Dell Data Protection | Encryption

Guia de instalação básica do Enterprise Edition v8.13

Notas, avisos e advertências

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.

Enterprise Edition Basic Installation Guide

2017 - 04

Rev. A01

Índice

Introdução

Este guia explica como instalar e configurar a aplicação utilizando o instalador principal do . Este guia proporciona assistência de instalação básica. Consulte o *Guia de instalação avançada* caso necessite de informações sobre a instalação dos instaladores subordinados, a configuração do EE Server/VE Server ou informações além da assistência básica com o programa de instalação principal do .

Todas as informações sobre políticas e as respetivas descrições podem ser encontradas em AdminHelp.

Antes de começar

1 Instale o EE Server/VE Server antes de implementar os clientes. Localize o guia correto como mostrado abaixo, siga as instruções e, em seguida, volte a este guia.

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

Certifique-se de que as políticas foram definidas da forma pretendida. Navegue no AdminHelp, disponível através de **?** no lado direito do ecrã. O AdminHelp é uma ajuda ao nível da página concebida para o ajudar a definir e modificar a política e a compreender as suas opções relativamente ao seu EE Server/VE Server.

2 Leia atentamente o capítulo Requisitos deste documento.

3 Implemente os clientes para utilizadores finais.

Utilizar este guia

Utilize este guia pela seguinte ordem.

- Consulte Requisitos para obter informações sobre os pré-requisitos do cliente.
- Selecione uma das seguintes ações:
  - Instalar interativamente utilizando o instalador principal do

    ou
  - Instalar por linha de comandos utilizando o instalador principal do

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.

Ajude-nos a garantir que o direcionamos rapidamente para o especialista técnico mais indicado para si tendo o seu Código de serviço disponível quando nos contactar.

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

Requisitos

Todos os clientes

- Durante a implementação, devem ser seguidas as melhores práticas de TI. Estas incluem, entre outras, ambientes de teste controlados para os testes iniciais e a implementação progressiva para os utilizadores.
- A conta de utilizador que realiza a instalação/atualização/desinstalação deve ser um utilizador administrador local ou de domínio, que poderá ser atribuído temporariamente por uma ferramenta de implementação, como o Microsoft SMS ou Dell KACE. Não são suportados utilizadores não administradores com privilégios elevados.
- Realize uma cópia de segurança de todos os dados importantes antes de iniciar a instalação/desinstalação.
- Não realize alterações no computador, incluindo inserir ou remover unidades externas (USB) durante a instalação.
- Se os clientes do instalador principal do estiverem autorizados a utilizar o Dell Digital Delivery (DDD), certifique-se de que a porta de saída 443 está disponível para comunicar com o EE Server/VE Server. A funcionalidade de elegibilidade não funcionará se a porta 443 estiver bloqueada (por qualquer motivo). O DDD não é utilizado se a instalação for efetuada utilizando os instaladores subordinados.
- Assegure-se de verificar periodicamente a página www.dell.com/support para procurar a documentação mais atual e Conselhos técnicos.

Todos os clientes - Pré-requisitos

- É necessário o Microsoft .Net Framework 4.5.2 (ou posterior) para os clientes de instalador principal e de instalador subordinado do . O instalador *não* instala o componente Microsoft .Net Framework.

  Todos os computadores enviados da fábrica da Dell são previamente equipados com a versão completa do Microsoft .Net Framework 4.5.2 (ou posterior). No entanto, se não instalar em hardware Dell ou se atualizar o cliente num hardware Dell mais antigo, deve verificar qual a versão do Microsoft .Net instalada e atualizar a versão, **antes de instalar o cliente** para impedir falhas na instalação/atualização. Para verificar a versão instalada do Microsoft .Net, siga estas instruções no computador onde pretende efetuar a instalação: http://msdn.microsoft.com/en-us/library/hh925568(v=vs.110).aspx. Para instalar o Microsoft .Net Framework 4.5.2, aceda a https://www.microsoft.com/en-us/download/details.aspx?id=42643.
- Os controladores e firmware do ControlVault, leitores de impressão digital e de smart cards (conforme abaixo ilustrado) não estão incluídos nos ficheiros executáveis do instalador principal ou do instalador subordinado do . Os controladores e firmware têm de ser mantidos atualizados e podem ser transferidos a partir de http://www.dell.com/support e selecionando o seu modelo de computador. Transfira os controladores e firmware adequados com base no seu hardware de autenticação.

  - ControlVault
  - NEXT Biometrics Fingerprint Driver
  - Validity FingerPrint Reader 495 Driver
  - O2Micro Smart Card Driver

  Se estiver a realizar a instalação em hardware não Dell, transfira os controladores e firmware atualizados a partir do Web site do fornecedor correspondente. As instruções de instalação dos controladores do ControlVault estão disponíveis em Atualizar firmware e controladores do Dell ControlVault.

Todos os clientes - Hardware

- A tabela seguinte apresenta o hardware de computador suportado.

Hardware

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

Todos os clientes - Suporte de idiomas

- Os clientes Encryption, e BitLocker Manager estão em conformidade com a norma Interface de Utilizador Multilingue (MUI) e suportam os seguintes idiomas.

Suporte de idiomas

- EN - Inglês
- ES - Espanhol
- FR - Francês
- IT - Italiano
- DE - Alemão
- JA - Japonês
- KO - Coreano
- PT-BR - Português, Brasil
- PT-PT - Português, Portugal (Ibérico)

- Os clientes SED e Advanced Authentication são uma Interface de Utilizador Multilingue (MUI) compatível e suportam os seguintes idiomas. O modo UEFI e a Autenticação de pré-arranque não são suportados em russo, chinês tradicional ou chinês simplificado.

Suporte de idiomas

- EN - Inglês
- FR - Francês
- IT - Italiano
- DE - Alemão
- ES - Espanhol
- JA - Japonês
- KO - Coreano
- ZH-CN - Chinês simplificado
- ZH-TW - Chinês tradicional/Taiwan
- PT-BR - Português, Brasil
- PT-PT - Português, Portugal (Ibérico)
- RU - Russo

Cliente Encryption

- O computador cliente deve ter conectividade de rede para ativar.
- Desative o modo de suspensão durante o varrimento de encriptação inicial para impedir a suspensão do computador caso este se encontre sem supervisão. A encriptação não é possível num computador em suspensão (tal como não é possível a desencriptação).
- O cliente Encryption não suporta configurações de duplo arranque, uma vez que é possível encriptar ficheiros de sistema do outro sistema operativo, o que poderia interferir com o respetivo funcionamento.
- O cliente Encryption foi sujeito a testes e é compatível com McAfee, com o cliente Symantec, Kaspersky e MalwareBytes. Existem exclusões implementadas para estes fornecedores de produtos anti-vírus, para evitar incompatibilidades entre a monitorização anti-vírus e a encriptação. O cliente Encryption foi também testado com o Microsoft Enhanced Mitigation Experience Toolkit.

  Se a sua organização utilizar um antivírus de um fornecedor não indicado na lista, consulte http://www.dell.com/support/Article/us/en/19/SLN298707 ou contacte o Dell ProSupport para obter assistência.
- Não é suportada a atualização de versão do sistema operativo com o cliente Encryption instalado. Desinstale e desencripte o cliente Encryption, atualize para o novo sistema operativo e, em seguida, reinstale o cliente Encryption.

Para além disso, não são suportadas reinstalações de sistema operativo. Para realizar a reinstalação do sistema operativo, faça uma cópia de segurança do computador em questão, realize a limpeza do computador, instale o sistema operativo e, em seguida, realize a recuperação dos dados encriptados seguindo os procedimentos de recuperação estabelecidos.

Pré-requisitos do Encryption Client

- O instalador principal do instala o Microsoft Visual C++ 2012 Update 4, se este ainda não estiver instalado no computador.

Pré-requisito

- Visual C++ 2012 Update 4 ou Redistributable Package posterior (x86 e x64)

Sistemas operativos do Encryption Client

- A tabela seguinte apresenta os sistemas operativos suportados.

Sistemas operativos Windows (32 e 64 bits)

- Windows 7 SP0-SP1: Enterprise, Professional, Ultimate
- Windows Embedded Standard 7 com modelo de Compatibilidade entre Aplicações (a encriptação do hardware não é suportada)
- Windows 8: Enterprise, Pro
- Windows 8.1 Atualização 0-1: Enterprise Edition, Pro Edition
- Windows Embedded 8.1 Industry Enterprise (a encriptação do hardware não é suportada)
- Windows 10: Education, Enterprise, Pro
- VMware Workstation 5.5 e posterior

> **NOTA:**
> O modo UEFI não é suportado no Windows 7, Windows Embedded Standard 7 ou Windows Embedded 8.1 Industry Enterprise.

Sistemas operativos do External Media Shield (EMS)

- A tabela seguinte apresenta os sistemas operativos suportados ao aceder a suportes com proteção EMS.

> **NOTA:**
> O External Media deve ter, aproximadamente, 55 MB disponíveis, bem como espaço livre no suporte multimédia igual ao maior ficheiro a encriptar para alojar o EMS.

> **NOTA:**
> O Windows XP é suportado apenas quando se utiliza o EMS Explorer.

Sistemas operativos Windows compatíveis para aceder a suportes multimédia protegidos pelo EMS (32 e 64 bits)

- Windows 7 SP0-SP1: Enterprise, Professional, Ultimate, Home Premium
- Windows 8: Enterprise, Pro, Consumer
- Windows 8.1 Atualização 0-1: Enterprise Edition, Pro Edition
- Windows 10: Education, Enterprise, Pro

Sistemas operativos Mac compatíveis para aceder a suportes multimédia protegidos pelo EMS (kernels de 64 bits)

- Mac OS X Yosemite 10.10.5
- Mac OS X El Capitan 10.11.6
- macOS Sierra 10.12.0

Cliente SED

- Para instalar a gestão SED com êxito, o computador deve possuir uma ligação à rede com fios.
- O IPv6 não é suportado.
- Prepare-se para encerrar e reiniciar o computador após aplicar as políticas e quando estiver pronto para começar a implementá-las.
- Os computadores equipados com unidades de encriptação automática não podem ser utilizados com placas HCA. Existem incompatibilidades que impedem o aprovisionamento do HCA. A Dell não vende computadores com unidades de encriptação automática compatíveis com o módulo HCA. Esta configuração não suportada seria uma configuração pós-venda.
- Se o computador destinado à encriptação estiver equipado com uma unidade de encriptação automática, certifique-se de que a opção do Active Directory, *O utilizador deve alterar a palavra-passe no próximo início de sessão*, está desativada. A Autenticação de pré-arranque não suporta esta opção do Active Directory.
- A Dell recomenda que não mude o método de autenticação depois de a PBA ter sido ativada. Se for necessário mudar para um método de autenticação diferente, deve:

  - Elimine todos os utilizadores da PBA.

  ou

  - Desative a PBA, altere o método de autenticação e, em seguida, volte a ativar a PBA.

  IMPORTANTE:
  Devido à natureza do RAID e SED, a gestão de SED não suporta RAID. O problema de *RAID=On* nas SED é que o RAID necessita de acesso ao disco para ler e gravar dados relacionados com o RAID num setor elevado não disponível numa SED bloqueada desde o arranque, e não pode esperar até o utilizador iniciar sessão para ler estes dados. Para solucionar este problema, altere a operação SATA no BIOS de *RAID=On* para *AHCI*. Se o sistema operativo não incluir controladores AHCI pré-instalados, o sistema operativo irá apresentar um ecrã azul quando alterar de *RAID=On* to *AHCI*.
- A Gestão SED não é suportada com o Server Encryption .

Pré-requisitos do cliente SED

- O instalador principal do instala o Microsoft Visual C++2010 SP1 **e** o Microsoft Visual C++ 2012 Update 4, se estes ainda não estiverem instalados no computador.

Pré-requisitos

- Visual C++ 2010 SP1 ou Redistributable Package posterior (x86 e x64)
- Visual C++ 2012 Update 4 ou Redistributable Package posterior (x86 e x64)

Hardware do cliente SED

Teclados internacionais

- A tabela que se segue indica teclados internacionais suportados com Autenticação de pré-arranque em computadores UEFI e não-UEFI.

Suporte de teclado internacional - UEFI

- DE-CH - Alemão (Suíça)
- DE-FR - Francês (Suíça)

Suporte de teclado internacional - Non-UEFI

- AR - Árabe (utilizando letras latinas)
- DE-CH - Alemão (Suíça)
- DE-FR - Francês (Suíça)

Sistemas operativos do cliente SED

- A tabela seguinte apresenta os sistemas operativos compatíveis.

Sistemas operativos Windows (32 e 64 bits)

- Windows 7 SP0-SP1: Enterprise, Professional (suportado com o modo de Arranque Legacy, mas não UEFI)

  NOTA:
  O modo de Arranque Legacy é suportado pelo Windows 7. A UEFI não é suportada pelo Windows 7.

- Windows 8: Enterprise, Pro,
- Windows 8.1: Enterprise Edition, Pro Edition
- Windows 10: Education, Enterprise, Pro

Cliente Advanced Authentication

- Ao utilizar Advanced Authentication, os utilizadores terão acesso seguro ao computador através de credenciais da autenticação avançada geridas e registadas utilizando o Security Tools. O Security Tools será o gestor principal das credenciais de autenticação para o Início de sessão do Windows, incluindo a palavra-passe do Windows, impressões digitais e smart cards. As credenciais de palavra-passe por imagem, PIN e impressão digital registadas através do sistema operativo da Microsoft não serão reconhecidas pelo Início de sessão do Windows.

  Para continuar a utilizar o sistema operativo da Microsoft para gerir as credenciais de utilizador, não instale ou desinstale o Security Tools.

- A funcionalidade Palavra-passe monouso (OTP) do Security Tools requer que um TPM esteja presente, ativado e que tenha proprietário. O OTP não é suportado com o TPM 2.0. Para eliminar e definir a propriedade do TPM, consulte https://technet.microsoft.com.

Hardware do Cliente Advanced Authentication

- A tabela seguinte lista a autenticação de hardware suportada.

Leitores de impressão digital e de smart cards

- Validity VFS495 em Modo seguro
- ControlVault Swipe Reader
- UPEK TCS1 FIPS 201 Secure Reader 1.6.3.379
- Leitores USB Authentec Eikon e Eikon To Go

Cartões sem contacto

- Cartões sem contacto com leitores de cartões sem contacto incorporados nos portáteis Dell especificados

Smart Cards

- Smart Cards PKCS #11 que utilizam o cliente ActivIdentity

  NOTA:
  O cliente ActivIdentity não se encontra pré-carregado e tem de ser instalado separadamente.

- Cartões CSP
- Cartão de acesso comum (CAC)
- Cartões SIPRNet/Classe B

Sistemas operativos do Cliente Advanced Authentication

Sistemas operativos Windows

- A tabela seguinte apresenta os sistemas operativos suportados.

Sistemas operativos Windows (32 e 64 bits)

- Windows 7 SP0-SP1: Enterprise, Professional, Ultimate
- Windows 8: Enterprise, Pro
- Windows 8.1 Atualização 0-1: Enterprise Edition, Pro Edition
- Windows 10: Education, Enterprise, Pro

  NOTA: O modo UEFI não é suportado pelo Windows 7.

Sistemas operativos de dispositivos móveis

- Os sistemas operativos móveis seguintes são suportados com a funcionalidade Palavra-passe monouso do Security Tools.

Sistemas operativos para Android

- 4.0 - 4.0.4 Ice Cream Sandwich
- 4.1 - 4.3.1 Jelly Bean
- 4.4 - 4.4.4 KitKat
- 5.0 - 5.1.1 Lollipop

Sistemas operativos iOS

- iOS 7.x
- iOS 8.x

Sistemas operativos Windows Phone

- Windows Phone 8.1
- Windows 10 Mobile

Cliente BitLocker Manager

- Se o BitLocker ainda não tiver sido implementado no seu ambiente, pondere a revisão dos requisitos do Microsoft BitLocker,
- Certifique-se de que a partição de PBA já está configurada. Se o BitLocker Manager for instalado antes da configuração da partição de PBA, não é possível ativar o BitLocker e o BitLocker Manager não irá funcionar.

- O teclado, o rato e os componentes de vídeo devem estar ligados diretamente ao computador. Não utilize um comutador KVM para gerir periféricos, uma vez que o comutador KVM pode interferir com a capacidade do computador para identificar corretamente o hardware.
- Ligue e ative o TPM. O BitLocker Manager assume a propriedade do TPM e não necessita de reinício. No entanto, se um TPM já tiver um proprietário, o BitLocker Manager inicia o processo de configuração da encriptação (não é necessário o reinício). O importante é que o TPM tenha um "proprietário" e esteja ativo.
- O BitLocker Manager não é suportado com o Server Encryption .

Pré-requisitos do cliente BitLocker Manager

- O instalador principal do instala o Microsoft Visual C++2010 SP1 **e** o Microsoft Visual C++ 2012 Update 4, se estes ainda não estiverem instalados no computador.

Pré-requisitos

- Visual C++ 2010 SP1 ou Redistributable Package posterior (x86 e x64)
- Visual C++ 2012 Update 4 ou Redistributable Package posterior (x86 e x64)

Sistemas operativos do cliente BitLocker Manager

- A tabela seguinte apresenta os sistemas operativos suportados.

Sistemas operativos Windows

- Windows 7 SP0-SP1: Enterprise, Ultimate (32 e 64 bits)
- Windows 8: Enterprise (64 bits)
- Windows 8.1: Enterprise Edition, Pro Edition (64 bits)
- Windows 10: Education, Enterprise, Pro
- Windows Server 2008 R2: Standard Edition, Enterprise Edition (64 bits)
- Windows Server 2012
- Windows Server 2012 R2: Standard Edition, Enterprise Edition (64 bits)
- Windows Server 2016

Instalar utilizando o instalador principal do

- As opções e parâmetros da linha de comandos são sensíveis a maiúsculas e minúsculas.
- Para instalar utilizando portas não predefinidas, utilize os instaladores subordinados em vez do instalador principal do .
- Os ficheiros de registo do instalador principal do estão localizados em **C:\ProgramData\Dell\Dell Data Protection\Installer.**
- Dê a instrução aos utilizadores para consultar o seguinte documento e ficheiros de ajuda para assistência de aplicação:
  - Consulte a *Ajuda do Dell Encrypt* para saber como utilizar a funcionalidade do Encryption Client. Aceda à ajuda a partir de **<Install dir>:\Program Files\Dell\Dell Data Protection\Encryption\Help**.
  - Consulte a *Ajuda do EMS* para saber como utilizar as funcionalidades do External Media Shield. Aceda à ajuda a partir de **<Install dir>:\Program Files\Dell\Dell Data Protection\Encryption\EMS**.
  - Consulte a *Ajuda das Security Tools* para saber como utilizar as funcionalidades de Advanced Authentication. Aceda à ajuda a partir de **<Install dir>:\Program Files\Dell\Dell Data Protection\Security Tools \Help**.
- Após a conclusão da instalação, os utilizadores devem atualizar as respetivas políticas clicando com o botão direito do rato no ícone do Dell Data Protection no tabuleiro do sistema e selecionando **Procurar atualizações de políticas**.
- O instalador principal do instala todo o conjunto de produtos. Existem dois métodos para instalar utilizando o instalador principal do . Escolha uma das seguintes opções.
  - Instalar interativamente utilizando o instalador principal do

  ou

  - Instalar por linha de comandos utilizando o instalador principal do

Instalar interativamente utilizando o instalador principal do

- O instalador principal do pode ser localizado em:
  - **Em support.dell.com** - Se necessário, Obter o software a partir de support.dell.com e, em seguida, Extrair os instaladores subordinados do instalador principal do .
  - **Na sua conta FTP Dell** - Localize o pacote de instalação em DDP-Enterprise-Edition-8.x.x.xxx.zip
- Utilize estas instruções para instalar interativamente o Dell Enterprise Edition utilizando o instalador principal do . Este método pode ser utilizado para instalar o conjunto de produtos num computador de cada vez.

1. Localize o **DDPSetup.exe** no suporte multimédia de instalação Dell. Copie-o para o computador local.
2. Faça duplo clique em para iniciar o instalador. Isto poderá demorar vários minutos.
3. Clique em **Seguinte** na caixa de diálogo Bem-vindo.
4. Leia o contrato de licença, aceite os termos e condições e clique em **Seguinte**.
5. Selecione **Enterprise Edition** e clique em **Seguinte**.

   Se pretende instalar apenas o External Media Edition, selecione apenas a caixa de verificação do External Media Edition
6. No campo **Nome do Enterprise Server**, introduza o nome de anfitrião totalmente qualificado do EE Server/VE Server que irá gerir o utilizador pretendido, por exemplo, server.organization.com.

   No campo **URL do Device Server**, introduza o URL do Device Server (Security Server) com o qual o cliente irá comunicar.

   Se o seu EE Server for anterior à v7.7, o formato é https://server.organization.com:**8081**/xapi.

Se o seu EE Server for v7.7 ou posterior, o formato é https://server.organization.com:**8443**/xapi**/** (incluindo a barra inclinada para a direita no final).

Clique em **Seguinte**.

7 Clique em **Seguinte** para instalar os produtos na localização predefinida **C:\Program Files\Dell\Dell Data Protection\. Dell recommends installing in the default location only**, uma vez que poderão surgir problemas ao efetuar a instalação noutras localizações.

8 Selecione os componentes a serem instalados.

Security Framework instala a framework de segurança subjacente e o Security Tools, o cliente de autenticação avançada que gere múltiplos métodos de autenticação, incluindo PBA e credenciais tais como impressões digitais e palavras-passe.

Advanced Authentication instala os ficheiros e serviços necessários para a Autenticação avançada. .

Encriptação instala o cliente Encryption, o componente que aplica a política de segurança, quer um computador esteja ligado à rede, desligado da rede, seja perdido ou roubado.

BitLocker Manager instala o cliente BitLocker Manager, projetado para melhorar a segurança das implementações do BitLocker pela simplificação e redução do custo de propriedade através da gestão centralizada das políticas de encriptação do BitLocker.

Clique em **Seguinte** quando concluir as suas seleções.

9 Clique em **Instalar** para dar início à instalação. A instalação irá demorar vários minutos.

10 Selecione **Sim, desejo reiniciar o computador agora** e clique em **Concluir**.

A instalação está concluída.

Instalar por linha de comandos utilizando o instalador principal do

- As opções devem ser especificadas em primeiro lugar numa instalação por linha de comandos. Outros parâmetros vão dentro de um argumento que é passado para a opção /v.

Opções

- A tabela seguinte descreve as opções que podem ser utilizadas com o instalador principal do .

Opção	Descrição
-y -gm2	Pré-extração do instalador principal do . As opções -y e -gm2 devem ser utilizadas em conjunto. Não separe as opções.
/S	Instalação silenciosa
/z	Passa variáveis para o .msi dentro do DDPSetup.exe

Parâmetros

- A tabela seguinte descreve os parâmetros que podem ser utilizados com o instalador principal do .

Parâmetro	Descrição
SUPPRESSREBOOT	Elimina o reinício automático após a conclusão da instalação. Pode ser utilizado no modo SILENCIOSO.
SERVIDOR	Especifica o URL do EE Server/VE Server.
InstallPath	Especifica o caminho da instalação. Pode ser utilizado no modo SILENCIOSO.
FUNÇÕES	Especifica os componentes que podem ser instalados no modo SILENCIOSO.

Parâmetro	Descrição
	DE = Encriptação de unidade (Encryption Client) EME = External Media Edition apenas BLM = Bitlocker Management SED = Gestão de unidades de encriptação automática (controladores EMAgent/Manager, PBA/GPE)
BLM_ONLY=1	Deve ser utilizado com FEATURES=BLM na linha de comandos para excluir o plug-in de Gestão SED.

Exemplo de linha de comandos

- Os parâmetros da linha de comandos são sensíveis a maiúsculas e minúsculas.
- Este exemplo instala todos os componentes utilizando o instalador principal do nas portas padrão, de forma silenciosa, na localização predefinida C:\Program Files\Dell\Dell Data Protection\, e configura-o para utilizar o EE Server/VE Server especificado.

```
"DDPSetup.exe" -y -gm2 /S /z"\"SERVER=server.organization.com\""
```

- Este exemplo instala a Gestão SED e External Media Edition com o instalador principal, nas portas padrão, de forma silenciosa, com um reinício suprimido, na localização predefinida C:\Program Files\Dell\Dell Data Protection\, e configura-o para utilizar o EE Server/VE Server especificado.

```
"DDPSetup.exe" -y -gm2 /S /z"\"SERVER=server.organization.com, FEATURES=EME-SED,
SUPPRESSREBOOT=1\""
```

- Este exemplo instala a Gestão SED com o instalador principal, nas portas padrão, de forma silenciosa, com um reinício suprimido, na localização predefinida C:\Program Files\Dell\Dell Data Protection\, e configura-o para utilizar o EE Server/VE Server especificado.

```
"DDPSetup.exe" -y -gm2 /S /z"\"SERVER=server.organization.com, FEATURES=SED,
SUPPRESSREBOOT=1\""
```

- Este exemplo instala a Gestão SED com o instalador principal, nas portas padrão, de forma silenciosa, na localização predefinida C:\Program Files\Dell\Dell Data Protection\, e configura-o para utilizar o EE Server/VE Server especificado.

```
"DDPSetup.exe" -y -gm2 /S /z"\"SERVER=server.organization.com, FEATURES=SED\""
```

- Este exemplo instala o Encryption Client e o BitLocker Manager (sem o plug-in de Gestão SED), com o instalador principal, nas portas padrão, de forma silenciosa, na localização predefinida C:\Program Files\Dell\Dell Data Protection\, e configura-o para utilizar o EE Server/VE Server especificado.

```
"DDPSetup.exe" -y -gm2 /S /z"\"SERVER=server.organization.com, FEATURES=DE-BLM, BLM_ONLY=1\""
```

- Este exemplo instala o BitLocker Manager (com o plug-in de Gestão SED) e External Media Edition, com o instalador principal, nas portas padrão, de forma silenciosa, com um reinício suprimido, na localização predefinida C:\Program Files\Dell\Dell Data Protection\, e configura-o para utilizar o EE Server/VE Server especificado.

```
"DDPSetup.exe" -y -gm2 /S /z"\"SERVER=server.organization.com, FEATURES=BLM-EME,
SUPPRESSREBOOT=1\""
```

- Este exemplo instala o BitLocker Manager (sem o plug-in de Gestão SED) e External Media Edition, com o instalador principal, nas portas padrão, de forma silenciosa, com um reinício suprimido, na localização predefinida C:\Program Files\Dell\Dell Data Protection\, e configura-o para utilizar o EE Server/VE Server especificado.

```
"DDPSetup.exe" -y -gm2 /S /z"\"SERVER=server.organization.com, FEATURES=BLM-EME, BLM_ONLY=1,
SUPPRESSREBOOT=1\""
```

Desinstalar utilizando o instalador principal do

- Cada componente deve ser desinstalado separadamente e, posteriormente, deve ser efetuada a desinstalação do instalador principal do . Os clientes devem ser desinstalados numa **ordem específica para impedir falhas na desinstalação**.
- Siga as instruções apresentadas em Extrair os instaladores subordinados do instalador principal do para obter instaladores subordinados.
- Certifique-se de que é utilizada a mesma versão do instalador principal do (e respetivos clientes) para a desinstalação e instalação.
- Este capítulo direciona-o para outros capítulos que contêm instruções *detalhadas* sobre como desinstalar os instaladores subordinados. Este capítulo explica **apenas** o último passo, a desinstalação do instalador principal do .
- Desinstale os clientes pela seguinte ordem.

  a Desinstalar o Encryption Client.

  b Desinstalar os clientes SED e Advanced Authentication.

  c Desinstalar o cliente BitLocker Manager.
- Avance para Desinstalar o instalador principal do .

Desinstalar o instalador principal do

Após desinstalar todos os clientes individuais, o instalador principal do pode ser desinstalado.

Desinstalação por linha de comando

- O exemplo seguinte desinstala o instalador principal do de forma silenciosa.

  ```
  "DDPSetup.exe" -y -gm2 /S /x
  ```

  Reinicie o computador quando concluído.

Desinstalar utilizando os instaladores subordinados

- Para desinstalar cada cliente individualmente, primeiro é necessário extrair os ficheiros executáveis subordinados do instalador principal do , conforme descrito em Extrair os instaladores subordinados do instalador principal do . Em alternativa, execute uma instalação administrativa para extrair o .msi.
- Certifique-se de que são utilizadas as mesmas versões do cliente para a desinstalação e para a instalação.
- As opções e parâmetros da linha de comandos são sensíveis a maiúsculas e minúsculas.
- Certifique-se de que inclui um valor que contenha um ou mais caracteres especiais, como um espaço em branco na linha de comandos, entre aspas duplas de escape. Os parâmetros da linha de comandos são sensíveis a maiúsculas e minúsculas.
- Utilize estes instaladores para desinstalar os clientes utilizando uma instalação com script, com ficheiros batch ou qualquer outra tecnologia push disponível na sua organização.
- Ficheiros de registo - O Windows cria ficheiros de registo de desinstalação do instalador subordinado únicos para o utilizador com sessão iniciada em %temp%, localizados em **C:\Users\<UserName>\AppData\Local\Temp.**

  Se decidir adicionar um ficheiro de registo separado quando executar o instalador, certifique-se de que ficheiro de registo tem um nome único uma vez que os ficheiros de registo de instalador subordinado não são acrescentados. O comando padrão .msi pode ser utilizado para criar um ficheiro de registo utilizando /l **C:\<any directory>\<any log file name>.log**. A Dell não recomenda a utilização de "/l*v" (registo verboso) na desinstalação através da linha de comandos, uma vez que o nome de utilizador/palavra-passe são guardados no ficheiro de registo.
- Todos os instaladores subordinados utilizam as mesmas opções de apresentação e parâmetros .msi básicos, exceto quando indicado, para as desinstalações através da linha de comandos. As opções devem ser especificadas em primeiro lugar. A opção /v é obrigatória e necessita de um argumento. Outros parâmetros vão dentro de um argumento que é passado para a opção /v.

  As opções de apresentação podem ser especificadas no final do argumento passado para a opção /v para alcançar o comportamento esperado. Não utilize /q e /qn na mesma linha de comandos. Utilize apenas ! e - após /qb.

Opção	Significado
/v	Passa variáveis para o .msi dentro do setup.exe. O conteúdo deve estar sempre dentro de aspas de texto simples.
/s	Modo silencioso
/x	Modo de desinstalação
/a	Instalação administrativa (irá copiar todos os ficheiros contidos no .msi)

NOTA:
Com /v, as opções predefinidas da Microsoft ficam disponíveis. Para ver uma lista de opções, consulte https://msdn.microsoft.com/en-us/library/windows/desktop/aa367988(v=vs.85).aspx .

Opção	Significado
/q	Sem caixa de diálogo de Progresso, reinicia-se após a conclusão do processo
/qb	Caixa de diálogo de Progresso com botão **Cancelar**, solicita o reinício

Opção	Significado
/qb-	Caixa de diálogo de Progresso com botão **Cancelar**, reinicia-se após a conclusão do processo
/qb!	Caixa de diálogo de Progresso sem botão **Cancelar**, solicita o reinício
/qb!-	Caixa de diálogo de Progresso sem botão **Cancelar**, reinicia-se após a conclusão do processo
/qn	Sem interface de utilizador

Desinstalar o Encryption e o Server Encryption Client

- Para reduzir o tempo de desencriptação, execute o Assistente de Limpeza de Disco do Windows para remover ficheiros temporários e outros dados desnecessários.
- Se possível, programe a desencriptação para ser feita durante a noite.
- Desative o modo de suspensão para impedir a suspensão do computador caso este se encontre sem supervisão. A desencriptação não é possível num computador em suspensão.
- Encerre todos os processos e aplicações para minimizar as falhas de desencriptação devidas a ficheiros bloqueados.
- Uma vez que a desinstalação está concluída e a desencriptação está em progresso, desative toda a conectividade à rede. Caso contrário, podem ser adquiridas novas políticas que voltam a ativar a encriptação.
- Siga o processo de desencriptação de dados existente, como, por exemplo, a emissão de uma atualização de política.
- O Windows e os EME Shields atualizam o EE Server/VE Server para alterar o estado para *Desprotegido* no início do processo de desinstalação do Shield. No entanto, caso o cliente não consiga contactar o EE Server/VE Server, independentemente do motivo, não é possível atualizar o estado. Neste caso, terá de *Remover o endpoint* manualmente na Remote Management Console. Se a sua organização utilizar este fluxo de trabalho por motivos de conformidade, a Dell recomenda que verifique se o estado *Desprotegido* foi definido da forma esperada na Remote Management Console ou no Compliance Reporter.

Processo

- O Key Server (e EE Server) deve ser configurado antes da desinstalação se estiver a utilizar a opção **Transferir chaves a partir do servidor do Encryption Removal Agent**. Consulte Configurar o Key Server para desinstalação do Encryption Client ativado no EE Server para obter instruções. Não é necessária qualquer ação anterior se o cliente a ser desinstalado está ativado em um VE Server, uma vez que o VE Server não utiliza o Key Server.
- Deve utilizar o Dell Administrative Utility (CMGAd) antes de iniciar o Encryption Removal Agent se estiver a utilizar a opção **Importar chaves a partir de um ficheiro do Encryption Removal Agent**. Este utilitário é utilizado para obter o pacote de chave de encriptação. Consulte Utilizar o Administrative Download Utility (CMGAd) para obter instruções. O utilitário pode estar localizado no suporte de instalação Dell.

Desinstalação por linha de comando

- Uma vez extraído do instalador principal do , o instalador do Encryption Client pode ser localizado em **C:\extracted\Encryption \DDPE_XXbit_setup.exe**.
- A tabela seguinte descreve os parâmetros disponíveis para a desinstalação.

Parâmetro	Seleção
CMG_DECRYPT	Propriedade para selecionar o tipo de instalação do Encryption Removal Agent 3 - Utilizar o pacote LSARecovery

Parâmetro	Seleção
	2 - Utilizar material da chave forense anteriormente transferido 1 - Transferir chaves do Servidor Dell 0 – Não instalar o Encryption Removal Agent
CMGSILENTMODE	Propriedade para a desinstalação silenciosa: 1 – Silenciosa 0 – Não silenciosa
Propriedades obrigatórias	
DA_SERVER	FQHN para o EE Server anfitrião da sessão de negociação.
DA_PORT	Porta do EE Server para pedidos (a predefinição é 8050)
SVCPN	Nome de utilizador, em formato UPN, com o qual o serviço Key Server tem sessão iniciada no EE Server.
DA_RUNAS	Nome de utilizador em formato compatível com SAM, sendo o pedido de recuperação de chaves realizado neste contexto. Este utilizador deve encontrar-se na lista do Key Server no EE Server.
DA_RUNASPWD	Palavra-passe do utilizador runas.
FORENSIC_ADMIN	A conta de Administrador forense no Servidor Dell, que pode ser utilizada para pedidos forenses para desinstalações ou chaves.
FORENSIC_ADMIN_PWD	A palavra-passe da conta de Administrador forense.
Propriedades opcionais	
SVCLOGONUN	Nome de utilizador em formato UPN para o início de sessão do serviço Encryption Removal Agent como parâmetro.
SVCLOGONPWD	Palavra-passe para início de sessão como utilizador.

- O seguinte exemplo desinstala silenciosamente o Encryption Client e transfere as chaves de encriptação a partir do EE Server.

  ```
  DDPE_XXbit_setup.exe /s /x /v"CMG_DECRYPT=1 CMGSILENTMODE=1 DA_SERVER=server.organization.com
  DA_PORT=8050 SVCPN=administrator@organization.com DA_RUNAS=domain\username
  DA_RUNASPWD=password /qn"
  ```

  Comando MSI:

  ```
  msiexec.exe /s /x "Dell Data Protection Encryption.msi" /qn REBOOT="ReallySuppress"
  CMG_DECRYPT="1" CMGSILENTMODE="1" DA_SERVER="server.organization.com" DA_PORT="8050"
  SVCPN="administrator@domain.com" DA_RUNAS="domain\username" DA_RUNASPWD="password" /qn
  ```

  Reinicie o computador quando concluído.

- O seguinte exemplo desinstala silenciosamente o Encryption Client e transfere as chaves de encriptação utilizando uma conta de Administrador forense.

  ```
  DDPE_XXbit_setup.exe /s /x /v"CMG_DECRYPT=1 CMGSILENTMODE=1
  FORENSIC_ADMIN=forensicadmin@organization.com FORENSIC_ADMIN_PWD=tempchangeit /qn"
  ```

  Comando MSI:

```
msiexec.exe /s /x "Dell Data Protection Encryption.msi" /qn CMG_DECRYPT=1 CMGSILENTMODE=1
FORENSIC_ADMIN=forensicadmin@organization.com FORENSIC_ADMIN_PWD=tempchangeit
REBOOT=REALLYSUPPRESS
```

Reinicie o computador quando concluído.

IMPORTANTE:

A Dell recomenda as seguintes ações quando utilizar uma palavra-passe de Administrador forense na linha de comandos:

1. Crie uma conta de Administrador forense na Remote Management Console para realizar a desinstalação silenciosa.
2. Utilize uma palavra-passe temporária exclusiva para essa conta e para esse período de tempo.
3. Após a conclusão da desinstalação silenciosa, remova a conta temporária da lista de administradores ou altere a respetiva palavra-passe.

NOTA:

Alguns clientes mais antigos poderão requerer caracteres de \" à volta dos valores dos parâmetros. Por exemplo:

```
DDPE_XXbit_setup.exe /x /v"CMG_DECRYPT=\"1\" CMGSILENTMODE=\"1\" DA_SERVER=
\"server.organization.com\" DA_PORT=\"8050\" SVCPN=\"administrator@organization.com\"
DA_RUNAS=\"domain\username\" DA_RUNASPWD=\"password\" /qn"
```

Desinstalar o External Media Edition

Uma vez extraído do instalador principal, o instalador do Encryption Client pode ser localizado em C:\extracted\Encryption \DDPE_XXbit_setup.exe.

Desinstalação por linha de comando

Execute uma linha de comandos idêntica a uma das seguintes:

```
DDPE_XXbit_setup.exe /s /x /v"/qn"
```

Reinicie o computador quando concluído.

Desinstalar os clientes SED e Advanced Authentication

- A ligação de rede ao EE Server/VE Server é necessária para desativar a PBA.

Processo

- Desativar a PBA, o que remove todos os dados da PBA do computador e desbloqueia as chaves SED.
- Desinstalar o software de cliente SED.
- Desinstalar o software de cliente Advanced Authentication.

Desativar a PBA

1. Como Administrador Dell, inicie sessão na Remote Management Console.
2. No painel do lado esquerdo, clique em **Proteger e gerir** > **Endpoints**.
3. Selecione o Tipo de endpoint adequado.
4. Selecione Mostrar >*Visível*, Oculto ou *Todos*.
5. Se souber o Nome de anfitrião do computador, introduza-o no campo Nome de anfitrião (os caracteres universais são suportados). Pode deixar o campo em branco, de modo a que sejam apresentados todos os computadores. Clique em **Procurar**.

Se não souber o Nome de anfitrião, procure na lista até encontrar o computador.

É apresentado um computador ou lista de computadores com base no seu filtro de pesquisa.

6 Selecione o ícone **Detalhes** do computador pretendido.

7 Clique em **Políticas de segurança** no menu superior.

8 Selecione **Unidades de encriptação automática** a partir do menu de lista pendente de **Categoria de política**.

9 Expanda a área **Administração SED** e altere as políticas **Permitir gestão SED** e **Ativar PBA** de *True* para ***False***.

10 Clique em **Guardar**.

11 No painel do lado esquerdo, clique em **Ações** > **Consolidar políticas**.

12 Clique em **Aplicar alterações**.

Aguarde que a política seja propagada do EE Server/VE Server para o computador onde pretende efetuar a desativação.

Desinstale os clientes SED e de Autenticação depois da PBA ser desativada.

Desinstale o cliente SED e clientes Advanced Authentication

Desinstalação por linha de comando

- Uma vez extraído do instalador principal do , o instalador do cliente SED pode ser localizado em C:\extracted\Security Tools \EMAgent_XXbit_setup.exe.
- Uma vez extraído do instalador principal do , o instalador do cliente SED pode ser localizado em C:\extracted\Security Tools \Authentication\<x64/x86>\setup.exe.
- O seguinte exemplo desinstala o cliente SED de forma silenciosa.

```
EMAgent_XXbit_setup.exe /x /s /v" /qn"
```

Encerre e reinicie o computador quando concluído.

Em seguida:

- O seguinte exemplo desinstala o cliente Advanced Authentication de forma silenciosa.

```
setup.exe /x /s /v" /qn"
```

Encerre e reinicie o computador quando concluído.

Desinstalar o cliente BitLocker Manager

Desinstalação por linha de comando

- Uma vez extraído do instalador principal do , o instalador do cliente BitLocker pode ser localizado em C:\extracted\Security Tools \EMAgent_XXbit_setup.exe.
- O seguinte exemplo desinstala o cliente BitLocker Manager de forma silenciosa.

```
EMAgent_XXbit_setup.exe /x /s /v" /qn"
```

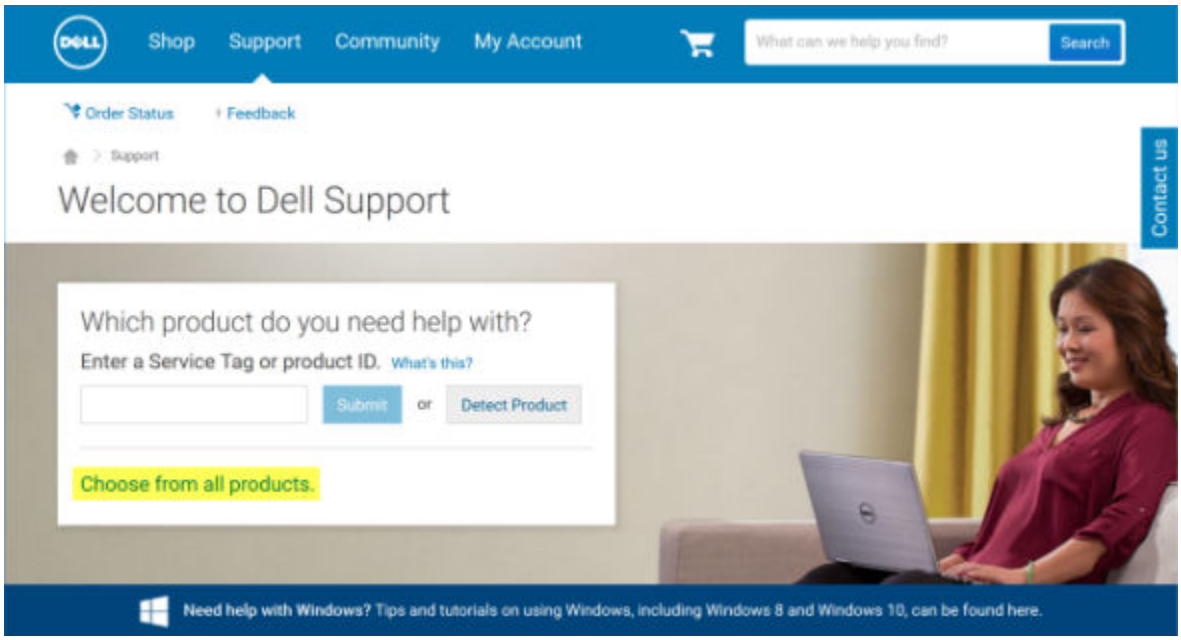
Reinicie o computador quando concluído.

Download the Software

Esta secção detalha a obtenção de software a partir de dell.com/support. Se já tiver o software, pode ignorar esta secção.

Aceda a dell.com/support para começar.

1 Na página Web de apoio técnico da Dell, selecione **Selecionar de entre todos os produtos**.



2 Select **Software & Security** from the list of products.

3 Select **Endpoint Security Solutions** in the *Software and Security* section.
Após efetuar esta seleção uma vez, o site irá memorizar as informações.

4 Selecione o produto Dell Data Protection.
Exemplos:

Dell Encryption

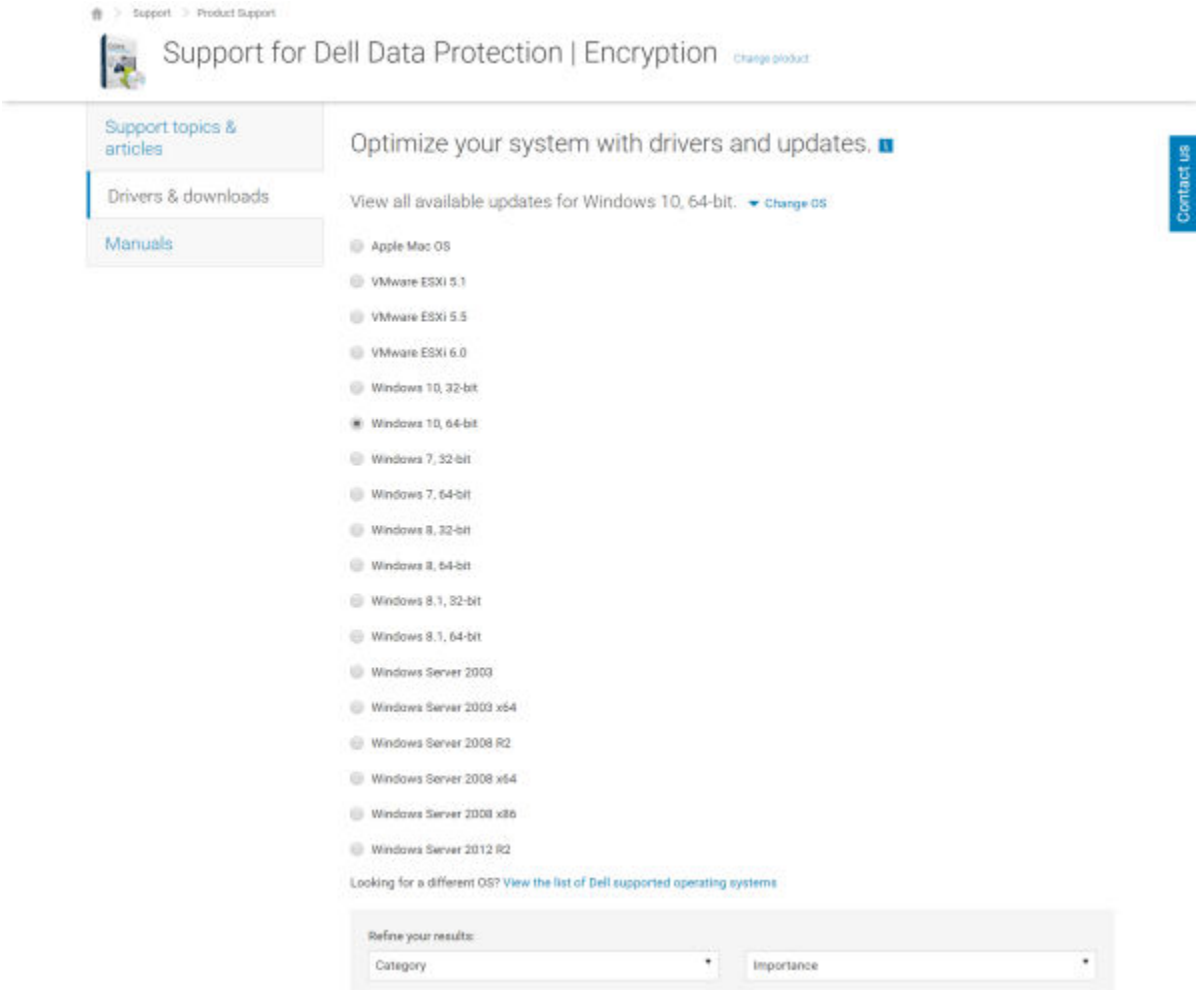
Dell Endpoint Security Suite

Dell Endpoint Security Suite Enterprise

5 Select **Drivers & downloads**.

6 Selecione o tipo de sistema operativo cliente desejado.

7 Select **Dell Data Protection (4 files)** in the matches. Isto é apenas um exemplo, pelo que, provavelmente, a realidade será ligeiramente diferente. Por exemplo, poderá não haver 4 ficheiros para escolha.



8 Select **Download File** or A**dd to My Download List #XX**.

Extrair os instaladores subordinados do instalador principal do

- O instalador principal do não é um *desinstalador* principal. Cada cliente deve ser desinstalado individualmente e, posteriormente, deve ser efetuada a desinstalação do instalador principal do . Utilize este processo para extrair os clientes do instalador principal do para que possam ser utilizados na desinstalação.

1 A partir do suporte multimédia de instalação Dell, copie o ficheiro **DDPSetup.exe** para o computador local.

2 Abra uma linha de comandos na mesma localização do ficheiro **DDPSetup.exe** e introduza:

```
DDPSetup.exe /z"\"EXTRACT_INSTALLERS=C:\extracted\""
```

O caminho de extração não pode exceder os 63 caracteres.

Os instaladores subordinados extraídos estão localizados em **C:\extracted\.**

Configurar o Key Server para desinstalação do Encryption Client ativado no EE Server

- Esta seção explica como configurar componentes para utilização com a autenticação/autorização Kerberos ao utilizar um EE Server. O VE Server não utiliza o Key Server.
- Se for necessário utilizar Autenticação/Autorização Kerberos, o servidor que contém o componente Key Server necessita fazer parte do domínio afetado.
- Dado que o VE Server não utiliza o Key Server, a desinstalação típica é afetada. Quando um Encryption Client ativado num VE Server é desinstalado, é utilizada a recuperação de chave forense padrão através do Security Server, em vez do método Kerberos do Key Server. Consulte Desinstalação por linha de comando para obter mais informações.

Painel de Serviços - Adicionar utilizador da conta do domínio

1 No EE Server, navegue até ao painel de Serviços (Iniciar > Executar... > services.msc > OK).

2 Clique com o botão direito do rato em Key Server e selecione **Propriedades**.

3 Selecione o separador Iniciar sessão e selecione a opção **Esta conta:**.

No campo *Esta conta:*, adicione o utilizador da conta do domínio. Este utilizador do domínio necessita possuir, pelo menos, direitos administrativos locais para a pasta do Key Server (necessita poder gravar no ficheiro de configuração do Key Server e também ter a capacidade de gravar no ficheiro log.txt).

Introduza e confirme a palavra-passe para o utilizador do domínio.

Clique em **OK**

4 Reinicie o serviço do Key Server (deixe o painel de Serviços aberto para continuar a utilizá-lo).

5 Navegue até <Key Server install dir>\log.txt para verificar se o serviço foi iniciado adequadamente.

Ficheiro de configuração do Key Server - Adicionar utilizador para comunicação do EE Server

1 Navegue até <Key Server install dir>.

2 Abra ***Credant.KeyServer.exe.config*** com um editor de texto.

3 Aceda a <add key="user" value="superadmin" /> e altere o valor "superadmin" para o nome do utilizador pretendido (pode também manter "superadmin").

4 Aceda a <add key="epw" value="<encrypted value of the password>" /> e altere "epw" para "password". Em seguida, altere o "<valor encriptado da palavra-passe>" para a palavra-passe do utilizador indicada no Passo 3. Esta palavra-passe é novamente encriptada quando reiniciar o EE Server.

Se, no Passo 3, utilizou "superadmin" e a palavra-passe do superadmin não for "changeit", precisa ser alterada aqui. Guarde e feche o ficheiro.

Painel de Serviços - Reiniciar o serviço Key Server

1 Volte ao painel de Serviços (Iniciar > Executar... > services.msc > OK).
2 Reinicie o serviço Key Server.
3 Navegue até <Key Server install dir>\log.txt para verificar se o serviço foi iniciado adequadamente.
4 Feche o painel Serviços.

Remote Management Console - Adicionar administrador forense

1 Caso necessário, inicie a sessão na Remote Management Console.
2 Clique em **Populações** > **Domínios**.
3 Selecione o Domínio adequado.
4 Clique no separador **Key Server**.
5 No campo Conta, adicione o utilizador que irá realizar as atividades de administrador. O formato é DOMAIN\UserName. Clique em **Adicionar conta**.
6 Clique em **Utilizadores** no menu à esquerda. Na caixa de pesquisa, procure o nome de utilizador adicionado no Passo 5. Clique em **Procurar**.
7 Depois de encontrar o utilizador correto, clique no separador **Administrador**.
8 Selecione **Administrador forense** e clique em **Atualizar**.
Os componentes estão agora configurados para autenticação/autorização Kerberos.

9

Utilizar o Administrative Download Utility (CMGAd)

- Este utilitário permite a transferência de um pacote de material de chave para utilização num computador que não está ligado a um servidor EE Server/VE Server.
- Este utilitário utiliza um dos seguintes métodos para transferir um pacote de chave, dependendo do parâmetro da linha de comandos passado à aplicação:
  - Modo forense - Utilizado se -f é passado na linha de comandos ou se não é utilizado qualquer parâmetro de linha de comandos.
  - Modo de administrador - Utilizado se -a é passado na linha de comandos.

  Os ficheiros de registo podem ser localizados em C:\ProgramData\CmgAdmin.log

Utilize o Administrative Download Utility no Modo forense

1 Clique duas vezes em **cmgad.exe** para iniciar o utilitário ou abrir uma linha de comandos onde o CMGAd está localizado e introduza **`cmgad.exe -f`** (ou **`cmgad.exe`**).

2 Introduza a seguinte informação (alguns campos podem ser pré-preenchidos).

URL do Device Server: URL do Security Server (Device Server) totalmente qualificado. O formato é https://securityserver.domain.com:8443/xapi/. Se o seu EE Server é pré-v7.7, o formato é https://deviceserver.domain.com:8081/xapi (diferente número de porta, sem a barra no final).

Administrador Dell: Nome do administrador com credenciais de administrador forense (ativado na Remote Management Console), por exemplo, jdoe

Palavra-passe: Palavra-passe de administrador forense

MCID: ID do computador, por exemplo, machineID.domain.com

DCID: Primeiros oito dígitos da ID Shield de 16 dígitos

> **SUGESTÃO:**
> Normalmente, é suficiente especificar o MCID *ou* DCID. No entanto, se ambos são conhecidos, é útil introduzir os dois. Cada parâmetro contém informação diferente sobre o cliente e o computador cliente.

Clique em **Seguinte**.

3 No campo Frase de acesso:, escreva uma frase de acesso para proteger o ficheiro de transferência. A frase de acesso deve ter pelo menos oito caracteres de comprimento, e conter pelo menos um carácter alfabético e um carácter numérico. Confirme a frase de acesso.

Aceite o nome e localização padrão onde o ficheiro será guardado ou clique em ... para selecionar uma localização diferente.

Clique em **Seguinte**.

É apresentada uma mensagem, indicando que o material de chave foi desbloqueado satisfatoriamente. Os ficheiros estão agora acessíveis.

4 Clique em **Concluir** quando tiver terminado.

Utilize o Administrative Download Utility no Modo de administrador

O VE Server não utiliza o Key Server, portanto o modo de Administrador não pode ser utilizado para obter um pacote de chave a partir de um VE Server. Utilize o Modo forense para obter o pacote de chaves se o cliente estiver ativado em um VE Server.

1 Abra uma linha de comandos onde o CMGAd está localizado e introduza **`cmgad.exe -a`**.

2 Introduza a seguinte informação (alguns campos podem ser pré-preenchidos).

Servidor: Nome de anfitrião totalmente qualificado do Key Server, por exemplo, keyserver.domain.com

Número da porta: A porta predefinida é 8050

Conta do servidor: O utilizador do domínio de execução do Key Server. O formato é domain\username. O utilizador do domínio que está a executar o utilitário deve estar autorizado para realizar a transferência a partir do Key Server

MCID: ID do computador, por exemplo, machineID.domain.com

DCID: Primeiros oito dígitos da ID Shield de 16 dígitos

> **SUGESTÃO:**
> Normalmente, é suficiente especificar o MCID *ou* DCID. No entanto, se ambos são conhecidos, é útil introduzir os dois. Cada parâmetro contém informação diferente sobre o cliente e o computador cliente.

Clique em **Seguinte**.

3 No campo Frase de acesso:, escreva uma frase de acesso para proteger o ficheiro de transferência. A frase de acesso deve ter pelo menos oito caracteres de comprimento, e conter pelo menos um carácter alfabético e um carácter numérico.

Confirme a frase de acesso.

Aceite o nome e localização padrão onde o ficheiro será guardado ou clique em ... para selecionar uma localização diferente.

Clique em **Seguinte**.

É apresentada uma mensagem, indicando que o material de chave foi desbloqueado satisfatoriamente. Os ficheiros estão agora acessíveis.

4 Clique em **Concluir** quando tiver terminado.

Resolução de problemas

Todos os clientes - Resolução de problemas

- **Os ficheiros de registo do instalador principal do** estão localizados em **C:\ProgramData\Dell\Dell Data Protection\Installer.**
- O Windows cria **ficheiros de registo de instalação do instalador subordinado** únicos para o utilizador com sessão iniciada em %temp %, localizados em **C:\Users\<UserName>\AppData\Local\Temp.**
- O Windows cria ficheiros de registo para pré-requisitos do cliente, como Visual C++, para o utilizador com sessão iniciada em %temp%, localizados em **C:\Users\<UserName>\AppData\Local\Temp. Por exemplo, C:\Users\<UserName>\AppData\Local\Temp \dd_vcredist_amd64_20160109003943.log**
- Siga as instruções apresentadas em http://msdn.microsoft.com para verificar a versão do Microsoft .Net instalada no computador onde pretende efetuar a instalação.

  Aceda a https://www.microsoft.com/en-us/download/details.aspx?id=30653 para transferir a versão completa do Microsoft .Net Framework 4.5.
- Consulte *Dell Data Protection | Security Tools Compatibility* se o computador onde pretende efetuar a instalação tiver (ou teve anteriormente) o Dell Access instalado. O DDP|A não é compatível com este conjunto de produtos.

Resolução de problemas do Encryption e do Server Encryption Client

Atualização para o Windows 10 Anniversary

Para atualizar para a versão de atualização do Windows 10 Anniversary, siga as instruções apresentadas no artigo seguinte: http://www.dell.com/support/article/us/en/19/SLN298382.

Ativação num sistema operativo de servidor

Quando o Encryption está instalado num sistema operativo de servidor, a ativação requer duas fases de ativação: a ativação inicial e a ativação do dispositivo.

Resolução de problemas da ativação inicial

A ativação inicial falha quando:

- Não é possível construir um UPN válido utilizando as credenciais fornecidas.
- As credenciais não se encontram no cofre da empresa.
- As credenciais utilizadas para ativação não são as credenciais do Administrador de domínio.

Mensagem de erro: Nome de utilizador desconhecido ou palavra-passe inválida

O nome de utilizador ou a palavra-passe não correspondem.

Solução possível**:** Tente iniciar sessão novamente, certificando-se que introduz o nome de utilizador e palavra-passe corretos.

Mensagem de erro: A ativação falhou porque a conta de utilizador não possui direitos de administrador de domínio.

As credenciais utilizadas para ativação não possuem direitos de administrador de domínio ou o nome de utilizador do administrador não está em formato UPN.

Solução possível**:** Na caixa de diálogo Ativação, introduza as credenciais de um Administrador de domínio e certifique-se de que estão em formato UPN.

Mensagens de erro: Não foi possível estabelecer a ligação ao servidor.

ou

`The operation timed out.`

O Server Encryption não consegue comunicar com a porta 8449 através de https no DDP Security Server.

Soluções Possíveis

- Ligue diretamente à sua rede e tente novamente ativar.
- Se estiver ligado via VPN, tente ligar diretamente à rede e tente novamente ativar.
- Verifique o URL do Servidor DDP para garantir que é o mesmo URL que o administrador forneceu. O URL e outros dados que o utilizador introduziu no programa de instalação estão armazenados no registo. Verifique a correção dos dados em [HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield] e [HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield\Servlet].
- Desconecte o servidor da rede. Reinicie o servidor e reconecte à rede.

Mensagem de erro: Ocorreu uma falha na ativação, uma vez que o Servidor não suporta este pedido.

Soluções Possíveis

- Não é possível ativar o Server Encryption num servidor legado; a versão do Servidor DDP deve ser a versão 9.1 ou superior. Se necessário, faça uma atualização de versão do seu Servidor DDP para a versão 9.1 ou superior.
- Verifique o URL do Servidor DDP para garantir que é o mesmo URL que o administrador forneceu. O URL e outros dados que o utilizador introduziu no programa de instalação estão armazenados no registo.
- Verifique a correção dos dados em [HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield] e [HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield\Servlet].

Processo de ativação inicial

O diagrama seguinte ilustra uma ativação inicial bem-sucedida.

O processo de ativação inicial do Server Encryption requer o acesso de um utilizador real ao servidor. O utilizador pode ser de qualquer tipo: utilizador de domínio ou sem domínio, ligado ao ambiente de trabalho remoto ou interativo, mas o utilizador deve ter acesso a credenciais de Administrador de domínio.

A caixa de diálogo Ativação é apresentada numa das duas situações seguintes:

- Um utilizador novo (não gerido) inicia sessão no computador.
- Quando um utilizador novo clica com o botão direito do rato no ícone do Encryption Client no tabuleiro do sistema e seleciona Ativar o Dell Encryption.

O processo de ativação inicial é o seguinte:

1. O utilizador inicia sessão.
2. Ao detetar um utilizador novo (não gerido), a caixa de diálogo Ativar é apresentada. O utilizador clica em **Cancelar**.
3. O utilizador abre a caixa "Acerca de" do Server Encryption para confirmar se está em execução no modo de Servidor.
4. O utilizador clica com o botão direito do rato no ícone do Encryption Client no tabuleiro do sistema e seleciona **Ativar o Dell Encryption**.
5. O utilizador introduz as credenciais de Administrador de domínio na caixa de diálogo Ativar.

NOTA:
O requisito de credenciais de Administrador de domínio é uma medida de segurança que impede que o Server Encryption seja implementado noutros ambientes de servidor que não suportam o mesmo. Para desativar o requisito de credenciais de Administrador de domínio, consulte Antes de começar.

6 O Servidor DDP verifica as credenciais no cofre da empresa (Active Directory ou equivalente) para confirmar se as mesmas são as credenciais de Administrador de domínio.

7 Um UPN é construído utilizando as credenciais.

8 Com o UPN, o Servidor DDP cria uma nova conta de utilizador para o utilizador do servidor virtual, e guarda as credenciais no cofre do Servidor DDP.

A **conta de utilizador do servidor virtual** destina-se a utilização exclusiva do Encryption Client. Esta será utilizada para autenticação no servidor, para gestão de chaves de encriptação Comuns e para receção de atualizações de política.

NOTA:
A palavra-passe e a autenticação DPAPI estão desativadas para esta conta de modo a que *apenas* o utilizador do servidor virtual tenha acesso a chaves de encriptação no computador. Esta conta não corresponde a qualquer outra conta de utilizador no computador ou no domínio.

9 Quando a ativação for bem-sucedida, o utilizador reinicia o computador, o que inicia a segunda parte da ativação, Autenticação e Ativação do dispositivo.

Resolução de problemas de autenticação e ativação do dispositivo

A ativação do dispositivo falha quando:

- Ocorre uma falha da ativação inicial.
- Não é possível estabelecer a ligação ao servidor.
- Não é possível validar o certificado de confiança.

Após a ativação, quando o computador é reiniciado, o Server Encryption inicia automaticamente sessão como utilizador do servidor virtual, solicitando a chave de Computador ao DDP Enterprise Server. Ocorre mesmo antes de qualquer utilizador iniciar sessão.

- Abra a caixa de diálogo "Acerca de" para confirmar se o Server Encryption está autenticado e no modo de Servidor.
- No caso de o Shield ID (ID de Proteção) exibir cor vermelha, a encriptação ainda não foi ativada.
- Na Remote Management Console, a versão de um servidor com o Server Encryption instalado é indicada como *Proteção para servidor*.
- Se a obtenção da chave de Computador falhar devido a uma falha de rede, o Server Encryption regista-se para receber notificações de rede do sistema operativo.
- Se a obtenção da chave de Computador falhar:
  - O início de sessão do utilizador no servidor virtual é, ainda assim, bem-sucedido.
  - Defina a política *Intervalo de Tempo entre Tentativas em caso de Falha de rede* para efetuar tentativas de obtenção da chave com um intervalo de tempo definido.

    Consulte AdminHelp, disponível na Remote Management Console, para obter detalhes sobre a política *Intervalo de tempo entre tentativas em caso de falha de rede*.

Autenticação e processo de ativação de dispositivos

O diagrama seguinte ilustra a autenticação e ativação do dispositivo bem-sucedidas.

1 Quando reiniciar após uma ativação inicial bem-sucedida, um computador com Server Encryption efetua automaticamente a autenticação utilizando a conta de utilizador do servidor virtual e executa o Encryption Client no modo de Servidor.

2 O computador verifica o respetivo estado de ativação de dispositivos com o Servidor DDP:

- Se o computador não tiver ativado o dispositivo anteriormente, o Servidor DDP atribui um MCID, um DCID e um certificado de confiança ao computador, e guarda todas as informações no cofre do Servidor DDP.

- Se o computador tiver anteriormente ativado o dispositivo, o Servidor DDP verifica o certificado de confiança.

3 Depois de o Servidor DDP atribuir o certificado de confiança ao servidor, este pode aceder às respetivas chaves de encriptação.

4 A ativação do dispositivo é bem-sucedida.

> **NOTA:**
> Quando estiver em execução no modo de Servidor, o Encryption Client deve ter acesso ao mesmo certificado utilizado na ativação do dispositivo para aceder às chaves de encriptação.

Interações com EMS e PCS

Para garantir que o suporte multimédia não está definido como apenas de leitura e que a porta não está bloqueada

A política de Acesso a suportes multimédia desprotegidos do EMS interage com o Sistema de controlo das portas - Classe de armazenamento: Política de controlo da unidade externa. Se pretender definir a política de Acesso de EMS a suportes multimédia desprotegidos como *Acesso Total*, certifique-se de que a Classe de armazenamento: Política de controlo da unidade externa também está definida como *Acesso Total* para garantir que o suporte multimédia não está definido como só de leitura e que a porta não está bloqueada.

Para encriptar os dados gravados em CD/DVD

- Defina EMS: Encriptar suporte multimédia externo = Verdadeiro.
- Definir EMS: excluir encriptação de CD/DVD = Falso.
- Defina a Subclasse de armazenamento: Controlo da unidade ótica = Apenas UDF.

Utilizar o WSScan

- O WSScan permite-lhe assegurar que todos os dados são desencriptados quando desinstalar o Encryption Client, para além de visualizar o estado de encriptação e identificar ficheiros desencriptados que devem ser encriptados.
- São necessários privilégios de administrador para executar este utilitário.

Execute a

1 Copie WSScan.exe do suporte de instalação Dell para o computador Windows a verificar.

2 Inicie uma linha de comandos na localização acima e introduza **wsscan.exe** na mesma. O WSScan é iniciado.

3 Clique em **Avançadas**.

4 Selecione o tipo de unidade a analisar no menu pendente: *Todas as unidades, Unidades fixas*, *Unidades amovíveis* ou *CDROM/DVDROM*.

5 Selecione o Tipo de relatório de encriptação pretendido no menu pendente: *Ficheiros encriptados*, *Ficheiros desencriptados*, *Todos os ficheiros* ou *Ficheiros desencriptados em violação*:
   - *Ficheiros encriptados* - Para assegurar que todos os dados são desencriptados quando desinstalar o Encryption Client. Siga o processo de desencriptação de dados existente, por exemplo, a emissão de uma atualização de política de desencriptação. Após desencriptar os dados, mas antes de reiniciar para preparar a desinstalação, execute o WSScan para garantir que todos os dados estão desencriptados.
   - *Ficheiros desencriptados* - Para identificar ficheiros que não estão encriptados, com indicação se os ficheiros devem ser encriptados (S/N).
   - *Todos os ficheiros* - Para indicar todos os ficheiros encriptados e desencriptados, com indicação se os ficheiros devem ser encriptados (S/N).
   - *Ficheiros desencriptados em violação* - Para identificar ficheiros que não estão encriptados e deviam estar.

6 Clique em **Procurar**.

OU

1 Clique em **Avançadas** para alternar a visualização para **Simples** para analisar uma pasta particular.

2 Aceda a Definições de análise e introduza o caminho da pasta no campo **Caminho da pesquisa**. Se este campo for utilizado, a seleção na caixa pendente será ignorada.

3 Caso não pretenda gravar os resultados de saída do WSScan num ficheiro, desmarque a caixa de verificação **Saída para ficheiro**.

4 Se pretender, altere o caminho e o nome de ficheiro predefinidos em *Caminho*.

5 Selecione **Adicionar a ficheiro existente** se não pretende substituir quaisquer ficheiros de saída WSScan existentes.

6 Escolha o formato de saída:

- Selecione Formato de relatório para obter uma lista de estilos de relatório de saída de análise. Este é o formato predefinido.
- Selecione Ficheiro de valor delimitado para uma saída que possa ser importada para uma aplicação de folha de cálculo. O delimitador predefinido é "|", embora possa ser alterado para, no máximo, 9 carateres alfanuméricos, um espaço ou sinais de pontuação do teclado.
- Selecione a opção Valores cotados para colocar cada valor entre aspas duplas.
- Selecione Ficheiro de largura fixa para uma saída não delimitada, com uma linha contínua de informações de comprimento fixo acerca de cada ficheiro encriptado.

7 Clique em **Procurar**.

Clique em **Parar a pesquisa** para parar a sua pesquisa. Clique em **Limpar** para eliminar as mensagens apresentadas.

Resultado do WSScan

As informações do WSScan acerca dos ficheiros encriptados contêm os seguintes dados.

Exemplo de saída:

[2015-07-28 07:52:33] SysData.7vdlxrsb._SDENCR_: "c:\temp\Dell - test.log" continua encriptado por AES256

Saída	Significado
Carimbo de data/hora	A data e a hora em que o ficheiro foi analisado.
Tipo de encriptação	O tipo de encriptação utilizado para encriptar o ficheiro. **SysData:** Chave de encriptação SDE. **Utilizador:** Chave de encriptação do utilizador. **Comum:** Chave de encriptação comum. O WSScan não indica ficheiros encriptados utilizando o Encrypt for Sharing.
KCID	A ID do computador principal. Tal como apresentado no exemplo acima, "**7vdlxrsb**" Se estiver a analisar uma unidade de rede mapeada, o relatório da análise não apresenta uma KCID.
UCID	A ID do utilizador. Tal como apresentado no exemplo acima, "**_SDENCR_**" A UCID é partilhada por todos os utilizadores desse computador.
Ficheiro	O caminho do ficheiro encriptado. Tal como apresentado no exemplo acima, "**c:\temp\Dell - test.log**"
Algoritmo	O algoritmo de encriptação utilizado para encriptar o ficheiro. Tal como apresentado no exemplo acima, "**continua encriptado por AES256**" RIJNDAEL 128 RIJNDAEL 256

Saída	Significado
	AES 128
	AES 256
	3DES

Verificar o estado do Encryption Removal Agent

O Encryption Removal Agent apresenta o respetivo estado na área de descrição do painel de Serviços (Iniciar > Executar... > services.msc > OK) da seguinte forma. Atualize periodicamente o Serviço (selecione o Serviço > clique com o botão direito do rato > Atualizar) para atualizar o respetivo estado.

- **A aguardar a desativação do SED** – O cliente Encryption continua instalado, continua configurado, ou ambos. A desencriptação não será iniciada antes de o cliente Encryption ser desinstalado.
- **Varrimento inicial** – O Serviço está a realizar um varrimento inicial, calculando o número de ficheiros encriptados e de bytes. O varrimento inicial ocorre uma vez.
- **Varrimento de desencriptação** – O Serviço está a desencriptar ficheiros e, possivelmente, a solicitar a desencriptação de ficheiros bloqueados.
- **Desencriptar no reinício (parcial)** – O varrimento de desencriptação está concluído e alguns ficheiros bloqueados (mas não todos) serão desencriptados no próximo reinício.
- **Desencriptar no reinício** – O varrimento de desencriptação está concluído e todos os ficheiros bloqueados serão desencriptados no próximo reinício.
- **Não foi possível desencriptar todos os ficheiros** – O varrimento de desencriptação foi concluído, mas não foi possível desencriptar todos os ficheiros. Este estado significa que ocorreu uma das seguintes situações:
  - Não foi possível agendar a desencriptação dos ficheiros bloqueados, uma vez que eram demasiado grandes ou ocorreu um erro ao realizar o pedido de desbloqueio dos mesmos.
  - Ocorreu um erro de entrada/saída ao desencriptar os ficheiros.
  - Não foi possível desencriptar os ficheiros através da política.
  - Os ficheiros estão marcados como devendo estar encriptados.
  - Ocorreu um erro durante o varrimento de desencriptação.
  - Em todos os casos, é criado um ficheiro de registo (se estiver configurada a criação de registos) quando estiver definido LogVerbosity=2 (ou superior). Para resolução de problemas, defina a verbosidade do registo para 2 e reinicie o serviço de Agente de Remoção de Encriptação para forçar outro varrimento de desencriptação.
- **Concluído** - O varrimento da desencriptação está concluído. É agendada a eliminação do Serviço, do executável, do controlador e do executável do controlador no próximo reinício.

Controladores do Dell ControlVault

Atualização de controladores e firmware do Dell ControlVault

Os controladores e firmware do Dell ControlVault instalados de fábrica nos computadores Dell estão desatualizados e devem ser atualizados mediante o procedimento abaixo descrito e na ordem em que se encontra.

Se uma mensagem de erro for apresentada durante a instalação do cliente e lhe pedir para sair do programa de instalação para atualizar os controladores do Dell ControlVault, pode seguramente dispensar a mensagem para continuar a instalação do cliente. Os controladores (e firmware) do Dell ControlVault podem ser atualizados após a conclusão da instalação do cliente.

Transferência dos controladores mais recentes

1 Aceda a support.dell.com.
2 Selecione o modelo do seu computador.

3 Selecione **Controladores e transferências**.
4 Selecione o **Sistema operativo** do computador de destino.
5 Expanda a categoria **Segurança**.
6 Transfira e guarde os controladores do Dell ControlVault.
7 Transfira e guarde o firmware do Dell ControlVault.
8 Copie os controladores e o firmware nos computadores de destino, se necessário.

Instale o controlador do Dell ControlVault

Navegue até à pasta para onde transferiu o ficheiro de instalação do controlador.

Clique duas vezes no controlador do Dell ControlVault para iniciar o ficheiro executável de extração automática.

:

Instale o controlador primeiro. O nome de ficheiro do controlador *quando este documento foi criado* é ControlVault_Setup_2MYJC_A37_ZPE.exe.

Clique em **Continuar** para iniciar.

Clique em **Ok** para descomprimir os ficheiros de controladores na localização predefinida em C:\Dell\Drivers\<New Folder>.

Clique em **Sim** para permitir a criação de uma nova pasta.

Clique em **Ok** quando for apresentada a mensagem de que a descompressão dos ficheiros foi bem-sucedida.

A pasta que contém os ficheiros deve ser apresentada após a extração. Caso não seja apresentada, navegue até à pasta na qual extraiu os ficheiros. Neste caso, a pasta é **JW22F**.

Clique duas vezes em **CVHCI64.MSI** para iniciar o programa de instalação dos controladores. [este exemplo é **CVHCI64.MSI** neste modelo (CVHCI para um computador de 32 bits)].

Clique em **Seguinte** no ecrã de boas-vindas.

Clique em **Seguinte** para instalar os controladores na localização predefinida de C:\Program Files\Broadcom Corporation\Broadcom USH Host Components\.

Selecione a opção **Completo** e clique em **Seguinte**.

Clique em **Instalar** para iniciar a instalação dos controladores.

Opcionalmente, marque a caixa para apresentar o ficheiro de registo do programa de instalação. Clique em **Concluir** para sair do assistente.

Verificação da instalação dos controladores

O Gestor de dispositivos terá um dispositivo Dell ControlVault (e outros dispositivos) dependendo da configuração de hardware e do sistema operativo.

Instalação do firmware do Dell ControlVault

1 Navegue até à pasta para onde transferiu o ficheiro de instalação do firmware.
2 Clique duas vezes no firmware do Dell ControlVault para iniciar o ficheiro executável de extração automática.
3 Clique em **Continuar** para iniciar.
4 Clique em **Ok** para descomprimir os ficheiros de controladores na localização predefinida em C:\Dell\Drivers\<New Folder>.
5 Clique em **Sim** para permitir a criação de uma nova pasta.
6 Clique em **Ok** quando for apresentada a mensagem de que a descompressão dos ficheiros foi bem-sucedida.
7 A pasta que contém os ficheiros deve ser apresentada após a extração. Caso não seja apresentada, navegue até à pasta na qual extraiu os ficheiros. Selecione a pasta de **firmware**.
8 Clique duas vezes em **ushupgrade.exe** para iniciar o programa de instalação do firmware.
9 Clique em **Iniciar** para iniciar a atualização do firmware.

:

No caso de atualização a partir de uma versão mais antiga de firmware, ser-lhe-á pedida a palavra-passe de administrador. Introduza **Broadcom** como palavra-passe e clique em **Enter** se esta caixa de diálogo for apresentada.

Várias mensagens de estado serão apresentadas.

10 Clique em **Reiniciar** para concluir a atualização do firmware.

A atualização dos controladores e do firmware do Dell ControlVault foi concluída.

Glossário

Advanced Authentication - O produto Advanced Authentication fornece opções de impressão digital, smart card e leitor de smart card sem contacto totalmente integradas. O Advanced Authentication ajuda a gerir estes múltiplos métodos de autenticação de hardware, suporta o início de sessão com unidades de encriptação automática, SSO e gere as credenciais e palavras-passe do utilizador. Adicionalmente, o Advanced Authentication pode ser utilizado para aceder não apenas a PCs, mas também a qualquer Web site, SaaS ou aplicação. Uma vez que os utilizadores inscrevem as suas credenciais, o Advanced Authentication permite a utilização dessas credenciais para iniciar sessão no dispositivo e realizar a substituição da palavra-passe.

BitLocker Manager - O BitLocker do Windows foi concebido para ajudar a proteger computadores Windows através da encriptação de ficheiros do sistema operativo e dados. Para melhorar a segurança das implementações do BitLocker e para simplificar e reduzir o custo de propriedade, a Dell fornece uma consola de gestão central e única que aborda muitas preocupações de segurança e oferece uma abordagem integrada para gerir a encriptação através de outras plataformas que não o BitLocker, seja de forma física, virtual ou baseada na nuvem. O BitLocker Manager suporta a encriptação do BitLocker para sistemas operativos, unidades fixas e BitLocker To Go. O BitLocker Manager permite-lhe integrar o BitLocker diretamente nas suas necessidades de encriptação existentes e gerir o BitLocker com o mínimo de esforço enquanto agiliza a segurança e conformidade. O BitLocker Manager fornece gestão integrada para a recuperação de chaves, gestão e aplicação de políticas, gestão TPM automatizada, conformidade FIPS e relatórios de conformidade.

Desativar - A desativação ocorre quando a gestão SED é definida para DESLIGADA na Consola de Gestão Remota. Após a desativação do computador, a base de dados da PBA é eliminada e deixa de existir registo dos utilizadores em cache.

EMS - External Media Shield - Este serviço dentro do cliente Dell Encryption aplica políticas a suportes de dados amovíveis e a dispositivos de armazenamento externos.

Código de acesso EMS - Este serviço do Dell Enterprise Server/VE permite a recuperação de dispositivos protegidos pelo External Media Shield, caso o utilizador se esqueça da palavra-passe e não consiga iniciar a sessão. Concluir este processo permite ao utilizador repor a palavra-passe definida no suporte de dados amovível ou no dispositivo de armazenamento externo.

Encryption Client - O Encryption Client é o componente no dispositivo que aplica as políticas de segurança, quer o endpoint esteja ligado à rede, desligado da rede, ou seja perdido ou roubado. Ao criar um ambiente de computação fidedigno para endpoints, o cliente Encryption funciona como uma camada no topo do sistema operativo do dispositivo e proporciona autenticação, encriptação e autorização aplicadas de forma consistente para maximizar a proteção de informações sensíveis.

Ponto final - Um computador portátil ou dispositivo de hardware móvel gerido pelo Dell Enterprise Server/VE.

Varrimento de encriptação - Um varrimento de encriptação é o processo de análise das pastas a serem encriptadas num ponto final gerido para assegurar que os ficheiros contidos estão no estado de encriptação adequado. As operações comuns de criação e mudança de nome de ficheiros não acionam um varrimento de encriptação. É importante entender quando pode ocorrer um varrimento de encriptação e o que pode afetar os tempos de varrimento resultantes, como se segue: - Um varrimento de encriptação irá ocorrer após a receção inicial de uma política com a encriptação ativada. Isto pode ocorrer imediatamente depois da ativação se a sua política tem a encriptação ativada. - Se a Estação de trabalho de análise na Política de início de sessão está ativada, as pastas especificadas para a encriptação serão submetidas a varrimento em cada início de sessão do utilizador. - Um varrimento pode ser acionado novamente sob determinadas alterações de política subsequentes. Qualquer alteração de política relacionada com a definição das pastas de encriptação, algoritmos de encriptação, utilização da chave de encriptação (como vs. utilizador), acionará um varrimento. Adicionalmente, a alternância entre a encriptação ativada e desativada irá acionar um varrimento de encriptação.

Chave de computador – Quando a encriptação está instalada num servidor, a chave de Computador protege as chaves de políticas e encriptação de ficheiros de um servidor. A Chave de Computador é armazenada no Dell Enterprise Server/VE. O novo Servidor troca de certificados com o Servidor DDP no decurso da ativação e usa o certificado nos eventos de autenticação subsequentes.

Palavra-Passe monouso (OTP) - Uma palavra-passe monouso é uma palavra-passe que apenas pode ser utilizada uma vez e que é válida por um período de tempo limitado. A OTP requer que o TPM esteja presente, ativado e tenha proprietário. Para ativar a palavra-passe monouso (OTP), um dispositivo móvel é emparelhado com o computador que está a utilizar a Consola de segurança e a aplicação Security Tools Mobile. A aplicação Security Tools Mobile gera a palavra-passe no dispositivo móvel que é utilizado para iniciar sessão no computador no ecrã de início de sessão do Windows. Com base na politica, a funcionalidade OTP pode ser utilizada para recuperar o acesso ao computador se uma palavra-passe expirou ou foi esquecida, se a OTP não foi utilizada para iniciar sessão no computador. A funcionalidade OTP pode ser utilizada para autenticação ou recuperação, mas não para ambas. A segurança da OTP excede a de outros métodos de autenticação, uma vez que a palavra-passe gerada apenas pode ser utilizada uma vez e expira num curto período de tempo.

Gestão SED - A Gestão SED disponibiliza uma plataforma para gerir de forma segura as unidades de encriptação automática. Embora as SEDs forneçam a sua própria encriptação, carecem de uma plataforma para gerir a sua encriptação e políticas disponíveis. A Gestão de SED é uma componente de gestão central e escalável que lhe permite proteger e gerir os seus dados de forma mais eficaz. A Gestão de SED assegura que será capaz de administrar a sua empresa de forma mais rápida e fácil.

Utilizador de servidor – Uma conta de utilizador virtual criada pelo Dell Server Encryption para gestão das atualizações de políticas e chaves de encriptação. Esta conta de utilizador não corresponde a nenhuma outra conta de utilizador do computador ou do domínio, não tendo nome de utilizador ou palavra-passe que possa ser fisicamente utilizada. É atribuído à conta um valor UCID exclusivo na Consola de Gestão Remota do Dell Enterprise Server/VE.