

Dell Data Protection | Endpoint Security Suite Enterprise for Mac

Administrator Guide v1.1



📌 | NOTA: Uma NOTA indica informações importantes que ajudam a melhorar a utilização do produto.

⚠️ | AVISO: Um AVISO indica potenciais danos do hardware ou a perda de dados e explica como evitar o problema.

⚠️ | ADVERTÊNCIA: Uma ADVERTÊNCIA indica potenciais danos no equipamento, lesões pessoais ou mesmo morte.

© 2017 Dell Inc. Todos os direitos reservados. Dell, EMC e outras marcas registadas são marcas registadas da Dell Inc. ou das suas subsidiárias. Outras marcas registadas podem ser marcas registadas dos seus respetivos proprietários.

Marcas comerciais e marcas comerciais registadas utilizadas no Dell Data Protection Encryption, Endpoint Security Suite, Endpoint Security Suite Enterprise, e conjunto de aplicações de documentos Dell Data Guardian: Dell™ e o logótipo Dell, Dell Precision™, OptiPlex™, ControlVault™, Latitude™, XPS® e KACE™ são marcas comerciais da Dell Inc. Cylance®, CylancePROTECT® e o logótipo Cylance são marcas registadas da Cylance, Inc. nos EUA e noutros países. McAfee® e o logótipo da McAfee são marcas comerciais ou marcas comerciais registadas da McAfee, Inc. nos Estados Unidos e noutros países. Intel®, Pentium®, Intel Core Inside Duo®, Itanium® e Xeon® são marcas comerciais registadas da Intel Corporation nos EUA e noutros países. Adobe®, Acrobat®, e Flash® são marcas registadas da Adobe Systems Incorporated. Authen Tec® e Eikon® são marcas registadas da Authen Tec. AMD® é marca registada da Advanced Micro Devices, Inc. Microsoft®, Windows® and Windows Server®, Internet Explorer®, MS-DOS®, Windows Vista®, MSN®, ActiveX®, Active Directory®, Access®, ActiveSync®, BitLocker®, BitLocker To Go®, Excel®, Hyper-V®, Silverlight®, Outlook®, PowerPoint®, OneDrive®, SQL Server® e Visual C++® são marcas comerciais ou marcas registadas da Microsoft Corporation nos Estados Unidos e/ou noutros países. VMware® é marca registada ou marca comercial da VMware, Inc. nos Estados Unidos ou noutros países. Box® é marca registada da Box. DropboxSM é uma marca de serviço da Dropbox, Inc. Google™, Android™, Google™ Chrome™, Gmail™, YouTube® e Google™ Play são marcas comerciais ou marcas comerciais registadas da Google Inc. nos Estados Unidos e noutros países. Apple®, Aperture®, App StoreSM, Apple Remote Desktop™, Apple TV®, Boot Camp™, FileVault™, iCloud®SM, iPad®, iPhone®, iPhoto®, iTunes Music Store®, Macintosh®, Safari® e Siri® são marcas de serviço, marcas comerciais ou marcas comerciais registadas da Apple, Inc. nos Estados Unidos e/ou noutros países. GO ID®, RSA® e SecurID® são marcas registadas da Dell EMC. EnCase™ e Guidance Software® são marcas comerciais ou marcas comerciais registadas da Guidance Software. Entrust® é marca registada da Entrust®, Inc. nos Estados Unidos e noutros países. InstallShield® é marca registada da Flexera Software nos Estados Unidos, China, Comunidade Europeia, Hong Kong, Japão, Taiwan, e Reino Unido. Micron® e RealSSD® são marcas registadas da Micron Technology, Inc. nos Estados Unidos e noutros países. Mozilla® Firefox® é uma marca comercial registada da Mozilla Foundation nos Estados Unidos e/ou noutros países. iOS® é uma marca comercial ou marca comercial registada da Cisco Systems, Inc. nos Estados Unidos e outros países e é utilizada sob licença. Oracle® e Java® são marcas registadas da Oracle e/ou suas afiliadas. Os outros nomes podem ser marcas comerciais dos respetivos proprietários. SAMSUNG™ é uma marca comercial da SAMSUNG nos Estados Unidos ou noutros países. Seagate® é marca registada da Seagate Technology LLC nos Estados Unidos e/ou noutros países. Travelstar® é marca registada da HGST, Inc. nos Estados Unidos e noutros países. UNIX® é marca registada da The Open Group. VALIDITY™ é uma marca comercial da Validity Sensors, Inc. nos Estados Unidos e noutros países. VeriSign® e outras marcas similares são marcas comerciais ou marcas comerciais registadas da VeriSign, Inc. ou respetivas filiais ou subsidiárias nos Estados Unidos e noutros países e licenciadas à Symantec Corporation. KVM on IP® é marca registada da Video Products. Yahoo!® é marca registada da Yahoo! Inc. Este produto utiliza partes do programa 7-Zip. O código-fonte encontra-se disponível em 7-zip.org. O licenciamento é efetuado ao abrigo da licença GNU LGPL + restrições unRAR (7-zip.org/license.txt).

Administrator Guide

2017 - 05

Rev. A02

Contents

1 Introdução.....	5
Descrição geral.....	5
Cliente de encriptação Dell e encriptação FileVault.....	5
Contacte o Dell ProSupport.....	5
2 Requisitos.....	7
Encryption Client.....	7
Hardware para o cliente de encriptação.....	7
Encryption Client Software.....	7
Advanced Threat Prevention.....	9
Hardware para Advanced Threat Prevention.....	9
Software Advanced Threat Prevention.....	9
Portas do Advanced Threat Prevention.....	9
3 Tarefas para o cliente de encriptação.....	10
Instalar/Atualizar o o cliente de encriptação.....	10
Pré-requisitos.....	10
Instalação/atualização e ativação interativas.....	11
Instalação/atualização através de linha de comandos.....	12
Ativar o o cliente de encriptação.....	14
Ver o estado e a política de encriptação.....	15
Ver a política e o estado no computador local.....	15
Ver a política e o estado na Remote Management Console.....	18
Volumes do sistema.....	19
Activar encriptação.....	19
Processo de encriptação.....	20
Reciclar chaves de recuperação do FileVault.....	23
Experiência do utilizador.....	23
Recuperação.....	25
Montar um volume.....	25
Aceitar nova configuração do sistema.....	26
Recuperação do FileVault.....	28
Suporte multimédia amovível.....	31
Formatos suportados.....	31
EMS e atualizações de política.....	32
Exceções de encriptação.....	32
Erros no separador Suporte multimédia amovível.....	32
Mensagens de auditoria.....	32
Recolher ficheiros de registo para o Endpoint Security Suite Enterprise.....	32
Desinstalar o cliente de encriptação para Mac.....	33
Ativação como administrador.....	33
Ativar.....	33
Ativar temporariamente.....	34



Referência do cliente de encriptação.....	34
Acerca da proteção opcional da palavra-passe do firmware.....	34
Utilizar o Boot Camp.....	35
Como obter uma palavra-passe de firmware.....	36
Client Tool.....	37
4 Tarefas de Advanced Threat Prevention.....	40
Instalar o Advanced Threat Prevention for Mac.....	40
Pré-requisitos.....	40
Instalação interativa do Advanced Threat Prevention.....	40
Instalação do Advanced Threat Prevention através da linha de comandos.....	41
Resolução de problemas do Advanced Threat Prevention for Mac.....	42
Verificar a instalação do Advanced Threat Prevention.....	43
Recolher ficheiros de registo para o Endpoint Security Suite Enterprise.....	43
Ver detalhes do Advanced Threat Prevention.....	43
Separador Ameaças.....	44
Separador Exploits.....	44
Separador Eventos.....	44
Configurar um inquilino para o Advanced Threat Prevention.....	45
Configurar um inquilino.....	45
Configurar a atualização automática do Advanced Threat Prevention Agent.....	45
Resolução de problemas do cliente Advanced Threat Prevention.....	46
Aprovisionamento e comunicação do agente do Advanced Threat Prevention.....	46
5 Glossário.....	49



Introdução

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

Tópicos

- [Descrição geral](#)
- [Cliente de encriptação Dell e encriptação FileVault](#)
- [Contacte o Dell ProSupport](#)

Descrição geral

O Endpoint Security Suite Enterprise for Mac proporciona uma prevenção avançada contra ameaças, no sistema operativo e nas camadas de memória, e encriptação, tudo isto gerido de forma central a partir do Dell Data Protection Server. Com uma gestão centralizada, relatórios de conformidade consolidados e alertas de ameaças à consola, as empresas podem facilmente aplicar e comprovar a conformidade de todos os seus endpoints. Os conhecimentos em termos de segurança estão integrados em funcionalidades como políticas predefinidas e modelos de relatório que ajudam as empresas a reduzir os custos e a complexidade da gestão das TI.

- Endpoint Security Suite Enterprise for Mac - um conjunto de software para encriptação de dados de clientes e prevenção avançada contra ameaças.
- [Proxy de políticas](#) - utilizado para distribuir as políticas
- [Security Server](#) - utilizado para as ativações do software de encriptação de cliente
- Enterprise Server ou Dell Enterprise Server - VE - proporciona uma administração centralizada de políticas de segurança, integra-se nos diretórios existentes na empresa e cria relatórios. Neste documento, ambos os servidores estão assinalados como Dell Server, a não ser que seja necessário indicar uma versão específica (por exemplo, um procedimento que seja diferente ao utilizar o Dell Enterprise Server - VE).

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

O Endpoint Security Suite Enterprise for Mac tem dois ficheiros .dmg - um para o cliente de encriptação e um para o Advanced Threat Prevention. Pode instalar ambos ou apenas um.

Cliente de encriptação Dell e encriptação FileVault

A opção para gerir a encriptação FileVault juntamente com o cliente de encriptação Dell está disponível com o Endpoint Security Suite Enterprise for Mac. A opção apropriada depende dos requisitos de encriptação da empresa. Para obter mais informações sobre as políticas de encriptação, consulte [Encriptação Mac > Encriptação de volume Dell](#).

Contacte o Dell ProSupport

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

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



Para número de telefone fora dos Estados Unidos, consulte [Dell ProSupport International Phone Numbers](#) (Números de telefone internacionais do Dell ProSupport).



Requisitos

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

Tópicos

- [Encryption Client](#)
- [Advanced Threat Prevention](#)

Encryption Client

Hardware para o cliente de encriptação

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

NOTA: O disco do sistema tem de ser dividido com o esquema de partição Tabela de partições GUID (GPT) e ter um formato Mac OS X Extended (Journaled).

Hardware

- 30 MB de espaço livre em disco
- Placa 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).

- ① **NOTE:** For information on disabling, see [Interactive Installation/Upgrade and Activation, step 4](#). Before disabling, see Apple's help for how this impacts security.
- ① **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.

- ① **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](#).
- ① **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

① **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

- Antes de instalar o cliente Advanced Threat Prevention, elimine as aplicações antivírus, anti-malware e anti-spyware de outros fornecedores para evitar falhas na instalação.

Hardware para Advanced Threat Prevention

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

Hardware

- 500 MB de espaço livre no disco, dependendo do sistema operativo
- 2 GB de RAM
- Placa de rede 10/100/1000 ou Wi-Fi

Software Advanced Threat Prevention

A tabela seguinte lista os softwares suportados.

Sistemas operativos (kernels de 64 bits)

- Mac OS X Mavericks 10.9.5

NOTE: Esta versão avançada aplica-se apenas ao Advanced Threat Prevention, não ao cliente de encriptação.

- Mac OS X Yosemite 10.10.5

- Mac OS X El Capitan 10.11.6

NOTE: Não existe suporte para sistemas de ficheiros sensíveis a maiúsculas/minúsculas.

Portas do Advanced Threat Prevention

- Os agentes do Advanced Threat Prevention são geridos por e informam a plataforma SaaS da consola de gestão. A porta 443 (https) é utilizada para comunicação e deve estar aberta na firewall para que os agentes comuniquem com a consola. A consola é alojada por Amazon Web Services e não tem quaisquer IP fixos. Se, por qualquer motivo, a porta 443 estiver bloqueada, não é possível transferir as atualizações, pelo que os computadores poderão não dispor da proteção mais recente. Certifique-se de que os computadores cliente conseguem aceder aos URL, da seguinte forma.

Utilizar	Protocolo de aplicação	Protocolo de transporte	Número da porta	Destino	Direção
Todas as comunicações	HTTPS	TCP	443	Todo o tráfego https para *.cylance.com	Porta de saída



Tarefas para o cliente de encriptação

Instalar/Atualizar o o cliente de encriptação

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

Há dois métodos para instalar/atualizar o cliente de encriptação para Mac. Selecione **uma** das seguintes ações:

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

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

NOTA: A Apple lança frequentemente novas versões dos sistemas operativos entre os lançamentos do Endpoint Security Suite Enterprise for Mac. Para fornecer apoio ao máximo de clientes possível, permitimos a modificação do ficheiro `com.dell.ddp.plist` para apoiar estes casos. Assim que a Apple lança uma nova versão, começamos a testá-la a fim de assegurar que é compatível com o cliente de encriptação para Mac.

Pré-requisitos

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

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

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

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

Guia de migração e instalação do Enterprise Server

Enterprise Server - Guia de instalação e Guia de início rápido do Virtual Edition

- Certifique-se de que tem os URL do Security Server e do proxy de políticas à mão. Ambos serão necessários para a instalação e a ativação do software cliente.
- Se a sua implementação utilizar uma configuração não predefinida, certifique-se de que sabe o número de porta do Security Server. Será necessário para a instalação e a ativação do software cliente.
- Certifique-se de que o computador de destino tem ligação por rede ao Security Server e ao proxy de políticas.
- Certifique-se de que tem uma conta de utilizador de domínio na instalação do Active Directory configurada para utilizar com o Dell Server. A conta de utilizador de domínio será utilizada para a ativação do software cliente. Não é necessária a configuração de endpoints Mac para a autenticação de domínio (rede).
- Para aplicar a encriptação no computador cliente, primeiro selecione a opção de encriptação adequada para a sua organização.

Encriptação Dell

Selecione esta opção para fazer o seguinte:

- Encriptar todas as partições no disco de arranque
- Ignorar a Autenticação de pré-arranque
- Utilizar a encriptação de 256 bits

NOTA: Se utiliza a encriptação Dell, tem de desativar o SIP (System Integrity Protection - Proteção de integridade do sistema). Consulte [Instalação/atualização e ativação interativas](#), passo 4.

Encriptação do FileVault

Selecione esta opção para fazer o seguinte:

- Encriptar unidades Fusion
- Utilizar a Autenticação de pré-arranque
- Implementar uma solução suportada pela Apple

NOTA: Se um Mac tem uma unidade Fusion, tem de ativar o FileVault para encriptar essa unidade.

As definições da política de encriptação têm de refletir a opção de encriptação que seleciona. Antes de configurar as políticas de encriptação, certifique-se de que compreende as políticas *Encriptar utilizando o FileVault para Mac* e *Volumes visados para encriptação*. Para utilizar a encriptação Dell ou a encriptação FileVault, a política *Encriptação de volume Dell* deve estar *Ligada*.

Para obter mais informações sobre as políticas de encriptação, consulte [Mac Encryption > Encriptação de volume Dell](#).

Instalação/atualização e ativação interativas

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

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

- 1 A partir do suporte de instalação da Dell, instale o ficheiro Dell-Data-Protection-<version>.dmg.
- 2 Faça duplo clique no instalador do pacote. É apresentada a seguinte mensagem:
Este pacote executará um programa que determinará se o software pode ser instalado.
- 3 Clique em **Continuar** para prosseguir.
- 4 Leia o texto de Boas-vindas e clique em **Continuar**.
- 5 Leia o acordo da licença, clique em **Continuar** e clique em **Aceito** para aceitar os termos do acordo da licença.
Se utilizar encriptação Dell com o Mac OS X v10.11 ou superior, é apresentada uma caixa de diálogo com o título *A proteção de integridade do sistema Mac OS está ativada*. Tem de desativar a Proteção de integridade do sistema (SIP - System Integrity Protection).

Siga estes passos:
 - a Consulte <http://www.dell.com/support/Article/us/en/19/SLN299063> para desativar a SIP.
 - b No assistente, clique em **OK** e prossiga com a *Configuração da proteção de dados Dell*.
- 6 No campo **Endereço do domínio:**, introduza o nome de domínio totalmente qualificado para os utilizadores alvo, como por exemplo *departamento.empresa.com*.
- 7 No campo **Nome apresentado (opcional):**, considere definir *Nome apresentado* para o nome NetBIOS (anterior ao Windows 2000) do domínio, que normalmente está em maiúsculas.
Se definido, este campo é apresentado em vez do Endereço de domínio na caixa de diálogo *Ativação*. Isto permite a coerência com o nome de domínio indicado nas caixas de diálogo *Autenticação* para computadores Windows geridos pelo domínio.
- 8 No campo **Security Server:**, introduza o nome do anfitrião do Security Server.
Se a sua implementação utiliza uma configuração não predefinida, atualize os campos das portas e a caixa de verificação **Utilizar SSL**.

Assim que uma ligação é estabelecida, o indicador de ligação ao Security Server muda de vermelho para verde.
- 9 No campo **Proxy de políticas:**, o nome de anfitrião do proxy de políticas é preenchido automaticamente com um anfitrião do proxy de políticas que corresponda ao anfitrião do Security Server. Este anfitrião é utilizado como proxy de políticas se não forem especificados anfitriões na configuração das políticas.
Assim que a ligação tiver sido estabelecida, o indicador de ligação ao proxy de políticas muda de vermelho para verde.
- 10 Assim que a caixa de diálogo Configuração Dell estiver concluída e a ligação ao Security Server e ao proxy de políticas tiver sido estabelecida, clique em **Continuar** para ver o tipo de instalação.



- 11 Algumas instalações em computadores específicos apresentam uma caixa de diálogo *Selecionar um destino* antes de a caixa de diálogo *Tipo de instalação* ser apresentada. Nesse caso, desmarque o disco do sistema atual da lista de discos apresentada. O ícone do disco do sistema atual tem uma seta verde a apontar para o disco. Clique em **Continuar**.
- 12 Depois de o tipo de instalação ser apresentado, clique em **Instalar** para prosseguir com a instalação.
- 13 Quando solicitado, introduza as credenciais da conta de administrador (exigidas pela aplicação de instalação para o Mac OS X) e, em seguida, clique em **OK**.

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

- 14 Clique em **Continuar a instalação**. A instalação é iniciada.
- 15 Quando a instalação estiver concluída, clique em **Reiniciar**.
- 16 Prossiga para [Ativar o cliente de encriptação para Mac](#).

Instalação/atualização através de linha de comandos

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

NOTA: Se utiliza a encriptação Dell com Mac OS X v10.11.x, tem de desativar o SIP. Consulte <http://www.dell.com/support/Article/us/en/19/SLN299063>.

- 1 A partir do suporte de instalação da Dell, instale o ficheiro Dell-Data-Protection-<version>.dmg.
- 2 Copie o pacote **Install Dell Data Protection** e o ficheiro **com.dell.ddp.plist** para a unidade de disco local.
- 3 Na Remote Management Console, modifique as seguintes políticas, se necessário. As definições das políticas substituem as definições do ficheiro .plist. Utilize as definições .plist se não existirem políticas na Remote Management Console.
 - **Modo de palavra-passe do firmware** - se pretende utilizar o Boot Camp em computadores Mac encriptados ou utilizar uma versão de um sistema operativo que ainda não seja totalmente suportada pela Dell, **tem** de definir esta política como *Opcional* para **não** utilizar a proteção da palavra-passe do firmware. Para obter mais informações, consulte [Acerca da proteção opcional da palavra-passe do firmware](#).

NOTA:

Quando a política FirmwarePasswordMode for definida como **Opcional**, tal só desativa a obrigatoriedade de proteção da palavra-passe do firmware imposta pelo software cliente. **Não** elimina qualquer proteção da palavra-passe do firmware. Depois de concluídos estes passos, da instalação estar completa e de o computador ser reiniciado, pode remover qualquer palavra-passe de firmware existente através do Utilitário de palavra-passe de firmware do Mac OS X.

- **Sem Lista de utilizadores autenticados** - em alguns casos, poderá desejar editar esta política para que os utilizadores especificados ou as classes de utilizadores não tenham de proceder à ativação no Dell Server. Por exemplo, em instalações educacionais, os professores seriam instruídos a ativar o seu computador no Dell Server, mas cada aluno individual que utilizasse os computadores do laboratório não seria. O administrador do laboratório poderia utilizar esta política e a conta ativada no Client Tool para que os estudantes pudessem iniciar sessão sem lhes ser solicitada a ativação. Para obter informações sobre o Client Tool, consulte [Client Tool](#). Se uma empresa precisar de saber que conta de utilizador está associada a cada computador Mac, todos os utilizadores têm de estar ativados no Dell Server, pelo que a empresa não editaria essa propriedade. No entanto, se um utilizador quiser fornecer suportes de dados EMS, este tem de ser autenticado no Dell Server.
- 4 Abra o ficheiro .plist e edite quaisquer valores de marcadores de posição adicionais:

NOTA:

A Apple lança frequentemente novas versões dos sistemas operativos entre os lançamentos do Endpoint Security Suite Enterprise for Mac. Para fornecer apoio ao máximo de clientes possível, permitimos a modificação do ficheiro .plist para apoiar estes casos. Assim que a Apple lança uma nova versão, a Dell começa a testá-la a fim de assegurar que é compatível com o cliente de encriptação 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 Guarde e feche o ficheiro .plist.
- 6 Para cada computador alvo, copie o pacote para uma pasta temporária e o ficheiro com.dell.ddp.plist para **/Library/Preferences**.
- 7 Execute a instalação do pacote a partir da linha de comandos através do comando **installer**:
`sudo installer -pkg "Install Dell Data Protection.pkg" -target /`
- 8 Reinicie o computador através da seguinte linha de comandos: `sudo shutdown -r now`
- 9 Prossiga para [Ativar o cliente de encriptação para Mac](#).

Ativar o o cliente de encriptação

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

📌 NOTA: Para obter instruções sobre como ativar um domínio não-Mac, consulte o [KB article SLN302497](#).

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

- 1 Introduza o nome de utilizador e a palavra-passe geridos pelo Active Directory.
 Se a caixa de diálogo da palavra-passe se fechar, prima **Atualizar** no separador Políticas. Em [Ver a política e o estado no computador local](#), consulte [passo 1](#).
- 2 Selecione o domínio em que pretende iniciar sessão.
 Se o Dell Server estiver configurado para suporte multidomínio e um domínio diferente for utilizado para ativação, utilize o Nome principal do utilizador (UPN), que tem a forma `<username>@<domain>`.
- 3 As opções são:
 - Clique em **Ativar**.
 - Se a ativação for bem-sucedida, é apresentada uma mensagem a indicar o êxito da mesma. O o cliente de encriptação para Mac fica assim totalmente operacional e gerido pelo Dell Server.
 - Se a ativação falhar, o software cliente permite três tentativas para introduzir as credenciais de domínio corretas. Se as três tentativas fracassarem, é novamente apresentada uma mensagem a solicitar as credenciais de domínio quando o próximo utilizador iniciar sessão.
 - Clique em **Agora não** para ignorar a caixa de diálogo, que será apresentada novamente no próximo início de sessão do utilizador.

NOTA: Quando o administrador precisar de descriptar uma unidade de um computador Mac, quer seja a partir de uma localização remota, executando um script, ou em pessoa, o software cliente vai solicitar ao utilizador que permita o acesso de administrador e irá requerer que o utilizador introduza a sua palavra-passe.

NOTA: Se configurar o computador para a encriptação FileVault e os ficheiros estiverem encriptados, certifique-se de que inicia sessão numa conta a partir da qual mais tarde pode reiniciar o sistema.

4 Proceda da seguinte forma:

- Se a encriptação **não** tiver sido ativada antes da ativação, prossiga para [Processo de encriptação](#).
- Se a encriptação **tiver** sido ativada antes da ativação, prossiga para [Ver o estado e a política de encriptação](#).

Ver o estado e a política de encriptação

Pode ver a política de encriptação e o estado no computador encriptado ou na [Remote Management Console](#).

Ver a política e o estado no computador local

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

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

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

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

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

Dependendo dos requisitos de encriptação da sua empresa, pode definir políticas para Dell Encryption ou encriptação FileVault. Esta tabela lista as opções de política para cada.

Encriptação Mac > Encriptação de volume Dell

Encriptação de volume Dell

Ligado ou *Desligado*

Esta é a “política principal” para todas as restantes políticas de Encriptação de volume Dell. Esta política deve ser definida como *Ligado* para que quaisquer outras políticas de Encriptação de volume Dell sejam aplicadas.

Ligado ativa a encriptação e inicia a encriptação de volumes descriptados, com base na política *Volumes visados para encriptação* **ou** *Encriptar utilizando o FileVault para Mac*. A predefinição é *Ligado*.

Desligado desativa a encriptação e inicia o varrimento de descriptação para quaisquer volumes totalmente ou parcialmente encriptados.

Encriptar utilizando o FileVault para Mac

Se planear utilizar a encriptação do FileVault, certifique-se de que primeiro define a [Encriptação de volume Dell](#) para *Ligado*.

Certifique-se de que a política *Encriptar utilizando o FileVault para Mac* está selecionada no Dell Server.

Quando ativado, o FileVault é utilizado para encriptar volumes do sistema, incluindo unidades Fusion, com base na definição de política *Volumes visados para encriptação*.

NOTA: Se utiliza a encriptação Dell (e não o FileVault) e esta política estiver ativada, vai ocorrer um conflito de políticas.



NOTA:

Se tenciona migrar do Dell Encryption para a encriptação FileVault, consulte [Migrar do Dell Volume Encryption para a Encriptação FileVault](#).

Encriptação Mac > Definições Globais Mac

Volumes visados para encriptação *Apenas volume do sistema* ou *Todas as unidades fixas*

A definição *Apenas volume do sistema* protege apenas o volume do sistema em execução no momento.

A definição **Todas as unidades fixas** protege todos os Volumes expandidos do Mac OS em todos os discos fixos, juntamente com o volume do sistema em execução no momento.

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

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










"Distrito",	Descrição
A restaurar para o estado original...	O software cliente está a restaurar o esquema de partição para o seu estado original no final do processo "A descriptar...". Este é o varrimento de descriptação equivalente ao estado "A preparar o volume para a encriptação".
Descriptado	O varrimento da descriptação está concluído.

Cor	Descrição
Verde	Porção encriptada
Vermelho	Porção descriptada
Amarelo	A porção está a ser reencriptada

Por exemplo, através de uma alteração nos algoritmos de encriptação. Os dados continuam seguros. Estão apenas a mudar para um tipo de encriptação diferente.

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

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

Distintivo	Tipo de volume e estado
	O volume do sistema Mac OS X atualmente iniciado. O distintivo X-folder indica a partição de arranque atual.
	A encriptação Dell não é compatível com a Proteção de integridade do sistema (SIP). Se esta condição incompatível for especificada pela política e a SIP estiver ativada, é apresentado um erro junto à unidade no separador Volumes do sistema. Para desativar a SIP, consulte Instalação/atualização e ativação interativa, passo 4 .
	Um volume configurado para encriptação. Este distintivo indica uma partição encriptada Dell.
	Um volume configurado para encriptação. O distintivo Segurança e Privacidade indica uma partição protegida pelo FileVault.
	Um volume que não é de arranque configurado para encriptação. O distintivo Segurança e Privacidade indica uma partição protegida pelo FileVault.
	Várias unidades e nenhuma encriptação.
	NOTA: O ícone do volume sem um distintivo indica que nada foi feito ao disco. Este não é um disco de arranque.



Distintivo

Tipo de volume e estado



Vários discos onde apenas o volume do sistema está encriptado. Este exemplo é uma partição encriptada Dell.

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

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

Distintivo

Estado



Um ícone de volume mais esbatido indica que o dispositivo não foi montado. As razões incluem:

- O utilizador pode ter decidido não fornecê-lo.
- O suporte multimédia pode estar bloqueado.

NOTA: Um distintivo com um círculo/barra vermelha indica uma partição que foi excluída da proteção porque não é suportada. Isto inclui volumes formatados FAT32.



Um ícone de volume mais escuro indica que o dispositivo foi montado. O distintivo sem escrita indica que é apenas de leitura. A encriptação está ativada, mas o suporte não está provisionado e a política Acesso EMS a suporte UnShieldable está definido como Só de leitura.



Suporte multimédia encriptado pelo EMS, indicado por um distintivo Dell.

Ver a política e o estado na Remote Management Console

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

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

NOTA: O carácter universal (*) pode ser utilizado, mas não é necessário no início ou fim do texto. Pode introduzir Nome comum, Nome principal universal ou sAMAccountName.

- 4 Clique no endpoint apropriado.
- 5 Clique no separador **Detalhes e ações**.

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

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

Para ver as políticas aplicadas, na secção Ações, clique em **Ver políticas aplicadas**.

- 6 Clique no separador **Políticas de segurança**. Neste separador, pode expandir os tipos de políticas e alterar cada uma das políticas.
 - a Quando terminar, clique em **Guardar**.
 - b No painel da esquerda, clique em **Management > Commit** (Gestão > Consolidar).

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

- c Introduza uma descrição das alterações na caixa Comentário e clique em **Consolidar políticas**.
- 7 Clique no separador **Utilizadores**. Esta secção apresenta uma lista de utilizadores ativados neste computador Mac. Clique no nome do utilizador para apresentar informações sobre todos os computadores no qual este utilizador efetuou a ativação.
- 8 Clique no separador **Grupos de endpoints**. Esta secção apresenta todos os grupos de endpoints aos quais este computador Mac pertence.

Volumes do sistema

Activar encriptação

NOTA: Apenas volumes Mac OS X Extended (Journaled) e discos do sistema que são particionados com o esquema de partições Tabela de partições GUID (GPT) são suportados para encriptação.

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

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

NOTA: O carácter universal (*) pode ser utilizado, mas não é necessário no início ou fim do texto. Pode introduzir Nome comum, Nome principal universal ou sAMAccountName.

- 4 Clique no endpoint apropriado.
- 5 Na página *Políticas de segurança*, clique no grupo de tecnologia **Encriptação Mac**.
Por predefinição, a política principal *Encriptação de volume Dell* está definida como *Ligada*.
- 6 Se um Mac tiver uma unidade Fusion, marque a caixa de verificação da política *Encriptar utilizando o FileVault for Mac*.

NOTA: Esta política requer que a política *Encriptação de volume Dell* também seja definida como *Ligada*. Contudo, quando a encriptação FileVault é ativada, nenhuma das restantes políticas do grupo será aplicada. Consulte [Encriptação Mac > Encriptação de volume Dell](#).

- 7 Se o FileVault for desativado, altere as outras políticas conforme pretender.
Para obter descrições de todas as políticas, consulte *AdminHelp* que está disponível a partir da Remote Management Console.
- 8 Quando terminar, clique em **Guardar**.
- 9 No painel da esquerda, clique em **Gestão > Consolidar**.
O número apresentado em Alterações às políticas pendentes é cumulativo. Pode incluir as alterações efetuadas noutros endpoints ou efetuadas por outros administradores que estão a utilizar a mesma conta.
- 10 Introduza uma descrição das alterações na caixa Comentário e clique em **Consolidar políticas**.
- 11 Para ver a definição da política no computador local depois de o Dell Server enviar a política, no painel Políticas das Preferências de Dell Data Protection, clique em **Atualizar**.



Processo de encriptação

O processo de encriptação varia consoante estes fatores:

- O início do volume de arranque quando a encriptação é ativada.
- Se é selecionada a encriptação Dell ou FileVault.

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

Selecione um dos seguintes:

- Encriptação Dell de uma unidade não encriptada
- Encriptação FileVault de um volume não encriptado
- Assumir a gestão de um volume com encriptação FileVault já existente

Encriptação Dell de uma unidade não encriptada

Depois de o software cliente receber a política de encriptação, executa uma validação do utilitário do disco nos volumes a encriptar e, em seguida, configura esses volumes para encriptação.

- 1 A barra de progresso indica o estado da verificação. Quando a verificação é concluída, os volumes selecionados são configurados para encriptação.

Este processo pode diminuir a capacidade de resposta do computador durante alguns minutos. Para cada volume a aguardar a encriptação, é apresentada uma caixa de diálogo ao utilizador a indicar que a operação está em curso.

- 2 Após a preparação da encriptação estar concluída, reinicie o computador.

NOTA: Consoante as políticas de experiência do utilizador definidas na Remote Management Console, o software cliente pode solicitar ao utilizador que reinicie o computador.

- 3 Após o reinício do computador, este deve ser ligado a uma rede para que o software cliente deposite as informações de recuperação no Dell Server.

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

Encriptação FileVault de um volume não encriptado

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

NOTA: Se deixar esta caixa de diálogo expirar, terá de reiniciar o computador ou iniciar sessão para que a caixa de diálogo da palavra-passe seja apresentada novamente.

- 4 Clique em **OK**.

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

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

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

NOTA: Consoante as políticas de experiência do utilizador definidas na Remote Management Console, o software cliente pode solicitar ao utilizador que reinicie o computador.

- 7 Após o reinício do computador, este deve ser ligado a uma rede para que o software cliente deposite as informações de recuperação no Dell Server.

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

Modificar a política para adicionar utilizadores do FileVault

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

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

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

NOTA: Se uma regra for formada incorretamente, é apresentada uma mensagem de erro no separador *Dell Data Protection > Preferências*.

O seguinte `<dict>` lista exemplos de duas teclas:

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

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



NOTA:

Neste exemplo, os asteriscos à direita representam a última parte dos registos de autoridade de autenticação. Normalmente, e para evitar subespecificações, inclua o registo completo em vez de um asterisco à direita, uma vez que o asterisco corresponde a qualquer informação depois de dois pontos no registo do OpenDirectory.

- A tecla NFSHomeDirectory requer que qualquer utilizador que passe pela primeira tecla tenha também de ter um diretório raiz em `/Users/`.

NOTA:

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

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

Para que um utilizador ative a sua conta do FileVault:

- 1 Inicie **Preferências do sistema** e clique em **Dell Data Protection**.
- 2 Clique no separador **Volumes do sistema**.
- 3 Clique na tecla Option e no botão direito do rato sobre a unidade Volume do sistema e selecione **Adicionar utilizadores do FileVault ao arranque do FileVault**.
- 4 No campo Procurar, introduza o nome de um utilizador ou percorra para baixo. As contas de utilizador só serão apresentadas se reunirem os critérios definidos pela política.
É apresentado um botão *Ativar utilizador* aos utilizadores locais e móveis.

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

NOTA:

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

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

Assumir a gestão de um volume com encriptação FileVault já existente

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

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

- 1 Selecione **Chave de recuperação pessoal** ou **Credenciais de conta de arranque**.
 - **Chave de recuperação pessoal - Se tem a chave de recuperação pessoal que recebeu quando a unidade foi encriptada pelo FileVault:**
 - 1 Introduza a chave.

Se um utilizador não tiver a chave existente, pode solicitá-la ao administrador.
 - 2 Clique em **OK**.

NOTA: Depois do processo de assunção estar concluído, é gerada e depositada uma nova chave de recuperação pessoal. A chave de recuperação anterior é invalidada e removida.

- **Credenciais de conta de arranque - Se tem o nome de utilizador e a palavra-passe de uma conta atualmente autorizada a arrancar a partir do volume:**

- 1 Introduza o nome de utilizador e a palavra-passe.
- 2 Clique em **OK**.
- 2 Quando for apresentada uma caixa de diálogo a indicar que a Dell está agora a gerir a encriptação do volume, clique em **OK**.

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

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

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

Se optar por não introduzir a palavra-passe, o conteúdo do volume ficará acessível e será encriptado com FileVault, mas a encriptação não será gerida pela Dell.

ⓘ | NOTA: Na Remote Management Console, o administrador pode ver que agora o Dell Server gere o endpoint.

Reciclar chaves de recuperação do FileVault

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

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

Para reciclar o material de chave:

- 1 Transfira um pacote de recuperação da Remote Management Console e copie-o para o ambiente de trabalho do computador.
- 2 Inicie *Preferências do sistema* e clique em **Proteção de dados Dell**.
- 3 Clique no separador **Volumes do sistema**.
- 4 Arraste o pacote de recuperação do passo 1 para a partição adequada.
É apresentada uma caixa de diálogo a solicitar que troque as chaves do FileVault.
- 5 Clique em **OK**.
É apresentada uma caixa de diálogo a confirmar o êxito da troca de chaves.
- 6 Clique em **OK**.

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

Experiência do utilizador

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

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

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

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



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

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

Copiar regra de lista branca

Um item oculto do menu permite a um utilizador copiar uma regra da lista branca para um suporte multimédia externo.

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

É apresentado o item de menu oculto.

- 4 Clique na opção **Copiar regra de lista branca** relativa ao suporte externo atual. A regra de lista branca é copiada para a Área de transferência.
- 5 Aceda à Área de transferência, copie a regra de lista branca aprovada e envie-a ao seu administrador.

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

Se pretende excluir um dispositivo ou um grupo de dispositivos para evitar a escrita de dados encriptados na unidade Thunderbolt ou em suportes EMS, pode utilizar a regra da lista branca para modificar os valores.

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

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

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

NOTA: Tem de ativar HFS Plus. Consulte [Ativar HFS Plus](#).

Para excluir dispositivos SATA da aplicação de política do EMS quando ligado através do Thunderbolt:

```
tbolt=1;bus=SATA
```

Também pode colocar na lista branca ou excluir suportes de EMS com base no seguinte:

• Tamanho do suporte

Crie uma regra na lista branca para excluir suportes grandes da proteção EMS:

```
size <op> <size specifier>
```

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

<size specifier> tem uma forma de número inteiro decimal com um sufixo opcional de {K, M, G, T} alinhado a 1000, não 1024. Por exemplo, para excluir suportes ou uma unidade maiores do que 500000000 bytes do EMS, utilize um dos seguintes:

```
size >= 500000000
```

```
size >= 500000K
```

```
size >= 500M
```

• Tipo de sistema de ficheiros



Regra de lista branca:

`fstype=<fstype>`

`<fstype>` pode ser ExFAT, FAT ou HFS+

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

`size>=1T;fstype=HFS+`

Recuperação

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

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

- Poderá ter de mover os dados encriptados de um utilizador para um computador Mac diferente, como parte de uma atualização de hardware.
- Poderá ter de aceder a um disco encriptado devido a uma falha no sistema operativo que faz com que o volume do sistema deixe de arrancar e precisa de executar vários utilitários para reparar o sistema operativo.
- Poderá ter de aceder aos dados encriptados de um utilizador porque o utilizador fez uma alteração às configurações não autorizada e precisa de resolver a situação.

Esta secção vai guiá-lo através do processo de utilizar **uma** das três operações de recuperação disponíveis.

Escolha **uma** opção abaixo:


- [Montar um volume](#)
- [Aceitar nova configuração do sistema](#)
- [Recuperação FileVault](#) - utilizada apenas se utilizar a encriptação FileVault no endpoint a recuperar. O FileVault pode ser utilizado com o cliente de encriptação executado no Mac OS X 10.10.5 ou posterior. A recuperação do FileVault também é utilizada em unidades Fusion.

Montar um volume

Pré-requisitos

- Um computador ou volume de recuperação externo desencriptado que irá executar o utilitário de recuperação
- Um cabo FireWire ou Thunderbolt, consoante o hardware
- O ID do dispositivo/ID único do computador visado para recuperação - Na maioria dos casos, pode encontrar o computador visado para recuperação na Remote Management Console ao pesquisar o nome de utilizador do proprietário e visualizar os dispositivos encriptados para esse utilizador. O formato do ID único/ID do dispositivo é "MacBook.Z4291LK58RH de Fulano de Tal".
- O suporte multimédia de instalação da Dell

Processo

- 1 Como Administrador Dell, inicie sessão na Remote Management Console.
- 2 No painel do lado esquerdo, clique em **Gestão > Recuperar Endpoint**.
- 3 No campo Procurar, introduza o nome de domínio totalmente qualificado do endpoint a recuperar e clique no ícone de Procurar.
- 4 Clique na ligação **Recuperar** do dispositivo.
- 5 Se o endpoint necessitar de uma recuperação avançada, é apresentado um pedido de palavra-passe. Atribua uma nova palavra-passe ao pacote de chaves que vai transferir.
 **NOTA: Terá de recordar esta palavra-passe para aceder às chaves de recuperação.**
- 6 Para guardar o pacote de recuperação no volume de recuperação externo ou no computador que executará o utilitário de recuperação para realizar a operação de recuperação, clique em **Transferir** e clique em **Guardar**.



O ficheiro de recuperação <machine_name.domain>.csv é transferido.

NOTA: Se a proteção da palavra-passe de firmware estiver ativada neste computador, será solicitada a palavra-passe de firmware para aceder ao Gestor de arranque em modo pré-arranque. Pode encontrar a palavra-passe de firmware deste computador no pacote de recuperação transferido em [guardar o pacote de recuperação](#). Consulte [Como ativar Mac OS X Boot Camp](#) para obter mais informações.

- Inicie o computador alvo a partir de um volume de recuperação externo criado previamente. Poderá conseguir isso executando o painel Iniciar disco, nas Preferências do sistema e selecionando o volume de recuperação, ou mantendo premida a tecla **Option** quando estiver a reiniciar este computador e selecionando o volume de recuperação no Gestor de arranque em modo pré-arranque. ou

Reinicie o computador alvo da recuperação no Modo disco de destino. Poderá conseguir isso executando o painel Iniciar disco, nas Preferências do sistema e clicando em **Modo de disco de destino**, ou mantendo premida a tecla **T** enquanto reinicia este computador.

NOTA: A proteção de palavra-passe de firmware impede que utilize a tecla **T** no arranque para entrar no Modo disco de destino. Encontre mais informações sobre o Modo de disco de destino disponibilizadas pela Apple em <http://support.apple.com/kb/HT1661>.

Agora ligue este computador ao computador anfitrião que irá executar a operação de recuperação através de um cabo FireWire ou Thunderbolt, consoante o hardware.

- Monte o ficheiro Dell-Data-Protection-<version>.dmg.

NOTA: O Utilitário de recuperação deverá ser o mesmo ou uma versão mais recente do que a versão do software cliente instalado no computador visado para recuperação.

- Na pasta Utilitários localizada no suporte de instalação da Dell, inicie o Utilitário de recuperação Dell. É apresentada a mensagem: "O kext de DDP [texto do kernel] tem de ser carregado para que possa modificar discos encriptados. Introduza a sua palavra-passe para permiti-lo."
- Introduza a palavra-passe do administrador ou do utilizador. É apresentada a mensagem: "Instalação necessária: é preciso instalar o Recovery."
- Clique em **Install** (Instalar).
- Selecione o volume ou a unidade que precisa de ser recuperada e clique em **Continuar**. A seleção da unidade irá recuperar todos os volumes contidos na mesma de uma só vez.
- Selecione o pacote de recuperação (guardado no passo [passo 6](#)) e clique em **Abrir**.
- Selecione a opção **Montar volume**.
- Clique em **Continuar** para confirmar *Montar volume*. É apresentada uma mensagem de êxito.
- Clique em **Fechar**.

Pode agora abrir uma janela no Finder e aceder a dados no volume encriptado, tal como o faria num volume normal. Todos os dados serão encriptados e desencriptados de forma transparente, uma vez que os ficheiros são transferidos entre os volumes.

Aceitar nova configuração do sistema

Se a alteração de uma palavra-passe de firmware ou outra configuração do sistema invalidou a chave de encriptação num computador encriptado, escolha esta opção para aceitar a configuração do sistema atualizado no próximo reinício e restaurar o acesso ao computador.

Como a encriptação está ligada à configuração específica do dispositivo, as alterações à configuração invalidam a chave de encriptação do software cliente. Ao escolher aceitar a nova configuração do sistema, basta dar instruções ao software cliente para repor a sua segurança com base na nova configuração. Por exemplo, poderá precisar de mover a unidade para um computador Mac diferente porque um utilizador quebrou o ecrã. Utilizando este método, dê instruções ao software cliente para aceitar esta "nova" configuração como válida.

Pré-requisitos

- Um computador ou volume de recuperação externo desencriptado que irá executar o utilitário de recuperação
- Um cabo FireWire ou Thunderbolt, consoante o hardware
- O ID do dispositivo/ID único do computador visado para recuperação - Na maioria dos casos, pode encontrar o computador visado para recuperação na Remote Management Console ao pesquisar o nome de utilizador do proprietário e visualizar os dispositivos encriptados para esse utilizador. O formato do ID único/ID do dispositivo é "MacBook.Z4291LK58RH de Fulano de Tal".

- O suporte multimídia de instalação da Dell

Processo

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

NOTA: Se a proteção da palavra-passe de firmware estiver ativada neste computador, ser-lhe-á solicitada a palavra-passe de firmware para aceder ao Gestor de arranque em modo pré-arranque. Pode encontrar a palavra-passe de firmware deste computador no pacote de recuperação transferido no **passo 7**. Consulte **Como ativar Mac OS X Boot Camp** para obter mais informações.

- 8 Inicie o computador alvo a partir de um volume de instalação externo pré-criado do SO completo. Poderá conseguir isso executando o painel Iniciar disco, nas Preferências do sistema e selecionando o volume de instalação do SO completo, ou mantendo premida a tecla **Option** quando estiver a reiniciar este computador e selecionando o volume de instalação do SO completo no Gestor de arranque em modo pré-arranque. Para criar um volume de arranque, consulte <https://support.apple.com/en-us/HT202796>.

ou

Reinicie o computador alvo da recuperação no Modo disco de destino. Poderá conseguir isso executando o painel Iniciar disco, nas Preferências do sistema e clicando em **Modo de disco de destino**, ou mantendo premida a tecla **T** enquanto reinicia este computador.

NOTA: A proteção de palavra-passe de firmware impede que utilize a tecla **T** no arranque para entrar no Modo disco de destino. Encontre mais informações sobre o Modo de disco de destino disponibilizadas pela Apple em <http://support.apple.com/kb/HT1661>.

- 9 Proceda da seguinte forma:
 - Ligue este computador ao computador anfitrião que irá executar a operação de recuperação através de um cabo FireWire ou Thunderbolt, consoante o hardware.ou
 - Mude o arranque para qualquer disco que tenha uma instalação de SO completo.
- 10 Monte o ficheiro Dell-Data-Protection-<version>.dmg.

NOTA: O Utilitário de recuperação deverá ser o mesmo ou uma versão mais recente do que a versão do software cliente instalado no computador visado para recuperação.

- 11 Na pasta Utilitários localizada no suporte de instalação da Dell, inicie o Utilitário de recuperação Dell. É apresentada a mensagem: "O kext de DDP [texto do kernel] tem de ser carregado para que possa modificar discos encriptados. Introduza a sua palavra-passe para permiti-lo."
- 12 Introduza a palavra-passe do administrador ou do utilizador. É apresentada a mensagem: "Instalação necessária: é preciso instalar o Recovery."
- 13 Clique em **Install** (Instalar).
- 14 Selecione o volume ou a unidade que precisa de ser recuperada e clique em **Continuar**. A seleção da unidade irá recuperar todos os volumes contidos na mesma de uma só vez.

É apresentada a janela de seletor de ficheiros.
- 15 Selecione o pacote de recuperação (guardado no passo [passo 7](#)) e clique em **Abrir**. É apresentada a caixa de diálogo *Selecionar operação de recuperação*.
- 16 Selecione a opção **Aceitar nova configuração do sistema**.
- 17 Clique em **Continuar** para confirmar *Aceitar nova configuração do sistema*.
- 18 Introduza a sua palavra-passe para repor a propriedade e aceitar a nova configuração do sistema.



19 Clique em **OK**.

É apresentada uma mensagem *Recuperação concluída* quando for reiniciado o volume do sistema interno original. Esta mensagem solicitar-lhe-á que reinicie novamente o computador. O software cliente aceita assim a configuração atualizada do sistema e o utilizador pode aceder ao seu computador normalmente.

Recuperação do FileVault

A recuperação de um volume gerido encriptado pelo FileVault é significativamente diferente da recuperação de um volume encriptado pela Dell. O processo de recuperação é ditado pela Apple e é automatizado sempre que possível, mas requer mais alguns passos.

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

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

Existem dois métodos de recuperação, dependendo do facto de a chave de recuperação do FileVault ser uma chave de recuperação pessoal ou institucional. Existe sempre uma chave de recuperação válida. Regra geral, utilize a chave de recuperação pessoal mais recente primeiro. Se essa chave não funcionar, utilize a keychain de recuperação institucional.

- [Chave de recuperação pessoal](#) - a encriptação FileVault existente é gerida pelo Dell Server. Este é o método preferido.

Se a entrada mais recente no pacote de recuperação contém uma entrada RecoveryKey, siga os passos de [Chave de recuperação pessoal](#). Segue-se um exemplo de RecoveryKey:

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

- [Keychain de recuperação](#) - Este método de recuperação baseia-se na utilização de uma chave de recuperação institucional do FileVault.

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

```
KeychainKey</key><data>a31jaAABAAAAA...
```

Chave de recuperação pessoal

Normalmente, a melhor prática é recuperar o volume de arranque antes de recuperar os volumes de não arranque. A recuperação do volume de arranque irá normalmente corrigir os problemas dos volumes de não arranque.

Pré-requisitos

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

Processo

- 1 Abra a Remote Management Console.
- 2 No painel esquerdo, clique em **Populações > Endpoints**.
- 3 Procure o dispositivo a recuperar.
- 4 Clique no nome do dispositivo para abrir a página Detalhe do Endpoint.



- 5 Clique no separador **Detalhes e ações**.
- 6 Em Detalhe de proteção, clique na ligação **Chaves de recuperação de dispositivos**.
- 7 Para guardar o pacote de recuperação no volume de recuperação externo ou no computador que executará o utilitário de recuperação para realizar a operação de recuperação, clique em **Transferir** e clique em **Guardar**.
- 8 Introduza uma localização para o pacote de recuperação e clique em **Guardar**.
- 9 Copie o pacote de recuperação e o ficheiro **Dell-Data-Protection-<version>.dmg** para a unidade USB de arranque.
- 10 Arranque o computador de destino a partir de um volume de instalação externo pré-criado do SO completo premindo a tecla **Option** enquanto reinicia este computador e, em seguida, selecione o volume de instalação externo pré-criado do SO completo no Gestor de arranque em modo pré-arranque. Para criar um volume de arranque, consulte <https://support.apple.com/en-us/HT202796>.
- 11 Monte o ficheiro Dell-Data-Protection-<version>.dmg.

NOTA:

O Utilitário de recuperação deverá ser o mesmo ou uma versão mais recente do que a versão do software cliente instalado no computador visado para recuperação.

- 12 Na pasta Utilitários localizada no suporte de instalação da Dell, inicie o Utilitário de recuperação Dell.
É apresentada a caixa de diálogo *Utilitário de recuperação Dell > Selecionar volumes*.
- 13 Selecione o volume do FileVault.
 - Para poder descriptar e montar a unidade, tem de ter uma partição de arranque da versão 10.9.5 ou superior. Caso contrário, só pode obter a chave de recuperação pessoal.
 - Se tem volumes de não arranque encriptados, por norma, terá de recuperar a partição de arranque primeiro.
- 14 Clique em **Continuar**.
É apresentada a caixa de diálogo *Escolher pacote de recuperação*.
- 15 Selecione o pacote recuperação (guardado no passo [passo 9](#)) e clique em **Abrir**.
É apresentada a caixa de diálogo *Selecionar registo de recuperação*.
- 16 Na coluna Data de depósito, selecione a data mais recente para o tipo de chave de recuperação pessoal e clique em **Continuar**.

NOTA:

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

O Resultado da operação de recuperação apresenta a chave.

- Para unidades de arranque, a ferramenta de recuperação oferece uma chave de recuperação pessoal que lhe permite efetuar o arranque através do método normal de recuperação do FileVault da Apple. Pode efetuar o arranque na partição de destino e introduzir a chave de recuperação pessoal para a Autenticação de pré-arranque, que pode variar consoante o SO.
 - Para unidades de não arranque, é apenas apresentada a chave de recuperação pessoal. Para montar um volume de não arranque, introduza a chave de recuperação na caixa de diálogo Palavra-passe do sistema operativo. Se anteriormente ignorou esta caixa de diálogo, pode agora selecionar Desbloquear através do Utilitário do disco para montar a partição encriptada.
- 17 Imprima ou anote a chave.
 - 18 Clique em **Fechar**.
 - 19 Efetue o arranque no volume de arranque externo mantendo premida a tecla **Option** durante o arranque.
 - 20 Se necessário, introduza a palavra-passe do firmware. Selecione o volume de arranque externo.
 - 21 Depois de o sistema reiniciar, clique em **?** no ecrã de início de sessão.
 - 22 Clique na seta apresentada.
 - 23 Escreva a chave de recuperação e prima **Enter**.
 - 24 Na caixa de diálogo, introduza uma nova palavra-passe.



Keychain de recuperação

Tem de executar o Dell Recovery Utility enquanto este é iniciado num volume de recuperação não encriptado. Não execute o Dell Recovery Utility a partir de um volume de arranque externo encriptado.

Pré-requisitos

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

Processo

- 1 Ligue um disco externo ao sistema a recuperar.

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

- 2 Efetue o arranque no volume de arranque externo mantendo premida a tecla **Option** durante o arranque.
- 3 Se necessário, introduza a palavra-passe do firmware. Selecione o volume de arranque externo.
- 4 Monte o ficheiro .dmg.
- 5 Na pasta Utilitários, execute o Utilitário de recuperação Dell.

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

- 6 Selecione o volume FileVault a recuperar e clique em **Continuar**.

É apresentada a caixa de diálogo *Escolher pacote de recuperação*.

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

Se houver mais do que uma chave de recuperação para esse disco, é apresentado o ecrã *Selecionar registo de recuperação*.

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



NOTA:

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

É apresentada a caixa de diálogo *Instruções de recuperação FileVault*.

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

É apresentada a caixa de diálogo *Confirmar operação de recuperação*.

- 10 Destaque o volume FileVault a recuperar e clique em **Continuar**.

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

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

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



NOTA:

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



11 Selecione uma localização e clique em **Guardar**.

É apresentada a caixa de diálogo *Resultado da operação de recuperação*, que indica os ficheiros que foram criados.

12 Clique em **Fechar**.

13 Depois do volume do Recovery HD reiniciar, introduza o nome e o caminho do script.



NOTA:

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

O Resultado da operação de recuperação apresenta a chave.

O utilitário Dell Recovery envia os ficheiros para a localização selecionada e, em seguida, apresenta os comandos exatos que precisará de executar a partir do volume Recovery HD para montar ou descriptar o volume FileVault.

14 Depois destes ficheiros serem gerados, copie as strings de comandos apresentadas na caixa de diálogo *Resultado da operação de recuperação*.

15 Reinicie o disco rígido de recuperação de uma das seguintes formas:

- Prima em simultâneo as teclas **Command** e **R** antes do sinal sonoro de Power-On/Self-Test e durante o arranque do computador.
ou
- Prima a tecla **Option** e utilize o seletor para selecionar o Recovery HD.
É apresentada a caixa de diálogo *Mac OS X Utilities*.

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

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

```
/Volumes/recoveryFOB/fv2mount.sh
```

18 Reinicie o computador.

Suporte multimédia amovível

Formatos suportados

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

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

Ativar o HFS Plus

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

```
<key>EMSHFSPlusOptIn</key>
```

```
<true/>
```

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

O HFS Plus não suporta:

- Versões - Os dados de versões existentes são removidos do disco.



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

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

EMS e atualizações de política

No sistema onde o suporte multimédia foi fornecido (ou recuperado), as políticas são atualizadas para o suporte multimédia no momento da montagem.

Exceções de encriptação

No suporte multimédia externo, os atributos expandidos não são copiados.

Erros no separador Suporte multimédia amovível

- Num computador desprotegido, não substitua um ficheiro encriptado por uma versão desencriptada do ficheiro. Mais tarde, isto poderá impedir a desencriptação. Isto também pode ser apresentado como um erro no separador Suporte multimédia amovível.
- Se um marcador no fim do ficheiro for invalidado, por exemplo, se um ficheiros for substituído por novo conteúdo fora do controlo do EMS e, em seguida, o montar no EMS, é apresentado um erro no fim do ficheiro no separador Suporte multimédia amovível.
- Quando converte ficheiros, o suporte multimédia tem de ter mais espaço livre do que o tamanho do maior ficheiro a converter. Se for apresentado um triângulo de aviso amarelo na área de estado do Suporte multimédia amovível, clique no mesmo. Se uma mensagem indicar *Espaço insuficiente*, faça o seguinte:
 - Tenha em atenção a quantidade de espaço que deve ser libertada no dispositivo. O relatório apresenta uma lista de ficheiros e o tamanho.
 - Esvazie o lixo. À medida que for libertando espaço, o EMS encripta automaticamente ficheiros adicionais.
 - Se eliminar algum ficheiro ou pasta, certifique-se de que esvazia o lixo novamente.

Mensagens de auditoria

As mensagens de auditoria são enviadas para o Dell Server.

Para o Endpoint Security Suite Enterprise for Mac, consulte a Remote Management Console e selecione **Populações > Empresa ou Endpoints**. Em seguida, selecione o separador **Eventos do Advanced Threat**. Para obter mais informações, consulte *AdminHelp*.

Recolher ficheiros de registo para o Endpoint Security Suite Enterprise

Os ficheiros DellLogs.zip contêm os registos da encriptação de cliente e do Advanced Threat Prevention.

Desinstalar o cliente de encriptação para Mac

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

NOTA: Antes de executar a aplicação de desinstalação, o disco tem de estar totalmente descriptado.

- 1 Se o disco estiver encriptado, defina a política **Encriptação de volume Dell** do computador para **Desligado** na Remote Management Console e consolide a política.
É apresentada uma caixa de diálogo que solicita o acesso às Preferências do sistema e o controlo do computador, de forma a que o software cliente possa descriptar o disco.
 - a Clique em **Abrir preferências do sistema**.
Se **Recusar** for selecionado, não é possível prosseguir com a desinstalação e a encriptação.
 - b Introduza a palavra-passe de administrador.
- 2 Depois do disco estar totalmente descriptado, reinicie o computador (quando solicitado).
- 3 Após o reinício do computador, inicie a aplicação **Uninstall Dell Data Protection** (localizada na pasta Utilities, em Dell-Data-Protection-<version>.dmg no suporte de instalação da Dell).
As mensagens apresentam o estado da desinstalação.

O cliente de encriptação para Mac fica assim desinstalado e o computador pode ser utilizado normalmente.

Ativação como administrador

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

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

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

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

Pré-requisitos

- O cliente de encriptação para Mac tem de ser instalado no computador remoto.
- Não efetue a ativação através da interface do utilizador do cliente antes de tentar efetuá-la a partir de uma localização remota.

Ativar

Utilize este comando para ativar o cliente como administrador.

Exemplo:

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



Ativar temporariamente

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

- 1 Abra uma shell ou utilize um script para ativar o software cliente:
client -at *username@domain.com password*
- 2 Utilize o Client Tool para obter informações sobre o software cliente, as suas políticas, o estado do disco, a conta de utilizador e mais. Para obter mais informações sobre o Client Tool, consulte [Client Tool](#).

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

Referência do cliente de encriptação

Acerca da proteção opcional da palavra-passe do firmware

NOTA: Os computadores Mac mais recentes não suportam a proteção da palavra-passe de firmware. A proteção da palavra-passe de firmware é suportada nos seguintes modelos:

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

Por exemplo, o iMac10.1, o iMac11.1 e o iMac11.2 suportam a proteção opcional da palavra-passe do firmware (conforme indicado pelo *), mas o iMac12.1 ou posterior não suportam.

NOTA: Quando a opção de chave `FirmwarePasswordMode` for definida para `Optional` (Opcional), só desativa a obrigatoriedade de proteção da palavra-passe do firmware imposta pelo software cliente. Não elimina qualquer proteção da palavra-passe do firmware. Pode remover qualquer palavra-passe de firmware existente através do Utilitário de palavra-passe de firmware do Mac OS X.

Se pretender utilizar o Boot Camp (consulte [Como ativar Mac OS X Boot Camp](#) para mais instruções) em computadores Mac encriptados, **deve** configurar o cliente para **não** utilizar a proteção da palavra-passe do firmware.

Os computadores Mac utilizam a proteção de palavra-passe de firmware para melhorar a segurança do acesso ao computador. Por predefinição, em computadores Mac, a proteção está definida para `DESLIGADA`. Durante instalação do cliente, quer seja uma nova instalação ou uma atualização de uma versão anterior do cliente, é possível editar o ficheiro `com.dell.ddp.plist` existente a fim de permitir a definição da chave `FirmwarePasswordMode` para `Required` (Obrigatória) ou `Optional` (Opcional). A opção `Required` (Obrigatória) é a predefinição que aplica a proteção da palavra-passe do firmware, enquanto a definição `Optional` (Opcional) faz com que a proteção da palavra-passe do firmware não seja imposta. Após a instalação ou atualização, o cliente avalia o ficheiro instalador modificado `com.dell.ddp.plist` durante o reinício.

NOTA: Para impedir que os utilizadores alterem a postura de segurança do computador, o cliente não aceita as alterações efetuadas à FirmwarePasswordMode após a instalação do software cliente.

Pode alterar o valor desta tecla após a instalação ou atualização ao iniciar um processo de descriptação do disco e, em seguida, voltar a ativar a encriptação.

Se pretender que a proteção da palavra-passe do firmware Mac OS X seja **obrigatória**, siga os procedimentos de instalação/atualização normais do cliente destacados em [Instalar/Atualizar o cliente de encriptação para Mac](#).

Utilizar o Boot Camp

Assistência Mac OS X Boot Camp

NOTA: Ao utilizar o Boot Camp, o sistema operativo Windows não pode ser encriptado.

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

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

NOTA: Windows 7 para o Boot Camp 4 ou 5.1. Windows 8 e posterior apenas para o Boot Camp 5.1.

Para utilizar o Endpoint Security Suite Enterprise for Windows no Boot Camp de um computador com Endpoint Security Suite Enterprise for Mac, o volume do sistema tem de ser encriptado pelo cliente de encriptação para Mac com o Dell Client Encryption ou o FileVault2. Tem de configurar a instalação do cliente para **não** utilizar a proteção da palavra-passe do firmware. Consulte [Instalação/atualização através de linha de comandos](#) para mais instruções.

NOTA:

Se a sua partição Windows é um candidato EMS, certifique-se de que o coloca na lista branca ou este será encriptado. Consulte [Copiar regra de lista branca](#).

NOTA:

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

Recuperação de Endpoint Security Suite Enterprise for Windows no Boot Camp

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

Pré-requisitos

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

Processo

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



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

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

- Unidade USB de arranque
- ou
- Partição FAT no volume Boot Camp externo

3 Desligue o computador com o volume Boot Camp para efetuar a recuperação.

4 Ligue a unidade externa ao computador.

Esta unidade contém o volume Boot Camp criado no [passo 1](#).

5 Para iniciar o computador a partir da unidade Boot Camp externa, prima a tecla **Option** enquanto liga o computador.

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

7 Na unidade USB ou na partição FAT, clique com o botão direito no pacote de recuperação (do [passo 2](#)) e selecione **Executar como administrador**.

8 Clique em **Sim**.

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

- *O meu sistema não arranca...* - Se o utilizador não consegue arrancar o sistema, selecione a primeira opção

ou

- *O meu sistema não permite que aceda a dados encriptados...* - Se o utilizador não conseguir aceder a alguns ficheiros encriptados ao iniciar sessão no sistema, selecione a segunda opção.

10 Clique em **Seguinte**.

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

11 Clique em **Seguinte**.

12 Selecione o volume Boot Camp a recuperar.

 **NOTA: Não é o volume Boot Camp externo.**

13 Clique em **Seguinte**.

14 Introduza a palavra-passe associada a este ficheiro.

15 Clique em **Seguinte**.

16 Clique em **Recuperar**.

17 Clique em **Concluir**.

18 Quando o reinício for solicitado, clique em **Sim**.

19 O sistema reinicia e pode iniciar sessão no Windows.

Como obter uma palavra-passe de firmware

Mesmo que o computador do cliente esteja configurado para a aplicação da palavra-passe de firmware, esta pode não ser necessária para a recuperação. Se o computador a recuperar for de arranque, defina alvo de arranque no painel de preferências do sistema do Disco de arranque.

Caso a palavra-passe de firmware seja necessária para realizar a recuperação (se o computador não for de arranque e a proteção de palavra-passe de firmware estiver aplicada) siga os passos abaixo.

Para obter uma palavra-passe de firmware, primeiro tem de obter o pacote de recuperação que contém as chaves de encriptação do disco.

1 Como Administrador Dell, inicie sessão na Remote Management Console.

- 2 No painel esquerdo, clique em **Populações > Endpoints**
- 3 Procure o dispositivo a recuperar.
- 4 Clique no nome do dispositivo para abrir a página Detalhe do Endpoint.
- 5 Clique no separador **Detalhes e ações**.
- 6 Em Detalhe de proteção, clique na ligação *Chaves de recuperação de dispositivos*.
- 7 Para guardar o pacote de recuperação no volume de recuperação externo ou no computador que executará o utilitário de recuperação para realizar a operação de recuperação, clique em **Transferir** e clique em **Guardar**.
- 8 Abra o pacote de recuperação para obter a palavra-passe de firmware para o computador alvo da recuperação. A palavra-passe de firmware encontra-se localizada nas etiquetas de string depois da chave **FirmwarePassword**.

Por exemplo:

```
<key>FirmwarePassword</key>
```

```
<string>Bo$vun8WDn</string>
```

Client Tool

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

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

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

Exemplo:

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

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

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

Tabela 1. Comandos do Client Tool

Comando	Propósito	Sintaxe	Resultados
Ativar	Ativa um cliente Mac com o Dell Server, mas sem passar pela sua interface de utilizador. Para ativar, é preciso introduzir um domínio, um nome de utilizador e uma palavra-passe válidos.	-a domainAccount domainPassword -a localAccount* domainAccount domainPassword domainAccount é a conta utilizada para ativar através do Client Tool. localAccount é opcional e é o utilizador atual, caso não seja especificado nenhum outro.	0 = Sucesso 2 = Falha na ativação e a razão da falha 6 = Utilizador não encontrado
	Com o Client Tool, pode ativar um utilizador local diferente daquele que iniciou sessão e associar as credenciais de domínio a esse utilizador.	O comando de ativação tem o seguinte formato: client -a <user to activate*> <domainUser> <domainPassword> Se utilizar a política <i>Sem Lista de utilizadores autenticados</i> para criar classes de utilizadores que não sejam ativadas no Dell Server, pode,	



Comando	Propósito	Sintaxe	Resultados
		opcionalmente, utilizar o Client Tool para especificar uma conta local diferente daquela em que iniciou sessão. Consulte a política Sem Lista de utilizadores autenticados no passo 3 .	
Ativar temporariamente	Ativa um cliente Mac sem deixar rastro.	-at domainAccount domainPassword -at localAccount* domainAccount domainPassword	
Disco	Solicita o estado do disco	-d	É apresentado o estado do disco, incluindo o ID do disco, o estado da encriptação e as políticas Se forem apresentadas chavetas vazias, significa que não existem discos encriptados.
Recuperação de alterações do FileVault	Troca chaves de recuperação para volumes FileVault	-fc deviceId recoveryPassphrase -fc deviceId personalRecoveryKey -fc deviceId pathToKeychain keychainPassword -fc deviceId recoveryFile	0 = Sucesso 7= LVUUID não encontrado 10 = Falha nas credenciais 11 = Falha na caução
		NOTA: O ID do dispositivo tem de ser um UUID de volume lógico ou resolvido para exatamente um LVUUID. Muitas vezes, um ponto de montagem ou devnode funcionará.	
Política	Solicita as políticas do cliente Mac	-p	São apresentadas as políticas
Servidor	Consulta o Dell Server para obter políticas atualizadas em nome do cliente Mac	-s	0 = Sucesso Qualquer outro valor indica que o Dell Server ou o software cliente do Mac estava ocupado ou não respondeu.
		NOTA: A consulta pode demorar vários minutos a ser concluída.	
Teste	Testar o estado de ativação do cliente Mac	-t localAccount*	0 (domainAccount) = Sucesso 1 = Desativado 6 = Utilizador não encontrado
Utilizador	Solicita informações sobre o utilizador	-u localAccount*	São apresentadas informações sobre a conta do utilizador: 0 (informações da conta) = Sucesso 6 = Utilizador não encontrado
Versão	Solicita a versão do cliente Mac	-v	É apresentada a versão do cliente Mac: Exemplo: 8.x.x.xxxx



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

A opção Plist

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

Exemplos

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

Para obter as políticas do cliente e imprimi-las.

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

Para ativar o cliente temporariamente e imprimir o resultado.

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

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

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

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

Códigos de retorno globais

Sem erros 0

Erro do parâmetro 4

Comando não reconhecido 5

Socket expirado 8

Erro interno 9



Tarefas de Advanced Threat Prevention

Instalar o Advanced Threat Prevention for Mac

Esta secção vai guiá-lo através da instalação do Advanced Threat Prevention.

Existem dois métodos para instalar o Advanced Threat Prevention.

- [Instalação interativa](#) - Este método de instalação é o mais fácil. No entanto, este método não permite quaisquer personalizações.
- [Instalação através de linha de comandos](#) - Este é um método avançado que só deve ser utilizado por administradores com experiência em sintaxe de linhas de comandos.

Pré-requisitos

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

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

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

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

Guia de migração e instalação do Enterprise Server

Enterprise Server - Guia de instalação e Guia de início rápido do Virtual Edition

- Certifique-se de que tem o nome do servidor anfitrião e a porta. Ambos serão necessários para a instalação do software cliente.
- Certifique-se de que o computador alvo dispõe de ligação de rede ao Dell Server.
- Se um certificado do servidor cliente faltar ou estiver autoatribuído, tem de desativar o certificado SSL fidedigno apenas no lado do cliente.

Instalação interativa do Advanced Threat Prevention

Esta secção vai guiá-lo através do processo de instalação avançada do Advanced Threat Prevention for Mac.

A instalação interativa é o método mais fácil para instalar ou atualizar o pacote de software cliente. No entanto, este método não permite quaisquer personalizações.

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

ⓘ | NOTA: Antes de começar, guarde o trabalho do utilizador e feche as outras aplicações.

- 1 A partir do suporte de instalação da Dell, monte o ficheiro **Endpoint-Security-Suite-Enterprise-<version>.dmg**. O pacote do Endpoint Security Suite Enterprise for Mac abre-se.
- 2 Faça duplo clique no instalador do pacote **Endpoint Security Suite Enterprise**. É apresentada a seguinte mensagem: *Este pacote executará um programa que determinará se o software pode ser instalado.*

- 3 Clique em **Continuar**.
- 4 Leia o texto de Boas-vindas e clique em **Continuar**.
- 5 Leia o acordo da licença, clique em **Continuar** e clique em **Aceito** para aceitar os termos do acordo da licença.
- 6 No campo **Anfitrião do servidor**, introduza o nome de anfitrião totalmente qualificado do Dell Server que irá gerir o utilizador pretendido, por exemplo, server.organization.com.
- 7 No campo **Porta do servidor**, introduza **8888** e clique em **Continuar**.
Assim que a ligação tiver sido estabelecida, o indicador de conectividade muda de vermelho para verde.

NOTA: A porta é a porta de serviço do Core Server, que é configurável. O número de porta predefinido é **8888**.

- 8 No ecrã Instalação, clique em **Instalar**.
- 9 Quando solicitado, introduza as credenciais da conta de administrador (exigidas pela aplicação de instalação para o Mac OS X) e, em seguida, clique em **OK**.
- 10 Quando a instalação estiver concluída, clique em **Fechar**.
O Advanced Threat Prevention client for Mac está instalado.
- 11 Consulte [Verificar a instalação do Advanced Threat Prevention](#).

Se a instalação falhar, determine se tem um certificado válido no seu Dell Server. Consulte [Desativar o certificado fidedigno SSL para o Advanced Threat Prevention](#).

Desinstalação interativa do Advanced Threat Prevention Client

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

- 1 Monte o ficheiro Endpoint-Security-Suite-Enterprise-<version>.dmg.
- 2 Na pasta Utilitários, execute a aplicação **Uninstall Endpoint Security Suite Enterprise**.
- 3 Clique em **Desinstalar**.
- 4 Quando solicitado, introduza as credenciais da conta de administrador (exigidas pela aplicação de instalação para o Mac OS X) e, em seguida, clique em **OK**.
As mensagens apresentam o estado da desinstalação.
- 5 Quando a desinstalação for confirmada, clique em **OK**.
O Advanced Threat Prevention for Mac fica assim desinstalado e o computador pode ser utilizado normalmente.

Instalação do Advanced Threat Prevention através da linha de comandos

Para instalar o Advanced Threat Prevention cliente através da linha de comandos, siga os passos abaixo.

- 1 A partir do suporte de instalação da Dell, instale o ficheiro Endpoint-Security-Suite-Enterprise-<version>.dmg. O pacote do Endpoint Security Suite Enterprise for Mac abre-se.
- 2 Na pasta Utilitários, copie o ficheiro **com.dell.esse.plist** para a unidade de disco local.
- 3 Abra o ficheiro .plist.
- 4 Edite os valores de variáveis com o nome de anfitrião totalmente qualificado do Dell Server que irá gerir o utilizador pretendido, por exemplo 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 do Core Server, que é configurável. O número de porta predefinido é **8888**.

- 5 Guarde e feche o ficheiro.
- 6 Para cada computador de destino, copie o instalador do pacote **Endpoint Security Suite Enterprise for Mac** para uma pasta temporária e o ficheiro **com.dell.esse.plist** modificado para **/Library/Preferences**.
- 7 Se solicitado, introduza as suas credenciais.
- 8 Inicie uma janela Terminal.
- 9 Execute a instalação do pacote a partir da linha de comandos através do comando **installer**:

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

NOTA: O caminho **-pkg** é o caminho para o instalador **.pkg** encontrado no ficheiro **.dmg**.

- 10 Prima **Enter**.
- 11 Consulte [Verificar a instalação do ESSE Advanced Threat Prevention](#).

Desinstalação através da linha de comandos do Advanced Threat Prevention

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

- 1 Inicie uma janela Terminal.
- 2 Execute a desinstalação do pacote a partir da linha de comandos através do comando **uninstaller**:

```
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 **--noui** é incluído no final do comando.

- 3 Prima **Enter**.
O Advanced Threat Prevention for Mac fica assim desinstalado e o computador pode ser utilizado normalmente.

Resolução de problemas do Advanced Threat Prevention for Mac

Desativar o certificado fidedigno SSL para o Advanced Threat Prevention

Se um certificado do servidor cliente faltar ou estiver autoatribuído, tem de desativar o certificado SSL fidedigno apenas no lado do cliente.

- 1 No cliente, abra uma janela Terminal.
- 2 Introduza o caminho para a **DellCSFConfig.app**:

```
cd /Volumes/Endpoint\ Security\ Suite\ Enterprise\ for\ Mac/Utilities/DellCSFConfig.app/Contents/MacOS/
```
- 3 Execute a **DellCSFConfig.app**:

```
sudo ./DellCSFConfig
```



São apresentadas as seguintes predefinições:

Current Settings:

```
ServerHost = deviceserver.company.com
```

```
ServerPort = 8888
```

```
DisableSSLCertTrust = False
```

```
DumpXmlInventory = False
```

```
DumpPolicies = False
```

- 4 Digite **-help** para ver a lista das opções.
- 5 Para desativar o certificado fidedigno SSL no cliente, altere `DisableSSLCertTrust` para **True** (Verdadeiro).


Adicionar inventário XML e alterações de políticas à pasta de registos

Para adicionar os ficheiros `inventory.xml` ou `policies.xml` à pasta Registos:

- 1 Execute a `DellCSFConfig.app` conforme descrito acima.
- 2 Altere `DumpXmlInventory` para **True** (Verdadeiro).
- 3 Altere `DumpPolicies` para **True** (Verdadeiro).
Os ficheiros de políticas só são descartados se tiver ocorrido uma alteração à política.
- 4 Para ver os ficheiros de registos `inventory.xml` e `policies.xml`, vá a `/Library/Application Support/Dell/Dell Data/Protection/`.

Verificar a instalação do Advanced Threat Prevention

Opcionalmente, pode verificar a instalação.

- 1 Confirme se o ícone Dell Advanced Threat Prevention tem um distintivo verde  na barra de comandos.
- 2 Se aparecer um ponto de exclamação no ícone, clique com o botão direito e seleccione **Mostrar detalhes**. Isso pode indicar que o utilizador não está registado.

Verificar a existência de atualizações - Verifica a existência de atualizações do motor Advanced Threat Prevention, não de atualizações de políticas do Dell Server.

Acerca de - Inclui o seguinte:

- Versão
 - Política - [online] indica uma política baseada em servidor e [offline] indica uma política baseada offline ou em Airgap
 - N.º de série - Utiliza esta função quando contactar a assistência técnica. Este é o identificador único da instalação.
- 3 Em `/Applications`, é criada a pasta Dell Advanced Threat Prevention.

Recolher ficheiros de registo para o Endpoint Security Suite Enterprise

Os ficheiros `DellLogs.zip` contêm os registos da encriptação de cliente e do Advanced Threat Prevention.

Para mais informações sobre como recolher os registos, consulte <http://www.dell.com/support/article/us/en/19/SLN303924>.

Ver detalhes do Advanced Threat Prevention

Após a instalação de um cliente Advanced Threat Prevention num computador endpoint, este é reconhecido pelo Dell Server como agente.



Clique com o botão direito no ícone Advanced Threat Prevention  na barra de comandos e selecione **Mostrar detalhes**. O ecrã Detalhes de Advanced Threat Prevention inclui os seguintes separadores.

Separador Ameaças

O separador Ameaças apresenta todas as ameaças detetadas no dispositivo e a ação adotada. As ameaças são uma categoria de eventos que são recém-detetados como ficheiros ou programas potencialmente inseguros e requerem uma correção orientada.

A coluna Categorias pode incluir as seguintes.

- **Não seguro** - Um ficheiro suspeito com probabilidade de ser malware
- **Anormal** - Um ficheiro suspeito que pode ser malware
- **Em quarentena** - Um ficheiro que foi movido da sua localização original, armazenado na pasta Quarentena e impedido de ser executado no dispositivo.
- **Dispensado** - Um ficheiro que pode ser executado no dispositivo.
- **Autorizado** - Um ficheiro que foi autorizado dentro da organização. Os ficheiros autorizados incluem ficheiros Dispensados, adicionados à lista Segura e eliminados da pasta Quarentena num dispositivo.

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

Separador Exploits

O separador Exploits lista exploits, que são considerados ameaças.

As políticas do Dell Server determinam a ação tomada quando é detetado um exploit:

- **Ignorar** - Não é realizada nenhuma ação relativamente às violações de memória identificadas.
- **Alerta** - A violação de memória é registada e comunicada ao Dell Server.
- **Bloquear** - A invocação do processo é bloqueada se uma aplicação tentar invocar um processo de violação de memória. A aplicação que efetuou a solicitação pode continuar a ser executada.
- **Terminar** - A invocação do processo é bloqueada se uma aplicação tentar invocar um processo de violação de memória. A aplicação que fez a invocação é terminada.

São detetados os seguintes tipos de exploits:

- Stack Pivot
- Proteção de pilha
- Pesquisa de memória do detetor de vírus
- Carga maliciosa

Para mais informações sobre as políticas de Exploits, consulte *AdminHelp*, disponível na Remote Management Console do Dell Server.

Separador Eventos

NOTA: Um evento não é necessariamente uma ameaça. Um evento é gerado quando um programa ou ficheiro reconhecido está em quarentena, na lista de ficheiros seguros ou dispensado.

O separador Eventos apresenta quaisquer ameaças que ocorram no dispositivo por tipo de evento conforme atribuído pelo Advanced Threat Prevention. Os dados são removidos quando o sistema for reiniciado.

Exemplos de tipos de evento:

Ameaça Encontrada

Ameaça Removida

Ameaças colocadas em quarentena

Ameaça dispensadas

Ameaça alteradas

Configurar um inquilino para o Advanced Threat Prevention

Se a sua organização utilizar o Advanced Threat Prevention, deve ser configurado um inquilino no Dell Server antes da ativação da aplicação de políticas do Advanced Threat Prevention.

Pré-requisitos

- Deve ser efetuado por um administrador com função de Administrador do sistema.
- Deve ter ligação à Internet para configuração no Dell Server.
- Deve ter ligação à Internet no cliente para visualizar a integração do serviço online do Advanced Threat Prevention na Remote Management Console.
- A configuração tem como base um token que é gerado a partir de um certificado durante a configuração.
- As licenças do Advanced Threat Prevention devem estar presentes no Dell Server.

Configurar um inquilino

- 1 Inicie sessão na Remote Management Console e navegue até **Gestão de serviços**.
- 2 Clique em **Configurar serviço Advanced Threat Protection**. Se ocorrer qualquer falha neste momento, importe as suas licenças ATP.
- 3 A configuração com assistente é iniciada imediatamente após as licenças serem importadas. Clique em **Seguinte** para começar.
- 4 Leia e aceite o EULA (a caixa de verificação está **desativada** por predefinição) e clique em **Seguinte**.
- 5 Disponibilize credenciais de identificação no Servidor DDP para configuração do Inquilino. Clique em **Seguinte**. *A configuração de um Inquilino existente da marca Cylance não é suportada.*
- 6 Transfira o Certificado. Este é necessário para recuperação em caso de desastres no Servidor DDP. Não são automaticamente efetuadas cópias de segurança deste Certificado através do "upgrader" v9.2. Efetue uma cópia de segurança do Certificado numa localização segura num computador diferente. Assinale a caixa de verificação para confirmar que efetuou uma cópia de segurança do Certificado e clique em **Seguinte**.
- 7 A configuração está concluída. Clique em **OK**.

Configurar a atualização automática do Advanced Threat Prevention Agent

Na Remote Management Console do Dell Server, pode subscrever a receção de autoatualizações do Advanced Threat Prevention Agent. A subscrição da receção de atualizações automáticas do agente permite aos clientes transferir e aplicar autoatualizações a partir do servidor de Advanced Threat Prevention. As atualizações são mensais.

ⓘ | NOTA: As autoatualizações do agente são suportadas com o Dell Server v9.4.1 ou posterior.

Receber autoatualizações do agente

Para se inscrever e receber autoatualizações do agente:

- 1 No painel esquerdo da Remote Management Console, clique em **Gestão > Gestão de serviços**.



- No separador **Ameaças avançadas**, sob Autoatualização do Agente, clique no botão **Ligar** e, em seguida, clique no botão **Guardar preferências**
Poderá demorar alguns momentos até as informações serem propagadas e as autoatualizações serem apresentadas.

Deixar de receber autoatualizações do agente

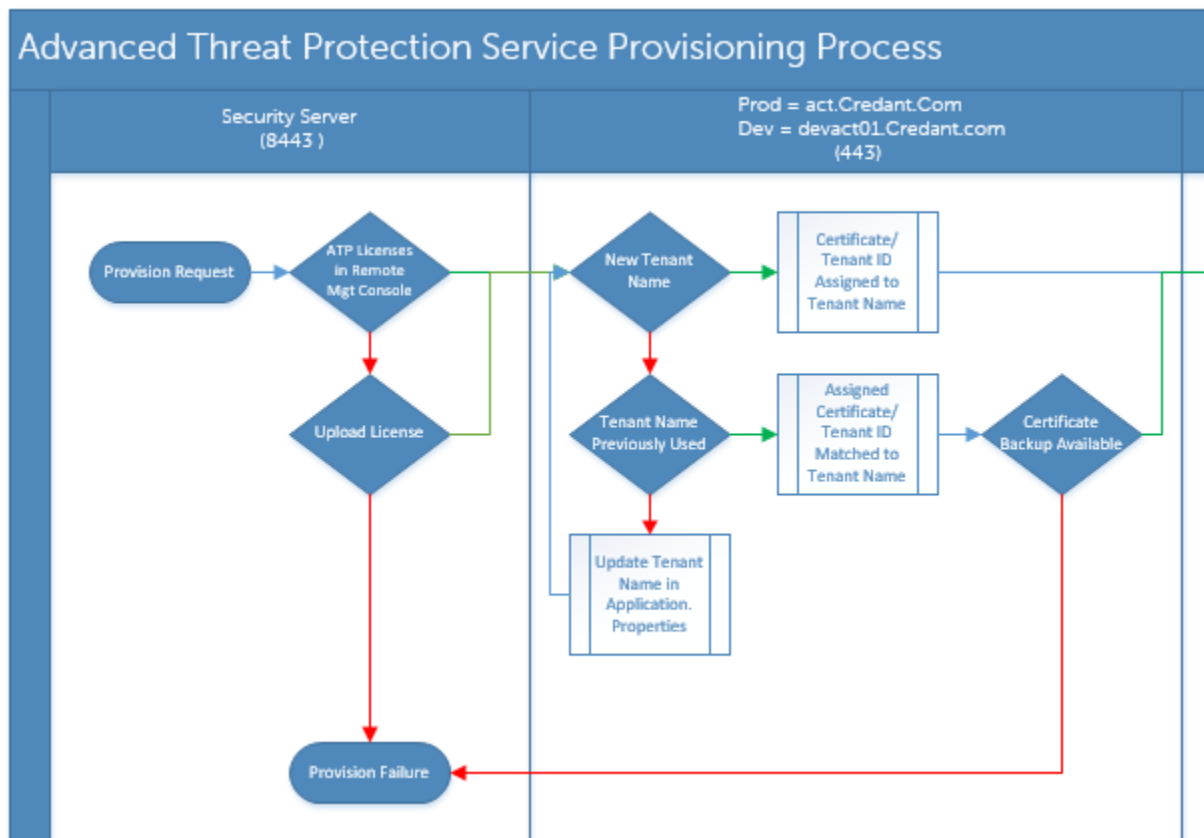
Para deixar de receber autoatualizações do agente:

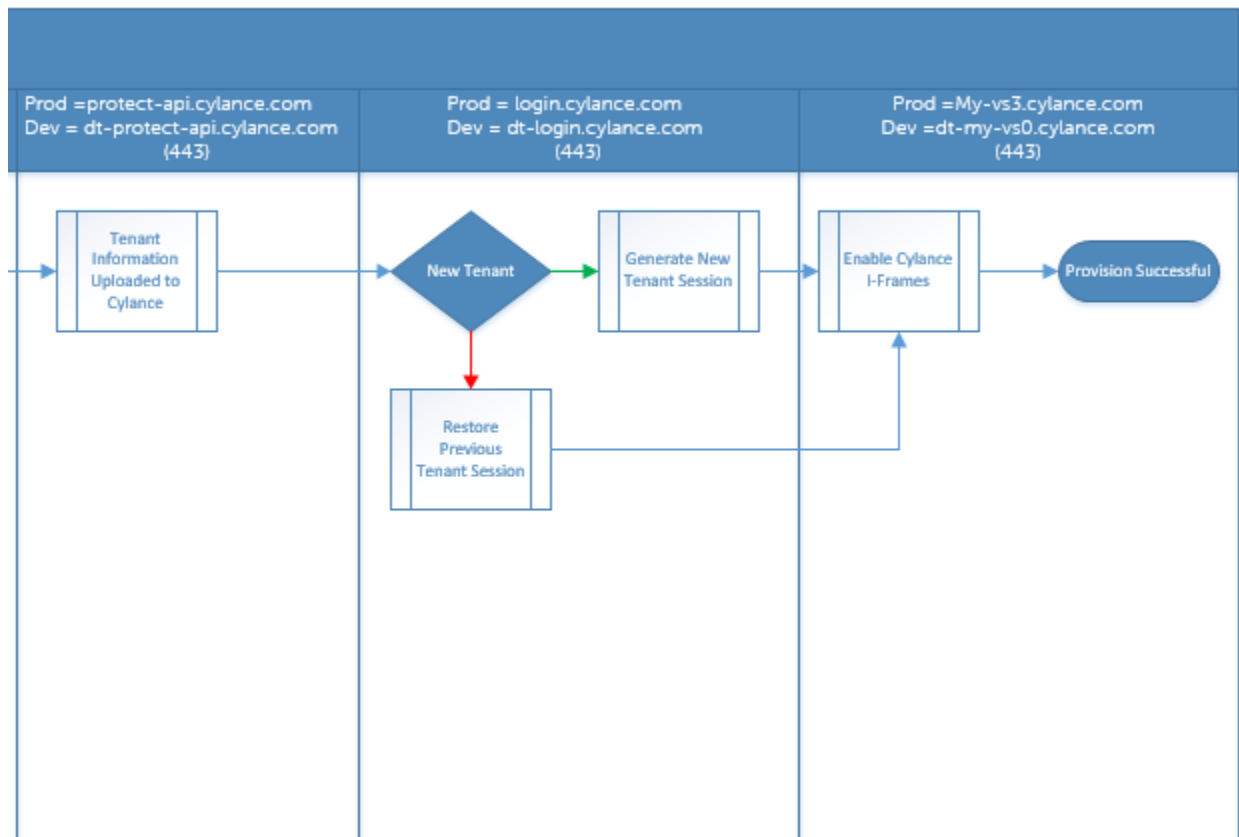
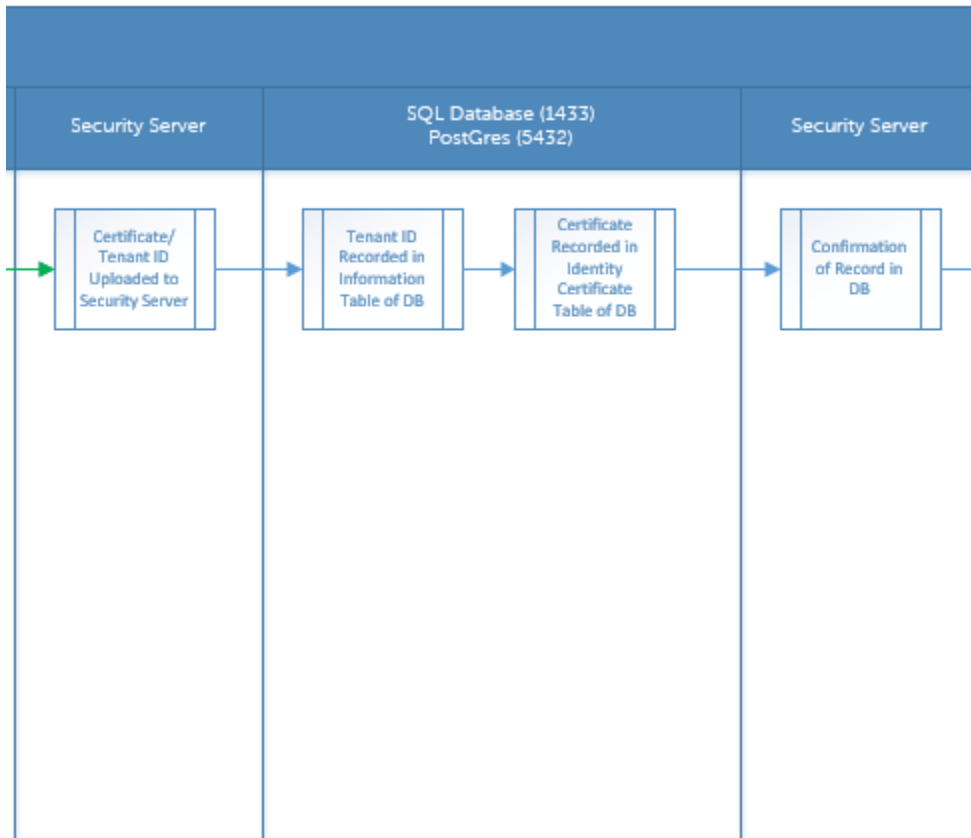
- No painel esquerdo da Remote Management Console, clique em **Gestão > Gestão de serviços**.
- No separador **Ameaças avançadas**, sob Autoatualização do Agente, clique no botão **Ligar** e, em seguida, clique no botão **Guardar preferências**

Resolução de problemas do cliente Advanced Threat Prevention

Aprovisionamento e comunicação do agente do Advanced Threat Prevention

Os diagramas seguintes ilustram o processo de aprovisionamento do serviço do Advanced Threat Prevention.

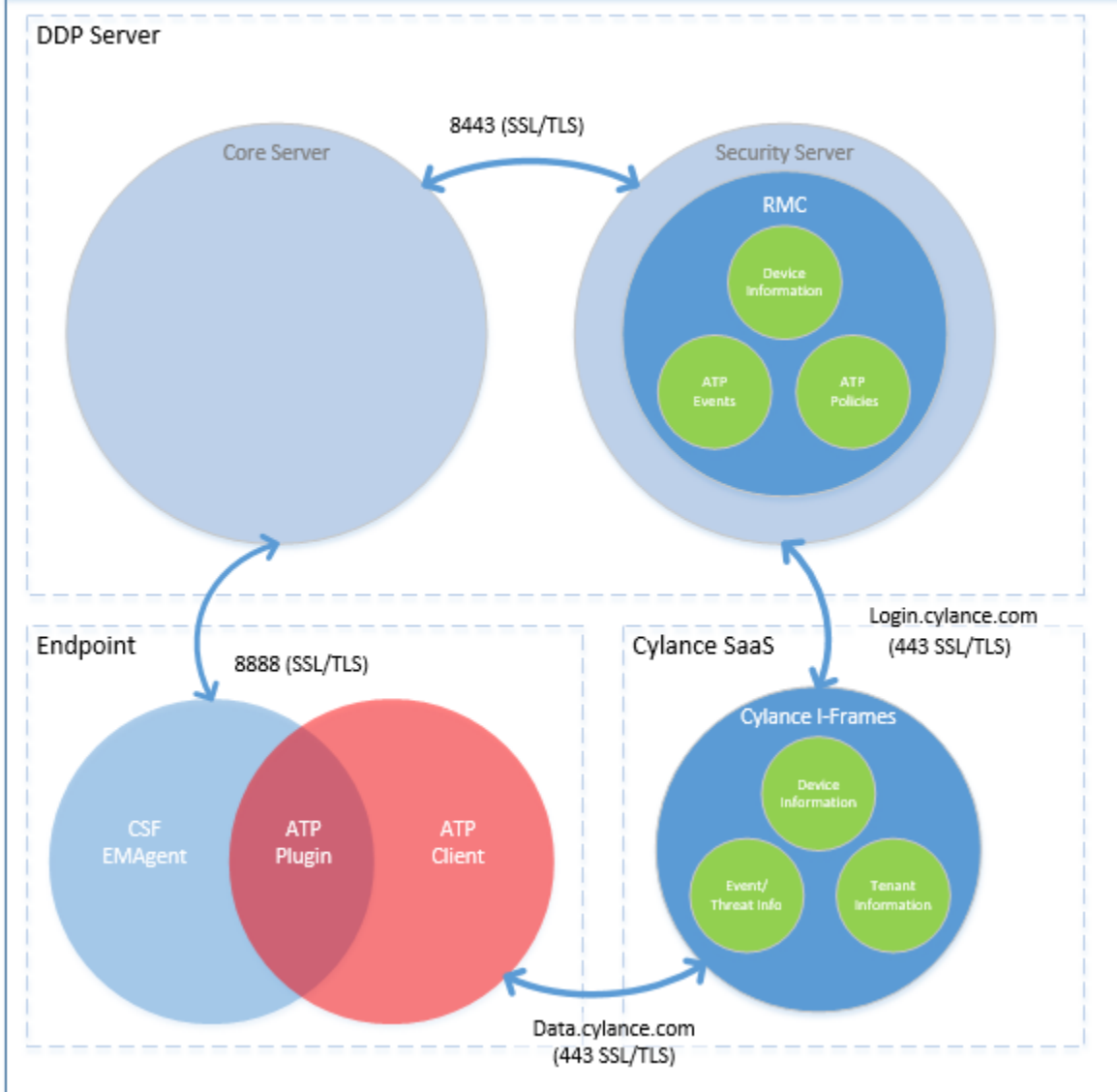




O diagrama seguinte ilustra o processo de comunicação do agente do Advanced Threat Prevention.



Endpoint Security Suite Enterprise Agent Communication



Glossário

Security Server - utilizado para as ativações de encriptação de cliente.

Proxy de políticas - Utilizado para distribuir políticas para o software cliente Endpoint Security Suite Enterprise for Mac.

Remote Management Console - A consola do administrador para implementação em toda a empresa.

Shield - Ocasionalmente, pode ver este termo na documentação e na interface do utilizador do cliente. O "Shield" é um termo utilizado para representar o software cliente.

