualização automática do agente, clique no botão **Ativar** e, em seguida, clique no botão **Salvar preferências**.

Pode demorar alguns minutos para que as informações sejam preenchidas e as atualizações automáticas, exibidas.

Para de receber atualizações automáticas do agente

Para parar de receber atualizações automáticas do agente:

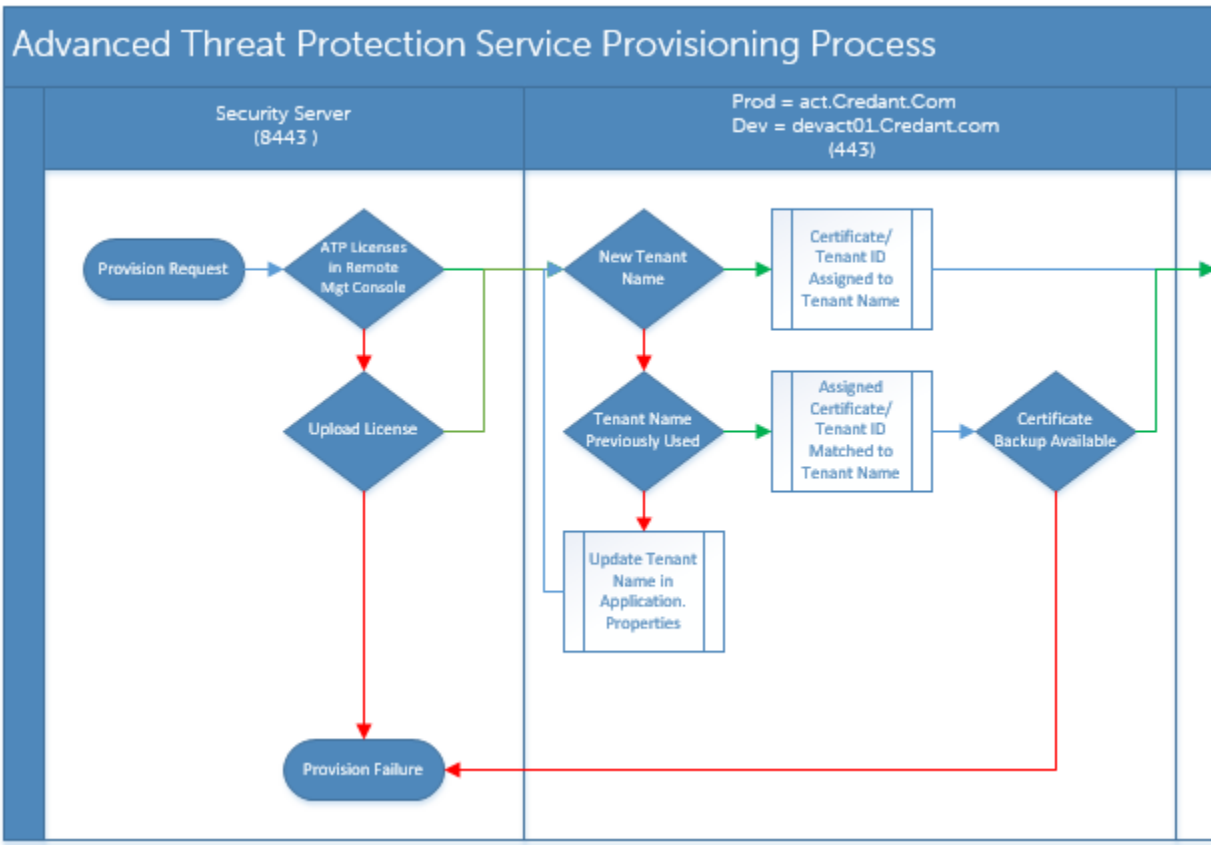
1 No painel esquerdo do Remote Management Console, clique em **Gerenciamento** > **Gerenciamento de serviços**.

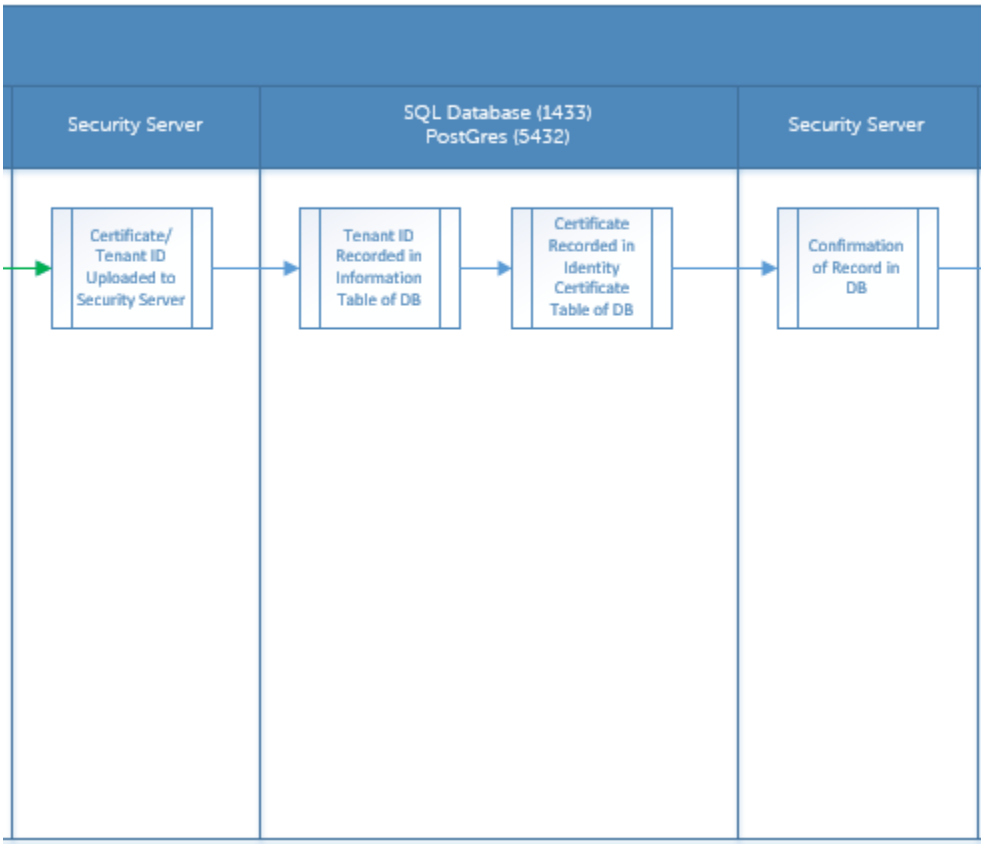
2 Na guia **Ameaças avançadas**, em Atualização automática do agente, clique no botão **Desativar** e, em seguida, clique no botão **Salvar preferências**.

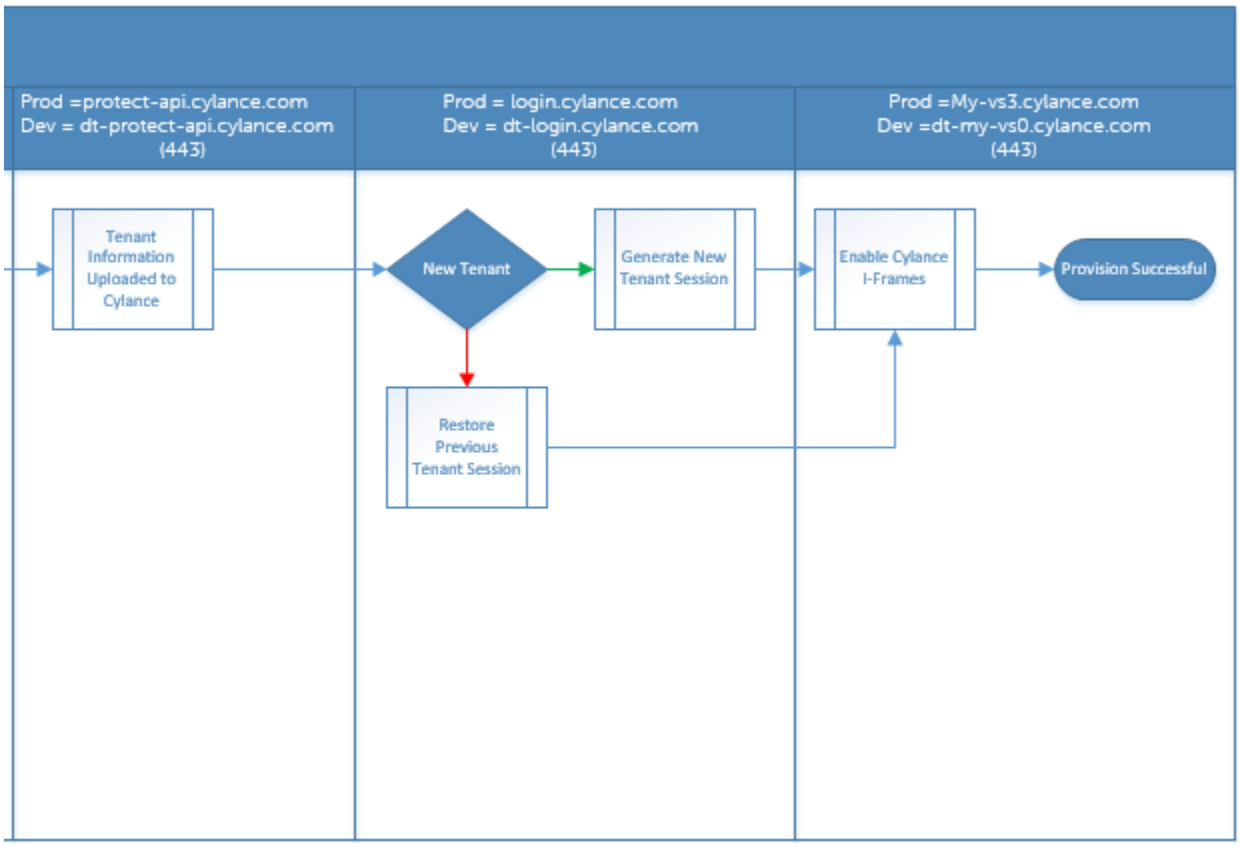
Solução de problemas do cliente do Advanced Threat Prevention

Provisionamento do Advanced Threat Prevention e comunicação do agente

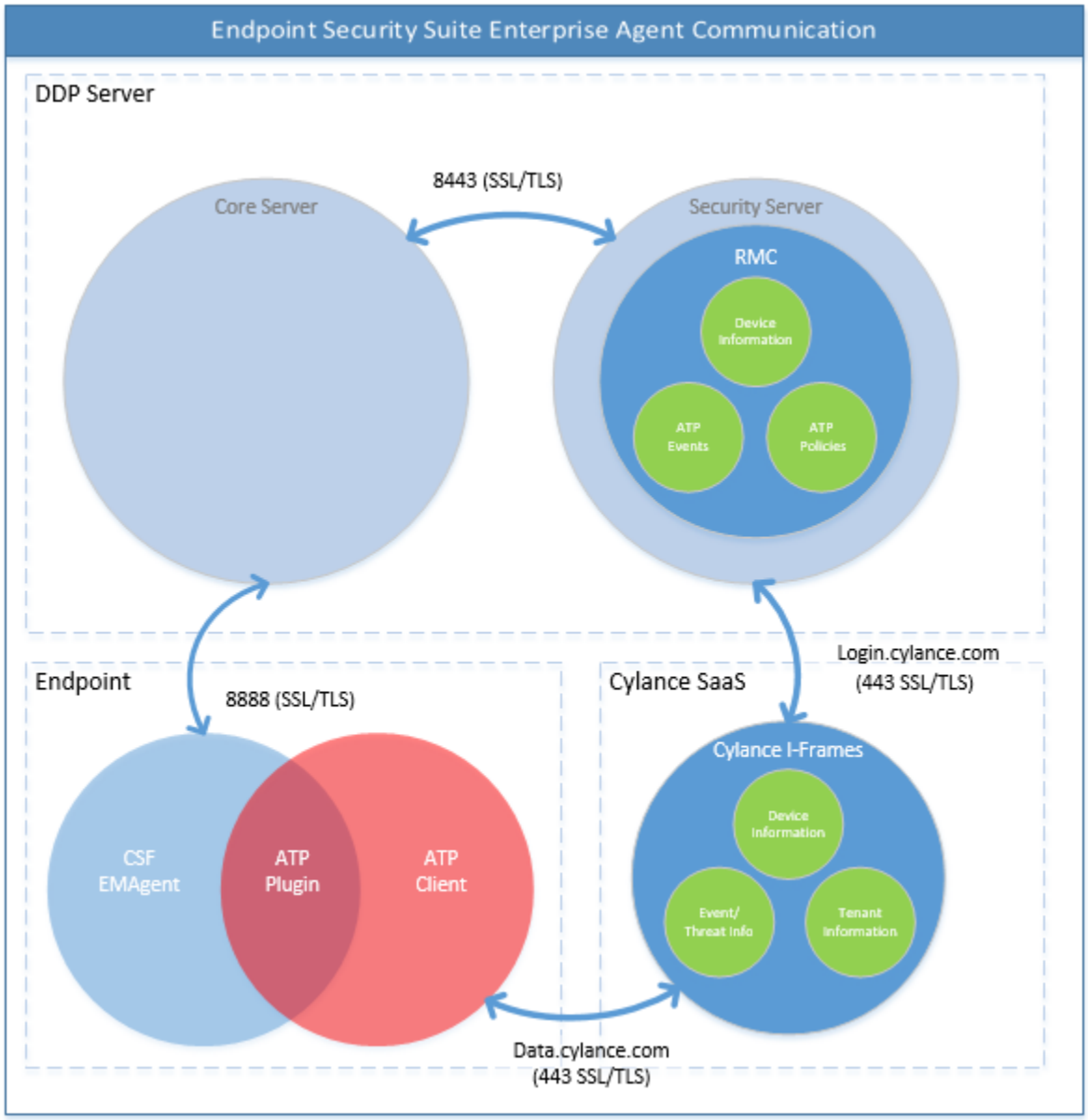
Os diagramas a seguir ilustram o processo de provisionamento do serviço Advanced Threat Prevention.







O diagrama a seguir ilustra o processo de comunicação do agente do Advanced Threat Prevention.


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)
Cylance SaaS
Login.cylance.com
(443 SSL/TLS)
CSF EMAgent
ATP Plugin
ATP Client
Cylance I-Frames
Device Information
Event/ Threat Info
Tenant Information
Data.cylance.com
(443 SSL/TLS)

5

Glossário

Servidor de segurança - usado para ativações do Client Encryption.

Proxy de política - usado para distribuir políticas ao Endpoint Security Suite Enterprise para software cliente Mac.

Remote Management Console - console do administrador para a implantação de todo o Enterprise.

Shield - é possível que você veja este termo na documentação e na interface do usuário do cliente. "Shield" é um termo usado para representar o software cliente.