


# Dell Encryption Enterprise

## Advanced Installation Guide v11.9

## Notas, avisos e advertências

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

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

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

© 2012-2024 Dell Inc. All rights reserved. Registered trademarks and trademarks used in the Dell Encryption and Endpoint Security Suite Enterprise suite of documents: Dell™ and the Dell logo, Dell Precision™, OptiPlex™, ControlVault™, Latitude™, XPS®, and KACE™ are trademarks of Dell Inc. Cylance®, CylancePROTECT, and the Cylance logo are registered trademarks of Cylance, Inc. in the U.S. and other countries. McAfee® and the McAfee logo are trademarks or registered trademarks of McAfee, Inc. in the US and other countries. Intel®, Pentium®, Intel Core Inside Duo®, Itanium®, and Xeon® are registered trademarks of Intel Corporation in the U.S. and other countries. Adobe®, Acrobat®, and Flash® are registered trademarks of Adobe Systems Incorporated. Authen tec® and Eikon® are registered trademarks of Authen tec. AMD® is a registered trademark of Advanced Micro Devices, Inc. Microsoft®, Windows®, and Windows Server®, Windows Vista®, Windows 10®, Active Directory®, Access®, BitLocker®, BitLocker To Go®, Excel®, Hyper-V®, Outlook®, PowerPoint®, Word®, OneDrive®, SQL Server®, and Visual C++® are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. VMware® is a registered trademark or trademark of VMware, Inc. in the United States and other countries. Box® is a registered trademark of Box. Dropbox<sup>SM</sup> is a service mark of Dropbox, Inc. Google™, Android™, Google™ Chrome™, Gmail™, and Google™ Play are either trademarks or registered trademarks of Google Inc. in the United States and other countries. Apple®, App Store<sup>SM</sup>, Apple Remote Desktop™, Boot Camp™, FileVault™, iPad®, iPhone®, iPod®, iPod touch®, iPod shuffle®, and iPod nano®, Macintosh®, and Safari® are either servicemarks, trademarks, or registered trademarks of Apple, Inc. in the United States and/or other countries. EnCase™ and Guidance Software® are either trademarks or registered trademarks of Guidance Software. Entrust® is a registered trademark of Entrust®, Inc. in the United States and other countries. Mozilla® Firefox® is a registered trademark of Mozilla Foundation in the United States and/or other countries. iOS® is a trademark or registered trademark of Cisco Systems, Inc. in the United States and certain other countries and is used under license. Oracle® and Java® are registered trademarks of Oracle and/or its affiliates. Travelstar® is a registered trademark of HGST, Inc. in the United States and other countries. UNIX® is a registered trademark of The Open Group. VALIDITY™ is a trademark of Validity Sensors, Inc. in the United States and other countries. VeriSign® and other related marks are the trademarks or registered trademarks of VeriSign, Inc. or its affiliates or subsidiaries in the U.S. and other countries and licensed to Symantec Corporation. KVM on IP® is a registered trademark of Video Products. Yahoo!® is a registered trademark of Yahoo! Inc. Bing® is a registered trademark of Microsoft Inc. Ask® is a registered trademark of IAC Publishing, LLC. Other names may be trademarks of their respective owners.

|                                                                                 |           |
|---------------------------------------------------------------------------------|-----------|
| <b>Chapter 1: Introdução.....</b>                                               | <b>6</b>  |
| Antes de começar.....                                                           | 6         |
| Utilizar este guia.....                                                         | 6         |
| Contacte o Dell ProSupport for Software.....                                    | 7         |
| <b>Chapter 2: Requisitos.....</b>                                               | <b>8</b>  |
| Todos os clientes.....                                                          | 8         |
| Encryption.....                                                                 | 9         |
| Full Disk Encryption.....                                                       | 11        |
| <b>Encryption em sistemas operativos de servidor.....</b>                       | <b>13</b> |
| SED Manager.....                                                                | 16        |
| BitLocker Manager.....                                                          | 19        |
| <b>Chapter 3: Definições de registo.....</b>                                    | <b>22</b> |
| Encryption.....                                                                 | 22        |
| SED Manager.....                                                                | 26        |
| Full Disk Encryption.....                                                       | 28        |
| BitLocker Manager.....                                                          | 30        |
| <b>Chapter 4: Instalar utilizando o instalador principal.....</b>               | <b>31</b> |
| Instalar interativamente utilizando o instalador principal.....                 | 31        |
| Instalar por linha de comandos utilizando o instalador principal.....           | 32        |
| <b>Chapter 5: Desinstalar o Instalador Principal.....</b>                       | <b>34</b> |
| Desinstalar o Instalador Principal do .....                                     | 34        |
| <b>Chapter 6: Instalar utilizando instaladores subordinados.....</b>            | <b>35</b> |
| Instalar controladores.....                                                     | 36        |
| Instalar o Encryption.....                                                      | 36        |
| Instalar a Full Disk Encryption.....                                            | 40        |
| Instalar o Encryption em sistemas operativos de servidor.....                   | 41        |
| Instalar interativamente.....                                                   | 42        |
| Instalar utilizando a Linha de comandos.....                                    | 43        |
| Ativar.....                                                                     | 45        |
| Instalar o SED Manager e a Autenticação Avançada PBA.....                       | 46        |
| Instalar o BitLocker Manager.....                                               | 47        |
| <b>Chapter 7: Desinstalar utilizando os instaladores subordinados.....</b>      | <b>49</b> |
| Desinstalar o Encryption e o Encryption em sistemas operativos de servidor..... | 50        |
| Desinstalar o Full Disk Encryption.....                                         | 52        |
| Desinstalar o SED Manager.....                                                  | 53        |
| Desinstalar o BitLocker Manager.....                                            | 54        |
| <b>Chapter 8: Desinstalador do Data Security.....</b>                           | <b>55</b> |

|                                                                                                                      |               |
|----------------------------------------------------------------------------------------------------------------------|---------------|
| <b>Chapter 9: Cenários normalmente utilizados.....</b>                                                               | <b>56</b>     |
| Cliente de encriptação, , e .....                                                                                    | 57            |
| SED Manager (incluindo a Autenticação Avançada) e o Encryption Client.....                                           | 57            |
| SED Manager e Encryption External Media.....                                                                         | 58            |
| BitLocker Manager e Encryption External Media.....                                                                   | 58            |
| <br><b>Chapter 10: Transferir o software.....</b>                                                                    | <br><b>59</b> |
| <br><b>Chapter 11: Configuração da pré-instalação para UEFI SED e BitLocker Manager.....</b>                         | <br><b>60</b> |
| Inicializar o TPM.....                                                                                               | 60            |
| Configuração da pré-instalação para computadores UEFI.....                                                           | 60            |
| Configuração da pré-instalação para configurar uma partição de PBA do BitLocker.....                                 | 61            |
| <br><b>Chapter 12: Designar o Dell Server através do Registo.....</b>                                                | <br><b>62</b> |
| <br><b>Chapter 13: Extrair os instaladores subordinados.....</b>                                                     | <br><b>63</b> |
| <br><b>Chapter 14: Configurar o Key Server.....</b>                                                                  | <br><b>64</b> |
| Painel de Serviços - Adicionar utilizador da conta do domínio.....                                                   | 64            |
| Ficheiro de configuração do Key Server - Adicionar utilizador para comunicação com o Security Management Server..... | 64            |
| Painel de Serviços - Reiniciar o serviço Key Server.....                                                             | 65            |
| Management Console - Adicionar administrador forense.....                                                            | 65            |
| <br><b>Chapter 15: Utilizar o Administrative Download Utility (CMGAd).....</b>                                       | <br><b>67</b> |
| Utilizar o Modo forense.....                                                                                         | 67            |
| Utilizar o Modo de administrador.....                                                                                | 67            |
| <br><b>Chapter 16: Configurar o Encryption em sistemas operativos de servidor.....</b>                               | <br><b>69</b> |
| <br><b>Chapter 17: Configurar a Ativação diferida.....</b>                                                           | <br><b>72</b> |
| Personalização da Ativação diferida.....                                                                             | 72            |
| Preparar o computador para instalação.....                                                                           | 72            |
| Instalar o Encryption com Ativação diferida.....                                                                     | 73            |
| Ativar o Encryption com a Ativação diferida.....                                                                     | 73            |
| Resolução de problemas da Ativação diferida.....                                                                     | 74            |
| <br><b>Chapter 18: Resolução de problemas.....</b>                                                                   | <br><b>76</b> |
| Todos os clientes - Resolução de problemas.....                                                                      | 76            |
| Todos os clientes - Estado de Proteção.....                                                                          | 76            |
| Resolução de problemas do Dell Encryption (cliente e servidor) .....                                                 | 76            |
| Resolução de problemas SED.....                                                                                      | 84            |
| Controladores do Dell ControlVault.....                                                                              | 85            |
| Atualização de controladores e firmware do Dell ControlVault.....                                                    | 85            |
| Computadores UEFI.....                                                                                               | 88            |
| TPM e BitLocker.....                                                                                                 | 88            |

**Chapter 19: Glossário..... 118**

# Introdução

Este guia explica como instalar e configurar o Encryption, SED Management, Full Disk Encryption, Web Protection and Client Firewall e BitLocker Manager.

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

## Antes de começar

1. Instale o Dell 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 Security Management Server](#)
  - [Guia de instalação e Guia de início rápido do Security Management Server Virtual](#)
  - Certifique-se de que as políticas foram definidas da forma pretendida. Navegue no AdminHelp, disponível através de **?** no canto superior 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 Dell Server.
2. Leia atentamente o capítulo [Requisitos](#) deste documento.
3. Implemente os clientes para utilizadores.

## Utilizar este guia

Utilize este guia pela seguinte ordem.

- Consulte [Requisitos](#) para obter informações sobre os pré-requisitos do cliente, hardware do computador e informações, limitações e modificações de registo especiais do software necessárias às funcionalidades.
- Se necessário, consulte [Configuração da pré-instalação para UEFI SED e BitLocker](#).
- Se os seus clientes forem elegíveis para utilizar o Dell Digital Delivery, consulte [Definir GPO no controlador do domínio para ativar elegibilidades](#).
- Se instalar clientes utilizando o instalador principal do , consulte:
  - [Instalar interativamente utilizando o instalador principal](#)  
ou em
  - [Instalar por linha de comandos utilizando o instalador principal](#)
- Se instalar clientes utilizando os instaladores subordinados, os ficheiros executáveis do instalador subordinado devem ser extraídos do instalador principal. Consulte [Extrair os Instaladores Subordinados do Instalador Principal](#) e, em seguida, regresse aqui.
  - Instalar instaladores subordinados através da linha de comandos:
    - [Instalar o Encryption](#) - utilize estas instruções para instalar o Encryption, que é o componente que aplica a política de segurança, quer o computador esteja ligado à rede, desligado da rede, ou seja perdido ou roubado.
    - [Instalar o cliente da Full Disk Encryption](#) - utilize estas instruções para instalar a Full Disk Encryption, que é o componente que aplica a política de segurança, quer o computador esteja ligado à rede, desligado da rede, ou seja perdido ou roubado.
    - [Instalar o SED Manager](#) – utilize estas instruções para instalar software de encriptação para SED. Embora as SED forneçam a sua própria encriptação, carecem de uma plataforma para gerir a sua encriptação e políticas. Com o SED Manager, todas as políticas, o armazenamento e a recuperação de chaves de encriptação ficam disponíveis numa só consola, reduzindo o risco de os computadores ficarem desprotegidos em caso de perda de acesso ou acesso não autorizado.
    - [Instalar o BitLocker Manager](#) - utilize estas instruções para instalar o BitLocker Manager, concebido para melhorar a segurança das implementações do BitLocker e para simplificar e reduzir o custo de propriedade.



**NOTA:**

A maioria dos instaladores subordinados pode ser instalado interativamente, mas o processo não é descrito neste guia.

- Consulte [Cenários normalmente utilizados](#) para obter scripts dos nossos cenários mais comuns.

## Contacte o Dell ProSupport for Software

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

Adicionalmente, o suporte online para os produtos Dell encontra-se disponível em [dell.com/support](https://dell.com/support). O suporte online inclui controladores, manuais, conselhos técnicos, perguntas frequentes e problemas emergentes.

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

Para números de telefone fora dos Estados Unidos, consulte [Números de telefone internacionais do Dell ProSupport for Software](#).

# Requisitos

## Todos os clientes

Estes requisitos aplicam-se a todos os clientes. Os requisitos indicados nas outras seções aplicam-se a clientes específicos.

- 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, o qual pode ser atribuído temporariamente por uma ferramenta de implementação, como o Microsoft SCCM. 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.
- Os administradores devem assegurar a disponibilidade de todas as portas necessárias.
- Certifique-se de que verifica periodicamente a página [dell.com/support](http://dell.com/support) para procurar a documentação e os avisos técnicos mais atuais.
- A linha de produtos Dell Data Security não é compatível com as versões do Windows Insider Preview.

## 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 os componentes Microsoft .Net Framework.
- Para verificar a versão instalada do Microsoft .Net, siga [estas](#) instruções no computador onde pretende efetuar a instalação. Consulte [estas](#) instruções para instalar o Microsoft .Net Framework 4.5.2.
- Se instalar o Encryption no modo FIPS, é necessário o Microsoft .Net Framework 4.6.

## Hardware

- A seguinte tabela apresenta o hardware de computador **mínimo** suportado.

| Hardware                                                                                                                                                                                                                                                                                                                              |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>○ Processador Intel Pentium ou AMD</li> <li>○ 110 MB de espaço livre em disco</li> <li>○ 512 MB de RAM</li> </ul> <p><b>NOTA:</b> É necessário espaço livre em disco adicional para encriptar ficheiros no endpoint. O tamanho varia de acordo com as políticas e a capacidade da unidade.</p> |

## Localização

- O Dell Encryption, o SED Manager, a autenticação avançada PBA, o e o e o BitLocker Manager estão em conformidade com a norma de interface de utilizador multilíngue e estão localizados nos seguintes idiomas.

| Suporte de idiomas |               |                           |
|--------------------|---------------|---------------------------|
| EN - Inglês        | IT - Italiano | KO - Coreano              |
| ES - Espanhol      | DE - Alemão   | PT-BR - Português, Brasil |

| Suporte de idiomas |              |                                       |
|--------------------|--------------|---------------------------------------|
| FR - Francês       | JA - Japonês | PT-PT - Português, Portugal (Ibérico) |

## Encryption

- O computador cliente deve ter conectividade de rede para ativar.
- Para ativar uma conta Microsoft Live com o Dell Encryption, consulte o artigo [124722](#) da BDC.
- Para reduzir o tempo de encriptação inicial, execute o Assistente de limpeza de disco do Windows para remover ficheiros temporários e quaisquer outros dados desnecessários.
- O suporte do Windows Hello for Business requer o Encryption Enterprise v11.0 ou posterior no Windows 10.
- O suporte do Windows Hello for Business requer a ativação num Dell Server com a versão v11.0 ou posterior.
- 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 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 Dell Encryption não pode ser atualizado para a v10.7.0 a partir de versões anteriores à v8.16.0. Os pontos terminais com versões anteriores à v8.16.0 têm de ser atualizados para a v8.16.0 e, posteriormente, atualizados para a v10.7.0.
- O instalador principal não suporta atualizações a partir de componentes anteriores à v8.0. Extraia os instaladores subordinados do instalador principal e atualize o componente individualmente. Consulte [Extrair os Instaladores Subordinados do Instalador Principal](#) para obter instruções sobre a extração.
- O Encryption agora suporta o modo Audit. O modo Audit permite que os administradores implementem o Encryption como parte da imagem corporativa, em vez de usar um SCCM de outros fabricantes ou uma solução semelhante. Para obter instruções sobre como instalar o Encryption numa imagem corporativa, consulte o artigo [129990](#) da BDC.
- O cliente de encriptação foi sujeito a testes e é compatível com vários antivírus baseados em assinatura populares e soluções antivírus baseadas em inteligência artificial, incluindo McAfee Virus Scan Enterprise, McAfee Endpoint Security, Symantec Endpoint Protection, CylancePROTECT, CrowdStrike Falcon, Carbon Black Defense e vários outros. As exclusões impostas estão incluídas por predefinição em muitos fornecedores de antivírus para evitar incompatibilidades entre a análise de vírus e a encriptação.

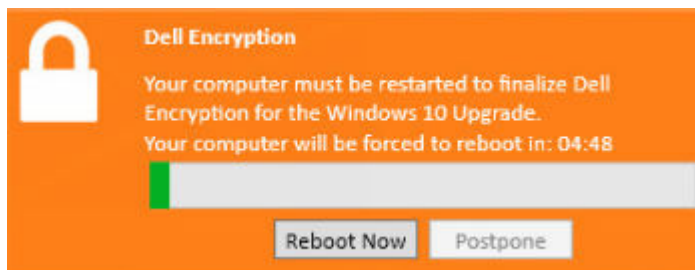
No caso de a sua organização utilizar um antivírus de um fornecedor que não esteja na lista, ou se estiver a experienciar quaisquer problemas de compatibilidade, consulte o artigo [126046](#) da BDC ou [contacte o Dell ProSupport](#) para obter assistência na validação da configuração de interoperabilidade entre as suas soluções de software e as soluções Dell Data Security.

- O Dell Encryption utiliza o conjunto de instruções de encriptação da Intel, Integrated Performance Primitives (IPP). Para obter mais informações, consulte o artigo [126015](#) da BDC.
- O TPM é utilizado para selar a General Purpose Key. Assim, se o Encryption for executado, limpe o TPM no BIOS antes de proceder à instalação de um novo sistema operativo no computador de destino.
- Não são suportadas reinstalações de sistema operativo no local. 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.
- O instalador principal instala estes componentes se ainda não estiverem instalados no computador de destino. **Quando utilizar o instalador subordinado**, deve instalar estes componentes antes de instalar os clientes.

| Pré-requisito                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>○ Visual C++ 2012 Update 4 ou Redistributable Package posterior (x86 ou x64)</li> <li>○ Visual C++ 2017 ou Redistributable Package posterior (x86 ou x64)</li> <li>○ Desde janeiro de 2020, os certificados de assinatura SHA1 deixam de ser válidos e não podem ser renovados. Os dispositivos que executam o Windows Server 2008 R2 devem instalar os artigos da BDC da Microsoft <a href="https://support.microsoft.com/help/4474419">https://support.microsoft.com/help/4474419</a> e <a href="https://support.microsoft.com/help/4490628">https://support.microsoft.com/help/4490628</a> para validar os certificados de assinatura SHA256 nas aplicações e nos pacotes de instalação.</li> </ul> <p>As aplicações e os pacotes de instalação com certificados de assinatura SHA1 irão funcionar, mas sem estas atualizações instaladas será apresentado um erro no ponto terminal durante a instalação ou a execução da aplicação</p> |

- As políticas *Ficheiro de hibernação do Windows seguro* e *Impedir hibernação não segura* não são suportadas no modo UEFI.

- A ativação diferida permite que a conta de utilizador do Active Directory utilizada durante a ativação seja independente da conta utilizada para iniciar sessão no ponto terminal. Em vez de o fornecedor de serviços de rede capturar as informações de autenticação, o utilizador especifica a conta baseada no Active Directory manualmente quando solicitado. Depois de serem introduzidas as credenciais, a informação de autenticação é enviada de uma forma segura para o Dell Server que a valida relativamente aos domínios do Active Directory configurados. Para obter mais informações, consulte o artigo [124736](#) da BDC.
- Após a atualização de funcionalidades do Windows 10, é **necessário** reiniciar para finalizar o Dell Encryption. A seguinte mensagem é exibida na área de notificação após as atualizações de funcionalidades do Windows 10:



## Hardware

- A tabela seguinte indica o hardware suportado.

| Hardware opcional incorporado                                      |
|--------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>○ TPM 1.2 ou 2.0</li> </ul> |

## Sistemas operativos

- A tabela seguinte apresenta os sistemas operativos suportados.

| Sistemas operativos Windows (32 e 64 bits)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>○ Windows 10: Education, Enterprise, Pro v1909-v22H2 (Atualização de novembro de 2019/19H2 — Atualização de novembro de 2022/22H2)</li> </ul> <p><b>Nota:</b> os OEMs e ODMs não são fornecidos com o Windows 10 v2004 (Atualização de maio de 2020/20H1 e posterior) com a arquitetura de 32 bits. Para obter mais informações, consulte <a href="https://docs.microsoft.com/windows-hardware/design/minimum/minimum-hardware-requirements-overview">https://docs.microsoft.com/windows-hardware/design/minimum/minimum-hardware-requirements-overview</a>.</p> <ul style="list-style-type: none"> <li>▪ Windows 10 2019 LTSC</li> <li>▪ Windows 10 2021 LTSC</li> </ul> <li>○ Windows 11: Enterprise, Pro v21H2 —22H2</li> <li>○ A <b>Ativação diferida</b> inclui suporte para todos os sistemas operativos acima</li> |

## Encryption External Media

### Sistemas operativos

- O suporte de dados externo tem de ter aproximadamente 55 MB disponíveis, bem como espaço livre no suporte de dados igual ao maior ficheiro a encriptar para alojar o Encryption External Media.
- A seguinte tabela indica os sistemas operativos compatíveis ao aceder a suportes de dados protegidos pelo Encryption External Media:

| Sistemas operativos Windows compatíveis para aceder a suportes de dados encriptados (32 e 64 bits)                                                                                   |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>○ Windows 10: Education, Enterprise, Pro v1909-v22H2 (Atualização de novembro de 2019/19H2 — Atualização de novembro de 2022/22H2)</li> </ul> |

### Sistemas operativos Windows compatíveis para aceder a suportes de dados encriptados (32 e 64 bits)

**Nota:** os OEMs e ODMs não são fornecidos com o Windows 10 v2004 (Atualização de maio de 2020/20H1 e posterior) com a arquitetura de 32 bits. Para obter mais informações, consulte <https://docs.microsoft.com/windows-hardware/design/minimum/minimum-hardware-requirements-overview>.

- Windows 10 2019 LTSC
- Windows 10 2021 LTSC
- Windows 11: Enterprise, Pro v21H2 —22H2
- A **Ativação diferida** inclui suporte para todos os sistemas operativos acima

### Sistemas operativos Mac compatíveis para aceder a suportes de dados encriptados (kernels de 64 bits)

- macOS High Sierra 10.13.5–10.13.6
- macOS Mojave 10.14.0–10.14.4
- macOS Catalina 10.15.5–10.15.6

## Full Disk Encryption

- A Full Disk Encryption requer ativação num Dell Server de versão v9.8.2 ou posterior.
- Atualmente, a Full Disk Encryption não é suportada em computadores do sistema anfitrião virtualizado.
- A Full Disk Encryption necessita de um TPM de hardware separado. De momento, os TPMs com base em firmware e em PTT não são suportados.
- Os fornecedores de credenciais de outros fabricantes não funcionarão com funcionalidades FDE instaladas e todos serão desativados quando a PBA for ativada.
- O computador cliente deve ter conectividade de rede ou um código de acesso para ativar.
- O computador tem de possuir uma ligação de rede com fios para que um utilizador de smart card possa iniciar sessão através da autenticação de pré-arranque pela primeira vez.
- As atualizações de funcionalidades do sistema operativo não são suportadas com o Full Disk Encryption.
- É necessária uma ligação com fios para que a PBA comunique com o Dell Server.
- Não pode estar presente uma SED no computador de destino.
- A Full Disk Encryption não é compatível com o BitLocker ou o BitLocker Manager. Não instale a Full Disk Encryption num computador que tenha o BitLocker ou o BitLocker Manager instalado.
- A Dell recomenda o controlador Intel Rapid Storage Technology mais recente com unidades NVMe.
- Qualquer unidade NVMe que esteja a ser utilizada para PBA:
  - Se o dispositivo Dell tiver sido fabricado em 2018 ou mais tarde: o RAID ON ou AHCI podem ser utilizados com unidades NVMe.
  - O modo de arranque do BIOS tem de ser definido para Unified Extensible Firmware Interface (UEFI). As ROMs de funcionamento antigas têm de ser desativadas.
- Qualquer unidade não-NVMe que esteja a ser utilizada para PBA:
  - A operação SATA do BIOS pode ser definida para AHCI ou RAID ON.
  - O sistema operativo falha quando alterado de RAID ON > AHCI, se os controladores do AHCI não estiverem pré-instalados. Para obter instruções sobre como alterar de RAID > AHCI (ou vice-versa), consulte o artigo [124714](#) da BDC.
- A gestão da Full Disk Encryption não é compatível com 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.
- Não são suportadas reinstalações de sistema operativo no local. 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.
- As Atualizações de Funcionalidades Diretas do Windows 10 v1607 (Atualização de Aniversário/Redstone 1) para o Windows 10 v1903 (Atualização de maio de 2019/19H1) não são suportadas com o FDE. A Dell recomenda a atualização do sistema operativo para uma Atualização de Funcionalidades mais recente se estiver a atualizar para o Windows 10 v1903. Qualquer tentativa de atualização direta do Windows 10 v1607 para o v1903 resulta numa mensagem de erro e a atualização é impedida.
- Todos os discos têm de ser inicializados e formatados antes de ativar a Full Disk Encryption.
- As configurações de encriptação em vários discos com o Full Disk Encryption exigem as seguintes condições:
  - Todos os discos do sistema de destino têm de ter a seguinte configuração:

- Unidades não-SED
- Configurados no mesmo modo de arranque
- Inicializados como Tabela de Partições GUID (GPT)
- Os discos têm de ser partições primárias
- Os discos têm de ter uma letra de unidade atribuída
- É necessário reiniciar para encriptar novos discos após a configuração inicial.
- É possível encriptar um máximo de 16 discos.
- No modo de arranque UEFI, o sistema operativo pode ser instalado em qualquer disco de destino.
- No modo de arranque Legacy, o sistema operativo tem de ser instalado no primeiro disco (Disco n.º 0). Se o sistema operativo não estiver instalado no primeiro disco, a encriptação em vários discos é desativada.

Ative a Encriptação em vários discos na Consola de Gestão. Consulte as [Definições de Registo](#) para ver os valores do Registo do Windows relativamente à Encriptação em vários discos e varrimento múltiplo.

- A Full Disk Encryption requer a utilização do fornecedor de credenciais personalizado da Dell para sincronizar as alterações de palavra-passe do Windows e as chaves de encriptação de dados. Se precisar de utilizar aplicações de terceiros que utilizam fornecedores de credenciais personalizados executados em computadores protegidos por Full Disk Encryption, terá de iniciar alterações de palavra-passe do Windows através da Data Security Console. Para obter mais informações sobre como alterar a palavra-passe na Data Security Console, consulte o capítulo *Palavra-passe* no [Guia do utilizador da Data Security Console](#).
- O instalador principal instala estes componentes se ainda não estiverem instalados no computador de destino. **Quando utilizar o instalador subordinado**, deve instalar estes componentes antes de instalar os clientes.

#### Pré-requisito

- Visual C++ 2017 ou Redistributable Package posterior (x86 ou x64)
  - Desde janeiro de 2020, os certificados de assinatura SHA1 deixam de ser válidos e não podem ser renovados. Os dispositivos que executam o Windows Server 2008 R2 devem instalar os artigos da BDC da Microsoft <https://support.microsoft.com/help/4474419> e <https://support.microsoft.com/help/4490628> para validar os certificados de assinatura SHA256 nas aplicações e nos pacotes de instalação.
- As aplicações e os pacotes de instalação com certificados de assinatura SHA1 irão funcionar, mas sem estas atualizações instaladas será apresentado um erro no ponto terminal durante a instalação ou a execução da aplicação

- **NOTA:** É necessária uma palavra-passe com autenticação de pré-arranque. A Dell recomenda a definição de um comprimento mínimo da palavra-passe, de acordo com as políticas de segurança internas.
- **NOTA:** Quando é utilizada a PBA, a política Sincronizar Todos os Utilizadores deve ser ativada se um computador tiver vários utilizadores. Além disso, todos os utilizadores devem ter palavras-passe. Os utilizadores sem palavras-passe serão bloqueados e ficarão sem acesso ao computador após a ativação.
- **NOTA:** Os computadores protegidos pelo Full Disk Encryption têm de ser atualizados para o Windows 10 v1703 (Atualização para Criativos/Redstone 2) ou posterior antes de serem atualizados para o Windows 10 v1903 (Atualização de maio de 2019/19H1) ou posterior. Se tentar este procedimento de atualização, é apresentada uma mensagem de erro.
- **NOTA:** A Full Disk Encryption deve ser configurada com o Algoritmo de encriptação definido como AES -256 e o Modo de encriptação definido como CBC.

## Hardware

- A tabela seguinte indica o hardware suportado.

#### Hardware opcional incorporado

- TPM 1.2 ou 2.0

## Opções de autenticação com o cliente da Full Disk Encryption

- É necessário um hardware específico, para utilizar smart cards e para autenticar em computadores UEFI. É necessária uma configuração para utilizar smart cards com autenticação de pré-arranque. As tabelas seguintes apresentam as opções de autenticação disponíveis por sistema operativo, quando os requisitos de hardware e de configuração são cumpridos.

| UEFI       |                                       |                   |                        |             |
|------------|---------------------------------------|-------------------|------------------------|-------------|
|            | PBA — em computadores Dell suportados |                   |                        |             |
|            | Palavra-passe                         | Impressão digital | Smart card de contacto | Cartão SIPR |
| Windows 10 | X <sup>1</sup>                        |                   | X <sup>1</sup>         |             |
| Windows 11 | X <sup>1</sup>                        |                   | X <sup>1</sup>         |             |

1. Disponível com computadores UEFI compatíveis.

## Modelos de computador Dell compatíveis com modo de arranque UEFI

- Para aceder à lista mais atualizada de plataformas suportadas pelo Full Disk Encryption, consulte o artigo [126855](#) da BDC.
- Para obter uma lista das estações de acoplamento e adaptadores compatíveis com o Full Disk Encryption, consulte o artigo [124241](#) da BDC.

## Sistemas operativos

- A tabela seguinte apresenta os sistemas operativos suportados.

| Sistemas operativos Windows (64 bits)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"><li>○ Windows 10: Education, Enterprise, Pro v1909-v22H2 (Atualização de novembro de 2019/19H2 — Atualização de novembro de 2022/22H2)<br/><b>Nota:</b> os OEMs e ODMs não são fornecidos com o Windows 10 v2004 (Atualização de maio de 2020/20H1 e posterior) com a arquitetura de 32 bits. Para obter mais informações, consulte <a href="https://docs.microsoft.com/windows-hardware/design/minimum/minimum-hardware-requirements-overview">https://docs.microsoft.com/windows-hardware/design/minimum/minimum-hardware-requirements-overview</a>.<ul style="list-style-type: none"><li>▪ Windows 10 2019 LTSC</li><li>▪ Windows 10 2021 LTSC</li></ul></li><li>○ Windows 11: Enterprise, Pro v21H2 — 22H2</li></ul> |

## Encryption em sistemas operativos de servidor

O Encryption em sistemas operativos de servidor destina-se a ser utilizado em computadores no modo de servidor, particularmente em servidores de ficheiros.

- O Encryption em sistemas operativos de servidor apenas é compatível com o Encryption Enterprise e com o Endpoint Security Suite Enterprise.
- O Encryption em sistemas operativos de servidor fornece:
  - A encriptação do software
  - Encriptação de suportes de dados amovíveis
  - Controlo de portas

### **NOTA:**

O servidor terá de suportar controlo de portas.

As políticas do Sistema de controlo de portas afetam os suportes de dados amovíveis em servidores protegidos, por exemplo, controlando o acesso e a utilização das portas USB do servidor pelos dispositivos USB. A política da porta USB aplica-se às portas USB externas. A funcionalidade das portas USB internas não é afetada pela política de portas USB. Se a política de portas USB estiver desativada, o teclado e o rato USB do cliente não funcionam e o utilizador não pode utilizar o computador, salvo se, antes da aplicação da política, for estabelecida uma Ligação ao Ambiente de Trabalho Remoto.

- O instalador principal instala estes componentes se ainda não estiverem instalados no computador de destino. **Quando utilizar o instalador subordinado**, deve instalar estes componentes antes de instalar os clientes.

#### Pré-requisito

- Visual C++ 2012 Update 4 ou Redistributable Package posterior (x86 ou x64)
- Visual C++ 2017 ou Redistributable Package posterior (x86 ou x64)
- Desde janeiro de 2020, os certificados de assinatura SHA1 deixam de ser válidos e não podem ser renovados. Os dispositivos que executam o Windows Server 2008 R2 devem instalar os artigos da BDC da Microsoft <https://support.microsoft.com/help/4474419> e <https://support.microsoft.com/help/4490628> para validar os certificados de assinatura SHA256 nas aplicações e nos pacotes de instalação.

As aplicações e os pacotes de instalação com certificados de assinatura SHA1 irão funcionar, mas sem estas atualizações instaladas será apresentado um erro no ponto terminal durante a instalação ou a execução da aplicação

#### O Encryption em sistemas operativos de servidor é utilizado para:

- Servidores de ficheiros com unidades de disco locais
- Convidados de Máquina Virtual (VM) com sistema operativo de servidor ou um sistema operativo que não seja de servidor funcionando simplesmente como servidor de ficheiros
- Configurações suportadas:
  - Servidores equipados com unidades RAID 5 ou 10; RAID 0 (striping) e RAID 1 (espelhamento) são suportados de forma independente um do outro.
  - Servidores equipados com unidades multi TB RAID
  - Servidores equipados com unidades que possam ser substituídas sem ter de desligar o computador
  - A Server Encryption é validada face a fornecedores de antivírus líderes do sector. Existem exclusões pré-programadas para estes fornecedores de antivírus, por forma evitar incompatibilidades entre a deteção de vírus e a encriptação. No caso de a sua organização utilizar um antivírus de um fornecedor que não esteja na lista, consulte o artigo [126046](#) da BDC ou [contacte o Dell ProSupport](#) para obter assistência.

#### O Encryption em sistemas operativos de servidor não é utilizado para:

- Security Management Servers/Security Management Server Virtuals ou servidores a executar bases de dados para Security Management Servers/Security Management Server Virtual.
- Encryption Personal.
- SED Manager, autenticação avançada PBA ou BitLocker Manager.
- Servidores que fazem parte de sistemas de ficheiros distribuídos (DFS).
- Migração para ou a partir do Encryption num sistema operativo de servidor. A atualização do External Media Edition para o Encryption em sistemas operativos de servidor requer a desinstalação completa do produto anterior antes de instalar o Encryption em sistemas operativos de servidor.
- Anfitriões VM (Uma VM contém, tipicamente, múltiplos convidados VM.)
- Controladores de Domínio
- Servidores Exchange
- Servidores que alberguem bases de dados (SQL, Sybase, SharePoint, Oracle, MySQL, Exchange, etc.)
- Servidores que façam uso de qualquer uma das seguintes tecnologias:
  - Sistemas de ficheiros resilientes
  - Sistemas de ficheiros fluidos
  - Espaços de armazenamento Microsoft
  - Soluções de armazenamento de rede SAN/NAS
  - Dispositivos conectados por iSCSI
  - Software de deduplicação
  - Deduplicação de hardware
  - RAIDs divididos (múltiplos volumes num único RAID)

- SEDs (RAID e NÃO-RAID)
- Microsoft Storage Server 2012
- O Encryption em sistemas operativos de servidor 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.
- Não são suportadas reinstalações de sistema operativo no local. Para realizar a reinstalação do sistema operativo, faça uma cópia de segurança do computador em questão, limpe o computador, instale o sistema operativo e, em seguida, realize a recuperação dos dados encriptados seguindo os procedimentos de recuperação. Para obter mais informações sobre a recuperação de dados encriptados, consulte o *Guia de recuperação*.

## Sistemas operativos

A tabela seguinte apresenta os sistemas operativos suportados.

| Sistemas operativos (32 e 64 bits)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>● Windows 10: Education, Enterprise, Pro v1909-v22H2 (Atualização de novembro de 2019/19H2 — Atualização de novembro de 2022/22H2)</li> </ul> <p><b>Nota:</b> os OEMs e ODMs não são fornecidos com o Windows 10 v2004 (Atualização de maio de 2020/20H1 e posterior) com a arquitetura de 32 bits. Para obter mais informações, consulte <a href="https://docs.microsoft.com/windows-hardware/design/minimum/minimum-hardware-requirements-overview">https://docs.microsoft.com/windows-hardware/design/minimum/minimum-hardware-requirements-overview</a>.</p> <ul style="list-style-type: none"> <li>○ Windows 10 2019 LTSC</li> <li>○ Windows 10 2021 LTSC</li> </ul> <ul style="list-style-type: none"> <li>● Windows 11: Enterprise, Pro v21H2 —22H2</li> <li>● A <b>Ativação diferida</b> inclui suporte para todos os sistemas operativos acima</li> </ul> |
| Sistemas Operativo de Servidor Suportados                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <ul style="list-style-type: none"> <li>● Windows Server 2008 R2 SP1: Standard Edition, Datacenter Edition, Enterprise Edition, Webserver Edition</li> <li>● Windows Server 2012: Standard Edition, Essentials Edition, Datacenter Edition (o Server Core não é suportado)</li> <li>● Windows Server 2012 R2: Standard Edition, Essentials Edition, Datacenter Edition (o Server Core não é suportado)</li> <li>● Windows Server 2016: Standard Edition, Essentials Edition, Datacenter Edition (o Server Core não é suportado)</li> <li>● Windows Server 2019: Standard Edition, Datacenter Edition</li> <li>● Windows Server 2022: Standard Edition, Datacenter Edition</li> </ul>                                                                                                                                                                                                                       |
| Sistemas operativos suportados com modo UEFI                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <ul style="list-style-type: none"> <li>● Windows 10: Education, Enterprise, Pro v1909-v22H2 (Atualização de novembro de 2019/19H2 — Atualização de novembro de 2022/22H2)</li> </ul> <p><b>Nota:</b> os OEMs e ODMs não são fornecidos com o Windows 10 v2004 (Atualização de maio de 2020/20H1 e posterior) com a arquitetura de 32 bits. Para obter mais informações, consulte <a href="https://docs.microsoft.com/windows-hardware/design/minimum/minimum-hardware-requirements-overview">https://docs.microsoft.com/windows-hardware/design/minimum/minimum-hardware-requirements-overview</a>.</p> <ul style="list-style-type: none"> <li>○ Windows 10 2019 LTSC</li> <li>○ Windows 10 2021 LTSC</li> </ul> <ul style="list-style-type: none"> <li>● Windows 11: Enterprise, Pro v21H2 —22H2</li> </ul>                                                                                              |

### **NOTA:**

Num computador compatível com UEFI, depois de selecionar **Reiniciar** no menu principal, o computador reinicia-se e apresenta um de dois ecrãs de início de sessão possíveis. O ecrã de início de sessão que surge é determinado por diferenças na arquitetura da plataforma do computador.

# Encryption External Media

## Sistemas operativos

- O suporte de dados externo tem de ter aproximadamente 55 MB disponíveis, bem como espaço livre no suporte de dados igual ao maior ficheiro a encriptar para alojar o Encryption External Media.
- As seguintes informações indicam os sistemas operativos compatíveis ao aceder a suportes de dados protegidos pela Dell:

### Sistemas operativos Windows compatíveis para aceder a suportes de dados encriptados (32 e 64 bits)

- Windows 10: Education, Enterprise, Pro v1909-v22H2 (Atualização de novembro de 2019/19H2 — Atualização de novembro de 2022/22H2)  
**Nota:** os OEMs e ODMs não são fornecidos com o Windows 10 v2004 (Atualização de maio de 2020/20H1 e posterior) com a arquitetura de 32 bits. Para obter mais informações, consulte <https://docs.microsoft.com/windows-hardware/design/minimum/minimum-hardware-requirements-overview>.
  - Windows 10 2019 LTSC
  - Windows 10 2021 LTSC
- Windows 11: Enterprise, Pro v21H2 —22H2
- A **Ativação diferida** inclui suporte para todos os sistemas operativos acima

### Sistemas Operativo de Servidor Suportados

- Windows Server 2012 R2

### Sistemas operativos Mac compatíveis para aceder a suportes de dados encriptados (kernels de 64 bits)

- macOS High Sierra 10.13.5–10.13.6
- macOS Mojave 10.14.0–10.14.4
- macOS Catalina 10.15.1–10.15.4

## SED Manager

- Para instalar o SED Manager com êxito, o computador deve possuir uma ligação à rede com fios.
- O computador tem de possuir uma ligação de rede com fios para que um utilizador de smart card possa iniciar sessão através da autenticação de pré-arranque pela primeira vez.
- Os fornecedores de credenciais de outros fabricantes não funcionarão com o SED Manager instalado e todos serão desativados quando a PBA for ativada.
- O IPv6 não é suportado.
- Atualmente, o SED Manager não é suportado em computadores do sistema anfitrião virtualizado.
- 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 em
  - Desative a PBA, altere o método de autenticação e, em seguida, volte a ativar a PBA.
- A configuração de unidades de encriptação automática para o SED Manager difere entre unidades NVMe e não-NVMe (SATA), conforme se segue.

- Qualquer unidade NVMe que esteja a ser utilizada para PBA:
  - Se o dispositivo Dell tiver sido fabricado em 2018 ou mais tarde: o RAID ON ou AHCI podem ser utilizados com unidades NVMe.
  - O modo de arranque do BIOS tem de ser definido para Unified Extensible Firmware Interface (UEFI). As ROMs de funcionamento antigas têm de ser desativadas.
- Qualquer unidade não-NVMe que esteja a ser utilizada para PBA:
  - A operação SATA do BIOS pode ser definida para AHCI ou RAID ON.
  - O sistema operativo falhará quando alterado de RAID ON > AHCI, se os controladores do AHCI não estiverem pré-instalados. Para obter instruções sobre como alterar de RAID > AHCI (ou vice-versa), consulte o artigo [124714](#) da BDC.

As SEDs compatíveis com OPAL suportadas requerem controladores Intel Rapid Storage Technology atualizados, localizados em [www.dell.com/support](http://www.dell.com/support). A Dell recomenda o controlador Intel Rapid Storage Technology mais recente.

**NOTA:** Os controladores Intel Rapid Storage Technology dependem da plataforma. Pode encontrar o controlador do sistema na ligação acima consoante o modelo do computador.

- O SED Manager requer a utilização do fornecedor de credenciais personalizado da Dell para sincronizar as alterações de palavra-passe do Windows e as chaves de encriptação de dados. Se precisar de utilizar aplicações de terceiros que utilizam fornecedores de credenciais personalizados executados em computadores protegidos por SED Manager, terá de iniciar alterações de palavra-passe do Windows através da Data Security Console. Para obter mais informações sobre como alterar a palavra-passe na Data Security Console, consulte o capítulo *Palavra-passe* no [Guia do utilizador da Data Security Console](#).
- O instalador principal instala estes componentes se ainda não estiverem instalados no computador de destino. **Quando utilizar o instalador subordinado**, deve instalar estes componentes antes de instalar os clientes.

| Pré-requisito                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>○ Visual C++ 2017 ou Redistributable Package posterior (x86 ou x64)</li> <li>○ Desde janeiro de 2020, os certificados de assinatura SHA1 deixam de ser válidos e não podem ser renovados. Os dispositivos que executam o Windows Server 2008 R2 devem instalar os artigos da BDC da Microsoft <a href="https://support.microsoft.com/help/4474419">https://support.microsoft.com/help/4474419</a> e <a href="https://support.microsoft.com/help/4490628">https://support.microsoft.com/help/4490628</a> para validar os certificados de assinatura SHA256 nas aplicações e nos pacotes de instalação.</li> </ul> <p>As aplicações e os pacotes de instalação com certificados de assinatura SHA1 irão funcionar, mas sem estas atualizações instaladas será apresentado um erro no ponto terminal durante a instalação ou a execução da aplicação</p> |

- O SED Manager não é compatível com o Encryption em sistemas operativos de servidor .
- As configurações de encriptação em vários discos com o SED Manager exigem as seguintes condições:
  - Todos os discos do sistema de destino têm de ter a seguinte configuração:
    - Unidades SED
    - Os discos têm de ter uma letra de unidade atribuída
  - No modo de arranque UEFI, o sistema operativo pode ser instalado em qualquer disco de destino.
  - No modo de arranque Legacy, o sistema operativo tem de ser instalado no primeiro disco (Disco n.º 0). Se o sistema operativo não estiver instalado no primeiro disco, a encriptação em vários discos é desativada.

Ative a Encriptação em vários discos na Consola de Gestão. Consulte as [Definições de Registo](#) para ver os valores do Registo do Windows relativamente à Encriptação em vários discos e varrimento múltiplo.
- **NOTA:** É necessária uma palavra-passe com autenticação de pré-arranque. A Dell recomenda a definição de um comprimento mínimo da palavra-passe, de acordo com as políticas de segurança internas.
- **NOTA:** Quando é utilizada a PBA, a política Sincronizar Todos os Utilizadores deve ser ativada se um computador tiver vários utilizadores. Além disso, todos os utilizadores devem ter palavras-passe. Os utilizadores sem palavras-passe serão bloqueados e ficarão sem acesso ao computador após a ativação.
- **NOTA:** Os computadores protegidos pelo SED Manager têm de ser atualizados para o Windows 10 v1703 (Atualização para Criativos/Redstone 2) ou posterior antes de serem atualizados para o Windows 10 v1903 (Atualização de maio de 2019/19H1) ou posterior. Se tentar este procedimento de atualização, é apresentada uma mensagem de erro.

## Hardware

### SEDs Compatíveis com OPAL

- Para aceder à lista mais atualizada de SEDs compatíveis com Opal suportadas pela gestão SED, consulte o artigo [126855](#) da BDC.
- Para aceder à lista mais atualizada de plataformas compatíveis com o SED Management, consulte o artigo [126855](#) da BDC.
- Para obter uma lista das estações de acoplamento e adaptadores compatíveis com o SED Manager, consulte o artigo [124241](#) da BDC.

## Opções de Autenticação de Pré-arranque com o SED Manager

- É necessário um hardware específico, para utilizar smart cards e para autenticar em computadores UEFI. É necessária uma configuração para utilizar smart cards com autenticação de pré-arranque. As tabelas seguintes apresentam as opções de autenticação disponíveis por sistema operativo, quando os requisitos de hardware e de configuração são cumpridos.

| Não UEFI                                                                                                                                  |                |                   |                        |             |
|-------------------------------------------------------------------------------------------------------------------------------------------|----------------|-------------------|------------------------|-------------|
|                                                                                                                                           | PBA            |                   |                        |             |
|                                                                                                                                           | Palavra-passe  | Impressão digital | Smart card de contacto | Cartão SIPR |
| Windows 10                                                                                                                                | X <sup>1</sup> |                   | X <sup>1 2</sup>       |             |
| Windows 11                                                                                                                                | X <sup>1</sup> |                   | X <sup>1 2</sup>       |             |
| 1. Disponível quando os controladores de autenticação são transferidos a partir de <a href="http://dell.com/support">dell.com/support</a> |                |                   |                        |             |
| 2. Disponível com uma SED com OPAL suportada                                                                                              |                |                   |                        |             |

| UEFI                                                                             |                                       |                   |                        |             |
|----------------------------------------------------------------------------------|---------------------------------------|-------------------|------------------------|-------------|
|                                                                                  | PBA — em computadores Dell suportados |                   |                        |             |
|                                                                                  | Palavra-passe                         | Impressão digital | Smart card de contacto | Cartão SIPR |
| Windows 10                                                                       | X <sup>1</sup>                        |                   | X <sup>1</sup>         |             |
| Windows 11                                                                       | X <sup>1</sup>                        |                   | X <sup>1</sup>         |             |
| 1. Disponível com uma SED com OPAL suportada em computadores com UEFI suportados |                                       |                   |                        |             |

## 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-FR — Francês (Suíça)                 | EN-GB — Inglês (Reino Unido) |
| DE-CH — Alemão (Suíça)                  | EN-CA — Inglês (Canadá)      |
| EN-US — Inglês (América)                |                              |

| Suporte de teclado internacional — Non-UEFI |                              |
|---------------------------------------------|------------------------------|
| AR — Árabe (utilizando letras latinas)      | EN-US — Inglês (América)     |
| DE-FR — Francês (Suíça)                     | EN-GB — Inglês (Reino Unido) |
| DE-CH — Alemão (Suíça)                      | EN-CA — Inglês (Canadá)      |

## Sistemas operativos

- A tabela seguinte apresenta os sistemas operativos compatíveis.

| Sistemas operativos Windows (32 e 64 bits)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>○ Windows 10: Education, Enterprise, Pro v1909-v22H2 (Atualização de novembro de 2019/19H2 — Atualização de novembro de 2022/22H2)</li> </ul> <p><b>Nota:</b> os OEMs e ODMs não são fornecidos com o Windows 10 v2004 (Atualização de maio de 2020/20H1 e posterior) com a arquitetura de 32 bits. Para obter mais informações, consulte <a href="https://docs.microsoft.com/windows-hardware/design/minimum/minimum-hardware-requirements-overview">https://docs.microsoft.com/windows-hardware/design/minimum/minimum-hardware-requirements-overview</a>.</p> <ul style="list-style-type: none"> <li>▪ Windows 10 2019 LTSC</li> <li>▪ Windows 10 2021 LTSC</li> </ul> <ul style="list-style-type: none"> <li>○ Windows 11: Enterprise, Pro v21H2 — 22H2</li> </ul> |

## Localização

O SED Manager está em conformidade com a norma de interface de utilizador multilíngue e está localizado nos seguintes idiomas. O modo UEFI e a autenticação avançada PBA são suportados nos seguintes idiomas:

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

## 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. Consulte [Configuração da pré-instalação para configurar uma partição de PBA do BitLocker](#).
- É necessário um Dell Server para utilizar o BitLocker Manager.
- Certifique-se de que está disponível um certificado de assinatura na base de dados. Para obter mais informações, consulte o artigo [124931](#) da BDC.
- 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 utiliza os algoritmos com validação FIPS AES aprovados se o modo FIPS for ativado para a definição de segurança GPO "Criptografia do sistema: utilizar algoritmos compatíveis com FIPS para encriptação, hashing e assinatura" no dispositivo e o mesmo for gerido através do nosso produto. O BitLocker Manager não força este modo como predefinição para clientes encriptados pelo BitLocker, uma vez que a Microsoft atualmente sugere que os clientes não utilizem a respetiva encriptação validada por FIPS devido a vários problemas com a compatibilidade da aplicação, a recuperação e a encriptação de suportes de dados: <http://blogs.technet.com>.
- O BitLocker Manager não é suportado com o Encryption em sistemas operativos de servidor .
- Quando utilizar uma Ligação ao Ambiente de Trabalho Remoto com um ponto terminal a tirar partido do BitLocker Manager, a Dell recomenda a execução de quaisquer sessões do Ambiente de trabalho remoto no modo de consola para evitar quaisquer problemas de interação de UI com a sessão de utilizador existente através do seguinte comando:
 

```
mstsc /admin /v:<target_ip_address>
```
- O instalador principal instala estes componentes se ainda não estiverem instalados no computador de destino. **Quando utilizar o instalador subordinado**, deve instalar estes componentes antes de instalar os clientes.

| Pré-requisito                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>○ Visual C++ 2017 ou Redistributable Package posterior (x86 ou x64)</li> <li>○ Desde janeiro de 2020, os certificados de assinatura SHA1 deixam de ser válidos e não podem ser renovados. Os dispositivos que executam o Windows Server 2008 R2 devem instalar os artigos da BDC da Microsoft <a href="https://support.microsoft.com/help/4474419">https://support.microsoft.com/help/4474419</a> e <a href="https://support.microsoft.com/help/4490628">https://support.microsoft.com/help/4490628</a> para validar os certificados de assinatura SHA256 nas aplicações e nos pacotes de instalação.</li> </ul> <p>As aplicações e os pacotes de instalação com certificados de assinatura SHA1 irão funcionar, mas sem estas atualizações instaladas será apresentado um erro no ponto terminal durante a instalação ou a execução da aplicação</p> |

- **NOTA:** Os computadores protegidos pelo SED Manager têm de ser atualizados para o Windows 10 v1703 (Atualização para Criativos/Redstone 2) ou posterior antes de serem atualizados para o Windows 10 v1903 (Atualização de maio de 2019/19H1) ou posterior. Se tentar este procedimento de atualização, é apresentada uma mensagem de erro.
- **NOTA:** As atualizações do sistema operativo para uma versão mais recente no local — como o Windows 10 — não são suportadas para o Windows 11.

## Hardware

- A tabela seguinte indica o hardware suportado.

| Hardware opcional incorporado                                      |
|--------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>○ TPM 1.2 ou 2.0</li> </ul> |

## Sistemas operativos

- As tabelas seguintes apresentam os sistemas operativos suportados.

| Sistemas operativos Windows                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>○ Windows 10: Education, Enterprise, Pro v1909-v22H2 (Atualização de novembro de 2019/19H2 — Atualização de novembro de 2022/22H2)</li> </ul> <p><b>Nota:</b> os OEMs e ODMs não são fornecidos com o Windows 10 v2004 (Atualização de maio de 2020/20H1 e posterior) com a arquitetura de 32 bits. Para obter mais informações, consulte <a href="https://docs.microsoft.com/windows-hardware/design/minimum/minimum-hardware-requirements-overview">https://docs.microsoft.com/windows-hardware/design/minimum/minimum-hardware-requirements-overview</a>.</p> <ul style="list-style-type: none"> <li>▪ Windows 10 2019 LTSC</li> <li>▪ Windows 10 2021 LTSC</li> </ul> <li>○ Windows 11: Enterprise, Pro v21H2 — 22H2</li> |

**Sistemas Operativos Windows Server**

- Windows Server 2008 R2: Standard Edition, Enterprise Edition (64 bits)
- Windows Server 2012 R2: Standard Edition, Enterprise Edition (64 bits)
- Windows Server 2016: Standard Edition, Datacenter Edition (64 bits)
- Windows Server 2019: Standard Edition, Datacenter Edition (64 bits)
- Windows Server 2022: Standard Edition, Datacenter Edition

## Definições de registo

- Esta secção explica todas as definições de registo aprovadas pelo Dell ProSupport para computadores **cliente** locais, independentemente do motivo da definição de registo. Se uma definição de registo se sobrepõe a dois produtos, tal é indicado em cada uma das categorias.
- Estas alterações de registo apenas devem ser efetuadas por administradores e podem não ser adequadas ou funcionar em todos os cenários.

### Encryption

- Se for utilizado um certificado autoassinado no Dell Server. Para Windows, a validação de confiança do certificado deve manter-se desativada no computador cliente (a validação de confiança está *desativada* por predefinição com o Dell Server). Antes de *ativar* a validação de confiança no computador cliente, devem ser cumpridos os seguintes requisitos.
  - É necessário importar para o Dell Server um certificado assinado por uma autoridade raiz, como EnTrust ou Verisign.
  - A cadeia de confiança completa do certificado deve ser armazenada na keystore da Microsoft no computador cliente.
  - Para *ativar* a validação de confiança para o Encryption, altere o valor das seguintes entradas de registo para 0 no computador de destino.
 

```
[HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield]
"IgnoreCertErrors"=DWORD:00000000
```

0 = Falha se for encontrado um erro de certificado  
1= Ignora os erros
- Para criar um ficheiro de registo para o Encryption Removal Agent, crie a seguinte entrada de registo no computador destinado à descriptação. Consulte [\(Opcional\) Criar um ficheiro de registo do Encryption Removal Agent](#).
 

```
[HKLM\Software\Credant\DecryptionAgent]
"LogVerbosity"=DWORD:2
```

0: sem registos  
1: regista os erros que impedem a execução do serviço  
2: regista os erros que impedem a descriptação total dos dados (nível recomendado)  
3: regista informações acerca de todos os ficheiros e volumes de descriptação  
5: regista as informações de depuração
- Para desativar a solicitação ao utilizador para reiniciar o computador depois de o Encryption Removal Agent concluir o seu estado final no processo de descriptação, modifique o seguinte valor de registo ou modifique a política *Forçar Reinício nas Atualizações* na Management Console.
 

```
[HKLM\Software\Dell\Dell Data Protection]
"ShowDecryptAgentRebootPrompt"=DWORD
```

1 = ativado (apresenta aviso)  
0 = desativado (oculta aviso)
- Por predefinição, durante a instalação, é apresentado o ícone da área de notificação. Utilize a seguinte definição de registo para ocultar o ícone da área de notificação para todos os utilizadores geridos num computador após a instalação original. Crie ou modifique a definição de registo:
 

```
[HKLM\Software\CREDANT\CMGShield]
"HIDESYSTRAYICON"=DWORD:1
```

- Por predefinição, durante a instalação, todos os ficheiros temporários no diretório c:\windows\temp são automaticamente eliminados. A eliminação dos ficheiros temporários acelera a encriptação inicial e ocorre antes do varrimento de encriptação inicial.

No entanto, se a sua organização utiliza uma aplicação de terceiros que exija que a estrutura de ficheiros dentro do diretório \temp seja preservada, deverá evitar esta eliminação.

Para desativar a eliminação de ficheiros temporários, crie ou modifique a configuração de registo da seguinte forma:

[HKLM\SOFTWARE\CREDANT\CMGShield]

"DeleteTempFiles"=REG\_DWORD:0

A não eliminação dos ficheiros temporários aumenta o tempo de encriptação inicial.

- O Encryption apresenta o aviso de *duração de cada atraso de atualização de política* a cada cinco minutos. Se o utilizador não responder ao comando, o atraso seguinte é automaticamente iniciado. O comando de atraso final inclui uma contagem decrescente e uma barra de progresso e é apresentado até que o utilizador responda ou até que o atraso final expire e o encerramento/reinício solicitado ocorra.

Pode alterar a ação do utilizador para iniciar ou atrasar a encriptação, para evitar o processamento da encriptação após a falta de resposta do utilizador ao comando. Para isso, defina o valor:

[HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield]

"SnoozeBeforeSweep"=DWORD:1

Qualquer valor diferente de zero altera a ação predefinida para suspensão. Quando não houver interação do utilizador, o processamento da encriptação é atrasado até ao número de atrasos permitidos especificados. O processamento da encriptação inicia quando o atraso final expirar.

Calcule o atraso máximo possível da seguinte forma (um atraso máximo implica que o utilizador nunca responda a um comando de atraso, que é apresentado durante 5 minutos):

(NÚMERO DE ATRASOS DE ATUALIZAÇÃO DE POLÍTICAS PERMITIDOS × DURAÇÃO DE CADA ATRASO DE ATUALIZAÇÃO DE POLÍTICA) + (5 MINUTOS × [NÚMERO DE ATRASOS DE ATUALIZAÇÃO DE POLÍTICAS PERMITIDOS - 1])

- Utilize a definição de registo para que o Encryption analise o Dell Server para uma atualização forçada da política. Crie ou modifique a definição de registo:

[HKLM\SOFTWARE\Credant\CMGShield\Notify]

"PingProxy"=valor DWORD:1

A configuração de registo desaparece automaticamente quando terminar.

- Utilize as definições de registo para permitir que o Encryption envie um inventário otimizado e completo (utilizadores ativados e desativados), ou completo (apenas utilizadores ativados) para o Dell Server.

- Enviar um inventário otimizado para o Dell Server:

Crie ou modifique a definição de registo:

[HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield]

"OnlySendInvChanges"=REG\_DWORD:1

Se não existir qualquer entrada, o inventário otimizado é enviado para o Dell Server.

- Enviar um inventário completo para o Dell Server:

Crie ou modifique a definição de registo:

[HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield]

"OnlySendInvChanges"=REG\_DWORD:0

Se não existir qualquer entrada, o inventário otimizado é enviado para o Dell Server.

- Enviar inventário completo de todos os utilizadores ativados

[HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield]

"RefreshInventory"=REG\_DWORD:1

Esta entrada é eliminada do registo imediatamente após o processamento. Este valor é guardado no cofre, pelo que, mesmo que o computador seja reiniciado antes do carregamento do inventário, o Encryption mantém o pedido no carregamento do inventário bem-sucedido seguinte.

Esta entrada substitui o valor de registo OnlySendInvChanges.

- A Ativação em intervalos é uma funcionalidade que permite dispersar as ativações de clientes ao longo de um determinado período de tempo para diminuir a carga do Dell Server durante uma implementação massiva. As ativações são atrasadas com base em períodos de tempo gerados através de um algoritmo para proporcionar uma distribuição uniforme dos tempos de ativação.

Para utilizadores que necessitam de ativação através de VPN, poderá ser necessária uma configuração de ativação em intervalos para o cliente, de modo a atrasar a ativação inicial pelo tempo suficiente para permitir ao cliente VPN estabelecer uma ligação de rede.

Estas entradas de registo requerem o reinício do computador para que as atualizações sejam aplicadas.

- **Ativação em intervalos**

Para ativar ou desativar esta funcionalidade, crie um DWORD com o nome **SlottedActivation** na chave principal:

[HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield\]

- **Intervalo de ativação**

Para ativar ou desativar esta funcionalidade, crie uma subchave com o nome **ActivationSlot** na chave principal:

[HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield\]

Intervalo de ativação - uma cadeia que define o período no qual o Encryption tenta ativar com o Dell Server. Estes valores são definidos em segundos e a sintaxe é definida por <lowervalue>,<uppervalue>. Um exemplo seria 120,300. Isto significa que o Encryption tenta ativar num intervalo aleatório de tempo entre 2 minutos e 5 minutos após o início de sessão do utilizador.

- **Repetir calendário**

Para ativar ou desativar esta funcionalidade, crie uma subchave com o nome **CalRepeat** na chave principal:

[HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield\ActivationSlot]

CalRepeat - Um DWORD que define o período de tempo em segundos em que ocorre o intervalo de ativação.

Utilize esta definição para substituir o período de tempo em segundos em que ocorre o intervalo de ativação. Estão disponíveis 25 200 segundos para ativações em intervalos durante um período de sete horas. A predefinição é de 86 400 segundos, o que representa um repetição diária. O valor decimal sugerido é de 600, o que representa 10 minutos.

- **Intervalo**

Para ativar ou desativar esta funcionalidade, crie uma subchave com o nome **SlotInterval** na chave principal:

[HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield\ActivationSlot]

Intervalo - Um valor de cadeia que define os intervalos entre as ativações. A definição sugerida é de 45,120. Isto representa o tempo de ativação a ser atribuído aleatoriamente entre 45 e 120 segundos.

- **Limiar perdido**

Para ativar ou desativar esta funcionalidade, crie uma subchave com o nome **MissThreshold** na chave principal:

[HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield\ActivationSlot]

MissThreshold - Um valor DWORD que contém um número inteiro positivo que define o número de tentativas de ativação antes de ser necessário encerrar a sessão. Se o MissThreshold for atingido, as tentativas de ativação param até ao próximo início de sessão para o utilizador não ativado. A contagem de MissThreshold é sempre repostada no encerramento de sessão.

As chaves do registo recolhem dados de utilizador de ativação em intervalos:

[HKCU\Software\CREDANT\ActivationSlot] (dados por utilizador)

Tempo diferido para tentar a ativação em intervalos, que é definido quando o utilizador inicia sessão na rede pela primeira vez após a ativação em intervalos ser ativada. O intervalo de ativação é novamente calculado para cada tentativa de ativação.

[HKCU\Software\CREDANT\SlotAttemptCount] (dados por utilizador)

Número de tentativas falhadas ou perdidas, quando o período de tempo é alcançado e há tentativa de ativação, mas esta falha. Quando este número alcança o limite definido em ACTIVATION\_SLOT\_MISSTHRESHOLD, o computador tenta uma ativação imediata após estabelecer ligação à rede.

- Para detetar utilizadores não geridos no computador cliente, defina o valor de registo no computador cliente:

[HKLM\SOFTWARE\Credant\CMGShield\ManagedUsers\]

"UnmanagedUserDetected"=valor DWORD:1

Detetar utilizadores não geridos neste computador=1

Não detetar utilizadores não geridos neste computador=0

- O acesso a suportes de dados externos encriptados com o Encryption External Media pode ser restrito a computadores com acesso ao Dell Server que produziu as chaves de encriptação com as quais o suporte de dados foi encriptado.

Esta funcionalidade é ativada através da definição do registo:

[ HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield]

"EnterpriseUsage"=DWORD:0

Desativado (predefinição)=0

Acesso ao ficheiro restrito para Enterprise=1

Se este valor for alterado depois de os ficheiros no suporte de dados serem encriptados, os ficheiros voltam a ser encriptados com base no valor atualizado da chave de registo quando o suporte de dados estiver ligado ao computador no qual a definição de registo foi atualizada.

- Para permitir a reativação automática silenciosa na rara eventualidade de um utilizador ficar desativado, o valor de registo deve ser definido no computador cliente.

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\CMGShield]

"AutoReactivation"=DWORD:00000001

0=Desativado (predefinição)

1=Ativado

- System Data Encryption (SDE) é imposta com base no valor da política para SDE Encryption Rules. Os diretórios adicionais são protegidos por predefinição quando a política SDE Encryption Enabled é Seleccionada. Para obter mais informações, procure "SDE Encryption Rules" em AdminHelp. Quando o Encryption estiver a processar uma atualização de política que inclua uma política SDE ativa, o diretório do perfil de utilizador atual é encriptado por predefinição com a chave SDUser (uma chave de Utilizador) e não com a chave SDE (uma chave de Dispositivo). A chave SDUser é também utilizada para encriptar ficheiros ou pastas que são copiadas (e não movidas) para um diretório de utilizadores não encriptado com SDE.

Para desativar a chave SDUser e utilizar a chave SDE para encriptar estes diretórios de utilizador, crie o registo no computador:

[HKEY\_LOCAL\_MACHINE\SOFTWARE\Credant\CMGShield]

"EnableSDUserKeyUsage"=DWORD:00000000

Se a chave de registo não estiver presente ou for definida para qualquer valor diferente de 0, a chave SDUser será utilizada para encriptar estes diretórios de utilizadores.

Para obter mais informações sobre o SDUser, consulte o artigo [131035](#) da BDC.

- Definir a entrada de registo, EnableNGMetadata, se ocorrerem erros relacionados com as atualizações da Microsoft em computadores com dados encriptados com chave comuns, ou com encriptação, desencriptação, ou ao descomprimir um grande número de ficheiros dentro de uma pasta.

Defina a entrada de registo EnableNGMetadata na seguinte localização:

[HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\CmgShieldFFE]

"EnableNGMetadata" = DWORD:1

0=Desativado (predefinição)

1=Ativado

- A funcionalidade de ativação dos não domínios pode ser ativada contactando o Dell ProSupport e pedindo instruções.
- Por predefinição, o Encryption Management Agent já não envia políticas. Para emitir políticas futuras utilizadas, crie a seguinte chave de registo:

HKLM\Software\Dell\Dell Data Protection\

" DumpPolicies" = DWORD

Value=1

**Nota:** os registos são gravados em C:\ProgramData\Dell\Dell Data Protection\Policy.

- Para desativar ou ativar a opção *Encrypt for Sharing* no menu do botão direito do rato, utilize a seguinte chave de registo.

HKEY\_LOCAL\_MACHINE\SOFTWARE\Dell\Dell Data Protection\Encryption

"DisplaySharing"=DWORD

0 = desativar a opção Encrypt for Sharing no menu de contexto do botão direito do rato

1 = ativar a opção Encrypt for Sharing no menu de contexto do botão direito do rato

## SED Manager

- Para definir o intervalo entre tentativas quando o Dell Server está indisponível para comunicar com o SED Manager, adicione o seguinte valor de registo.

[HKLM\System\CurrentControlSet\Services\DellMgmtAgent\Parameters]

"CommErrorSleepSecs"=DWORD:300

Este valor corresponde ao número de segundos que o SED Manager espera para tentar contactar o Dell Server, se este estiver indisponível para comunicar. A predefinição é de 300 segundos (5 minutos).

- Se for utilizado um certificado autoassinado no Dell Server para o SED Manager, a validação de confiança SSL/TLS deve permanecer desativada no computador cliente (a validação de confiança SSL/TLS está *desativada* por predefinição com o SED Manager). Antes de *ativar* a validação de confiança SSL/TLS no computador cliente, os requisitos seguintes devem ser cumpridos.
  - É necessário importar para o Dell Server um certificado assinado por uma autoridade raiz, como EnTrust ou Verisign.
  - A cadeia de confiança completa do certificado deve ser armazenada na keystore da Microsoft no computador cliente.
  - Para *ativar* a validação de confiança SSL/TLS para o SED Manager, altere o valor da seguinte entrada de registo para 0 no computador cliente.

[HKLM\System\CurrentControlSet\Services\DellMgmtAgent\Parameters]

"DisableSSLCertTrust"=DWORD:0

0 = Ativado

1 = Desativado

- Para determinar se a PBA está ativada, certifique-se de que está definido o seguinte valor:

[HKLM\SYSTEM\CurrentControlSet\services\DellMgmtAgent\Parameters]

"PBAsActivated"=DWORD (32 bits):1

O valor 1 significa que a PBA está ativada. O valor 0 significa que a PBA não está ativada.

- Para determinar se o smart card está presente e ativo, certifique-se de que está definido o seguinte valor:

HKLM\SOFTWARE\Dell\Dell Data Protection\

"SmartcardEnabled"=DWORD:1

Se SmartcardEnabled não existir ou tiver zero como valor, o Fornecedor de Credenciais irá apresentar apenas a palavra-passe para autenticação.

Se SmartcardEnabled tiver um valor diferente de zero, o Fornecedor de Credenciais irá apresentar opções de palavra-passe e autenticação de smart card.

- O seguinte valor de registo indica se o Winlogon deve gerar uma notificação para eventos de início de sessão de smart cards.

HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify

"SmartCardLogonNotify"=DWORD:1

0 = Desativado

1 = Ativado

- Para evitar que o SED Manager desative fornecedores de credenciais externos, crie a seguinte chave de registo:

HKLM\SOFTWARE\Dell\Dell Data Protection\

"AllowOtherCredProviders" = DWORD:1

0=Desativado (predefinição)

1=Ativado

**Nota:** este valor pode impedir que o fornecedor de credenciais da Dell sincronize corretamente as credenciais inicialmente, devido à desativação dos fornecedores de credenciais externos. Certifique-se de que os dispositivos que utilizam esta chave de registo podem comunicar corretamente com o Dell Server.

- Para definir o intervalo em que o SED Manager tenta contactar o Dell Server quando o mesmo está indisponível para comunicar, defina o seguinte valor no computador de destino:

```
[HKLM\System\CurrentControlSet\Services\DellMgmtAgent\Parameters]
```

```
"CommErrorSleepSecs"=Valor DWORD:300
```

Este valor corresponde ao número de segundos que o SED Manager espera para tentar contactar o Dell Server, se este estiver indisponível para comunicar. A predefinição é de 300 segundos (5 minutos).

- Se necessário, o anfitrião do Security Server poderá ser mudado do local de instalação original. As informações do anfitrião são lidas sempre que ocorrer uma consulta de política. Altere o seguinte valor de registo no computador cliente:

```
[HKLM\SYSTEM\CurrentControlSet\services\DellMgmtAgent]
```

```
"ServerHost"=REG_SZ:<newname>.<organization>.com
```

- Se necessário, a porta do Security Server poderá ser mudada do local de instalação original. Este valor é lido sempre que ocorrer uma consulta de política. Altere o seguinte valor de registo no computador cliente:

```
[HKLM\SYSTEM\CurrentControlSet\services\DellMgmtAgent]
```

```
ServerPort=REG_SZ:8888
```

- Se necessário, o URL do Security Server poderá ser mudado do local de instalação original. Este valor é lido pelo computador cliente sempre que ocorrer uma consulta de política. Altere o seguinte valor de registo no computador cliente:

```
[HKLM\SYSTEM\CurrentControlSet\services\DellMgmtAgent]
```

```
"ServerUrl"=REG_SZ:https://<newname>.<organization>.com:8888/agent
```

- (Apenas com autenticação de pré-arranque) Se **não** pretender que a autenticação avançada PBA altere os serviços associados a smart cards e dispositivos biométricos para um tipo de arranque "automático", desative a funcionalidade de arranque de serviços. A desativação desta funcionalidade também suprime alertas associados aos serviços necessários que não estão a ser executados.

Quando **desativada**, a autenticação avançada PBA não tentará iniciar estes serviços:

- SCardSvr - Gere o acesso a smart cards lidos pelo computador. Se este serviço for interrompido, o computador não consegue ler smart cards. Se este serviço estiver desativado, não é possível iniciar quaisquer serviços que dele dependam explicitamente.
- SCPolicySvc - Permite que o sistema seja configurado de modo a bloquear o ambiente de trabalho do utilizador aquando da remoção de smart cards.
- WbioSvc - O serviço de biometria do Windows permite que aplicações cliente capturem, comparem, manipulem e armazenem dados biométricos sem obter acesso direto a amostras ou hardware de biometria. O serviço é alojado num processo SVCHOST privilegiado.

Por predefinição, se a chave de registo não existe ou o valor está definido para 0, esta funcionalidade está ativada.

```
[HKLM\SOFTWARE\DELL\Dell Data Protection]
```

```
SmartCardServiceCheck=REG_DWORD:0
```

0 = Ativado

1 = Desativado

- Para utilizar smart cards com Autenticação PBA da SED, o valor de registo seguinte deve ser configurado no computador cliente equipado com SED.

```
[HKLM\SOFTWARE\DigitalPersona\Policies\Default\SmartCards]
```

```
"MSSmartcardSupport"=DWORD:1
```

Configure a política de Método de autenticação para smart card na Management Console e aplique a alteração.

- Para suprimir todas as notificações de alerta do Encryption Management Agent, o seguinte valor de registo deve ser configurado no computador cliente.

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Dell\Dell Data Protection]
```

```
"PbaToastersAllowClose" =DWORD:1
```

0=Ativado (predefinição)

1=Desativado

## Full Disk Encryption

- Esta secção explica todas as definições de registo aprovadas pelo Dell ProSupport para computadores locais, independentemente do motivo da definição de registo. Se uma configuração de registo se sobrepõe a dois produtos, está indicada em cada uma das categorias.
- Estas alterações de registo apenas devem ser efetuadas por administradores e poderão não ser adequadas ou funcionar em todos os cenários.
- Para definir o intervalo entre tentativas quando o Dell Server está indisponível para comunicar com a Full Disk Encryption, adicione o seguinte valor de registo.

```
[HKLM\System\CurrentControlSet\Services\DellMgmtAgent\Parameters]
```

```
"CommErrorSleepSecs"=DWORD:300
```

Este valor corresponde ao número de segundos que a Full Disk Encryption espera para tentar contactar o Dell Server, se este estiver indisponível para comunicar com a Full Disk Encryption. A predefinição é de 300 segundos (5 minutos).

- Se for utilizado um certificado autoassinado no Dell Server para a Full Disk Encryption, a validação de confiança SSL/TLS tem de permanecer desativada no computador cliente (a validação de confiança SSL/TLS está *desativada* por predefinição com a Full Disk Encryption). Antes de *ativar* a validação de confiança SSL/TLS no computador cliente, os requisitos seguintes devem ser cumpridos.
  - É necessário importar para o Dell Server um certificado assinado por uma autoridade raiz, como EnTrust ou Verisign.
  - A cadeia de confiança completa do certificado deve ser armazenada na keystore da Microsoft no computador cliente.
  - Para *ativar* a validação de confiança SSL/TLS da gestão Dell Encryption, altere o valor da seguinte entrada de registo para 0 no computador cliente.

```
[HKLM\System\CurrentControlSet\Services\DellMgmtAgent\Parameters]
```

```
"DisableSSLCertTrust"=DWORD:0
```

0 = Ativado


1 = Desativado

- Para determinar se a PBA está ativada, certifique-se de que está definido o seguinte valor:

```
[HKLM\SYSTEM\CurrentControlSet\services\DellMgmtAgent\Parameters]
```

```
"PBAIsActivated"=DWORD (32 bits):1
```

O valor 1 significa que a PBA está ativada. O valor 0 significa que a PBA não está ativada.

 **NOTA:** Eliminar esta chave manualmente pode criar resultados indesejados para utilizadores que estejam a sincronizar com a PBA, resultando na necessidade de uma recuperação manual.

- Para determinar se o smart card está presente e ativo, certifique-se de que está definido o seguinte valor:

```
HKLM\SOFTWARE\Dell\Dell Data Protection\
```

```
"SmartcardEnabled"=DWORD:1
```

Se SmartcardEnabled não existir ou tiver zero como valor, o Fornecedor de Credenciais irá apresentar apenas a palavra-passe para autenticação.

Se SmartcardEnabled tiver um valor diferente de zero, o Fornecedor de Credenciais irá apresentar opções de palavra-passe e autenticação de smart card.

- O seguinte valor de registo indica se o Winlogon deve gerar uma notificação para eventos de início de sessão de smart cards.

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify
```

```
"SmartCardLogonNotify"=DWORD:1
```

0 = Desativado

1 = Ativado

- Se necessário, o anfitrião do Security Server poderá ser mudado do local de instalação original. As informações do anfitrião são lidas pelo computador cliente sempre que ocorrer uma consulta de política. Altere o seguinte valor de registo no computador cliente:

[HKLM\SYSTEM\CurrentControlSet\Services\DellMgmtAgent]

"ServerHost"=REG\_SZ:<newname>.<organization>.com

- Se necessário, a porta do Security Server poderá ser mudada do local de instalação original. Este valor é lido pelo computador cliente sempre que ocorrer uma consulta de política. Altere o seguinte valor de registo no computador cliente:

[HKLM\SYSTEM\CurrentControlSet\Services\DellMgmtAgent]

ServerPort=REG\_SZ:8888

- (Apenas com autenticação de pré-arranque) Se **não** pretender que a autenticação avançada PBA altere os serviços associados a smart cards e dispositivos biométricos para um tipo de arranque "automático", desative a funcionalidade de arranque de serviços. A desativação desta funcionalidade também suprime alertas associados aos serviços necessários que não estão a ser executados.

Quando **desativada**, a autenticação avançada PBA não tentará iniciar estes serviços:

- SCardSvr - Gere o acesso a smart cards lidos pelo computador. Se este serviço for interrompido, o computador não consegue ler smart cards. Se este serviço estiver desativado, não é possível iniciar quaisquer serviços que dele dependam explicitamente.
- SCPolicySvc - Permite que o sistema seja configurado de modo a bloquear o ambiente de trabalho do utilizador aquando da remoção de smart cards.
- WbioSrv - O serviço de biometria do Windows permite que aplicações cliente capturem, comparem, manipulem e armazenem dados biométricos sem obter acesso direto a amostras ou hardware de biometria. O serviço é alojado num processo SVCHOST privilegiado.

Por predefinição, se a chave de registo não existe ou o valor está definido para 0, esta funcionalidade está ativada.

[HKLM\SOFTWARE\DELL\Dell Data Protection]

SmartCardServiceCheck=REG\_DWORD:0

0 = Ativado

1 = Desativado

- Para evitar que o Full Disk Encryption desative fornecedores de credenciais externos, crie a seguinte chave de registo:

HKLM\SOFTWARE\Dell\Dell Data Protection\

"AllowOtherCredProviders" = DWORD:1

0=Desativado (predefinição)

1=Ativado

**Nota:** este valor pode impedir que o fornecedor de credenciais da Dell sincronize corretamente as credenciais inicialmente, devido à desativação dos fornecedores de credenciais externos. Certifique-se de que os dispositivos que utilizam esta chave de registo podem comunicar corretamente com o Dell Server.

- Para suprimir todas as notificações de alerta do Encryption Management Agent, o seguinte valor de registo deve ser configurado no computador cliente.

[HKEY\_LOCAL\_MACHINE\SOFTWARE\Dell\Dell Data Protection]

"PbaToastersAllowClose" =DWORD:1

0=Ativado (predefinição)

1=Desativado

- Para permitir a instalação da Full Disk Encryption com a Policy Based Encryption, o seguinte valor de registo deve ser definido no computador cliente.

[HKEY\_LOCAL\_MACHINE\SOFTWARE\Dell\Dell Data Protection]

" EnableFDE" = DWORD: 1

0=Desativado (predefinição)

1=Ativado

# BitLocker Manager

- Se for utilizado um certificado autoassinado no Dell Server para o BitLocker Manager, a validação de confiança SSL/TLS tem de permanecer desativada no computador cliente (a validação de confiança SSL/TLS está *desativada* por predefinição com o BitLocker Manager). Antes de *ativar* a validação de confiança SSL/TLS no computador cliente, os requisitos seguintes devem ser cumpridos.
  - É necessário importar para o Dell Server um certificado assinado por uma autoridade raiz, como EnTrust ou Verisign.
  - A cadeia de confiança completa do certificado deve ser armazenada na keystore da Microsoft no computador cliente.
  - Para *ativar* a validação de confiança SSL/TLS do BitLocker Manager, altere o valor da seguinte entrada de registo para 0 no computador cliente.

[HKLM\System\CurrentControlSet\Services\DellMgmtAgent\Parameters]

"DisableSSLCertTrust"=DWORD:0

0 = Ativado

1 = Desativado

- Para evitar que o Bitlocker Manager detete discos amovíveis como discos fixos, adicione a seguinte chave de registo:

HKLM\Software\Dell\Dell Data Protection\

"UseEncryptableVolumeType" = DWORD:1

0=Desativado (predefinição),

1=Ativado

## Instalar utilizando o instalador principal

- 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.
  - Os ficheiros de registo do instalador principal do encontram-se em `C:\ProgramData\Dell\Dell Data Protection\Installer`.
- NOTA:** Se a Encriptação Baseada em Políticas for instalada antes do Encryption Management Agent, poderá ocorrer uma falha do computador. Este problema é causado devido à falha ao carregar o controlador de encriptação do modo Suspensão que gere o ambiente PBA. Como solução alternativa, utilize o instalador principal ou certifique-se de que a Encriptação Baseada em Políticas é instalada depois do Encryption Management Agent.
- 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 as funcionalidades do Encryption. Aceda à ajuda a partir de `<Install dir>\Program Files\Dell\Dell Data Protection\Encryption\Help`.
    - Consulte a *Ajuda do Encryption External Media* para saber como utilizar as funcionalidades do Encryption External Media. Aceda à ajuda a partir de `<Install dir>\Program Files\Dell\Dell Data Protection\Encryption\EMS`.
    - Consulte a *Ajuda do Encryption Enterprise Endpoint Security Suite Enterprise* para saber como utilizar as funcionalidades do . Aceda à ajuda a partir de `<Install dir>\Program Files\Dell\Dell Data Protection\Client Security Framework\Help`.
  - Após a conclusão da instalação, os utilizadores devem atualizar as respetivas políticas clicando com o botão direito do rato no ícone do Dell Encryption, na área de notificação e selecionando **Procurar atualizações de políticas**.
  - O instalador principal instala todo o conjunto de produtos. Existem dois métodos para instalar utilizando o instalador principal. Escolha uma das seguintes opções.
    - [Instalar interativamente utilizando o instalador principal](#)
- ou em
- [Instalar por linha de comandos utilizando o instalador principal](#)

## Instalar interativamente utilizando o instalador principal

- O instalador principal do pode ser localizado em:
  - **Em [dell.com/support](https://dell.com/support)** - Se necessário, [Obter o software](#) a partir de **dell.com/support**
  - **Na sua conta FTP Dell** - localize o pacote de instalação em `Dell-Encryption-8.x.x.xxx.zip`
- Utilize estas instruções para instalar ou atualizar interativamente o Dell Encryption Enterprise utilizando o instalador principal do . Este método pode ser utilizado para instalar o conjunto de produtos num computador de cada vez.
  1. Localize o **DDSetup.exe** no suporte multimédia de instalação Dell. Copie-o para o computador local.
  2. Clique duas vezes 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. Em *Nome de Dell Server no local*, introduza o nome de anfitrião totalmente qualificado do Dell Server para gerir o utilizador pretendido.

Introduza os valores das portas em *Porta do Core Server* e *Porta do Security Server* se a sua organização utilizar portas não padrão.

Clique em **Seguinte**.

6. Clique em **Seguinte** para instalar o produto na localização predefinida C:\Program Files\Dell\Dell Data Protection\. Dell recommends installing in the default location only, uma vez que podem surgir problemas ao efetuar a instalação noutras localizações.
7. Selecione os componentes a serem instalados.
  - O *Security Framework* instala a framework de segurança subjacente, o Encryption Management Agent e a autenticação PBA.
  - O *BitLocker Manager* instala o cliente BitLocker Manager, concebido 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.
  - O *Encryption* instala o componente que aplica a política de segurança, quer um computador esteja ligado à rede, desligado da rede, seja perdido ou roubado.
  - O *Encryption External Media* instala o componente que aplica o Encryption External Media.
  - A *Full Disk Encryption* instala o componente que aplica a Full Disk Encryption.

Clique em **Seguinte** quando concluir as suas seleções.
8. Clique em **Instalar** para dar início à instalação. A instalação demora vários minutos.
9. Selecione **Sim, desejo reiniciar o computador agora** e clique em **Concluir**.  
A instalação está concluída.

## Instalar por linha de comandos utilizando o instalador principal

- Numa instalação com linha de comandos, primeiro é necessário especificar as opções. 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 .

**NOTA:** Se a sua organização requer a utilização de fornecedores de credenciais externos, o Encryption Management Agent tem de ser instalado ou atualizado com o parâmetro FEATURE=BLM ou FEATURE=BASIC.

| Opção | Descrição                                         |
|-------|---------------------------------------------------|
| /s    | Instalação silenciosa                             |
| /z    | Passa variáveis para o .msi dentro do DDSetup.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 Dell Server.                                                                                                                                                             |
| InstallPath    | Especifica o caminho da instalação. Pode ser utilizado no modo SILENCIOSO.                                                                                                                   |
| FUNÇÕES        | Especifica os componentes que podem ser instalados no modo SILENCIOSO.<br>DE = Cliente de Encriptação de Unidade apenas<br>EME = Encryption External Media apenas<br>BLM = BitLocker Manager |

| Parâmetro  | Descrição                                                                                       |
|------------|-------------------------------------------------------------------------------------------------|
|            | SED = SED Manager (Encryption Management Agent/Manager, Controladores PBA/GPE)                  |
| BLM_ONLY=1 | Deve ser utilizado com FEATURES=BLM na linha de comandos para excluir o plug-in do SED Manager. |

### 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 em portas padrão, de forma silenciosa, na localização predefinida C:\Program Files\Dell\Dell Data Protection\ e configura-os para utilizar o Dell Server especificado.  

```
"DDSSetup.exe" /s /z\"SERVER=server.organization.com\""
```
- Este exemplo instala o SED Manager e o Encryption External Media 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-os para utilizar o Dell Server especificado.  

```
"DDSSetup.exe" /s /z\"SERVER=server.organization.com, FEATURES=EME-SED, SUPPRESSREBOOT=1\""
```
- Este exemplo instala o SED Manager 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 Dell Server especificado.  

```
"DDSSetup.exe" /s /z\"SERVER=server.organization.com, FEATURES=SED, SUPPRESSREBOOT=1\""
```
- Este exemplo instala o SED Manager 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 Dell Server especificado.  

```
"DDSSetup.exe" /s /z\"SERVER=server.organization.com, FEATURES=SED\""
```
- Este exemplo instala o Encryption e o BitLocker Manager (sem o plug-in do SED Manager), com o instalador principal, nas portas padrão, de forma silenciosa, na localização predefinida C:\Program Files\Dell\Dell Data Protection\ e configura-os para utilizar o Dell Server especificado.  

```
"DDSSetup.exe" /s /z\"SERVER=server.organization.com, FEATURES=DE-BLM, BLM_ONLY=1\""
```
- Este exemplo instala o BitLocker Manager (com o plug-in do SED Manager) e o Encryption External Media, 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-os para utilizar o Dell Server especificado.  

```
"DDSSetup.exe" /s /z\"SERVER=server.organization.com, FEATURES=BLM-EME, SUPPRESSREBOOT=1\""
```
- Este exemplo instala o BitLocker Manager (sem o plug-in do SED Manager) e o Encryption External Media, 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-os para utilizar o Dell Server especificado.  

```
"DDSSetup.exe" /s /z\"SERVER=server.organization.com, FEATURES=BLM-EME, BLM_ONLY=1, SUPPRESSREBOOT=1\""
```

# Desinstalar o Instalador Principal

- A Dell recomenda a utilização do [Desinstalador do Data Security](#) para remover o conjunto de aplicações do Data Security.
- Cada componente deve ser desinstalado separadamente e, em seguida, deve ser efetuada a desinstalação do instalador principal do . Os clientes devem ser desinstalados numa **ordem específica para impedir falhas na desinstalação**.
- Sigas as instruções que constam em [Extrair os Instaladores Subordinados do Instalador Principal](#) para obter instaladores subordinados.
- Certifique-se de que é utilizada a mesma versão do instalador principal (e, por conseguinte, clientes) do .
- Este capítulo direciona-o para outros capítulos que contêm instruções *detalhadas* sobre como desinstalar os instaladores subordinados. Este capítulo explica **apenas** o último passo da desinstalação do instalador principal.
- Desinstale os clientes pela seguinte ordem.
  1. [Desinstalar o Encryption](#).
  2. [Desinstalar o SED Manager](#).
  3. [Desinstalar o Full Disk Encryption](#)
  4. [Desinstalar o BitLocker Manager](#).
- Avance para [Desinstalar o instalador principal](#).

## Desinstalar o Instalador Principal do

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

### Desinstalação por linha de comando

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

```
"DDSSetup.exe" /s /x
```

Reinicie o computador quando concluído.

## Instalar utilizando instaladores subordinados

- Para instalar ou atualizar 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](#).
- Os exemplos de comandos incluídos nesta secção assumem que os comandos são executados a partir de C:\extracted.
- 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.
- Utilize estes instaladores para instalar os clientes utilizando uma instalação com script, ficheiros batch ou qualquer outra tecnologia push disponível na sua organização.
- Nestes exemplos de linha de comandos, o reinício foi suprimido. No entanto, é necessário um eventual reinício.

**Nota:** a Encriptação Baseada em Políticas só pode ser iniciada após o reinício do computador.

- Ficheiros de registo - O Windows cria ficheiros de registo de instalação do instalador subordinado únicos para o utilizador com sessão iniciada em %temp%, localizados em C:\Users\\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 .msi padrão pode ser utilizado para criar um ficheiro de registo, utilizando /I\*v C:\<any directory>\<any log file name>.log.

- Todos os instaladores subordinados utilizam as mesmas opções .msi básicas e as mesmas opções de visualização em instalações por linha de comandos, exceto onde referido. 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                                                                                           |

### NOTA:

Com /v, as opções predefinidas da Microsoft ficam disponíveis. Para ver uma lista de opções, consulte [este artigo](#).

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

| Opção      | Significado       |
|------------|-------------------|
| /norestart | Suprimir reinício |


- Dê a instrução aos utilizadores para consultar o seguinte documento e ficheiros de ajuda para assistência de aplicação:
  - Consulte a *Dell Encrypt Help (Ajuda do Dell Encrypt)* para saber como utilizar as funcionalidades do Encryption. Aceda à ajuda a partir de <Install dir>\Program Files\Dell\Dell Data Protection\Encryption\Help.
  - Consulte a *Encryption External Media Help (Ajuda do Encryption External Media)* para saber como utilizar as funcionalidades do Encryption External Media. Aceda à ajuda a partir de <Install dir>\Program Files\Dell\Dell Data Protection\Encryption\EMS.
  - Consulte a *Encryption Enterprise* para saber como utilizar as funcionalidades da autenticação PBA, . Aceda à ajuda a partir de <Install dir>\Program Files\Dell\Dell Data Protection\Client Security Framework\Help.

## Instalar controladores

- Os controladores e firmware do ControlVault, leitores de impressão digital e smart cards não estão incluídos nos ficheiros executáveis do instalador principal ou do instalador subordinado do . Os controladores e firmware devem 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 vendedor correspondente.

## Instalar o Encryption

- Se a sua organização utilizar um certificado assinado por uma autoridade raiz, como EnTrust ou Verisign, consulte os [Requisitos do Encryption](#). É necessária uma alteração na configuração de registo no computador cliente para ativar a validação do certificado.
- Após a conclusão da instalação, os utilizadores devem atualizar as respetivas políticas clicando com o botão direito do rato no ícone do Dell Encryption, na área de notificação e selecionando *Procurar atualizações de políticas*.
- O instalador do Encryption está localizado em:
  - **Em [dell.com/support](http://dell.com/support)** - Se necessário, [Obter o software](#) a partir de [dell.com/support](http://dell.com/support) e, em seguida, [Extrair os Instaladores Subordinados do Instalador Principal](#). Após a extração, localize o ficheiro em C : \extracted\Encryption.
  - **Na sua conta FTP Dell** - Localize o pacote de instalação em Encryption-Enterprise-10.x.x.xxx.zip e, em seguida, [Extrair os instaladores subordinados do instalador principal](#). Após a extração, localize o ficheiro em C : \extracted\Encryption.
  -  **NOTA:** Os registos Dell Encryption não especificam se a falha da instalação resultou de espaço insuficiente no disco.

## Instalação com linha de comandos

- A tabela seguinte descreve os parâmetros disponíveis para a instalação.

| Parâmetros                                                            |
|-----------------------------------------------------------------------|
| SERVERHOSTNAME=<ServerName> (FQDN do Dell Server para reativação)     |
| POLICYPROXYHOSTNAME=<RGKName> (FQDN do Proxy de política predefinido) |


| Parâmetros                                                                                                                              |
|-----------------------------------------------------------------------------------------------------------------------------------------|
| MANAGEDDOMAIN=<MyDomain> (o domínio a ser utilizado pelo dispositivo)                                                                   |
| DEVICESTERVERURL=<DeviceServerName/SecurityServerName> (URL utilizado para ativação; normalmente inclui nome do servidor, porta e xapi) |
| GKPORT=<NewGKPort> (Porta do Gatekeeper)                                                                                                |
| MACHINEID=<MachineName> (Nome do computador)                                                                                            |
| RECOVERYID=<RecoveryID> (ID de recuperação)                                                                                             |
| REBOOT=ReallySuppress (o valor zero permite a reinicialização automática, ReallySuppress desativa a reinicialização)                    |
| HIDEOVERLAYICONS=1 (0 ativa os ícones sobrepostos, 1 desativa os ícones sobrepostos)                                                    |
| HIDESYSTRAYICON=1 (0 ativa o ícone na área de notificação, 1 desativa o ícone na área de notificação)                                   |
| ENABLE_FDE_LM=1 (permite a instalação do Dell Encryption num computador com a Full Disk Encryption ativa)                               |
| EME=1 (Instala o modo Encryption External Media)                                                                                        |

Para obter uma lista computadores basic .msi e opções de visualização que podem ser utilizadas em linhas de comandos, consulte [Instalar utilizando os instaladores subordinados](#).

- A tabela que se segue detalha os parâmetros opcionais adicionais relacionados com a ativação.

| Parâmetros                                                                                                                                                                              |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SLOTTEDACTIVATON=1 (0 desativa as ativações adiadas/programadas, 1 ativa as ativações adiadas/programadas)                                                                              |
| SLOTINTERVAL=45.120 (programa as ativações através da notação x,x, onde o primeiro valor é o limite inferior da programação e o segundo valor é o limite superior - em segundos)        |
| CALREPEAT=600 (TEM de igualar ou exceder o limite superior definido em SLOTINTERVAL. Número de segundos que o Encryption aguarda antes de gerar uma ativação com base no SLOTINTERVAL.) |

### Exemplo de linha de comandos

 **NOTA:** Substitua DEVICESTERVERURL=https://server.organization.com:8081/xapi (sem a barra à direita) se o seu Security Management Server for anterior a v7.7.

- O seguinte exemplo instala o Dell Encryption com parâmetros predefinidos (Encryption, Encrypt for Sharing, sem caixas de diálogo, sem barra de progresso, reinício automático, instalado na localização predefinida C:\Program Files\Dell\Dell Data Protection\Encryption).

```
DDPE_XXbit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com
POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION
DEVICESTERVERURL=https://server.organization.com:8443/xapi/ /qn"
```

Comando MSI:

```
msiexec.exe /i "Dell Data Protection Encryption.msi" /qn REBOOT="ReallySuppress"
SERVERHOSTNAME="server.organization.com" POLICYPROXYHOSTNAME="rgk.organization.com"
MANAGEDDOMAIN="ORGANIZATION" DEVICESTERVERURL="https://server.organization.com:8443/xapi/"
```

- O seguinte exemplo instala o Encryption e o Encrypt for Sharing, oculta o ícone Dell Encryption da área de notificação, oculta os ícones de sobreposição, sem caixas de diálogo, sem barra de progresso, suprime o reinício, instalado na localização predefinida C:\Program Files\Dell\Dell Data Protection\Encryption.

```
DDPE_XXbit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com
POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION"
```

```
DEVICESTERVERURL=https://server.organization.com:8443/xapi/ HIDESTRAYICON=1  
HIDEOVERLAYICONS=1 REBOOT=ReallySuppress /qn"
```

Comando MSI:

```
msiexec.exe /i "Dell Data Protection Encryption.msi" /qn REBOOT="ReallySuppress"  
SERVERHOSTNAME="server.organization.com" POLICYPROXYHOSTNAME="rgk.organization.com"  
MANAGEDDOMAIN="ORGANIZATION" DEVICESTERVERURL="https://server.organization.com:8443/xapi/"  
HIDESTRAYICON="1" HIDEOVERLAYICONS="1"
```

### Exemplo de linha de comandos para instalar apenas o Encryption External Media

- Instalação silenciosa, sem barra de progresso, reinício automático, instalado na localização predefinida C:\Program Files\Dell\Dell Data Protection\Encryption.

```
DDPE_XXbit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com  
POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION  
DEVICESTERVERURL=https://server.organization.com:8443/xapi/ EME=1 /qn"
```

Comando MSI:

```
msiexec.exe /i "Dell Data Protection Encryption.msi" /qn REBOOT="ReallySuppress"  
SERVERHOSTNAME="server.organization.com" POLICYPROXYHOSTNAME="rgk.organization.com"  
MANAGEDDOMAIN="ORGANIZATION" DEVICESTERVERURL="https://server.organization.com:8443/xapi/"
```

- Instalação silenciosa, sem reinício, instalado na localização predefinida C:\Program Files\Dell\Dell Data Protection\Encryption).

```
DDPE_XXbit_setup.exe /s /v"EME=1  
SERVERHOSTNAME=server.organization.com POLICYPROXYHOSTNAME=rgk.organization.com  
DEVICESTERVERURL=https://server.organization.com:8443/xapi/ MANAGEDDOMAIN=ORGANIZATION /  
norestart /qn"
```

Comando MSI:

```
msiexec.exe /i "Dell Data Protection Encryption.msi" /qn REBOOT="ReallySuppress" EME="1"  
SERVERHOSTNAME="server.organization.com" POLICYPROXYHOSTNAME="rgk.organization.com"  
DEVICESTERVERURL="https://server.organization.com:8443/xapi/" MANAGEDDOMAIN="ORGANIZATION"
```

- **NOTA:**

Embora a caixa Acerca de no cliente apresente as informações do número de versão do software, não indica se está instalado o Encryption (instalação completa) ou apenas o Encryption External Media. Para localizar estas informações, aceda a C:\ProgramData\Dell\Dell Data Protection\Encryption\CMGShield.log e procure a seguinte entrada:

```
[<date/timestamp> DeviceInfo: < >] Informação do Shield - SM=Apenas suporte multimédia externo, SB=DELL,  
UNF=FQUN, último varrimento={0, 0}
```

### Exemplo de linha de comandos para converter o Encryption External Media para o Encryption (instalação completa)

- **NOTA:** A conversão do Encryption External Media para o Encryption (instalação completa) não é suportada com atualizações.

- A descriptação não é necessária durante a conversão do Encryption External Media para o Encryption (instalação completa).

```
DDPE_XXbit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com  
POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION  
DEVICESTERVERURL=https://server.organization.com:8443/xapi/ REINSTALL=ALL EME=0  
REINSTALLMODE=vamus /qn"
```

Comando MSI:

```
msiexec.exe /i "Dell Data Protection Encryption.msi" /qn REBOOT="ReallySuppress"  
SERVERHOSTNAME="server.organization.com" POLICYPROXYHOSTNAME="rgk.organization.com"  
MANAGEDDOMAIN="ORGANIZATION" DEVICESTERVERURL="https://server.organization.com:8443/xapi/"  
REINSTALL="ALL" EME="0" REINSTALLMODE="vamus"
```

- **Exemplo de linha de comandos para instalar o Dell Encryption com a Full Disk Encryption**

**\Encryption**

- O seguinte exemplo instala o Dell Encryption com parâmetros predefinidos (Encryption, Encrypt for Sharing, sem caixas de diálogo, sem barra de progresso, reinício automático, instalado na localização predefinida C:\Program Files\Dell\Dell Data Protection\Encryption).

```
DDPE_XXbit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com
POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION
DEVICESTERURL=https://server.organization.com:8443/xapi/ /qn"
```

De seguida:

### \Encryption Management Agent

O exemplo seguinte instala a Full Disk Encryption gerida remotamente e permite a instalação num computador protegido por Dell Encryption (instalação automática, sem reinício, sem entrada na lista de Programas do Painel de controlo, instalada na localização predefinida C:\Program Files\Dell\Dell Data Protection\Encryption).

```
EMAgent_64bit_setup.exe /s /v"CM_EDITION=1 ENABLE_FDE_LM=1
FEATURE=FDE SERVERHOST=server.organization.com SERVERPORT=8888
SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443 ARPSYSTEMCOMPONENT=1 /
norestart /qn"
```

- **Exemplo de linha de comandos para instalar o Encryption External Media e a Full Disk Encryption.**

### \Encryption

O exemplo seguinte instala o Encryption External Media com uma instalação silenciosa, sem barra de progresso, reinício automático, instalado na localização predefinida C:\Program Files\Dell\Dell Data Protection\Encryption.

```
DDPE_XXbit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com
POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION
DEVICESTERURL=https://server.organization.com:8443/xapi/ EME=1 /qn"
```

De seguida:

### \Encryption Management Agent

O exemplo seguinte instala a Full Disk Encryption gerida remotamente e permite a instalação num computador protegido por Dell Encryption (instalação automática, sem reinício, sem entrada na lista de Programas do Painel de controlo, instalado na localização predefinida C:\Program Files\Dell\Dell Data Protection).

```
EMAgent_64bit_setup.exe /s /v"CM_EDITION=1 ENABLE_FDE_LM=1
FEATURE=FDE SERVERHOST=server.organization.com SERVERPORT=8888
SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443 ARPSYSTEMCOMPONENT=1 /
norestart /qn"
```

- **Exemplo de linha de comandos para instalar o Encryption External Media e substituir uma instalação da Full Disk Encryption existente.**

O exemplo seguinte permite instalar o Encryption External Media e substituir a instalação da Full Disk Encryption existente com uma instalação silenciosa, sem barra de progresso, reinício automático, instalado na localização predefinida C:\Program Files\Dell\Dell Data Protection.

```
DDPE_XXbit_setup.exe /s /v"EME=1 SERVERHOSTNAME=server.organization.com
POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION
DEVICESTERURL=https://server.organization.com:8443/xapi/ ENABLE_FDE_LM=1 /
norestart /qn"
```

- **Exemplo de linha de comandos para instalar um cliente de encriptação gerido remotamente e substituir uma instalação Full Disk Encryption existente.**

O exemplo seguinte permite instalar o Dell Encryption e substituir uma instalação Full Disk Encryption existente com parâmetros predefinidos (cliente do Encryption, Encrypt for Sharing, sem caixas de diálogo, sem barra de progresso, reinício automático, instalado na localização predefinida C:\Program Files\Dell\Dell Data Protection) e com registos de instalação em C:\Dell. **Nota:** para uma criação de registos bem-sucedida, o diretório C:\Dell tem de existir antes da instalação.

```
DDPE_XXbit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com
POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION
DEVICESTERURL=https://server.organization.com:8443/xapi/ ENABLE_FDE_LM=1 /
norestart /qn /l*v C:\Dell\DellEncryptionInstall.log"
```

**NOTA:** Algumas versões mais antigas poderão requerer caracteres de \" à volta dos valores dos parâmetros. Por exemplo:

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

## Instalar a Full Disk Encryption

- Se a sua organização utilizar um certificado assinado por uma autoridade raiz, como EnTrust ou Verisign, consulte os [Requisitos da Full Disk Encryption](#). É necessária uma alteração na configuração de registro no computador cliente para ativar a validação de confiança SSL/TLS.
- Os utilizadores iniciam sessão na PBA utilizando as respetivas credenciais do Windows.

## Instalação com linha de comandos

- A tabela seguinte descreve os parâmetros disponíveis para a instalação.

| Parâmetros                                                                                                |
|-----------------------------------------------------------------------------------------------------------|
| CM_EDITION=1 (gestão remota)                                                                              |
| INSTALLDIR=(alterar o destino da instalação)                                                              |
| SERVERHOST=(securityserver.organization.com)                                                              |
| SERVERPORT=8888                                                                                           |
| SECURITYSERVERHOST=(securityserver.organization.com)                                                      |
| SECURITYSERVERPORT=8443                                                                                   |
| FEATURE=FDE                                                                                               |
| ENABLE_FDE_LM=1 (permite a instalação da Full Disk Encryption num computador com o Dell Encryption ativo) |

Para obter uma lista computadores basic .msi e opções de visualização que podem ser utilizadas em linhas de comandos, consulte [Instalar utilizando os instaladores subordinados](#).

### Exemplo de linha de comandos

#### Encryption Management Agent

- O exemplo seguinte instala a Full Disk Encryption gerida remotamente (instalação silenciosa, sem reinício e instalada na localização predefinida C:\Program Files\Dell\Dell Data Protection\Encryption).

```
EMAgent_64bit_setup.exe /s /v"CM_EDITION=1 FEATURE=FDE SERVERHOST=server.organization.com
SERVERPORT=8888 SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443 /
norestart /qn"
```

- **Encryption Management Agent**

- O exemplo seguinte instala a Full Disk Encryption gerida remotamente e permite a instalação num computador protegido por Dell Encryption (instalação automática, sem reinício e instalada na localização predefinida C:\Program Files\Dell\Dell Data Protection\Encryption).

```
EMAgent_64bit_setup.exe /s /v"CM_EDITION=1 ENABLE_FDE_LM=1
FEATURE=FDE SERVERHOST=server.organization.com SERVERPORT=8888
SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443 /norestart /qn"
```

- **Exemplo de linha de comandos para instalar a Full Disk Encryption e o Encryption External Media.**

#### Encriptação

O exemplo seguinte instala o Encryption External Media com uma instalação silenciosa, sem barra de progresso, reinício automático, instalado na localização predefinida C:\Program Files\Dell\Dell Data Protection\Encryption.

```
DDPE_XXbit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com  
POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION  
DEVICESTERURL=https://server.organization.com:8443/xapi/ EME=1 /qn"
```

Em seguida:

### Encryption Management Agent

O exemplo seguinte instala a Full Disk Encryption gerida remotamente e permite a instalação num computador protegido por Dell Encryption (instalação automática, sem reinício, sem entrada na lista de Programas do Painel de controlo, instalada na localização predefinida C:\Program Files\Dell\Dell Data Protection\Encryption).

```
EMAgent_64bit_setup.exe /s /v"CM_EDITION=1 ENABLE_FDE_LM=1  
FEATURE=FDE SERVERHOST=server.organization.com SERVERPORT=8888  
SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443 /norestart /qn"
```

## Instalar o Encryption em sistemas operativos de servidor

Existem dois métodos disponíveis para instalar o Encryption em sistemas operativos de servidor. Selecione um dos seguintes métodos:

- [Instalar interativamente o Encryption em sistemas operativos de servidor](#)

O Encryption em sistemas operativos de servidor apenas pode ser instalado interativamente em computadores com sistemas operativos de servidor em execução. A instalação em computadores com sistemas operativos que não sejam de servidor deve ser efetuada por linha de comandos, com o parâmetro SERVERMODE=1 especificado.

- [Instalar o Encryption em sistemas operativos de servidor utilizando a Linha de comandos](#)

### Conta de utilizador virtual

- Como parte do processo de instalação, é criada uma **conta de utilizador do servidor virtual** para utilização exclusiva do Encryption em sistemas operativos de servidor. A palavra-passe e a autenticação DPAPI estão desativadas, de forma a que apenas o utilizador do servidor virtual tenha acesso às chaves de encriptação.

### Antes de começar

- A conta de utilizador com a qual se realiza a instalação deve ser de utilizador do domínio, com permissões com nível de administrador.
- Para ignorar o requisito ou executar o Encryption em sistemas operativos de servidor em servidores sem domínio ou com vários domínios, defina a propriedade `ssos.domainadmin.verify` para `false` no ficheiro `application.properties`. O ficheiro é guardado nos seguintes caminhos de ficheiro, com base no Dell Server utilizado:

Security Management Server - `<installation_dir>/Security Server/conf/application.properties`

Security Management Server Virtual - `/opt/dell/server/security-server/conf/application.properties`

- O servidor terá de suportar controlo de portas.

As políticas do Sistema de controlo de portas afetam os suportes de dados amovíveis em servidores protegidos, por exemplo, controlando o acesso e a utilização das portas USB do servidor pelos dispositivos USB. A política da porta USB aplica-se às portas USB externas. A funcionalidade das portas USB internas não é afetada pela política de portas USB. Se a política de portas USB estiver desativada, o teclado e o rato USB não funcionam e o utilizador não pode utilizar o computador, salvo se, antes da aplicação da política, for estabelecida uma Ligação ao Ambiente de Trabalho Remoto.

- Para uma ativação bem-sucedida, o computador deve estar ligado à rede.
- Quando o Trusted Platform Module (TPM) estiver disponível, é utilizado para selar a Chave para Fins Gerais no hardware Dell. Se não estiver disponível um TPM, é utilizada a API de Proteção de Dados (DPAPI) da Microsoft para proteger a Chave para Fins Gerais.

Quando instalar um novo sistema operativo num computador Dell com TPM e com o Server Encryption em execução, elimine o TPM do BIOS. Consulte [este artigo](#) para obter instruções.

- O ficheiro de registo de instalação está localizado no diretório `%temp%` do utilizador, localizado em `C:\Users\<user name>\AppData\Local\Temp`. Para localizar o ficheiro de registo correto, encontre o ficheiro cujo nome comece com MSI e termine com a extensão `.log`. O ficheiro inclui um carimbo de data/hora coincidente com a hora em que o instalador foi executado.

- O Encryption não é suportado em servidores que fazem parte de sistemas de ficheiros distribuídos (DFS).

### Extrair os instaladores subordinados

- Para instalar o Encryption em sistemas operativos de servidor, deve primeiro extrair o instalador subordinado, **DDPE\_xxbit\_setup.exe**, do instalador principal. Consulte [Extrair os Instaladores Subordinados do Instalador Principal](#).

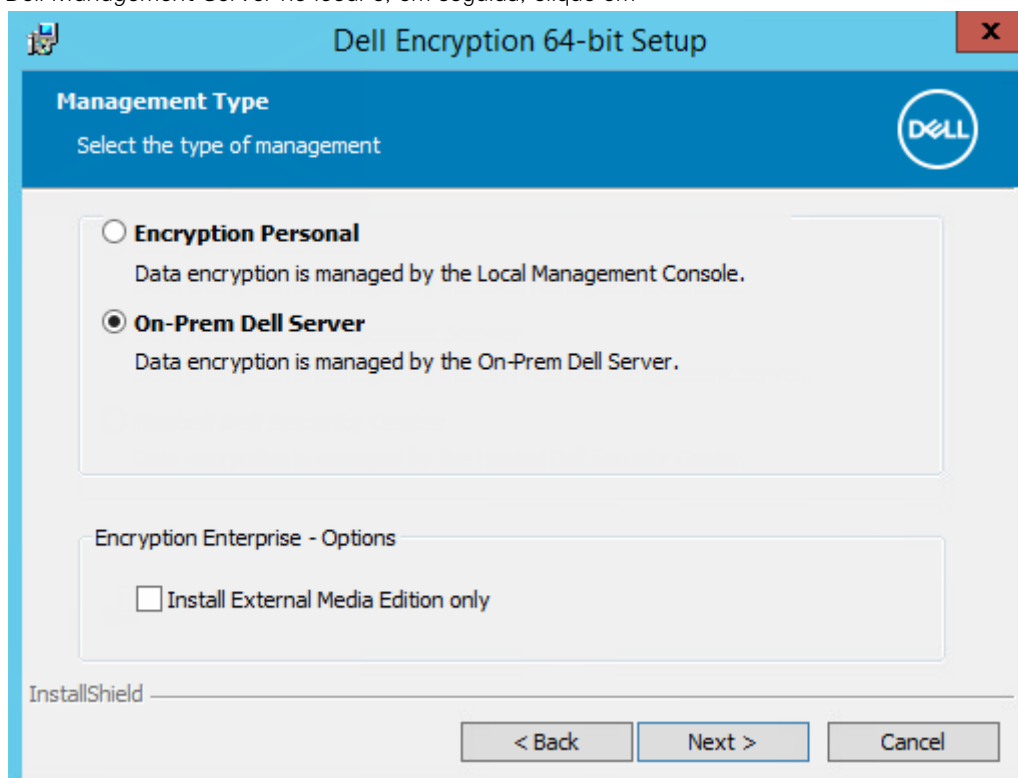
## Instalar interativamente

- Utilize estas instruções para instalar o Encryption em sistemas operativos de servidor de forma interativa. Este instalador inclui os componentes de que necessita para realizar encriptação de software.
1. Localize o ficheiro **DDPE\_XXbit\_setup.exe** na pasta `C:\extracted\Encryption`. Copie-o para o computador local.
  2. Se estiver a instalar o Encryption em sistemas operativos de servidor, faça duplo clique em **DDPE\_XXbit\_setup.exe** para abrir o instalador.

### NOTA:

Quando o Encryption em sistemas operativos de servidor é instalado num computador que tenha um sistema operativo de servidor, como o Windows Server 2012 R2, a instalação é realizada automaticamente em SERVERMODE.

3. Na caixa de diálogo de Boas-vindas, clique em **Seguinte**.
4. No ecrã Contrato de licença, leia o contrato, aceite os termos e clique em **Seguinte**.
5. Selecione *Dell Management Server no local* e, em seguida, clique em



**Seguinte.**

6. Clique em **Seguinte** para instalar na localização predefinida.
7. Clique em **Seguinte** para ignorar a caixa de diálogo *Tipo de gestão*.
8. Em *Nome do Security Management Server*, introduza/valide o nome de anfitrião totalmente qualificado do Dell Server para gerir o utilizador pretendido (por exemplo, `server.organization.com`).  
Introduza o nome de domínio em *Domínio gerido* (por exemplo, organização). Clique em **Seguinte**.
9. Na porta e nome do anfitrião da Policy Proxy, introduza/valide a informação e clique em **Seguinte**.
10. No URL do Device Server, introduza/valide a informação e clique em **Seguinte**.
11. Clique em **Instalar** para dar início à instalação.  
A instalação poderá demorar vários minutos.

12. Quando a configuração estiver concluída, clique em **Concluir**.

A instalação está concluída.

13. Reinicie o computador. A Dell recomenda suspender o reinício apenas se precisar de tempo para guardar o seu trabalho e fechar aplicações. A encriptação só pode ser iniciada após o reinício do computador.

## Instalar utilizando a Linha de comandos

### Localize o instalador em C:\extracted\Encryption

- Utilize o **DDPE\_xxbit\_setup.exe** para instalar ou atualizar utilizando uma instalação com script, ficheiros de batch ou qualquer outra tecnologia disponível na sua organização.

### Opções

A tabela seguinte descreve as opções disponíveis para a instalação.

| Opção | Significado                                                |
|-------|------------------------------------------------------------|
| /v    | Passa variáveis para o .msi dentro do DDPE_XXbit_setup.exe |
| /a    | Instalação administrativa                                  |
| /s    | Modo silencioso                                            |

### Parâmetros

A tabela seguinte descreve os parâmetros disponíveis para a instalação.


| Componente        | Ficheiro de registo             | Parâmetros da Linha de Comandos                  |
|-------------------|---------------------------------|--------------------------------------------------|
| Todos             | /I*v [fullpath][filename].log * | SERVERHOSTNAME=<Security Management Server Name> |
|                   |                                 | SERVERMODE=1                                     |
|                   |                                 | POLICYPROXYHOSTNAME=<RGK Name>                   |
|                   |                                 | MANAGEDDOMAIN=<My Domain>                        |
|                   |                                 | DEVICESTRIVERURL=<Activation Server Name>        |
|                   |                                 | GKPORT=<New GK Port>                             |
|                   |                                 | MACHINEID=<Machine Name>                         |
|                   |                                 | RECOVERYID=<Recovery ID>                         |
|                   |                                 | REBOOT=ReallySuppress                            |
|                   |                                 | HIDEOVERLAYICONS=1                               |
| HIDESYSTRAYICON=1 |                                 |                                                  |
|                   |                                 | EME=1                                            |

#### **NOTA:**

Embora seja possível suprimir o reinício, este será eventualmente necessário. A encriptação só pode ser iniciada após o reinício do computador.

### Opções

A tabela seguinte descreve as opções de visualização que podem ser especificadas no final do argumento passado para a opção /v.

| Opção                                                                                                                                                                             | Significado                                                                                        |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------|
| /q                                                                                                                                                                                | Sem caixa de diálogo de Progresso, reinicia-se após a conclusão do processo                        |
| /qb                                                                                                                                                                               | Caixa de diálogo de Progresso com botão <b>Cancelar</b> , solicita o reinício                      |
| /qb-                                                                                                                                                                              | Caixa de diálogo de Progresso com botão <b>Cancelar</b> , reinicia-se após a conclusão do processo |
| /qb!                                                                                                                                                                              | Caixa de diálogo de Progresso sem botão <b>Cancelar</b> , solicita o reinício                      |
| /qb!-                                                                                                                                                                             | Caixa de diálogo de Progresso sem botão <b>Cancelar</b> , reinicia-se após a conclusão do processo |
| /qn                                                                                                                                                                               | Sem interface de utilizador                                                                        |
|  <b>NOTA:</b><br>Não utilize /q e /qn na mesma linha de comandos. Utilize apenas ! e - após /qb. |                                                                                                    |

- O parâmetro da linha de comandos, SERVERMODE=1, é considerado apenas durante novas instalações. O parâmetro é ignorado nas desinstalações.
- Inclua um valor que contenha um ou mais caracteres especiais, como um espaço em branco, entre aspas duplas de escape.
- O parâmetro DEVICESERVERURL é sensível a maiúsculas e minúsculas.

#### Exemplo de instalação com Linha de Comandos

- O exemplo seguinte instala o Encryption no modo do sistemas operativo do servidor com parâmetros predefinidos (Encryption, instalação silenciosa, Encrypt for Sharing, sem caixas de diálogo, sem barra de progresso, reinício automático, instalado na localização predefinida C:\Program Files\Dell\Dell Data Protection).

```
DDPE_XXbit_setup.exe /s /v"SERVERMODE=1 SERVERHOSTNAME=server.organization.com
POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION
DEVICESERVERURL=https://server.organization.com:8443/xapi/ /qn"
```

Comando MSI:

```
msiexec.exe /i "Dell Data Protection Encryption.msi" /qn
REBOOT="ReallySuppress" SERVERMODE="1" SERVERHOSTNAME="server.organization.com"
POLICYPROXYHOSTNAME="rgk.organization.com" MANAGEDDOMAIN="ORGANIZATION"
DEVICESERVERURL="https://server.organization.com:8443/xapi/"
```

- O exemplo seguinte instala o Encryption no modo de sistema operativo do servidor com um ficheiro de registo e parâmetros predefinidos (Encryption, instalação silenciosa, Encrypt for Sharing, sem caixas de diálogo, sem barra de progresso, sem reinício, instalado na localização predefinida C:\Program Files\Dell\Dell Data Protection\Encryption) e especifica um nome de ficheiro de registo personalizado que termina com um número (DDP\_ssos-090.log), que é incrementado se a linha de comandos for executada mais do que uma vez no mesmo servidor. Para especificar uma localização de registo diferente da localização predefinida onde está localizado o executável, forneça o caminho completo no comando. Por exemplo, /!v C:\Logs\DDP\_ssos-090.log cria registos de instalação em C:\Logs.

```
DDPE_XXbit_setup.exe /s /v"SERVERMODE=1 SERVERHOSTNAME=server.organization.com
POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION
DEVICESERVERURL=https://server.organization.com:8443/xapi/ /!v DDP_ssos-090.log /
norestart/qn"
```

Comando MSI:

```
msiexec.exe /i "Dell Data Protection Encryption.msi" /qn SERVERMODE="1"
SERVERHOSTNAME="server.organization.com" POLICYPROXYHOSTNAME="rgk.organization.com"
MANAGEDDOMAIN="ORGANIZATION" DEVICESERVERURL="https://server.organization.com:8443/
xapi/" /!v DDP_ssos-090.log /norestart/qn"
```

Reinicie o computador após a instalação. A Dell recomenda suspender o reinício apenas se precisar de tempo para guardar o seu trabalho e fechar aplicações. A encriptação só pode ser iniciada após o reinício do computador.

## Ativar

- Certifique-se de que o nome do computador do servidor é o nome do endpoint a visualizar na Management Console.
- Para a ativação inicial, um utilizador interativo com credenciais de administrador do domínio deve iniciar sessão no servidor, pelo menos, uma vez. O utilizador com sessão iniciada pode ser de qualquer tipo: utilizador de domínio ou de fora do domínio, ligado ao ambiente de trabalho remoto ou interativo no servidor, mas a ativação requer credenciais de administrador do domínio.
- No seguimento do reinício após a instalação, é apresentada a caixa de diálogo Ativação. O administrador deve introduzir as credenciais de administrador de domínio com um nome de utilizador no formato Nome Principal de Utilizador (UPN). O Encryption em sistemas operativos de servidor não é ativado automaticamente.
- Durante a ativação inicial, é criada a conta de utilizador do servidor virtual. Após a ativação inicial, o computador é reiniciado para que a ativação do dispositivo possa começar.
- Durante a fase de autenticação e ativação do dispositivo, é atribuída ao computador uma ID de máquina única, são criadas e agrupadas chaves de encriptação e é estabelecida uma relação entre o grupo de chaves de encriptação e o [utilizador do servidor virtual](#). O grupo de chaves de encriptação associa as políticas e as chaves de encriptação ao novo utilizador do servidor virtual para criar uma relação inquebrável entre os dados encriptados, o computador específico e o utilizador do servidor virtual. Após a ativação do dispositivo, o utilizador do servidor virtual é apresentado na Management Console como SERVER-USER@<fully qualified server name>. Para obter mais informações sobre a ativação, consulte [Ativação num sistema operativo de servidor](#).

### NOTA:

Se mudar o nome do servidor após a ativação, o nome do mesmo não é alterado na Management Console. No entanto, se o Encryption em sistemas operativos de servidor for novamente ativado depois de alterar o nome do servidor, o novo nome do servidor será apresentado na Management Console.

Uma vez após cada reinício, será apresentada a caixa de diálogo Ativação para solicitar ao utilizador a ativação do Encryption em sistemas operativos de servidor. Para concluir a ativação, siga estes passos:

1. Inicie sessão no servidor no próprio servidor ou através de uma Ligação ao Ambiente de Trabalho Remoto.
2. Introduza o nome de utilizador de um administrador do domínio no formato UPN e a respetiva palavra-passe e clique em **Ativar**. Esta é a mesma caixa de diálogo de Ativação que surge sempre que um sistema não ativado é reiniciado.

O Dell Server emite uma chave de encriptação para a ID de máquina, cria a **conta de utilizador do servidor virtual**, cria uma chave de encriptação para a conta de utilizador, agrupa as chaves de encriptação e cria a relação entre o pacote de encriptação e a conta de utilizador do servidor virtual.

3. Clique em **Fechar**.

Após a ativação, é iniciada a encriptação.

4. Quando o varrimento de encriptação estiver concluído, reinicie o computador para processar quaisquer ficheiros anteriormente utilizados. Este passo é importante por questões de segurança.

### NOTA:

Se a política *Credenciais do Windows seguras* estiver ativada, o Encryption em sistemas operativos de servidor encripta os ficheiros `\windows\system32\config`, que incluem credenciais do Windows. Os ficheiros em `\Windows\system32\config` são encriptados mesmo que a política *Encriptação SDE ativada* esteja desativada. Por predefinição, a política *Credenciais do Windows seguras* está selecionada.

### NOTA:

Depois de reiniciar o computador, a autenticação em conformidade com a chave de encriptação Comum requer *sempre* a chave de Computador do servidor protegido. O Dell Server devolverá uma chave de desbloqueio para aceder às chaves de encriptação e políticas do cofre (as chaves e políticas são para o servidor, não para o utilizador). Sem a chave de Computador do servidor, não é possível desbloquear a chave de encriptação Comum e o computador não pode receber atualizações de política.

### Confirmar ativação

Na consola local, abra a caixa de diálogo **Acerca de** para se certificar de que o Encryption em sistemas operativos de servidor está instalado, autenticado e no modo de Servidor. Se a ID do Encryption Client apresentar cor **vermelha**, a encriptação ainda não foi ativada.

## Utilizador do servidor virtual

- Na Management Console, os servidores protegidos podem ser encontrados pelo nome da máquina. Além disso, cada servidor protegido tem a sua própria conta de utilizador do servidor virtual. Cada conta tem um nome de utilizador estático exclusivo e um nome de máquina exclusivo.
- A conta de utilizador do servidor virtual apenas é utilizada pelo Encryption em sistemas operativos de servidor e é, de outra forma, transparente na operação do servidor protegido. O utilizador do servidor virtual está associado ao grupo de chaves de encriptação e à Proxy de política.
- Após a ativação, a conta de utilizador do servidor virtual é a conta de utilizador ativada e associada ao servidor.
- Uma vez ativado o utilizador do servidor virtual, serão ignoradas todas as notificações de início/fim de sessão do servidor. Em vez disso, durante o arranque, o computador efetua automaticamente a autenticação com o utilizador do servidor virtual e, em seguida, transfere a chave de computador do Dell Server.

## Instalar o SED Manager e a Autenticação Avançada PBA

- Se a sua organização utilizar um certificado assinado por uma autoridade raiz, como EnTrust ou Verisign, consulte os [Requisitos SED](#). É necessária uma alteração na configuração de registo no computador cliente para ativar a validação de confiança SSL/TLS.
- Os utilizadores iniciam sessão na PBA utilizando as respetivas credenciais do Windows.
- Os instaladores do SED Manager e da Autenticação Avançada PBA encontram-se em:
  - **Em [dell.com/support](#)** - Se necessário, [Obter o software](#) a partir de [dell.com/support](#) e, em seguida, [Extrair os Instaladores Subordinados do Instalador Principal](#). Após a extração, localize o ficheiro em `C:\extracted\Encryption Management Agent`.
  - **Na sua conta FTP Dell** - Localize o pacote de instalação em `Encryption-Enterprise-10.x.x.xxx.zip` e, em seguida, [Extrair os instaladores subordinados do instalador principal](#). Após a extração, localize o ficheiro em `C:\extracted\Encryption Management Agent`.

## Instalação com linha de comandos

- A tabela seguinte descreve os parâmetros disponíveis para a instalação.

| Parâmetros                                                         |
|--------------------------------------------------------------------|
| CM_EDITION=1 <remote management>                                   |
| INSTALLDIR=<change the installation destination>                   |
| SERVERHOST=<securityserver.organization.com>                       |
| SERVERPORT=8888                                                    |
| SECURITYSERVERHOST=<securityserver.organization.com>               |
| SECURITYSERVERPORT=8443                                            |
| ARPSYSTEMCOMPONENT=1 <no entry in the Control Panel Programs list> |

Para obter uma lista computadores basic .msi e opções de visualização que podem ser utilizadas em linhas de comandos, consulte [Instalar utilizando os instaladores subordinados](#).

O exemplo que se segue ordena a instalação ou a atualização do Encryption Management Agent.

### Exemplo de linha de comandos

**\Encryption Management Agent**

- O seguinte exemplo instala o SED Manager gerido remotamente, o Encryption Management Agent e a consola de segurança local (instalação silenciosa, sem reinício, sem entrada na lista de Programas do Painel de Controlo, instalado na localização predefinida C:\Program Files\Dell\Dell Data Protection\Encryption).

```
EMAgent_XXbit_setup.exe /s /v"CM_EDITION=1 SERVERHOST=server.organization.com
SERVERPORT=8888 SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443
ARPSYSTEMCOMPONENT=1 /norestart /qn"
```

## Instalar o BitLocker Manager

- **NOTA:** Se a sua organização requer a utilização de fornecedores de credenciais externos, o Encryption Management Agent tem de ser instalado ou atualizado com o parâmetro FEATURE=BLM ou FEATURE=BASIC.
- Se a sua organização utilizar um certificado assinado por uma autoridade raiz, como EnTrust ou Verisign, reveja os [Requisitos do cliente BitLocker Manager](#). É necessária uma alteração na configuração de registo no computador cliente para ativar a validação de confiança SSL/TLS.
- Os instaladores do cliente BitLocker Manager estão localizados em:
  - **Em dell.com\support** - Se necessário, [Obter o software](#) a partir de [support.dell.com](#) e, em seguida, [Extrair os Instaladores Subordinados do Instalador Principal](#). Após a extração, localize o ficheiro em C:\extracted\Encryption Management Agent.
  - **Na sua conta FTP Dell** - Localize o pacote de instalação em Encryption-Enterprise-10.x.x.xxx.zip e, em seguida, [Extrair os instaladores subordinados do instalador principal](#). Após a extração, localize o ficheiro em C:\extracted\Encryption Management Agent.

## Instalação com linha de comandos

- A tabela seguinte descreve os parâmetros disponíveis para a instalação.

| Parâmetros                                                         |
|--------------------------------------------------------------------|
| CM_EDITION=1 <remote management>                                   |
| INSTALLDIR=<change the installation destination>                   |
| SERVERHOST=<securityserver.organization.com>                       |
| SERVERPORT=8888                                                    |
| SECURITYSERVERHOST=<securityserver.organization.com>               |
| SECURITYSERVERPORT=8443                                            |
| FEATURE=BLM <install BitLocker Manager only>                       |
| FEATURE=BLM,SED <install BitLocker Manager with SED>               |
| ARPSYSTEMCOMPONENT=1 <no entry in the Control Panel Programs list> |

Para obter uma lista comutadores basic .msi e opções de visualização que podem ser utilizadas em linhas de comandos, consulte [Instalar utilizando os instaladores subordinados](#).

### Exemplo de linha de comandos

- O exemplo seguinte instala apenas o BitLocker Manager (instalação silenciosa, sem reinício, sem entrada na lista de Programas do Painel de controlo, instalado na localização predefinida C:\Program Files\Dell\Dell Data Protection)

```
EMAgent_XXbit_setup.exe /s /v"CM_EDITION=1 SERVERHOST=server.organization.com
SERVERPORT=8888 SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443
FEATURE=BLM /norestart /qn"
```

- O exemplo seguinte instala o BitLocker Manager com SED (instalação silenciosa, sem reinício, sem entrada na lista de Programas do Painel de controlo, instalado na localização predefinida C:\Program Files\Dell\Dell Data Protection)

```
EMAgent_XXbit_setup.exe /s /v"CM_EDITION=1 SERVERHOST=server.organization.com  
SERVERPORT=8888 SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443  
FEATURE=BLM,SED /norestart /qn"
```

- **Exemplo de linha de comandos para instalar o BitLocker Manager e o Dell Encryption**

O exemplo seguinte instala apenas o BitLocker Manager (instalação silenciosa, sem reinício, sem entrada na lista de Programas do Painel de controlo, instalado na localização predefinida C:\Program Files\Dell\Dell Data Protection)

```
EMAgent_XXbit_setup.exe /s /v"CM_EDITION=1 SERVERHOST=server.organization.com  
SERVERPORT=8888 SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443  
FEATURE=BLM /norestart /qn"
```

*Em seguida:*

O exemplo seguinte instala o cliente com parâmetros predefinidos (Encryption Client, Encrypt for Sharing, sem caixas de diálogo, sem barra de progresso, reinício automático, instalado na localização predefinida C:\Program Files\Dell\Dell Data Protection).

```
DDPE_XXbit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com  
POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION  
DEVICESTSERVERURL=https://server.organization.com:8443/xapi/ /qn"
```

# Desinstalar utilizando os instaladores subordinados

- A Dell recomenda a utilização do [Desinstalador do Data Security](#) para remover o conjunto de aplicações do Data Security.
- 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](#). 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\\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 /I C:\<any directory>\<any log file name>.log. A Dell não recomenda a utilização de "/I\*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 (copia todos os ficheiros contidos no .msi)                                           |

## NOTA:

Com /v, as opções predefinidas da Microsoft ficam disponíveis. Para obter uma lista de opções, consulte [https://msdn.microsoft.com/en-us/library/windows/desktop/aa367988\(v=vs.85\).aspx](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 <b>Cancelar</b> , solicita o reinício                      |
| /qb-  | Caixa de diálogo de Progresso com botão <b>Cancelar</b> , reinicia-se após a conclusão do processo |

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

## Desinstalar o Encryption e o Encryption em sistemas operativos de servidor

- Para reduzir o tempo de descriptação, execute o Assistente de Limpeza de Disco do Windows para remover ficheiros temporários e outros dados desnecessários.
- Se possível, programe a descriptação para ser feita durante a noite.
- Desative o modo de suspensão para impedir a suspensão do computador caso este se encontre sem supervisão. A descriptação não é possível num computador em suspensão.
- Encerre todos os processos e aplicações para minimizar as falhas de descriptação devidas a ficheiros bloqueados.
- Uma vez que a desinstalação está concluída e a descriptação 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 descriptação de dados existente, como, por exemplo, a emissão de uma atualização de política.
- O Encryption e o Encryption External Media atualizam o Dell Server para alterar o estado para *Desprotegido* no início de um processo de desinstalação do cliente. No entanto, caso o cliente não consiga contactar o Dell Server, independentemente do motivo, não é possível atualizar o estado. Neste caso, terá de *Remover o Endpoint* manualmente na 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 Management Console ou em Gerir relatórios.

### Processo

- **Antes de iniciar o processo de desinstalação**, consulte [\(Opcional\) Criar um ficheiro de registo do Encryption Removal Agent](#). Este ficheiro de registo é útil para deteção e resolução de problemas numa operação de desinstalação/descriptação. Se não pretender descriptar ficheiros durante o processo de desinstalação, não é necessário criar um ficheiro de registo do Agente de remoção de encriptação.
- O Key Server (e o Security Management 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 Security Management Server](#) para obter instruções. Não é necessária qualquer ação anterior se o cliente a ser desinstalado estiver ativado num Security Management Server Virtual, uma vez que o Security Management Server Virtual 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.
- Após concluir a desinstalação, mas antes de reiniciar o computador, execute o WSScan para assegurar que todos os dados foram descriptados. Consulte [Utilizar o WSScan](#) para obter instruções.
- Periodicamente, [verifique o estado do Encryption Removal Agent](#). Se o serviço Encryption Removal Agent ainda se encontrar no painel de serviços, a descriptação de dados ainda está a ser processada.

### Desinstalação Por Linha de Comandos

- Uma vez extraído do instalador principal do , o instalador do Encryption encontra-se 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<br>3 — Utilizar o pacote LSARecovery<br>2 — Utilizar material da chave forense anteriormente transferido<br>1 — Transferir chaves do Dell Server<br>0 — Não instalar o Encryption Removal Agent |
| CMGSILENTMODE                    | Propriedade para a desinstalação silenciosa:<br>1 — Silencioso — necessário ao executar com variáveis msiexec. contendo /q ou /qn<br>0 — Não Silencioso — apenas possível quando não existem variáveis msiexec contendo /q na sintaxe de linhas de comandos                  |
| <b>Propriedades obrigatórias</b> |                                                                                                                                                                                                                                                                              |
| DA_KM_PATH                       | O caminho totalmente qualificado para o pacote de chaves.                                                                                                                                                                                                                    |
| DA_KM_PW                         | A palavra-passe definida no pacote de chaves.                                                                                                                                                                                                                                |
| DA_SERVER                        | FQHN para o Security Management Server anfitrião da sessão de negociação.                                                                                                                                                                                                    |
| DA_PORT                          | Porta do Security Management Server para pedidos (a predefinição é 8050).                                                                                                                                                                                                    |
| SVCPN                            | Nome de utilizador no formato UPN no qual o serviço Key Server tem sessão iniciada no Security Management Server.                                                                                                                                                            |
| DA_RUNAS                         | Nome de utilizador no formato compatível com SAM, sendo o pedido de recuperação de chaves realizado neste contexto. Este utilizador necessita de estar na lista do Key Server do Security Management Server.                                                                 |
| DA_RUNASPWD                      | Palavra-passe do utilizador runas.                                                                                                                                                                                                                                           |
| FORENSIC_ADMIN                   | A conta de administrador forense no Dell Server, que pode ser utilizada para pedidos forenses para desinstalações ou chaves.                                                                                                                                                 |
| FORENSIC_ADMIN_PWD               | A palavra-passe da conta de administrador forense.                                                                                                                                                                                                                           |
| <b>Propriedades opcionais</b>    |                                                                                                                                                                                                                                                                              |
| SVCLOGONUN                       | Nome de utilizador no 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 e transfere as chaves de encriptação a partir do Security Management 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"  
SVCPCN="administrator@domain.com" DA_RUNAS="domain\username" DA_RUNASPWD="password" /qn
```

Reinicie o computador quando concluído.

- O seguinte exemplo desinstala silenciosamente o Encryption 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.

- O seguinte exemplo desinstala silenciosamente o Encryption utilizando chaves pré-transferidas localizadas em C:\Users\administrator\Desktop\Admin\ utilizando a palavra-passe do administrador forense e registos de escrita para C:\ShieldUninstall.

```
DDPE_XXbit_setup.exe /s /x /v"CMG_DECRYPT=2 CMGSILENT=1 DA_KM_PATH=C:  
\Users\administrator\Desktop\Admin\<HOSTNAME>.bin DA_KM_PW=qwert12345 /1*v c:  
\ShieldUninstall.log /qn /norestart"
```

Comando MSI

```
msiexec.exe /s /x "Dell Data Protection Encryption.msi" CMG_DECRYPT=2 CMGSILENT=1  
DA_KM_PATH=C:\Users\administrator\Desktop\Admin\<HOSTNAME>.bin DA_KM_PW=qwert12345 /1*v  
c:\ShieldUninstall.log /qn /norestart
```

### **NOTA:**

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

1. Crie uma conta de administrador forense na 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.

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\"  
SVCPCN=\"administrator@organization.com\" DA_RUNAS=\"domain\username\"  
DA_RUNASPWD=\"password\" /qn"
```

## Desinstalar o Encryption External Media

Uma vez extraído do instalador principal, o instalador Encryption encontra-se em C:\extracted\Encryption\DDPE\_XXbit\_setup.exe.

### **Desinstalação Por Linha de Comandos**

Execute uma linha de comandos idêntica a uma das seguintes:

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

Reinicie o computador quando concluído.

## Desinstalar o Full Disk Encryption

- Para desativar a PBA, é necessária uma ligação de rede ao Dell Server.

## Processo

- Desativar a PBA, o que remove todos os dados da PBA do computador e desbloqueia as chaves do Full Disk Encryption.
- Desinstalar o Full Disk Encryption.

## Desativar a PBA

1. Como administrador Dell, inicie sessão na Management Console.
2. No painel esquerdo, clique em **Populações > Pontos terminais**.
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 nome de anfitrião do computador pretendido.
7. Clique em **Políticas de segurança** no menu superior.
8. Selecione **Full Disk Encryption** no grupo **Encriptação do Windows**.
9. Altere o **Full Disk Encryption** e a política de *On* para **Off**.
10. Clique em **Guardar**.
11. No painel do lado esquerdo, clique na faixa **Consolidar políticas**.
12. Clique em **Consolidar políticas**.

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

Desinstale o Full Disk Encryption e a Autenticação Avançada PBA após a PBA ser desativada.

## Desinstalar o cliente de Full Disk Encryption

### Desinstalação por linha de comando

- Uma vez extraído do instalador principal, o Full Disk Encryption pode ser encontrado em `C:\extracted\Encryption Management Agent\EMAgent_XXbit_setup.exe`.
  - O seguinte exemplo desinstala o Full Disk Encryption de forma silenciosa.

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

Encerre e reinicie o computador quando concluído.

## Desinstalar o SED Manager

- Para desativar a PBA, é necessária uma ligação de rede ao Dell Server.

## Processo

- Desativar a PBA, o que remove todos os dados da PBA do computador e desbloqueia as chaves SED.
- Desinstalar o SED Manager.

## Desativar a PBA

1. Como administrador Dell, inicie sessão na Management Console.
2. No painel esquerdo, clique em **Populações > Pontos terminais**.
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 nome de anfitrião do computador pretendido.
7. Clique em **Políticas de segurança** no menu superior.
8. Selecione **Unidades de encriptação automática** na página **Categoria de política**.
9. Altere a **Unidade de encriptação automática (SED)** e a política de *On* para *Off*.
10. Clique em **Guardar**.
11. No painel do lado esquerdo, clique na faixa **Consolidar políticas**.
12. Clique em **Consolidar políticas**.

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

Desinstale o SED Manager e a Autenticação Avançada PBA após a PBA ser desativada.

## Desinstalar o cliente SED

### Desinstalação por linha de comando

- Uma vez extraído do instalador principal, o instalador do SED Manager pode ser encontrado em C : \extracted\Encryption Management Agent\EMAgent\_XXbit\_setup.exe.
  - O seguinte exemplo desinstala o SED Manager de forma silenciosa.

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

Encerre e reinicie o computador quando concluído.

## Desinstalar o BitLocker Manager

### Desinstalação por linha de comando

- Uma vez extraído do instalador principal do , o instalador do BitLocker Manager pode ser localizado em C : \extracted\Encryption Management Agent\EMAgent\_XXbit\_setup.exe.
- O seguinte exemplo desinstala o BitLocker Manager de forma silenciosa.

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

Reinicie o computador quando concluído.

# Desinstalador do Data Security

## Desinstalar

A Dell fornece o Data Security Uninstaller como o desinstalador principal. Este utilitário reúne os produtos instalados atualmente e remove-os na ordem apropriada.

Este Data Security Uninstaller está disponível em: `C:\Program Files (x86)\Dell\Dell Data Protection`

Para obter mais informações, ou para utilizar a interface de linha de comandos (CLI), consulte o artigo [125052](#) da BDC.

Os registos são gerados em `C:\ProgramData\Dell\Dell Data Protection\` para todos os componentes que são removidos.

Para executar o utilitário, abra a respetiva pasta, clique com o botão direito do rato em **DataSecurityUninstaller.exe** e seleccione **Executar como administrador**.

Clique em **Seguinte**.

Opcionalmente, desmarque a remoção de qualquer aplicação e clique em **Seguinte**.

As dependências necessárias são automaticamente seleccionadas ou desmarcadas.

Para remover aplicações sem instalar o Encryption Removal Agent, escolha **Não instalar o Encryption Removal Agent** e seleccione **Seguinte**.

Selecione **Encryption Removal Agent - Transferir chaves a partir do servidor**.

Introduza as credenciais totalmente qualificadas de um administrador forense e seleccione **Seguinte**.

Selecione **Remove** para iniciar a desinstalação.

Clique em **Terminar** para concluir a remoção e reinicie o computador. **Reiniciar o computador depois de clicar em terminar** está seleccionado por predefinição.

A desinstalação e remoção estão concluídas.

## Cenários normalmente utilizados

- Para instalar 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](#).
- 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.
- Utilize estes instaladores para instalar os clientes utilizando uma instalação com script, ficheiros batch ou qualquer outra tecnologia push disponível na sua organização.
- Nestes exemplos de linha de comandos, o reinício foi suprimido. No entanto, é necessário um eventual reinício. A encriptação só pode ser iniciada após o reinício do computador.
- Ficheiros de registo - O Windows cria ficheiros de registo de instalação do instalador subordinado únicos para o utilizador com sessão iniciada em %temp%, localizados em C:\Users\\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 .msi padrão pode ser utilizado para criar um ficheiro de registo, utilizando /I\*v C:\<any directory>\<any log file name>.log.

- Todos os instaladores subordinados utilizam as mesmas opções .msi básicas e as mesmas opções de visualização em instalações por linha de comandos, exceto onde referido. 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 *.exe |
| /s    | Modo silencioso                             |
| /i    | Modo de instalação                          |

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

- Dê a instrução aos utilizadores para consultar o seguinte documento e ficheiros de ajuda para assistência de aplicação:
  - Consulte a *Dell Encrypt Help (Ajuda do Dell Encrypt)* para saber como utilizar as funcionalidades do Encryption. Aceda à ajuda a partir de <Install dir>:\Program Files\Dell\Dell Data Protection\Encryption\Help.
  - Consulte a *Encryption External Media Help (Ajuda do Encryption External Media)* para saber como utilizar as funcionalidades do Encryption External Media. Aceda à ajuda a partir de <Install dir>:\Program Files\Dell\Dell Data Protection\Encryption\EMS

- Consulte a *Encryption Enterprise Help (Ajuda do Encryption Enterprise)* para saber como utilizar as funcionalidades do. Aceda à ajuda a partir de <Install\_dir>:\Program Files\Dell\Dell Data Protection\Authentication \Help.

## Cliente de encriptação, , e

- O seguinte exemplo instala o SED Management e Encryption Management Agent (instalação silenciosa, sem reinício, sem entrada na lista de Programas do Painel de controlo, instalado na localização predefinida C:\Program Files\Dell\Dell Data Protection\Encryption).

```
EMAgent_XXbit_setup.exe /s /v"CM_EDITION=1 SERVERHOST=server.organization.com
SERVERPORT=8888 SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443
ARPSYSTEMCOMPONENT=1 /norestart /qn"
```

De seguida:

- O seguinte exemplo instala o Encryption com parâmetros predefinidos (Encryption e Encrypt for Sharing, sem caixas de diálogo, sem barra de progresso, sem reinício, instalado na localização predefinida C:\Program Files\Dell\Dell Data Protection\Encryption).

```
DDPE_XXbit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com
POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION
DEVICESTSERVERURL=https://server.organization.com:8443/xapi/ /norestart /qn"
```

Substitua DEVICESTSERVERURL=https://server.organization.com:**8081/xapi** (sem a barra à direita) se o seu Security Management Server for anterior a v7.7.

## SED Manager (incluindo a Autenticação Avançada) e o Encryption Client

- O exemplo seguinte instala os controladores do Trusted Software Stack (TSS) para o TPM e as correções da Microsoft na localização especificada, não cria uma entrada na lista de Programas do Painel de controlo e suprime o reinício.

Estes controladores devem ser instalados quando instalar o Encryption Client.

```
setup.exe /S /z""InstallPath=<c:\location>, ARPSYSTEMCOMPONENT=1, SUPPRESSREBOOT=1""
```

De seguida:

- O exemplo seguinte instala o SED Manager gerido remotamente (instalação silenciosa, sem reinício, sem entrada na lista de Programas do Painel de Controlo, instalado na localização predefinida C:\Program Files\Dell\Dell Data Protection).

```
EMAgent_XXbit_setup.exe /s /v"CM_EDITION=1 SERVERHOST=server.organization.com
SERVERPORT=8888 SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443
ARPSYSTEMCOMPONENT=1 /norestart /qn"
```

De seguida:

- O exemplo seguinte instala o cliente Advanced Authentication (instalação silenciosa, sem reinício, instalado na localização predefinida C:\Program Files\Dell\Dell Data Protection\Authentication).

```
setup.exe /s /v"/norestart /qn ARPSYSTEMCOMPONENT=1"
```

De seguida:

- O exemplo seguinte instala o cliente com parâmetros predefinidos (Encryption Client e Encrypt for Sharing, sem caixas de diálogo, sem barra de progresso, sem reinício, instalado na localização predefinida C:\Program Files\Dell\Dell Data Protection).

```
DDPE_XXbit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com
POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION
DEVICESTSERVERURL=https://server.organization.com:8443/xapi/ /norestart /qn"
```

Substitua DEVICESTSERVERURL=https://server.organization.com:**8081/xapi** (sem a barra à direita) se o seu Security Management Server for anterior a v7.7.

## SED Manager e Encryption External Media

- O seguinte exemplo instala o SED Manager, o Encryption Management Agent e a consola de segurança local (instalação silenciosa, sem reinício, sem entrada na lista de Programas do Painel de controlo, instalado na localização predefinida C:\Program Files\Dell\Dell Data Protection\Encryption).

```
EMAgent_XXbit_setup.exe /s /v"CM_EDITION=1 SERVERHOST=server.organization.com  
SERVERPORT=8888 SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443  
ARPSYSTEMCOMPONENT=1 /norestart /qn"
```

De seguida:

- O exemplo seguinte instala apenas o Encryption External Media (instalação silenciosa, sem reinício, instalado na localização predefinida C:\Program Files\Dell\Dell Data Protection).

```
DDPE_XXbit_setup.exe /s /v"EME=1  
SERVERHOSTNAME=server.organization.com POLICYPROXYHOSTNAME=rgk.organization.com  
DEVICESTERVERURL=https://server.organization.com:8443/xapi/ MANAGEDDOMAIN=ORGANIZATION /  
norestart /qn"
```

Substitua DEVICESTERVERURL=https://server.organization.com:**8081/xapi** (sem a barra à direita) se o seu Security Management Server for anterior a v7.7.

## BitLocker Manager e Encryption External Media

- O BitLocker Manager e o Encryption External Media interagem com base na sequência de encriptação. Se uma unidade encriptada BitLocker Manager for inserida num computador com Encryption External Media, a palavra-passe do BitLocker Manager **tem** de ser introduzida antes de o Encryption External Media poder ler e encriptar a unidade.
- Se o Encryption External Media estiver ativo numa unidade, a encriptação do BitLocker Manager pode ser aplicada à mesma unidade.
- O exemplo seguinte instala o BitLocker Manager (instalação automática, sem reinício, sem entrada na lista de Programas do Painel de controlo, instalado na localização predefinida C:\Program Files\Dell\Dell Data Protection).

```
EMAgent_XXbit_setup.exe /s /v"CM_EDITION=1 SERVERHOST=server.organization.com  
SERVERPORT=8888 SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443  
FEATURE=BLM /norestart /qn"
```

Em seguida:

- O exemplo seguinte instala apenas o Encryption External Media (instalação silenciosa, sem reinício, instalado na localização predefinida C:\Program Files\Dell\Dell Data Protection).

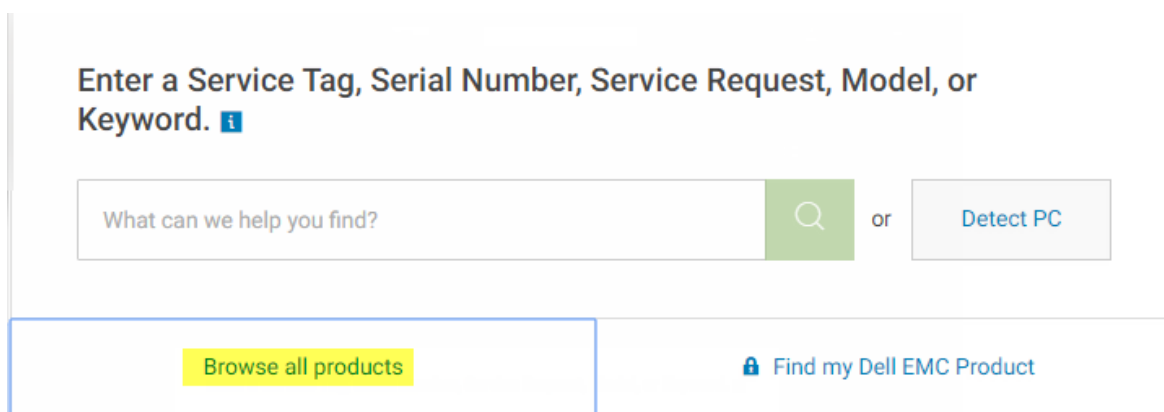
```
DDPE_XXbit_setup.exe /s /v"EME=1  
SERVERHOSTNAME=server.organization.com POLICYPROXYHOSTNAME=rgk.organization.com  
DEVICESTERVERURL=https://server.organization.com:8443/xapi/ MANAGEDDOMAIN=ORGANIZATION /  
norestart /qn"
```

Substitua DEVICESTERVERURL=https://server.organization.com:**8081/xapi** (sem a barra à direita) se o seu Security Management Server for anterior a v7.7.


## Transferir o software

Esta secção detalha a obtenção de software a partir de [dell.com/support](https://dell.com/support). Se já tiver o software, pode ignorar esta secção. Aceda a [dell.com/support](https://dell.com/support) para começar.

1. Na página Web de apoio técnico da Dell, seleccione **Procurar todos os produtos**.



Enter a Service Tag, Serial Number, Service Request, Model, or Keyword. **i**

What can we help you find?  or [Detect PC](#)

[Browse all products](#) [Find my Dell EMC Product](#)

2. Seleccione **Segurança** na lista de produtos.
3. Seleccione **Dell Data Security**.  
Após efetuar esta seleção uma vez, o site memoriza as informações.
4. Seleccione o produto Dell.  
Exemplos:  
**Dell Encryption Enterprise**  
**Dell Endpoint Security Suite Enterprise**
5. Seleccione **Controladores e Transferências**.
6. Seleccione o tipo de sistema operativo cliente desejado.
7. Seleccione **Dell Encryption** nas correspondências. Isto é apenas um exemplo, pelo que, provavelmente, a realidade será ligeiramente diferente. Por exemplo, é possível que não existem quatro ficheiros para escolha.
8. Seleccione **Transferir**.

# Configuração da pré-instalação para UEFI SED e BitLocker Manager

## Inicializar o TPM

- Tem de ser membro do grupo de administradores locais ou equivalente.
- O computador tem de estar equipado com um BIOS e um TPM compatíveis.
- Siga as instruções localizadas em <http://technet.microsoft.com/en-us/library/cc753140.aspx>.

## Configuração da pré-instalação para computadores UEFI

### Ativar a ligação à rede durante a Autenticação do pré-arranque UEFI

Para que a autenticação de pré-arranque seja bem-sucedida num computador com firmware UEFI, o modo PBA tem de ter ligação à rede. Por predefinição, os computadores com firmware UEFI não têm ligação à rede até que o sistema operativo seja carregado, o que ocorre depois do modo PBA.

O procedimento seguinte ativa a ligação à rede durante a PBA em computadores com UEFI ativado. Uma vez que os passos de configuração podem variar consoante o modelo de computador UEFI, o procedimento seguinte é apenas um exemplo.

1. Inicie a configuração do firmware UEFI.
2. Prima F2 continuamente durante o arranque até ser apresentada no canto superior direito do ecrã uma mensagem como "a preparar o menu de arranque único".
3. Se solicitado, introduza a palavra-passe de administrador do BIOS.

#### **NOTA:**

Normalmente, tratando-se de um computador novo, tal não é solicitado, uma vez que a palavra-passe do BIOS ainda não foi definida.

4. Selecione **Configuração do sistema**.
5. Selecione **NIC integrado**.
6. Selecione a caixa de verificação **Ativar a pilha da rede UEFI**.
7. Selecione **Ativado** ou **Ativado c/PXE**.
8. Selecione **Aplicar**

#### **NOTA:**

Os computadores *sem* firmware UEFI não necessitam de configuração.

## Desativar ROMs de opção legadas

Certifique-se de que a definição **Ativar ROMs de opção legadas** está desativada no BIOS.

1. Reinicie o computador.
2. À medida que se reinicia, prima **F12** repetidamente to para abrir as definições de arranque do computador com UEFI.
3. Prima a seta para baixo, realce a opção **Definições do BIOS** e prima **Enter**.
4. Selecione **Definições** > **Geral** > **Opções de arranque avançadas**.
5. Desmarque a caixa de verificação **Ativar ROMs de opção legadas** e clique em **Aplicar**.

# Configuração da pré-instalação para configurar uma partição de PBA do BitLocker

- Deve criar a partição de PBA **antes** de instalar o BitLocker Manager.
- Ligue e ative o TPM **antes** de instalar o BitLocker Manager. O BitLocker Manager assume a propriedade do TPM (não é necessário reiniciar). No entanto, se o TPM já tiver um proprietário, o BitLocker Manager inicia o processo de configuração da encriptação. O importante é que o TPM tenha um proprietário e esteja ativo.
- Poderá ter de realizar a partição do disco manualmente. Consulte a descrição da Microsoft para a Ferramenta de Preparação da Unidade BitLocker para obter mais informações.
- Utilize o comando BdeHdCfg.exe para criar a partição de PBA. O parâmetro predefinido indica que a ferramenta da linha de comandos segue o mesmo processo do Assistente de configuração do BitLocker.

```
BdeHdCfg -target default
```

## **NOTA:**

Para obter mais opções disponíveis para o comando BdeHdCfg, consulte a [Referência do parâmetro BdeHdCfg.exe da Microsoft](#).

## Designar o Dell Server através do Registo

- Se os seus clientes obtiverem elegibilidade através do Dell Digital Delivery, siga estas instruções para definir um registo através dos Objetos de Política de Grupo para predefinir o Dell Server a utilizar após a instalação.
- A estação de trabalho deve fazer parte da UO onde os Objetos de Política de Grupo estão aplicados ou as definições de registo devem ser definidas manualmente no ponto terminal.
- Certifique-se de que a porta de saída 443 está disponível para comunicar a partir do Dell Server para cloud.dell.com. Se a porta 443 estiver bloqueada (por qualquer motivo), a obtenção da elegibilidade falha e é acionada uma elegibilidade a partir do conjunto disponível.

**NOTA:** Se não definir este valor de registo ao tentar instalar através do Dell Digital Delivery ou não especificar um SERVIDOR no Instalador Principal, o URL de ativação é predefinido para 199.199.199.199.

### Definir Manualmente a Chave de Registo

Para pontos terminais que não estão associados a um domínio ou nos quais não seja possível definir um Objeto de Política de Grupo, predefina uma chave de registo para ativar num Dell Server específico durante a instalação.

1. Na caixa de pesquisa na barra de tarefas, escreva **regedit** e, em seguida, clique com o botão direito do rato e selecione **Executar como administrador**.

2. Navegue até e crie a seguinte chave de registo:

HKEY\_LOCAL\_MACHINE\SOFTWARE\Dell\Dell Data Protection

REG\_SZ: Dados

do Servidor: <FQDN ou endereço IP do Dell Server>

3. Instalar o Encryption através do Dell Digital Delivery ou do Instalador Principal.

### Criar o Objeto de Política de Grupo

1. No controlador de domínio para gerir os clientes, clique em **Iniciar > Ferramentas administrativas > Gestão de Políticas de Grupo**.
2. Clique com o botão direito do rato na OU onde a política deve ser aplicada e selecione **Criar um GPO neste domínio e Ligá-lo aqui**.
3. Introduza um nome para o novo GPO, selecione (nenhum) para GPO de arranque de origem e clique em **OK**.
4. Clique com o botão direito no GPO que foi criado e selecione **Editar**.
5. É carregado o Editor de gestão de política de grupo. Aceda a **Configuração do computador > Preferências > Definições do Windows > Registo**.
6. Clique com o botão direito do rato no Registo e selecione **Novo > Item do registo**. Execute as seguintes ações.

Ação: Criar

Ramo de registo: HKEY\_LOCAL\_MACHINE

Caminho da chave: SOFTWARE\Dell\Dell Data Protection

Nome do valor: Servidor

Tipo do valor: REG\_SZ

Dados do valor: <FQDN ou endereço IP do Dell Server>

7. Clique em **OK**.

8. Termine sessão e, em seguida, inicie novamente sessão na estação de trabalho ou execute **gpupdate /force** para aplicar a política de grupo.

## Extrair os instaladores subordinados

- Para instalar cada cliente individualmente, extraia os ficheiros executáveis subordinados do instalador.
- O instalador principal não é um *desinstalador* principal. Cada cliente tem de ser desinstalado separadamente, seguido pela desinstalação do instalador principal. Utilize este processo para extrair os clientes do instalador principal para que possam ser utilizados para a desinstalação.

1. A partir do suporte multimédia de instalação Dell, copie o ficheiro **DDSSetup.exe** para o computador local.
2. Abra uma linha de comandos na mesma localização do ficheiro **DDSSetup.exe** e introduza:

```
DDSSetup.exe /s /z "\"EXTRACT_INSTALLERS=C:\Extracted\""
```

O caminho de extração não pode exceder os 63 caracteres.

Antes de iniciar a instalação, certifique-se de que todos os pré-requisitos foram cumpridos e de que todo o software necessário foi instalado para cada instalador subordinado que pretende instalar. Consulte os [Requisitos](#) para obter mais informações.

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

## Configurar o Key Server

- Esta secção explica como configurar componentes para utilização com a autenticação/autorização Kerberos ao utilizar um Security Management Server. O Security Management Server Virtual não utiliza o Key Server.

O Key Server consiste num serviço que verifica os clientes que se ligam a um socket. Depois de um cliente se ligar, é estabelecida, autenticada e encriptada uma ligação segura através de APIs Kerberos (se não for possível estabelecer uma ligação segura, o cliente é desligado).

O Key Server verifica então no Security Server (anteriormente no Device Server) se o utilizador que está a executar o cliente tem permissão para aceder às chaves. Este acesso é concedido através de domínios individuais na Management Console.

- Se for necessário utilizar a autenticação/autorização Kerberos, o servidor que contém o componente Key Server tem de fazer parte do domínio afetado.
- Dado que o Security Management Server Virtual não utiliza o Key Server, a desinstalação típica é afetada. Quando um Encryption Client ativado num Security Management Server Virtual 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 Security Management 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**:

Em *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 o continuar a utilizar).
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 com o Security Management 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").

O formato "superadmin" pode representar qualquer método que possa ser autenticado no Security Management Server. O nome de conta SAM, UPN ou o DOMÍNIO\Nome de utilizador são aceitáveis. Qualquer método que possa ser autenticado no Security Management Server é aceitável, uma vez que é necessária a validação para essa conta de utilizador no Active Directory.

Por exemplo, num ambiente com vários domínios, a introdução apenas do nome de conta SAM como "jdoe" irá provavelmente falhar, uma vez que o Security Management Server não consegue autenticar "jdoe", pois não consegue

encontrar "jdoe". Num ambiente de vários domínios, é recomendada a utilização do UPN, embora também seja aceitável o formato DOMÍNIO\Nome de utilizador. Num ambiente de domínio único, é aceitável o nome de conta SAM.

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

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

## Exemplo de ficheiro de configuração

```
<?xml version="1.0" encoding="utf-8" ?>
<configuration>
<appSettings>
<add key="port" value="8050" /> [porta TCP escutada pelo Key Server. A predefinição é 8050.]
<add key="maxConnections" value="2000" /> [número de ligações de socket ativas permitidas pelo Key Server]
<add key="url" value="https://keyserver.domain.com:8443/xapi/" /> [URL do Security Server (anteriormente Device Server)
(o formato é 8081/xapi para um Security Management Server anterior a v7.7)]
<add key="verifyCertificate" value="false" /> [se verdadeiro, verifica certificados/defina como falso para não verificar ou se
utilizar certificados auto-assinados]
<add key="user" value="superadmin" /> [Nome de utilizador usado para comunicar com o Security Server. Este utilizador
precisa de ter a função de administrador selecionada na Management Console. O formato "superadmin" pode representar
qualquer método que possa ser autenticado no Security Management Server. O nome de conta SAM, UPN ou o
DOMÍNIO\Nome de utilizador são aceitáveis. Qualquer método que possa ser autenticado no Security Management Server
é aceitável, uma vez que é necessária a validação para essa conta de utilizador no Active Directory. Por exemplo, num ambiente
com vários domínios, a introdução apenas do nome de conta SAM como "jdoe" irá provavelmente falhar, uma vez que o Security
Management Server não consegue autenticar "jdoe", pois não consegue encontrar "jdoe". Num ambiente de vários domínios, é
recomendada a utilização do UPN, embora também seja aceitável o formato DOMÍNIO\Nome de utilizador. Num ambiente de
domínio único é aceitável o nome de conta SAM.]
<add key="cacheExpiration" value="30" /> [A frequência (em segundos) com que o Serviço deve verificar quem tem permissão
para solicitar chaves. O serviço mantém uma cache e regista o quão antiga ela é. Quando a cache for anterior ao valor, é obtida
uma nova lista. Quando um utilizador se liga, o Key Server necessita de transferir utilizadores autorizados do Security Server. Se
estes utilizadores não estiverem em cache ou se a lista não tiver sido transferida nos últimos "x" segundos, esta será transferida
novamente. Não existe qualquer consulta, mas este valor configura quão obsoleta a lista se pode tornar antes de ser atualizada
quando necessário.]
<add key="epw" value="encrypted value of the password" /> [Palavra-passe utilizada para comunicar com o Security
Management Server. Se a palavra-passe de superadmin tiver sido alterada, deve ser alterada aqui.]
</appSettings>
</configuration>
```

## 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 de serviços.

## Management Console - Adicionar administrador forense

1. Como administrador Dell, inicie sessão na Management Console.

2. Clique em **Populações > Domínios**.
3. Selecione o Domínio adequado.
4. Clique no separador **Key Server**.
5. Em *Conta*, adicione o utilizador que irá efetuar as atividades de administrador. O formato é DOMÍNIO\Nome de utilizador. 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.

# 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 Dell Server.
- Este utilitário utiliza um dos seguintes métodos para transferir um pacote de material 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`

## Utilizar o 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 Dell 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, como "jdoe" (ativado na Management Console)

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

### NOTA:

Normalmente, é suficiente especificar o MCID *ou* DCID. No entanto, se ambos são conhecidos, é útil introduzir os dois. Cada parâmetro contém informações diferentes utilizadas por este utilitário.

Clique em **Seguinte**.

3. Em *Frase de acesso*, introduza 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 outra localização.

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.

## Utilizar o Modo de administrador

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

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 DOMÍNIO\Nome de utilizador. 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

 **NOTA:**

Normalmente, é suficiente especificar o MCID *ou* DCID. No entanto, se ambos são conhecidos, é útil introduzir os dois. Cada parâmetro contém informações diferentes utilizadas por este utilitário.

Clique em **Seguinte**.

3. Em *Frase de acesso*, introduza 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 seleccionar outra localização.

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.

# Configurar o Encryption em sistemas operativos de servidor

## Ativar o Encryption em sistemas operativos de servidor

### **NOTA:**

A encriptação de sistemas operativos de servidor converte a encriptação de Utilizador para encriptação Comum.

1. Como administrador Dell, inicie sessão na Management Console.
2. Selecione **Grupo de endpoints** (ou **Endpoint**), procure o endpoint ou grupo de endpoints a ativar, selecione **Políticas de segurança** e, em seguida, selecione a categoria de política **Encriptação do servidor**.
3. Defina as seguintes políticas:
  - Server Encryption - **Selecione** para ativar o Encryption em sistemas operativos de servidor as políticas relacionadas.
  - Encriptação SDE ativada - **Selecione** para ligar a encriptação SDE.
  - Encriptação ativada - **Selecione** para ligar a encriptação Comum.
  - Credenciais do Windows seguras - Esta política está **Selecioneada** por predefinição.

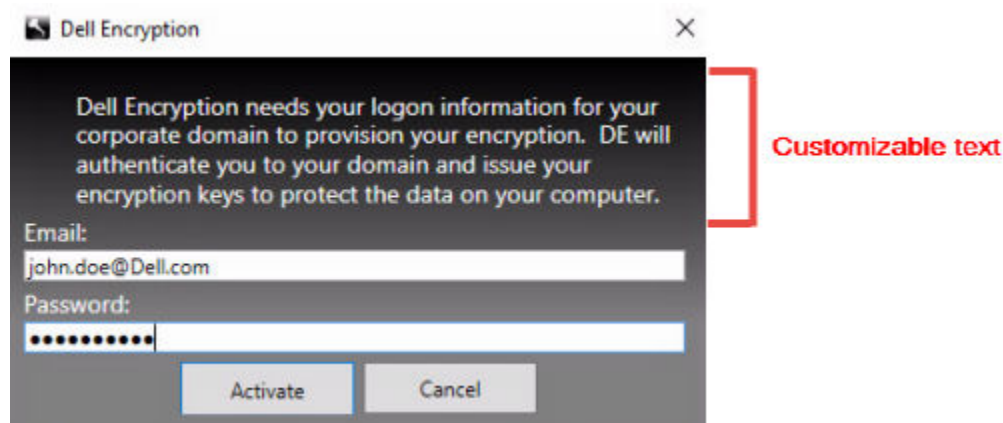
Quando a política *Credenciais do Windows seguras* está **Selecioneada** (predefinição), todos os ficheiros da pasta de ficheiros `\Windows\system32\config` são encriptados, incluindo as credenciais Windows. Para evitar a encriptação das credenciais do Windows, defina a política *Credenciais do Windows seguras* para **Não selecionada**. A encriptação das credenciais Windows ocorre independentemente de qual seja a definição da política *Encriptação SDE Ativada*.

4. Guarde e consolide as políticas.

## Personalizar a caixa de diálogo Início de sessão de Ativação

A caixa de diálogo Início de sessão de Ativação é exibida:

- Quando um utilizador não gerido inicia sessão.
- Quando o utilizador seleciona Ativar o Dell Encryption no menu do ícone Encriptação, localizado na área de notificação.



## Configurar políticas do Encryption External Media

O **computador de encriptação original** é o computador no qual originalmente foi encriptado um dispositivo amovível. Quando o computador original é um **servidor protegido** - um servidor com o Encryption em sistemas operativos de servidor instalado e

ativado - e o servidor protegido detetar a presença, pela primeira vez, de um dispositivo amovível, é solicitado ao utilizador que encripte o dispositivo amovível.

- As políticas do Encryption External Media controlam, entre outros aspetos, o acesso de suportes de dados amovíveis ao servidor, autenticação e encriptação.
- As políticas de controlo de portas afetam os suportes de dados amovíveis em servidores protegidos, por exemplo, controlando o acesso e a utilização das portas USB do servidor pelos dispositivos USB.

As políticas para encriptação de suportes de dados amovíveis podem ser encontradas na Management Console, no grupo de tecnologia *Server Encryption*.

### Encryption em sistemas operativos de servidor e suportes de dados externos

Quando a política *Suporte de dados externo de encriptação EMS* do servidor protegido é **Selecionada**, o suporte de dados externo é encriptado. O Encryption associa o dispositivo ao servidor protegido com a chave de computador, e ao utilizador, com a chave de Roaming de utilizador do proprietário/utilizador do dispositivo amovível. Todos os ficheiros adicionados ao dispositivo amovível são então encriptados com essas mesmas chaves, independentemente do computador ao qual se encontra ligado.

#### **NOTA:**

O Encryption em sistemas operativos de servidor converte a encriptação de Utilizador para encriptação Comum, exceto em dispositivos amovíveis. Em dispositivos amovíveis, a encriptação é realizada com a chave de roaming de utilizador associada ao computador.

Quando o utilizador não concorda com a encriptação de um dispositivo amovível, o acesso do utilizador ao dispositivo poderá ser definido para *bloqueado*, quando for utilizado no servidor protegido, *Só de leitura*, enquanto for utilizado no servidor protegido ou *Acesso total*. As políticas do servidor protegido determinam o nível de acesso de um dispositivo amovível desprotegido.

As atualizações de política ocorrem quando o dispositivo amovível é reintroduzido no servidor protegido original.

### Autenticação e Suportes de Dados Externos

As políticas do servidor protegido determinam a funcionalidade da autenticação.

Depois de um dispositivo amovível ter sido encriptado, apenas o respetivo proprietário/utilizador pode aceder ao dispositivo amovível no servidor protegido. Os restantes utilizadores não podem aceder aos ficheiros encriptados no suporte de dados amovível.

A autenticação local automática permite que o suporte de dados amovível protegido seja automaticamente autenticado quando inserido no servidor protegido e o proprietário desse suporte de dados tiver sessão iniciada. Quando a autenticação automática estiver desativada, o proprietário/utilizador deve efetuar a autenticação para aceder ao dispositivo amovível protegido.

Quando o computador de encriptação original de um dispositivo de dados amovível for um servidor protegido, o proprietário/utilizador deve sempre iniciar sessão no dispositivo amovível quando o utilizar em computadores que não sejam o computador de encriptação original, independentemente das definições de política do Encryption External Media definidas nos outros computadores.

Consulte AdminHelp para obter informações sobre o Controlo de Portas e políticas do Encryption External Media do Server Encryption.

## Suspender o Encryption em sistemas operativos de servidor

A suspensão de um servidor encriptado impede o acesso aos respetivos dados encriptados após um reinício. O utilizador do servidor virtual não pode ser suspenso. Em vez disso, é suspensa a chave de Computador do servidor encriptado.

#### **NOTA:**

A suspensão do endpoint do servidor não suspende imediatamente o servidor. A suspensão ocorre quando a chave for novamente solicitada, tipicamente quando o servidor é reiniciado.

#### **NOTA:**

Use esta função com cautela. A suspensão de um servidor encriptado poderá originar instabilidade, dependendo das definições de política e se o servidor protegido está suspenso enquanto se encontra desligado da rede.

### Pré-requisitos

- Os direitos de administrador de suporte técnico, atribuídos na Management Console, são necessários para suspender um endpoint.
- O administrador tem de ter sessão iniciada na Management Console.

No painel esquerdo da Management Console, clique em **Populações > Pontos terminais**.

Procure ou selecione um nome do anfitrião e, em seguida, clique no separador **Detalhes e ações**.

Em *Controlo de dispositivos do servidor*, clique em **Suspender** e, em seguida, em **Sim**.

 **NOTA:**

Clique em **Restabelecer** para permitir que o Encryption em sistemas operativos de servidor aceda a dados encriptados no servidor após reiniciar.

## Configurar a Ativação diferida

O Encryption Client com Ativação diferida é diferente da ativação do Encryption Client de duas formas:

### Políticas de encriptação com base no dispositivo

As políticas do Encryption Client são baseadas no utilizador; as políticas de encriptação do Encryption Client com Ativação diferida baseiam-se no dispositivo. A encriptação de utilizador é convertida em encriptação Comum. Esta diferença permite ao utilizador usar um dispositivo pessoal no domínio da organização, enquanto a organização mantém a sua segurança gerindo centralmente as políticas de encriptação.

### Ativação

Com o Encryption Client, a ativação é automática. Quando o com Ativação diferida é instalado, a ativação automática é desativada. Alternativamente, o utilizador escolhe se pretende ativar a encriptação e quando pretende fazê-lo.

#### NOTA:

Antes de um utilizador sair permanentemente da organização e enquanto o seu endereço de e-mail ainda estiver ativo, o utilizador deve executar o Encryption Removal Agent e desinstalar o Encryption Client do seu computador pessoal.

## Personalização da Ativação diferida

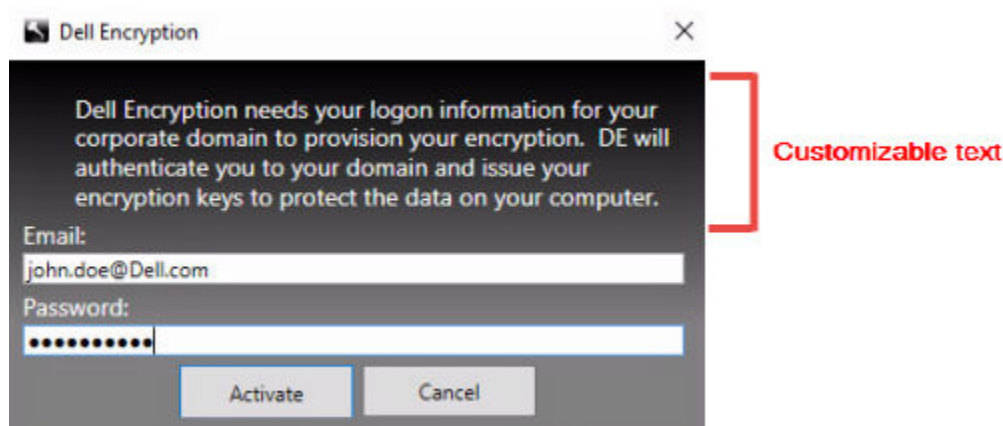
Estas tarefas do lado do cliente permitem a personalização da Ativação diferida.

- Adicionar uma exclusão de responsabilidade à caixa de diálogo Início de sessão de Ativação
- Desativar a reativação automática (opcional)

Adicionar uma exclusão de responsabilidade à caixa de diálogo Início de sessão de Ativação

A caixa de diálogo Início de sessão de Ativação é apresentada nas seguintes ocasiões:

- Quando um utilizador não gerido inicia sessão.
- Quando o utilizador seleciona Ativar o Dell Encryption no menu do ícone Encriptação, localizado na área de notificação.



## Preparar o computador para instalação

Se os dados tiverem sido encriptados num produto de encriptação que não seja da Dell, antes de instalar o Encryption Client, desencripte os dados utilizando o software de encriptação existente e, em seguida, desinstale o software de encriptação existente. Se o computador não reiniciar automaticamente, reinicie o computador.

### Crie uma palavra-passe do Windows

A Dell recomenda vivamente que seja criada uma palavra-passe do Windows (se ainda não existir nenhuma) para proteger o acesso aos dados encriptados. A criação de uma palavra-passe para o computador evita que outros iniciem sessão na sua conta de utilizador sem a sua palavra-passe.

### Desinstalar versões anteriores do Encryption Client

Antes de desinstalar uma versão anterior do Encryption Client, pare ou interrompa um varrimento de encriptação, se necessário.

Se o computador estiver a executar uma versão do Dell Encryption anterior à v8.6, desinstale o Encryption Client a partir da linha de comandos. Para obter instruções, consulte *Desinstalar o Encryption e o Server Encryption Client*.

#### **NOTA:**

Se planejar instalar a versão mais recente do Encryption Client imediatamente após a desinstalação, não é necessário executar o Encryption Removal Agent para descriptar os ficheiros.

Para atualizar uma versão anterior do Encryption Client instalado com a Ativação diferida, desinstale com o [Desinstalador do Data Security](#) ou os [Instaladores subordinados](#). Estes métodos de desinstalação são possíveis mesmo que a definição OPTIN esteja desativada.

#### **NOTA:**

Se não tiver sido ativado nenhum utilizador anteriormente, o Encryption Client desmarca a definição de OPTIN do cofre SDE uma vez que é uma definição residual de uma instalação anterior. O Encryption Client bloqueia as Ativações diferidas se tiverem sido ativados utilizadores anteriormente, mas o sinalizador OPTIN não tiver sido definido no cofre SDE.

## Instalar o Encryption com Ativação diferida

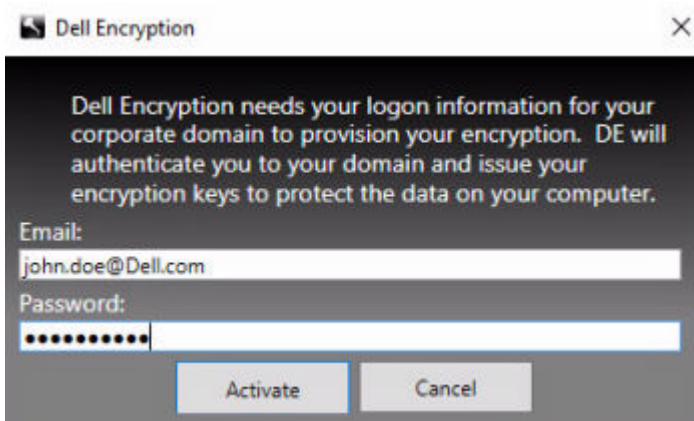
Para instalar o Encryption Client com Ativação diferida, instale o Encryption Client com o parâmetro OPTIN=1. Para obter mais informações sobre a instalação do cliente com o parâmetro OPTIN=1, consulte [Instalar o Encryption](#).

## Ativar o Encryption com a Ativação diferida

- A ativação associa um utilizador de domínio a uma conta de utilizador local e a um computador específico.
- É possível ativar vários utilizadores no mesmo computador, desde que utilizem contas locais exclusivas e tenham endereços de e-mail de domínio exclusivos.
- Um utilizador só pode ativar um Encryption Client uma vez por conta de domínio.

Antes de ativar o Encryption Client:

- Inicie sessão na conta local que utiliza mais frequentemente. Os dados associados a esta conta são os dados a encriptar.
  - Estabeleça ligação à rede da sua organização.
1. Inicie sessão na estação de trabalho ou no servidor.
  2. Introduza o endereço de e-mail de domínio e a palavra-passe e clique em **Ativar**.



#### **NOTA:**

Os endereços de e-mail fora do domínio ou pessoais não podem ser utilizados para a ativação.

3. Clique em **Fechar**.

O Servidor Dell combina o grupo de chaves de encriptação com as credenciais do utilizador e com o ID exclusivo do computador (ID de máquina), criando uma relação inquebrável entre o grupo de chaves, o computador específico e o utilizador.

4. Reinicie o computador para dar início ao varrimento de encriptação.

**NOTA:**

A Management Console local, acessível a partir do ícone na área de notificação, mostra as políticas enviadas pelo servidor e não a política em vigor.

## Resolução de problemas da Ativação diferida

### Resolução de problemas da ativação

#### **Problema: não é possível aceder a determinados ficheiros e pastas**

A incapacidade de aceder a determinados ficheiros e pastas é um sintoma de ter iniciado sessão numa conta diferente daquela em que o utilizador foi ativado.

A caixa de diálogo Início de sessão de Ativação é apresentada automaticamente mesmo que o utilizador tenha sido ativado anteriormente.

#### **Solução possível**

Termine sessão e inicie sessão novamente com as credenciais da conta ativada e tente aceder de novo aos ficheiros.

Nos casos raros em que o Encryption Client não conseguir autenticar o utilizador, a caixa de diálogo Início de sessão de Ativação solicita a introdução das credenciais do utilizador para autenticar e aceder às chaves de encriptação. Para utilizar a funcionalidade de reativação automática, AMBAS as chaves do Registo *AutoReactivation* e *AutoPromptForActivation* têm de estar ativadas. Embora a funcionalidade esteja ativada por predefinição, pode ser desativada manualmente. Para obter mais informações, consulte [Desativar a reativação automática](#).

#### **Mensagem de erro: falha na autenticação do servidor**

O servidor não conseguiu autenticar o endereço de e-mail e a palavra-passe.

#### **Soluções Possíveis**

- Utilize o endereço de e-mail associado à organização. Os endereços de e-mail pessoais não podem ser utilizados para a ativação.
- Introduza novamente o endereço de e-mail e a palavra-passe e certifique-se de que não existem erros tipográficos.
- Solicite que o administrador verifique se a conta de e-mail está ativa e não se encontra bloqueada.
- Solicite que o administrador reponha a palavra-passe do domínio do utilizador.

#### **Mensagem de erro: erro de ligação de rede**

O Encryption Client não conseguiu comunicar com o Servidor Dell.

#### **Soluções Possíveis**

- Ligue diretamente à rede da organização e tente ativar novamente.
- Se for necessário o acesso VPN para estabelecer ligação à rede, verifique a ligação VPN e tente novamente.
- Verifique o URL do Dell Server para garantir que corresponde ao URL fornecido pelo administrador.

O URL e outros dados que o utilizador introduziu no programa de instalação estão armazenados no registo. Verifique a exatidão dos dados em [HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield] e [HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield\Servlet]

- Desligue e ligue novamente:

Desligue o computador da rede.

Volte a conectar à rede.

Reinicie o computador.

Tente novamente ligar à rede.

**Mensagem de erro: Legacy Server não suportado**

Não é possível ativar a encriptação num servidor legado; o Dell Server tem de ser da versão v9.1 ou superior.

**Solução possível**

- Verifique o URL do Dell Server para garantir que corresponde ao URL fornecido pelo administrador.  
O URL e outros dados que o utilizador introduziu no programa de instalação estão armazenados no registo.
- Verifique a exatidão dos dados em [HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield] e [HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield\Servlet]

**Mensagem de erro: utilizador de domínio já ativado**

Um segundo utilizado iniciou sessão no computador local e tentou a ativação numa conta de domínio que já tinha sido ativada.

Um utilizador só pode ativar um Encryption Client uma vez por conta de domínio.

**Solução possível**

Desencripte e desinstale o Encryption Client tendo sessão iniciada como o segundo utilizador ativado.

**Mensagem de erro: erro no servidor geral**

Ocorreu um erro no servidor.

**Solução possível**

O administrador deverá verificar os registos do servidor para garantir que os serviços estão a ser executados.

O utilizador deve tentar ativar mais tarde.

**Ferramentas**

CMGAd

Utilize o utilitário CMGAd antes de iniciar o Encryption Removal Agent para obter o grupo de chaves de encriptação. O utilitário CMGAd e respetivas instruções estão localizados no suporte de dados de instalação Dell (Dell-Offline-Admin-XXbit)

**Ficheiros de registo**

Em C:\ProgramData\Dell\Dell Data Protection\Encryption, procure o ficheiro de registo com o nome **CmgSysTray**.

Procure "Resultado da ativação manual".

O código de erro encontra-se na mesma linha, seguido por " status = " (estado); o estado indica o erro ocorrido.

## Resolução de problemas

### Todos os clientes - Resolução de problemas

- **Os ficheiros de registo do instalador do conjunto principal do** encontram-se 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\<NomeDeUtilizador>\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\<NomeDeUtilizador>\AppData\Local\Temp`. Por exemplo, `C:\Users\<NomeDeUtilizador>\AppData\Local\Temp\dd_vccredist_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 4.5.2 ou posterior.
- Consulte [este documento](#) se o computador onde pretende efetuar a instalação tiver (ou teve anteriormente) o Dell Access instalado. O Dell Access não é compatível com este conjunto de produtos.

### Todos os clientes - Estado de Proteção

Foi implementado um novo método para determinar o estado protegido de um dispositivo no Dell Server v9.8.2. Anteriormente, a área de estado protegido do endpoint no dashboard da Management Console apenas indicaria o estado de encriptação por dispositivo.

Com o Dell Server v9.8.2, o estado protegido é indicado agora se forem cumpridos todos os critérios a seguir enunciados:

- O Advanced Threat Prevention está instalado e ativado.
- O Web Protection ou o Client Firewall está instalado e a política do Web Protection ou do Client Firewall está ativada.
- O Self-Encrypting Drive Manager está instalado, ativado e a PBA está ativada.
- A Full Disk Encryption está instalada, ativada e a PBA está ativada.
- O BitLocker Manager está instalado, ativado e a encriptação foi concluída.
- O Dell Encryption (Mac) está instalado e ativado e a política *Encriptar utilizando FileVault para Mac* foi implementada.
- O Dell Encryption (Windows) está instalado, ativado, a encriptação baseada em políticas foi definida para o ponto final e os varrimentos do dispositivo estão concluídos.

## Resolução de problemas do Dell Encryption (cliente e servidor)

### 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 do 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 do domínio ou o nome de utilizador do administrador não está no formato UPN.

Solução possível: na caixa de diálogo Ativação, introduza as credenciais de um administrador do domínio no 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 Dell 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 Dell Server para garantir que corresponde ao URL fornecido pelo administrador. 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 Dell Server deve ser a versão 9.1 ou superior. Se necessário, faça uma atualização do seu Dell Server para a versão 9.1 ou superior.
- Verifique o URL do Dell Server para garantir que corresponde ao URL fornecido pelo administrador. 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 Encryption em sistemas operativos de servidor requer o acesso de um utilizador real ao servidor. O utilizador pode ser de qualquer tipo: utilizador de domínio ou de fora do domínio, ligado ao ambiente de trabalho remoto ou interativo, mas este deve ter acesso a credenciais de administrador do domínio.

A caixa de diálogo de Ativação é apresentada num dos seguintes fluxos de trabalho:

- Um utilizador novo (não gerido) inicia sessão no computador.
- Quando um utilizador novo clica com o botão direito do rato no ícone *Encryption* na área de notificação 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 *Encryption* na área de notificação 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 do domínio é uma medida de segurança que impede que o Encryption em sistemas operativos de servidor seja implementada em ambientes de servidor não suportados. Para desativar o requisito de credenciais de administrador do domínio, consulte [Antes de começar](#).

6. O Dell Server verifica as credenciais no cofre da empresa (Active Directory ou equivalente) para confirmar se as mesmas são as credenciais do administrador do domínio.
7. Um UPN é construído utilizando as credenciais.

- Com o UPN, o Dell Server cria uma nova conta de utilizador para o utilizador do servidor virtual e guarda as credenciais no cofre do Dell Server.

A **conta de utilizador do servidor virtual** destina-se a utilização exclusiva do Encryption Client. Esta é utilizada para a autenticação no servidor, para a 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.

- Quando a ativação for bem-sucedida, o utilizador reinicia o computador, o que inicia a segunda fase, a autenticação e a 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 Encryption em sistemas operativos de servidor inicia automaticamente sessão como utilizador do servidor virtual, solicitando a chave de Computador ao Dell Server. Ocorre mesmo antes de qualquer utilizador iniciar sessão.

- Abra a caixa de diálogo "Acerca de" para confirmar se o Encryption em sistemas operativos de servidor está autenticado e no modo de Servidor.
- Se a ID do Encryption client apresentar cor vermelha, a encriptação ainda não foi ativada.
- Na 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.

Para obter mais informações sobre a política de *Intervalo de Tempo entre Tentativas em caso de Falha de rede*, consulte AdminHelp, disponível na Management Console.

### Autenticação e ativação de dispositivos

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

- 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.
- O computador verifica o respetivo estado de ativação de dispositivos com o Dell Server:
  - Se o computador não tiver ativado o dispositivo anteriormente, o Dell Server atribui um MCID, um DCID e um certificado de confiança ao computador e guarda todas as informações no cofre do Dell Server.
  - Se o computador tiver anteriormente ativado o dispositivo, o Dell Server verifica o certificado de confiança.
- Depois de o Dell Server atribuir o certificado de confiança ao servidor, este pode aceder às respetivas chaves de encriptação.
- 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.

## (Opcional) Criar um ficheiro de registo do Encryption Removal Agent

- Antes de iniciar o processo de desinstalação, é possível criar, de forma opcional, um ficheiro de registo do Agente de remoção de encriptação. Este ficheiro de registo é útil para resolução de problemas numa operação de desinstalação/

desencriptação. Se não pretender desencriptar ficheiros durante o processo de desinstalação, não é necessário criar este ficheiro de registo.

- O ficheiro de registo do Encryption Removal Agent apenas é criado após a execução do serviço Encryption Removal Agent, que ocorre somente quando o computador é reiniciado. Quando o cliente for desinstalado com êxito e o computador for totalmente desencriptado, o ficheiro de registo é eliminado definitivamente.
- O caminho do ficheiro de registo é `C:\ProgramData\Dell\Dell Data Protection\Encryption`.
- Crie a seguinte entrada de registo no computador destinado à desencriptação.

```
[HKLM\Software\Credant\DecryptionAgent]
```

```
"LogVerbosity"=DWORD:2
```

0: sem registos

1: regista os erros que impedem a execução do serviço

2: regista os erros que impedem a desencriptação total dos dados (nível recomendado)

3: regista informações acerca de todos os ficheiros e volumes de desencriptação

5: regista as informações de depuração

## Encontrar versão do TSS

- O TSS é um componente que interage com o TPM. Para encontrar a versão do TSS, aceda a (localização predefinida) `C:\Program Files\Dell\Dell Data Protection\Drivers\TSS\bin > tcscd_win32.exe`. Clique com o botão direito do rato no ficheiro e selecione **Propriedades**. Verifique a versão do ficheiro no separador **Detalhes**.

## Interações de PCS e Encryption External Media

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


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

### Para encriptar os dados gravados em CD/DVD

- Defina a encriptação de suportes de dados do Windows = Ligado.
- Defina EMS: Excluir encriptação de CD/DVD = não selecionado.
- 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, 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.

 **NOTA:** Se um ficheiro de destino for propriedade da conta do sistema, o WSScan deve ser executado no modo de sistema com a ferramenta PsExec.

### 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 **wsscscan.exe** na mesma. O WSScan é iniciado.
3. Clique em **Avançadas**.
4. Selecione o tipo de unidade a analisar: *Todas as unidades, Unidades fixas, Unidades amovíveis* ou *CDROM/DVDROM*.
5. Selecione o tipo de relatório de encriptação: *Ficheiros encriptados, Ficheiros não encriptados, Todos os ficheiros* ou *Ficheiros não encriptados em violação*:
  - *Ficheiros encriptados* - Para assegurar que todos os dados são desencriptados quando desinstalar o Encryption. Siga o processo de desencriptação de dados existente, por exemplo, a emissão de uma atualização de política de

descriptação. Após descriptar os dados, mas antes de reiniciar para preparar a desinstalação, execute o WSScan para garantir que todos os dados estão descriptados.

- *Ficheiros descriptados* - 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 descriptados, com indicação se os ficheiros devem ser encriptados (S/N).
- *Ficheiros descriptados 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 **Simple** 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 no menu é 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 caracteres 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.

#### Utilização da linha de comandos do WSScan

```
WSScan [-ta] [-tf] [-tr] [-tc] [drive] [-s] [-o<filepath>] [-a] [-f<format specifier>] [-r] [-u[a][-|v]] [-d<delimiter>] [-q] [-e] [-x<exclusion directory>] [-y<sleep time>]
```

| Opção   | Significado                                                                                                                                                           |
|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Unidade | Unidade a analisar. Se não for especificada, serão assumidas, por predefinição, todas as unidades de disco rígido fixas locais. Pode ser uma unidade de rede mapeada. |
| -ta     | Analisar todas as unidades                                                                                                                                            |
| -tf     | Analisar as unidades fixas (predefinição)                                                                                                                             |
| -tr     | Analisar as unidades amovíveis                                                                                                                                        |
| -tc     | Analisar CDROM/DVDROM                                                                                                                                                 |
| -s      | Operação silenciosa                                                                                                                                                   |
| -o      | Caminho do ficheiro de saída                                                                                                                                          |
| -a      | Anexar ao ficheiro de saída. O ficheiro de saída é truncado pelo comportamento predefinido.                                                                           |
| -f      | Reportar o especificador de formato (Reportar, Fixo, Delimitado)                                                                                                      |
| -r      | Executar o WSScan sem privilégios de administrador. <b>Neste modo, alguns ficheiros podem não ficar visíveis.</b>                                                     |
| -u      | Incluir ficheiros descriptados no ficheiro de saída.                                                                                                                  |

| Opção | Significado                                                                                                                                                         |
|-------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|       | Esta opção é sensível à ordem: "u" deve ser utilizado primeiro, "a" deve ser o segundo (ou ser omitido), "-" ou "v" deve ser o último.                              |
| -u-   | Incluir apenas ficheiros descriptados no ficheiro de saída                                                                                                          |
| -ua   | Reportar também ficheiros descriptados, mas utilizar todas as políticas do utilizador para apresentar o campo "should".                                             |
| -ua-  | Reportar apenas ficheiros descriptados, mas utilizar todas as políticas do utilizador para apresentar o campo "should".                                             |
| -uv   | Reportar ficheiros descriptados que apenas violem a política (Is=No/Should=Y)                                                                                       |
| -uav  | Reportar ficheiros descriptados que apenas violem a política (Is=No/Should=Y), utilizando todas as outras políticas de utilizador.                                  |
| -d    | Especificar o que é utilizado como separador de valores para uma saída delimitada                                                                                   |
| -q    | Especificar os valores que devem ser colocados entre aspas para uma saída delimitada                                                                                |
| -e    | Incluir campos de encriptação alargada em saída delimitada                                                                                                          |
| -x    | Excluir o diretório da análise. São permitidas várias exclusões.                                                                                                    |
| -y    | Tempo de suspensão (em milissegundos) entre os diretórios. Esta opção resulta em análises mais lentas, mas potencialmente num CPU com maior capacidade de resposta. |

### 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.<br><b>SysData:</b> chave SDE.<br><b>Utilizador:</b> chave de encriptação do utilizador.<br><b>Comum:</b> chave de encriptação Comum.<br>O WSScan não indica ficheiros encriptados utilizando o Encrypt for Sharing. |
| KCID                 | A ID do computador principal.<br>Tal como apresentado no exemplo acima, " <b>7vdlxrsb</b> "<br>Se estiver a analisar uma unidade de rede mapeada, o relatório da análise não apresenta uma KCID.                                                                               |
| UCID                 | A ID do utilizador.<br>Tal como apresentado no exemplo acima, " <b>_SDENCR_</b> "<br>A UCID é partilhada por todos os utilizadores desse computador.                                                                                                                           |
| Ficheiro             | O caminho do ficheiro encriptado.<br>Tal como apresentado no exemplo acima, " <b>c:\temp\Dell - test.log</b> "                                                                                                                                                                 |

| Saída     | Significado                                                                                                                                                                                                                                    |
|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Algoritmo | <p>O algoritmo de encriptação utilizado para encriptar o ficheiro.</p> <p>Tal como apresentado no exemplo acima, "<b>continua encriptado por AES256</b>"</p> <p>RIJNDAEL 128</p> <p>RIJNDAEL 256</p> <p>AES-128</p> <p>AES-256</p> <p>3DES</p> |

## Utilizar o WSProbe

O Probing Utility pode ser utilizado com todas as versões do Encryption, exceto as políticas do Encryption External Media. Utilize o Probing Utility para:

- Analisar ou agendar análises de um computador encriptado. O Probing Utility verifica a política de Prioridade de análise da estação de trabalho.
- Desative temporariamente ou volte a ativar o Application Data Encryption List do utilizador atual.
- Adicione ou remova nomes de processos na lista de privilégios.
- Efetue a resolução de problemas de acordo com as instruções do Dell ProSupport.

### Abordagens ao Data Encryption

Se especificar políticas de encriptação de dados em dispositivos Windows, pode utilizar qualquer uma das seguintes abordagens:

- A primeira abordagem é aceitar o comportamento predefinido do cliente. Se especificar pastas em Pastas encriptadas comuns ou Pastas encriptadas do utilizador, ou definir Encriptar "Meus documentos", Encriptar pastas pessoais do Outlook, Encriptar ficheiros temporários, Encriptar ficheiros temporários da Internet ou Encriptar ficheiro de paginação do Windows para selecionado, os ficheiros afetados são encriptados quando são criados, ou (depois de serem criados por um utilizador não gerido) quando um utilizador gerido inicia sessão. O cliente também analisa as pastas especificadas ou relacionadas com estas políticas para uma possível encriptação/desencriptação, quando o nome de uma pasta é alterado ou quando o cliente recebe alterações a estas políticas.
- Também pode definir Analisar estação de trabalho no início de sessão para Selecionado. Se Analisar estação de trabalho no início de sessão estiver definido para Selecionado, quando um utilizador iniciar sessão, o cliente compara a forma como os ficheiros estão encriptados nas pastas encriptadas, anterior e atualmente, com as políticas do utilizador, e efetua as alterações necessárias.
- Para encriptar ficheiros que cumpram os critérios de encriptação, mas que foram criados antes da entrada em vigor das políticas de encriptação, sem qualquer impacto no desempenho da análise frequente, pode utilizar este utilitário para analisar ou agendar a análise do computador.

### Pré-requisitos

- O dispositivo Windows a utilizar tem estar encriptado.
- O utilizador a utilizar tem de ter sessão iniciada.

### Utilizar o Probing Utility

O WSProbe.exe está localizado no suporte multimédia de instalação.

#### Sintaxe

```
wsprobe [path]
wsprobe [-h]
wsprobe [-f path]
wsprobe [-u n] [-x process_names] [-i process_names]
```

#### Parâmetros

| Parâmetro | Para                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| caminho   | Especificação opcional de um caminho específico no dispositivo a analisar para uma possível encriptação/desencriptação. Se não especificar um caminho, este utilitário analisa todas as pastas relacionadas com as suas políticas de encriptação.                                                                                                                                                                                          |
| -h        | Consulte a Ajuda da linha de comandos.                                                                                                                                                                                                                                                                                                                                                                                                     |
| -f        | Efetue a resolução de problemas de acordo com as instruções do Dell ProSupport                                                                                                                                                                                                                                                                                                                                                             |
| -u        | Desative temporariamente ou volte a ativar o Application Data Encryption List do utilizador. Esta lista apenas é eficaz se a opção Encriptação ativada estiver selecionada no utilizador atual. Especifique o valor 0 para desativar ou 1 para voltar a ativar. A atual política em vigor para o utilizador é restabelecida no próximo início de sessão.                                                                                   |
| -x        | Adicione nomes de processos à lista de privilégios. Os nomes de processos do computador e do instalador indicados nesta lista, incluindo os adicionados utilizando este parâmetro ou HKLM\Software\CREDANT\CMGShield\EUWPrivilegedList, são ignorados se forem especificados no Application Data Encryption List. Separe os nomes de processos com vírgulas. Se a sua lista incluir um ou mais espaços, delimite a lista com aspas duplas. |
| -i        | Elimine os nomes de processos previamente adicionados à lista de privilégios (não é possível eliminar nomes de processos codificados). Separe os nomes de processos com vírgulas. Se a sua lista incluir um ou mais espaços, delimite a lista com aspas duplas.                                                                                                                                                                            |

## 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 Encryption continua instalado, continua configurado, ou ambos. A desencriptação apenas tem início quando o Encryption for 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 a resolução de problemas, defina a verbosidade do registo para 2 e reinicie o serviço do Agente de Remoção de Encriptação para forçar outro varrimento de desencriptação. Consulte [\(Opcional\) Criar um ficheiro de registo do Encryption Removal Agent](#) para obter instruções.
- **Concluído** - O varrimento da desencriptação está concluído. É agendada a eliminação do serviço, do executável, do controlador e do executável do controlador para a reinicialização de sistema seguinte.

# Resolução de problemas SED

## Utilizar o Código de acesso inicial

- Esta política é utilizada para iniciar sessão num computador quando o acesso à rede não se encontra disponível. Ou seja, o acesso ao Dell Server e ao AD não se encontram disponíveis. Utilize a política de *Código de acesso inicial* apenas se for absolutamente necessário. A Dell não recomenda este método para iniciar sessão. A utilização da política de *Código de acesso inicial* não proporciona o mesmo nível de segurança que o método comum de início de sessão utilizando o nome do utilizador, domínio e palavra-passe.

Além de ser um método de início de sessão menos seguro, se um utilizador for ativado utilizando o *Código de acesso inicial*, não existe qualquer registo no Dell Server da ativação desse utilizador neste computador. Além disso, não há forma de gerar um código de resposta no Dell Server para o utilizador, caso este erre a palavra-passe e as perguntas de autoajuda.

- O *Código de acesso inicial* só pode ser utilizado **uma** vez, imediatamente após a ativação. Após o início de sessão de um utilizador final, o *Código de acesso inicial* fica indisponível. O primeiro início de sessão do domínio que ocorre depois de introduzir o *Código de acesso inicial*, será colocado em cache e o campo para a introdução do *Código de acesso inicial* não é apresentado novamente.
- O *Código de acesso inicial* **apenas** é apresentado nas seguintes condições:
  - Nunca foi ativado um utilizador dentro da PBA.
  - O cliente não tem ligação à rede nem ao Dell Server.

### Utilizar o Código de acesso inicial

1. Defina um valor para a política de **Código de acesso inicial** na Management Console.
2. Guarde e consolide a política.
3. Inicie o computador local.
4. Introduza o **Código de acesso inicial** quando for apresentado o ecrã Código de acesso.
5. Clique na **seta azul**.
6. Clique em **OK** quando for apresentado o ecrã Aviso legal.
7. Inicie sessão no Windows com as credenciais de utilizador deste computador. Estas credenciais devem fazer parte do domínio.
8. Após iniciar sessão, abra a Data Security Console e verifique se o utilizador da PBA foi criado com êxito.

Clique em **Registo** no menu superior e procure a mensagem *Criado utilizador da PBA para <DOMAIN\Username>*, que indica que o processo foi bem-sucedido.
9. Encerre e reinicie o computador.
10. No ecrã de início de sessão, introduza o nome de utilizador, o domínio e a palavra-passe anteriormente utilizados para iniciar sessão no Windows.

Tem de fazer corresponder o formato do nome de utilizador que foi utilizado ao criar o utilizador da PBA. Desta forma, se tiver utilizado o formato DOMÍNIO\Nomedeuutilizador, tem de introduzir DOMÍNIO\Nomedeuutilizador no campo Nome de utilizador.
11. Clique em **Iniciar sessão** quando for apresentado o ecrã Aviso legal.

O Windows é, então, iniciado e é possível utilizar o computador da forma habitual.

## Criar um ficheiro de registo de PBA para resolução de problemas

- Poderão existir casos em que é necessário um ficheiro de registo de PBA para a resolução de problemas com a PBA, tais como:
  - Não consegue ver o ícone de ligação à rede, embora saiba que existe conectividade de rede. O ficheiro de registo contém informações de DHCP para resolver o problema.
  - Não consegue ver o ícone de ligação do Dell Server. O ficheiro de registo contém informações para ajudar a diagnosticar problemas de conectividade.
  - A autenticação falha mesmo ao introduzir as credenciais corretas. O ficheiro de registo utilizado nos registos de servidor do Dell Server pode ajudar a diagnosticar o problema.

### Captar registos aquando do arranque através da PBA (PBA legada)

1. Crie uma pasta numa unidade USB, no nível da raiz, e atribua-lhe o nome **\CredantSED**.
2. Crie um ficheiro com o nome actions.txt e coloque-o na pasta **\CredantSED**.
3. No ficheiro actions.txt, adicione a linha:  
**get logs**
4. Guarde e feche o ficheiro.  
*Não introduza a unidade USB quando o computador estiver desligado. Se a unidade USB já estiver inserida durante o processo de encerramento, remova-a.*
5. Ligue o computador e reproduza o problema. Insira a unidade USB no computador do qual serão recolhidos os registos durante este passo.
6. Depois de introduzir a unidade USB, aguarde entre 5 e 10 segundos e, em seguida, retire a unidade.  
Um ficheiro credpbaenv.tgz é criado na pasta **\CredantSED** que contém os ficheiros de registo necessários.

#### **Captar registos aquando do arranque através da PBA (PBA UEFI)**

1. Crie um ficheiro com o nome **PBAErr.log** no nível da raiz da unidade USB.
2. Introduza a unidade USB **antes** de ligar o computador.
3. Remova a unidade USB **depois** de reproduzir o problema que requer os registos.

O ficheiro PBAErr.log é atualizado e gravado em tempo real.

## **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 [dell.com/support](http://dell.com/support).
2. Selecione o modelo do seu computador.
3. Selecione **Controladores e transferências**.
4. Selecione o **Sistema operativo** do computador de destino.
5. Selecione 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**

1. Navegue até à pasta para onde transferiu o ficheiro de instalação do controlador.
2. Clique duas vezes no controlador do Dell ControlVault para iniciar o ficheiro executável de extração automática.

#### **NOTA:**

Instale o controlador primeiro. O nome de ficheiro do controlador *quando este documento foi criado* é ControlVault\_Setup\_2MYJC\_A37\_ZPE.exe.

3. Clique em **Continuar** para iniciar.
4. Clique em **Ok** para descomprimir os ficheiros de controladores na localização predefinida em C:\Dell\Drivers\- 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.

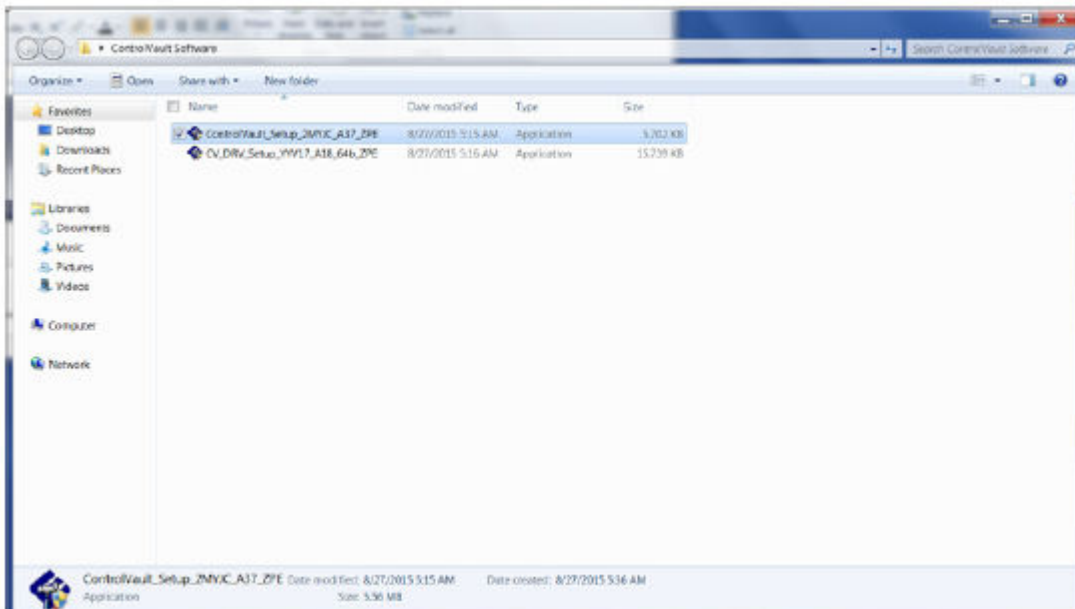
7. A pasta que contém os ficheiros deve ser apresentada após a extração. Caso não seja apresentada, navegue até à pasta na qual extraiu os ficheiros. Neste caso, a pasta é **JW22F**.
8. Clique duas vezes em **CVHCI64.MSI** para iniciar o programa de instalação dos controladores. [este exemplo é **CVHCI64.MSI** neste modelo (CVHCI para um computador de 32 bits)].
9. Clique em **Seguinte** no ecrã de boas-vindas.
10. Clique em **Seguinte** para instalar os controladores na localização predefinida em C:\Program Files\Broadcom Corporation\Broadcom USH Host Components\.
11. Selecione a opção **Completo** e clique em **Seguinte**.
12. Clique em **Instalar** para iniciar a instalação dos controladores.
13. 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

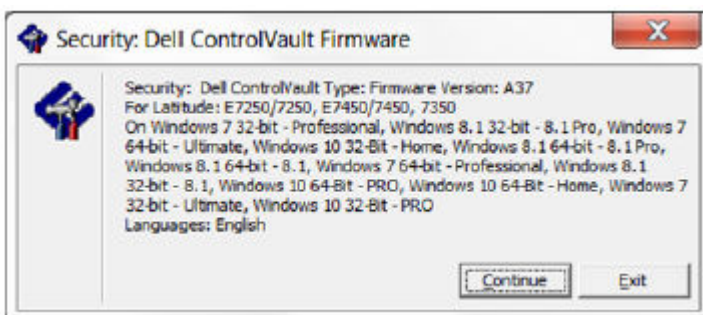
- O Gestor de dispositivos terá um dispositivo Dell ControlVault (e outros dispositivos) dependendo da configuração de hardware e do sistema operativo.

### Instalação do firmware do Dell ControlVault

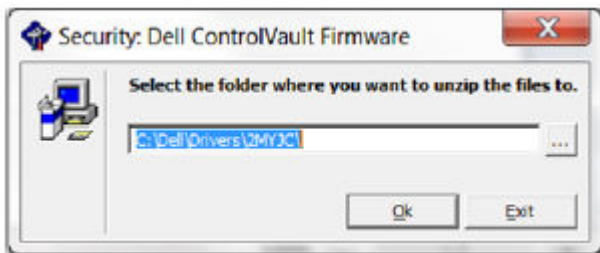
1. Navegue até à pasta para onde transferiu o ficheiro de instalação do firmware.



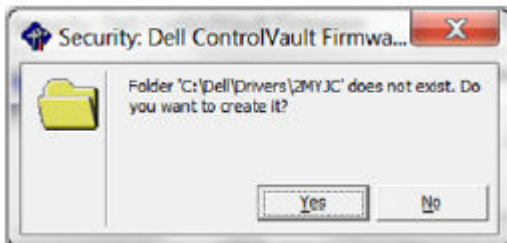
2. Clique duas vezes no firmware do Dell ControlVault para iniciar o ficheiro executável de extração automática.
3. Clique em **Continuar** para iniciar.



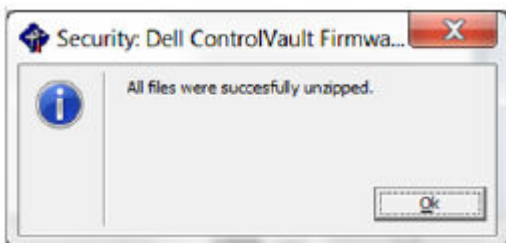
4. Clique em **Ok** para descomprimir os ficheiros de controladores na localização predefinida em C:\Dell\Drivers\



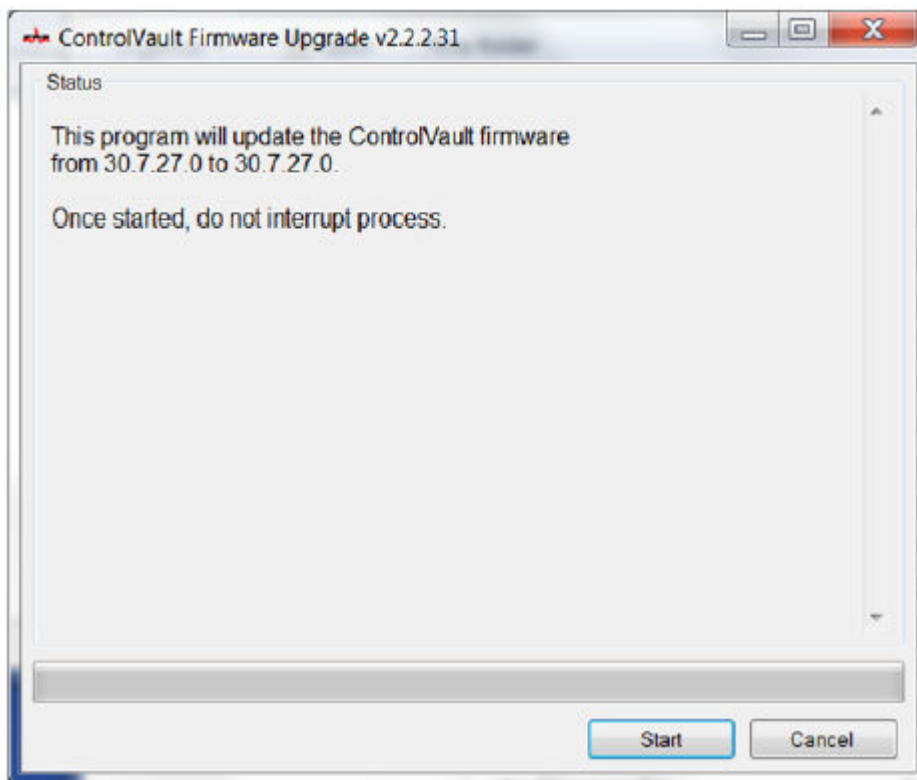
5. Clique em **Sim** para permitir a criação de uma nova pasta.



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.



**NOTA:**

No caso de atualização a partir de uma versão mais antiga de firmware, pode ser-lhe solicitada 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.

## Computadores UEFI

### Resolução de problemas de ligação à rede

- Para que a autenticação de pré-arranque seja bem-sucedida num computador com firmware UEFI, o modo PBA tem de ter ligação à rede. Por predefinição, os computadores com firmware UEFI não têm ligação à rede até que o sistema operativo seja carregado, o que ocorre depois do modo PBA. Se o procedimento do computador descrito em [Configuração da pré-instalação para computadores UEFI](#) for concluído com sucesso e configurado corretamente, o ícone de ligação à rede é apresentado no ecrã de autenticação de pré-arranque quando o computador estiver ligado à rede.



- Verifique o cabo de rede para garantir que está ligado ao computador caso o ícone de ligação continue a não ser apresentado durante a autenticação de pré-arranque. Reinicie o computador para reiniciar o modo PBA caso o mesmo não esteja ligado ou esteja solto.

## TPM e BitLocker

### Códigos de erro do TPM e BitLocker

| Constante/Valor                    | Descrição                                                                                                           |
|------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| TPM_E_ERROR_MASK<br>0x80280000     | Trata-se de uma máscara de erro para converter erros de hardware de TPM em erros do Windows.                        |
| TPM_E_AUTHFAIL<br>0x80280001       | A autenticação falhou.                                                                                              |
| TPM_E_BADINDEX<br>0x80280002       | O índice para um PCR, DIR ou outro registo é incorreto.                                                             |
| TPM_E_BAD_PARAMETER<br>0x80280003  | Um ou mais parâmetros estão errados.                                                                                |
| TPM_E_AUDITFAILURE<br>0x80280004   | Uma operação foi concluída com êxito, mas a auditoria dessa operação falhou.                                        |
| TPM_E_CLEAR_DISABLED<br>0x80280005 | O sinalizador de desativação de limpeza está definido e todas as operações de limpeza requerem agora acesso físico. |
| TPM_E_DEACTIVATED                  | Ativa o TPM.                                                                                                        |

| <b>Constante/Valor</b>                | <b>Descrição</b>                                                       |
|---------------------------------------|------------------------------------------------------------------------|
| 0x80280006                            |                                                                        |
| TPM_E_DISABLED<br>0x80280007          | Ativa o TPM.                                                           |
| TPM_E_DISABLED_CMD<br>0x80280008      | O comando de destino foi desativado.                                   |
| TPM_E_FAIL<br>0x80280009              | Falha na operação.                                                     |
| TPM_E_BAD_ORDINAL<br>0x8028000A       | O ordinal era desconhecido ou inconsistente.                           |
| TPM_E_INSTALL_DISABLED<br>0x8028000B  | A capacidade de instalar um proprietário está desativada.              |
| TPM_E_INVALID_KEYHANDLE<br>0x8028000C | Não é possível interpretar o identificador da chave.                   |
| TPM_E_KEYNOTFOUND<br>0x8028000D       | O identificador da chave aponta para uma chave inválida.               |
| TPM_E_INAPPROPRIATE_ENC<br>0x8028000E | Esquema de encriptação inaceitável.                                    |
| TPM_E_MIGRATEFAIL<br>0x8028000F       | Falha na autorização de migração.                                      |
| TPM_E_INVALID_PCR_INFO<br>0x80280010  | Não foi possível interpretar as informações de PCR.                    |
| TPM_E_NOSPACE<br>0x80280011           | Não existe espaço para carregar a chave.                               |
| TPM_E_NOSRK<br>0x80280012             | Não existe qualquer conjunto SRK (Storage Root Key).                   |
| TPM_E_NOTSEALED_BLOB<br>0x80280013    | Um blob encriptado é inválido ou não foi criado por este TPM.          |
| TPM_E_OWNER_SET<br>0x80280014         | O TPM já tem um proprietário.                                          |
| TPM_E_RESOURCES<br>0x80280015         | O TPM tem recursos internos insuficientes para executar a ação pedida. |
| TPM_E_SHORTRANDOM<br>0x80280016       | Uma cadeia aleatória era demasiado curta.                              |
| TPM_E_SIZE                            | O TPM não tem espaço para executar a operação.                         |

| <b>Constante/Valor</b>                 | <b>Descrição</b>                                                                                                                                                                                                                                          |
|----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 0x80280017                             |                                                                                                                                                                                                                                                           |
| TPM_E_WRONGPCRVAL<br>0x80280018        | O valor de PCR nomeado não corresponde ao valor de PCR atual.                                                                                                                                                                                             |
| TPM_E_BAD_PARAM_SIZE<br>0x80280019     | O argumento paramSize do comando tem um valor incorreto                                                                                                                                                                                                   |
| TPM_E_SHA_THREAD<br>0x8028001A         | Não existe qualquer thread SHA-1.                                                                                                                                                                                                                         |
| TPM_E_SHA_ERROR<br>0x8028001B          | O cálculo não pode prosseguir porque o thread SHA-1 existente já encontrou um erro.                                                                                                                                                                       |
| TPM_E_FAILEDSELFTEST<br>0x8028001C     | O dispositivo de hardware de TPM reportou uma falha durante o respetivo autoteste interno. Experimente reiniciar o computador para resolver o problema. Se o problema continuar, poderá ser necessário substituir a placa principal ou o hardware de TPM. |
| TPM_E_AUTH2FAIL<br>0x8028001D          | A autorização da segunda chave numa função de 2 chaves falhou.                                                                                                                                                                                            |
| TPM_E_BADTAG<br>0x8028001E             | O valor da etiqueta enviado para um comando é inválido.                                                                                                                                                                                                   |
| TPM_E_IOERROR<br>0x8028001F            | Ocorreu um erro de ES ao transmitir informações para o TPM.                                                                                                                                                                                               |
| TPM_E_ENCRYPT_ERROR<br>0x80280020      | Ocorreu um problema no processo de encriptação.                                                                                                                                                                                                           |
| TPM_E_DECRYPT_ERROR<br>0x80280021      | O processo de desencriptação não foi concluído.                                                                                                                                                                                                           |
| TPM_E_INVALID_AUTHHANDLE<br>0x80280022 | Foi utilizado um identificador inválido.                                                                                                                                                                                                                  |
| TPM_E_NO_ENDORSEMENT<br>0x80280023     | O TPM não tem uma Chave de Endossamento (EK) instalada.                                                                                                                                                                                                   |
| TPM_E_INVALID_KEYUSAGE<br>0x80280024   | Não é permitida a utilização de uma chave.                                                                                                                                                                                                                |
| TPM_E_WRONG_ENTITYTYPE<br>0x80280025   | O tipo de entidade submetido não é permitido.                                                                                                                                                                                                             |
| TPM_E_INVALID_POSTINIT<br>0x80280026   | O comando foi recebido na sequência errada relativamente a TPM_Init e a um TPM_Startup subsequente.                                                                                                                                                       |
| TPM_E_INAPPROPRIATE_SIG<br>0x80280027  | Os dados assinados não podem incluir informações de DER adicionais.                                                                                                                                                                                       |

| <b>Constante/Valor</b>                     | <b>Descrição</b>                                                                                                                                                                               |
|--------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| TPM_E_BAD_KEY_PROPERTY<br>0x80280028       | As propriedades das chaves nos TPM_KEY_PARMs não são suportadas por este TPM.                                                                                                                  |
| TPM_E_BAD_MIGRATION<br>0x80280029          | As propriedades de migração desta chave estão incorretas.                                                                                                                                      |
| TPM_E_BAD_SCHEME<br>0x8028002A             | O esquema de encriptação ou assinatura desta chave estão incorretos ou não são permitidos nesta situação.                                                                                      |
| TPM_E_BAD_DATASIZE<br>0x8028002B           | O parâmetro de tamanho dos dados (ou blob) está incorreto ou é inconsistente com a chave referenciada.                                                                                         |
| TPM_E_BAD_MODE<br>0x8028002C               | Um parâmetro de modo é incorreto, tal como capArea ou subCapArea para TPM_GetCapability, o parâmetro physicalPresence para TPM_PhysicalPresence ou migrationType para TPM_CreateMigrationBlob. |
| TPM_E_BAD_PRESENCE<br>0x8028002D           | Os bits de physicalPresence ou physicalPresenceLock têm um valor incorreto.                                                                                                                    |
| TPM_E_BAD_VERSION<br>0x8028002E            | O TPM não pode executar esta versão da capacidade.                                                                                                                                             |
| TPM_E_NO_WRAP_TRANSPORT<br>0x8028002F      | O TPM não permite sessões de transporte moldadas.                                                                                                                                              |
| TPM_E_AUDITFAIL_UNSUCCESSFUL<br>0x80280030 | A construção da auditoria do TPM falhou e o comando subjacente também devolveu um código de falha.                                                                                             |
| TPM_E_AUDITFAIL_SUCCESSFUL<br>0x80280031   | A construção da auditoria do TPM falhou e o comando subjacente devolveu um código de êxito.                                                                                                    |
| TPM_E_NOTRESETABLE<br>0x80280032           | Tentativa de repor um registo PCR que não tem o atributo de reposição.                                                                                                                         |
| TPM_E_NOTLOCAL<br>0x80280033               | Tentativa de repor um registo PCR que necessita da localidade e o modificador de localidade não faz parte do transporte do comando.                                                            |
| TPM_E_BAD_TYPE<br>0x80280034               | Make identity blob não está escrito corretamente.                                                                                                                                              |
| TPM_E_INVALID_RESOURCE<br>0x80280035       | O tipo de gravação de recurso identificado pelo contexto não corresponde ao recurso propriamente dito.                                                                                         |
| TPM_E_NOTFIPS<br>0x80280036                | O TPM está a tentar executar um comando que só está disponível no modo FIPS.                                                                                                                   |
| TPM_E_INVALID_FAMILY<br>0x80280037         | O comando está a tentar utilizar um ID de família inválido.                                                                                                                                    |
| TPM_E_NO_NV_PERMISSION<br>0x80280038       | A permissão para manipular a memória NV não está disponível.                                                                                                                                   |

| <b>Constante/Valor</b>                | <b>Descrição</b>                                                                                 |
|---------------------------------------|--------------------------------------------------------------------------------------------------|
| TPM_E_REQUIRES_SIGN<br>0x80280039     | A operação necessita de um comando assinado.                                                     |
| TPM_E_KEY_NOTSUPPORTED<br>0x8028003A  | Operação incorreta para carregar uma chave NV.                                                   |
| TPM_E_AUTH_CONFLICT<br>0x8028003B     | NV_LoadKey blob necessita da autorização do proprietário e do blob.                              |
| TPM_E_AREA_LOCKED<br>0x8028003C       | A área NV está bloqueada e não podem ser escritos dados na mesma.                                |
| TPM_E_BAD_LOCALITY<br>0x8028003D      | A localidade está incorreta para a operação tentada.                                             |
| TPM_E_READ_ONLY<br>0x8028003E         | A área NV é só de leitura e não é possível escrever na mesma.                                    |
| TPM_E_PER_NOWRITE<br>0x8028003F       | Não existe proteção para a escrita na área NV.                                                   |
| TPM_E_FAMILYCOUNT<br>0x80280040       | O valor de contador de famílias não coincide.                                                    |
| TPM_E_WRITE_LOCKED<br>0x80280041      | Já foram escritos dados na área NV.                                                              |
| TPM_E_BAD_ATTRIBUTES<br>0x80280042    | Os atributos da área NV estão em conflito.                                                       |
| TPM_E_INVALID_STRUCTURE<br>0x80280043 | A etiqueta de estrutura e a versão são inválidas ou inconsistentes.                              |
| TPM_E_KEY_OWNER_CONTROL<br>0x80280044 | A chave está sob controlo do Proprietário do TPM e só pode ser expulsa pelo Proprietário do TPM. |
| TPM_E_BAD_COUNTER<br>0x80280045       | O identificador de contador está incorreto.                                                      |
| TPM_E_NOT_FULLWRITE<br>0x80280046     | A ação de escrita não é uma ação de escrita completa da área.                                    |
| TPM_E_CONTEXT_GAP<br>0x80280047       | O intervalo entre as contagens de contexto guardadas é demasiado grande.                         |
| TPM_E_MAXNVWRITES<br>0x80280048       | Foi excedido o número máximo de escritas NV sem um proprietário.                                 |
| TPM_E_NOOPERATOR<br>0x80280049        | Não existe qualquer valor AuthData de operador definido.                                         |

| <b>Constante/Valor</b>                     | <b>Descrição</b>                                                                                         |
|--------------------------------------------|----------------------------------------------------------------------------------------------------------|
| TPM_E_RESOURCEMISSING<br>0x8028004A        | O recurso apontado pelo contexto não está carregado.                                                     |
| TPM_E_DELEGATE_LOCK<br>0x8028004B          | A administração de delegado está bloqueada.                                                              |
| TPM_E_DELEGATE_FAMILY<br>0x8028004C        | Foi efetuada uma tentativa de gerir uma família que não é a família delegada.                            |
| TPM_E_DELEGATE_ADMIN<br>0x8028004D         | A gestão de tabelas de delegação não está ativada.                                                       |
| TPM_E_TRANSPORT_NOTEXCLUSIVE<br>0x8028004E | Foi executado um comando fora de uma sessão de transporte exclusiva.                                     |
| TPM_E_OWNER_CONTROL<br>0x8028004F          | Foi efetuada uma tentativa de guardar o contexto de uma chave com expulsão controlada pelo proprietário. |
| TPM_E_DAA_RESOURCES<br>0x80280050          | O comando DAA não tem quaisquer recursos disponíveis para executar o comando.                            |
| TPM_E_DAA_INPUT_DATA0<br>0x80280051        | A verificação de consistência do parâmetro inputData0 de DAA falhou.                                     |
| TPM_E_DAA_INPUT_DATA1<br>0x80280052        | A verificação de consistência do parâmetro inputData1 de DAA falhou.                                     |
| TPM_E_DAA_ISSUER_SETTINGS<br>0x80280053    | A verificação de consistência de DAA_issuerSettings falhou.                                              |
| TPM_E_DAA_TPM_SETTINGS<br>0x80280054       | A verificação de consistência de DAA_tpmSpecific falhou.                                                 |
| TPM_E_DAA_STAGE<br>0x80280055              | O processo atômico indicado pelo comando DAA submetido não é o processo esperado.                        |
| TPM_E_DAA_ISSUER_VALIDITY<br>0x80280056    | A verificação de validade do emissor detetou uma inconsistência.                                         |
| TPM_E_DAA_WRONG_W<br>0x80280057            | Falha na verificação de consistência em w.                                                               |
| TPM_E_BAD_HANDLE<br>0x80280058             | O identificador está incorreto.                                                                          |
| TPM_E_BAD_DELEGATE<br>0x80280059           | A delegação não está correta.                                                                            |
| TPM_E_BADCONTEXT<br>0x8028005A             | O blob de contexto é inválido.                                                                           |

| <b>Constante/Valor</b>                           | <b>Descrição</b>                                                                                                             |
|--------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|
| TPM_E_TOOMANYCONTEXTS<br>0x8028005B              | Demasiados contextos mantidos pelo TPM.                                                                                      |
| TPM_E_MA_TICKET_SIGNATURE<br>0x8028005C          | Falha de validação da assinatura da autoridade de migração.                                                                  |
| TPM_E_MA_DESTINATION<br>0x8028005D               | Destino de migração não autenticado.                                                                                         |
| TPM_E_MA_SOURCE<br>0x8028005E                    | Origem de migração incorreta.                                                                                                |
| TPM_E_MA_AUTHORITY<br>0x8028005F                 | Autoridade de migração incorreta.                                                                                            |
| TPM_E_PERMANENTEK<br>0x80280061                  | Foi efetuada uma tentativa de revogar a EK e a EK não é revogável.                                                           |
| TPM_E_BAD_SIGNATURE<br>0x80280062                | Assinatura incorreta da permissão de CMK.                                                                                    |
| TPM_E_NOCONTEXTSPACE<br>0x80280063               | Não existe espaço na lista de contextos para contextos adicionais.                                                           |
| TPM_E_COMMAND_BLOCKED<br>0x80280400              | O comando foi bloqueado.                                                                                                     |
| TPM_E_INVALID_HANDLE<br>0x80280401               | O identificador especificado não foi encontrado.                                                                             |
| TPM_E_DUPLICATE_VHANDLE<br>0x80280402            | O TPM devolveu um identificador duplicado e o comando tem de ser submetido novamente.                                        |
| TPM_E_EMBEDDED_COMMAND_BLOCKED<br>0x80280403     | O comando contido no transporte estava bloqueado.                                                                            |
| TPM_E_EMBEDDED_COMMAND_UNSUPPORTED<br>0x80280404 | O comando existente no transporte não é suportado.                                                                           |
| TPM_E_RETRY<br>0x80280800                        | O TPM está demasiado ocupado para responder ao comando imediatamente, mas o comando pode ser novamente submetido mais tarde. |
| TPM_E_NEEDS_SELFTEST<br>0x80280801               | SelfTestFull não foi executado.                                                                                              |
| TPM_E_DOING_SELFTEST<br>0x80280802               | O TPM está atualmente a executar um autoteste completo.                                                                      |
| TPM_E_DEFEND_LOCK_RUNNING<br>0x80280803          | O TPM está a defender-se contra ataques de dicionário e encontra-se num período de tempo limite.                             |

| <b>Constante/Valor</b>                     | <b>Descrição</b>                                                                                    |
|--------------------------------------------|-----------------------------------------------------------------------------------------------------|
| TBS_E_INTERNAL_ERROR<br>0x80284001         | Foi detetado um erro de software interno.                                                           |
| TBS_E_BAD_PARAMETER<br>0x80284002          | Um ou mais parâmetros de entrada estão incorretos.                                                  |
| TBS_E_INVALID_OUTPUT_POINTER<br>0x80284003 | Um apontador de saída especificado está incorreto.                                                  |
| TBS_E_INVALID_CONTEXT<br>0x80284004        | O identificador de contexto especificado não se refere a um contexto válido.                        |
| TBS_E_INSUFFICIENT_BUFFER<br>0x80284005    | Uma memória intermédia de saída especificada é demasiado pequena.                                   |
| TBS_E_IOERROR<br>0x80284006                | Ocorreu um erro ao comunicar com o TPM.                                                             |
| TBS_E_INVALID_CONTEXT_PARAM<br>0x80284007  | Um ou mais parâmetros de contexto são inválidos.                                                    |
| TBS_E_SERVICE_NOT_RUNNING<br>0x80284008    | O serviço TBS não está em execução e não pode ser iniciado.                                         |
| TBS_E_TOO_MANY_TBS_CONTEXTS<br>0x80284009  | Não foi possível criar um novo contexto porque existem demasiados contextos abertos.                |
| TBS_E_TOO_MANY_RESOURCES<br>0x8028400A     | Não foi possível criar um novo recurso virtual porque existem demasiados recursos virtuais abertos. |
| TBS_E_SERVICE_START_PENDING<br>0x8028400B  | O serviço TBS foi iniciado mas ainda não está em execução.                                          |
| TBS_E_PPI_NOT_SUPPORTED<br>0x8028400C      | A interface de presença física não é suportada.                                                     |
| TBS_E_COMMAND_CANCELED<br>0x8028400D       | O comando foi cancelado.                                                                            |
| TBS_E_BUFFER_TOO_LARGE<br>0x8028400E       | A memória intermédia de entrada ou saída é demasiado grande.                                        |
| TBS_E_TPM_NOT_FOUND<br>0x8028400F          | Não é possível localizar um Dispositivo de Segurança de TPM compatível neste computador.            |
| TBS_E_SERVICE_DISABLED<br>0x80284010       | O serviço TBS foi desativado.                                                                       |
| TBS_E_NO_EVENT_LOG<br>0x80284011           | Não está disponível nenhum registo de eventos TCG.                                                  |

| <b>Constante/Valor</b>                        | <b>Descrição</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| TBS_E_ACCESS_DENIED<br>0x80284012             | O emissor não tem os direitos adequados para executar a operação pedida.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| TBS_E_PROVISIONING_NOT_ALLOWED<br>0x80284013  | A ação de aprovisionamento de TPM não é permitida pelos sinalizadores especificados. Para que o aprovisionamento seja efetuado com êxito, poderá ser necessária uma de várias ações. A ação da consola de gestão de TPM (tpm.msc) para preparar o TPM para utilização poderá ajudar. Para mais informações, consulte a documentação do método WMI Win32_Tpm 'Provision'. (As ações que poderão ser necessárias incluem importar o valor de Autorização de Proprietário de TPM para o sistema, chamar o método WMI Win32_Tpm para aprovisionar o TPM e especificar TRUE para 'ForceClear_Allowed' ou para 'PhysicalPresencePrompts_Allowed' (como indicado pelo valor devolvido nas Informações Adicionais), ou ativar o TPM no BIOS do sistema.) |
| TBS_E_PPI_FUNCTION_UNSUPPORTED<br>0x80284014  | A Interface de Presença Física deste firmware não suporta o método pedido.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| TBS_E_OWNERAUTH_NOT_FOUND<br>0x80284015       | O valor OwnerAuth de TPM pedido não foi encontrado.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| TBS_E_PROVISIONING_INCOMPLETE<br>0x80284016   | O aprovisionamento de TPM não foi concluído. Para mais informações sobre a conclusão do aprovisionamento, chame o método WMI Win32_Tpm para aprovisionar o TPM ('Provision') e consulte as informações devolvidas.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| TPMAPI_E_INVALID_STATE<br>0x80290100          | A memória intermédia de comandos não está no estado correto.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| TPMAPI_E_NOT_ENOUGH_DATA<br>0x80290101        | A memória intermédia de comandos não contém dados suficientes para satisfazer o pedido.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| TPMAPI_E_TOO_MUCH_DATA<br>0x80290102          | A memória intermédia de comandos não contém mais dados.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| TPMAPI_E_INVALID_OUTPUT_POINTER<br>0x80290103 | Um ou vários parâmetros de saída eram NULL ou inválidos.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| TPMAPI_E_INVALID_PARAMETER<br>0x80290104      | Um ou mais parâmetros de entrada são inválidos.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| TPMAPI_E_OUT_OF_MEMORY<br>0x80290105          | Não existe memória suficiente disponível para satisfazer o pedido.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| TPMAPI_E_BUFFER_TOO_SMALL<br>0x80290106       | A memória intermédia especificada era demasiado pequena.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| TPMAPI_E_INTERNAL_ERROR<br>0x80290107         | Foi detetado um erro interno.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| TPMAPI_E_ACCESS_DENIED                        | O emissor não tem os direitos adequados para executar a operação pedida.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

| <b>Constante/Valor</b>                                      | <b>Descrição</b>                                                                       |
|-------------------------------------------------------------|----------------------------------------------------------------------------------------|
| 0x80290108                                                  |                                                                                        |
| TPMAPI_E_AUTHORIZATION_FAILED<br>0x80290109                 | As informações de autorização especificadas são inválidas.                             |
| TPMAPI_E_INVALID_CONTEXT_HANDLE<br>0x8029010A               | O identificador de contexto especificado não era válido.                               |
| TPMAPI_E_TBS_COMMUNICATION_ERROR<br>0x8029010B              | Ocorreu um erro ao comunicar com o TBS.                                                |
| TPMAPI_E_TPM_COMMAND_ERROR<br>0x8029010C                    | O TPM devolveu um resultado inesperado.                                                |
| TPMAPI_E_MESSAGE_TOO_LARGE<br>0x8029010D                    | A mensagem era demasiado grande para o esquema de codificação.                         |
| TPMAPI_E_INVALID_ENCODING<br>0x8029010E                     | A codificação do blob não foi reconhecida.                                             |
| TPMAPI_E_INVALID_KEY_SIZE<br>0x8029010F                     | O tamanho da chave não é válido.                                                       |
| TPMAPI_E_ENCRYPTION_FAILED<br>0x80290110                    | Falha na operação de encriptação.                                                      |
| TPMAPI_E_INVALID_KEY_PARAMS<br>0x80290111                   | A estrutura dos parâmetros chave não era válida                                        |
| TPMAPI_E_INVALID_MIGRATION_AUTHORIZATION_BLOB<br>0x80290112 | Os dados fornecidos pedidos não parecem ser um blob de autorização de migração válido. |
| TPMAPI_E_INVALID_PCR_INDEX<br>0x80290113                    | O índice de PCR especificado era inválido                                              |
| TPMAPI_E_INVALID_DELEGATE_BLOB<br>0x80290114                | Os dados indicados não parecem ser um blob delegado válido.                            |
| TPMAPI_E_INVALID_CONTEXT_PARAMS<br>0x80290115               | Um ou vários parâmetros de contexto especificados não são válidos.                     |
| TPMAPI_E_INVALID_KEY_BLOB<br>0x80290116                     | Os dados indicados não parecem ser um blob de chave válido                             |
| TPMAPI_E_INVALID_PCR_DATA<br>0x80290117                     | Os dados de PCR especificados eram inválidos.                                          |
| TPMAPI_E_INVALID_OWNER_AUTH<br>0x80290118                   | O formato dos dados de autenticação do proprietário era inválido.                      |

| <b>Constante/Valor</b>                          | <b>Descrição</b>                                                                                                        |
|-------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|
| TPMAPI_E_FIPS_RNG_CHECK_FAILED<br>0x80290119    | O número aleatório gerado não passou na verificação FIPS RNG.                                                           |
| TPMAPI_E_EMPTY_TCG_LOG<br>0x8029011A            | O Registo de Eventos TCG não contém quaisquer dados.                                                                    |
| TPMAPI_E_INVALID_TCG_LOG_ENTRY<br>0x8029011B    | Uma entrada no Registo de Eventos TCG era inválida.                                                                     |
| TPMAPI_E_TCG_SEPARATOR_ABSENT<br>0x8029011C     | Um Separador TCG não foi encontrado.                                                                                    |
| TPMAPI_E_TCG_INVALID_DIGEST_ENTRY<br>0x8029011D | Um valor de resumo numa entrada do Registo TCG não correspondeu aos dados com hash.                                     |
| TPMAPI_E_POLICY_DENIES_OPERATION<br>0x8029011E  | A operação pedida foi bloqueada pela política de TPM atual. Contacte o administrador de sistema para obter assistência. |
| TBSIMP_E_BUFFER_TOO_SMALL<br>0x80290200         | A memória intermédia especificada era demasiado pequena.                                                                |
| TBSIMP_E_CLEANUP_FAILED<br>0x80290201           | Não foi possível limpar o contexto.                                                                                     |
| TBSIMP_E_INVALID_CONTEXT_HANDLE<br>0x80290202   | O identificador de contexto especificado é inválido.                                                                    |
| TBSIMP_E_INVALID_CONTEXT_PARAM<br>0x80290203    | Foi especificado um parâmetro de contexto inválido.                                                                     |
| TBSIMP_E_TPM_ERROR<br>0x80290204                | Ocorreu um erro ao comunicar com o TPM                                                                                  |
| TBSIMP_E_HASH_BAD_KEY<br>0x80290205             | Não foi encontrada qualquer entrada com a chave especificada.                                                           |
| TBSIMP_E_DUPLICATE_VHANDLE<br>0x80290206        | O identificador virtual especificado corresponde a um identificador virtual que já está a ser utilizado.                |
| TBSIMP_E_INVALID_OUTPUT_POINTER<br>0x80290207   | O apontador para a localização do identificador devolvida era NULL ou inválido                                          |
| TBSIMP_E_INVALID_PARAMETER<br>0x80290208        | Um dos parâmetros não é válido.                                                                                         |
| TBSIMP_E_RPC_INIT_FAILED<br>0x80290209          | Não foi possível inicializar o subsistema de RPC.                                                                       |
| TBSIMP_E_SCHEDULER_NOT_RUNNING<br>0x8029020A    | O programador de TBS não está em execução.                                                                              |

| <b>Constante/Valor</b>                         | <b>Descrição</b>                                                                                    |
|------------------------------------------------|-----------------------------------------------------------------------------------------------------|
| TBSIMP_E_COMMAND_CANCELED<br>0x8029020B        | O comando foi cancelado.                                                                            |
| TBSIMP_E_OUT_OF_MEMORY<br>0x8029020C           | Não existe memória suficiente disponível para satisfazer o pedido                                   |
| TBSIMP_E_LIST_NO_MORE_ITEMS<br>0x8029020D      | A lista especificada está vazia ou a iteração alcançou o final da lista.                            |
| TBSIMP_E_LIST_NOT_FOUND<br>0x8029020E          | O item especificado não foi encontrado na lista.                                                    |
| TBSIMP_E_NOT_ENOUGH_SPACE<br>0x8029020F        | O TPM não tem espaço suficiente para carregar o recurso pedido.                                     |
| TBSIMP_E_NOT_ENOUGH_TPM_CONTEXTS<br>0x80290210 | Existem demasiados contextos de TPM em utilização.                                                  |
| TBSIMP_E_COMMAND_FAILED<br>0x80290211          | Falha do comando de TPM.                                                                            |
| TBSIMP_E_UNKNOWN_ORDINAL<br>0x80290212         | O TBS não reconhece o ordinal especificado.                                                         |
| TBSIMP_E_RESOURCE_EXPIRED<br>0x80290213        | O recurso pedido já não se encontra disponível.                                                     |
| TBSIMP_E_INVALID_RESOURCE<br>0x80290214        | O tipo de recurso não é igual.                                                                      |
| TBSIMP_E_NOTHING_TO_UNLOAD<br>0x80290215       | Não é possível descarregar recursos.                                                                |
| TBSIMP_E_HASH_TABLE_FULL<br>0x80290216         | Não podem ser adicionadas novas entradas na tabela hash.                                            |
| TBSIMP_E_TOO_MANY_TBS_CONTEXTS<br>0x80290217   | Não foi possível criar um novo contexto de TBS porque existem demasiados contextos abertos.         |
| TBSIMP_E_TOO_MANY_RESOURCES<br>0x80290218      | Não foi possível criar um novo recurso virtual porque existem demasiados recursos virtuais abertos. |
| TBSIMP_E_PPI_NOT_SUPPORTED<br>0x80290219       | A interface de presença física não é suportada.                                                     |
| TBSIMP_E_TPM_INCOMPATIBLE<br>0x8029021A        | O TBS não é compatível com a versão de TPM encontrada no sistema.                                   |
| TBSIMP_E_NO_EVENT_LOG<br>0x8029021B            | Não está disponível nenhum registo de eventos TCG.                                                  |

| <b>Constante/Valor</b>                         | <b>Descrição</b>                                                                                                                                                                   |
|------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| TPM_E_PPI_ACPI_FAILURE<br>0x80290300           | Foi detetado um erro geral ao tentar adquirir a resposta do BIOS a um comando de Presença Física.                                                                                  |
| TPM_E_PPI_USER_ABORT<br>0x80290301             | O utilizador não conseguiu confirmar o pedido de operação do TPM.                                                                                                                  |
| TPM_E_PPI_BIOS_FAILURE<br>0x80290302           | A falha do BIOS impediu a execução com êxito da operação do TPM pedida (por ex.: pedido de operação do TPM inválido, erro de comunicação do BIOS com o TPM).                       |
| TPM_E_PPI_NOT_SUPPORTED<br>0x80290303          | O BIOS não suporta a interface de presença física.                                                                                                                                 |
| TPM_E_PPI_BLOCKED_IN_BIOS<br>0x80290304        | O comando de Presença Física foi bloqueado pelas definições de BIOS atuais. O proprietário do sistema poderá conseguir reconfigurar as definições de BIOS para permitir o comando. |
| TPM_E_PCP_ERROR_MASK<br>0x80290400             | Trata-se de uma máscara de erro para converter erros do Fornecedor Criptográfico da Plataforma em erros do Windows.                                                                |
| TPM_E_PCP_DEVICE_NOT_READY<br>0x80290401       | O Dispositivo Criptográfico da Plataforma não está preparado neste momento. O dispositivo necessita de ser totalmente provisionado para estar operacional.                         |
| TPM_E_PCP_INVALID_HANDLE<br>0x80290402         | O identificador fornecido ao Fornecedor Criptográfico da Plataforma é inválido.                                                                                                    |
| TPM_E_PCP_INVALID_PARAMETER<br>0x80290403      | Um parâmetro fornecido ao Fornecedor Criptográfico da Plataforma é inválido.                                                                                                       |
| TPM_E_PCP_FLAG_NOT_SUPPORTED<br>0x80290404     | Um sinalizador fornecido ao Fornecedor Criptográfico da Plataforma não é suportado.                                                                                                |
| TPM_E_PCP_NOT_SUPPORTED<br>0x80290405          | A operação pedida não é suportada por este Fornecedor Criptográfico da Plataforma.                                                                                                 |
| TPM_E_PCP_BUFFER_TOO_SMALL<br>0x80290406       | A memória intermédia é demasiado pequena para conter todos os dados. Não foram escritas informações na memória intermédia.                                                         |
| TPM_E_PCP_INTERNAL_ERROR<br>0x80290407         | Ocorreu um erro interno inesperado no Fornecedor Criptográfico da Plataforma.                                                                                                      |
| TPM_E_PCP_AUTHENTICATION_FAILED<br>0x80290408  | Falha na autorização para utilizar um objeto de fornecedor.                                                                                                                        |
| TPM_E_PCP_AUTHENTICATION_IGNORED<br>0x80290409 | O Dispositivo Criptográfico da Plataforma ignorou a autorização para o objeto de fornecedor, para mitigar um ataque de dicionário.                                                 |
| TPM_E_PCP_POLICY_NOT_FOUND<br>0x8029040A       | A política referenciada não foi encontrada.                                                                                                                                        |

| <b>Constante/Valor</b>                     | <b>Descrição</b>                                                                                                                                          |
|--------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| TPM_E_PCP_PROFILE_NOT_FOUND<br>0x8029040B  | O perfil referenciado não foi encontrado.                                                                                                                 |
| TPM_E_PCP_VALIDATION_FAILED<br>0x8029040C  | A validação não foi concluída com êxito.                                                                                                                  |
| PLA_E_DCS_NOT_FOUND<br>0x80300002          | O Conjunto de Recoletores de Dados não foi encontrado.                                                                                                    |
| PLA_E_DCS_IN_USE<br>0x803000AA             | O Conjunto de Recoletores de Dados ou das respetivas dependências está em utilização.                                                                     |
| PLA_E_TOO_MANY_FOLDERS<br>0x80300045       | Não é possível iniciar o Conjunto de Recoletores de Dados porque existem demasiadas pastas.                                                               |
| PLA_E_NO_MIN_DISK<br>0x80300070            | Não existe espaço livre suficiente em disco para iniciar o Conjunto de Recoletores de Dados.                                                              |
| PLA_E_DCS_ALREADY_EXISTS<br>0x803000B7     | O Conjunto de Recoletores de Dados já existe.                                                                                                             |
| PLA_S_PROPERTY_IGNORED<br>0x00300100       | O valor da propriedade será ignorado.                                                                                                                     |
| PLA_E_PROPERTY_CONFLICT<br>0x80300101      | Conflito de valores da propriedade.                                                                                                                       |
| PLA_E_DCS_SINGLETON_REQUIRED<br>0x80300102 | A configuração atual deste Conjunto de Recoletores de Dados necessita que este contenha exatamente um Recoletor de Dados.                                 |
| PLA_E_CREDENTIALS_REQUIRED<br>0x80300103   | É necessária uma conta de utilizador para consolidar as propriedades atuais do Conjunto de Recoletores de Dados.                                          |
| PLA_E_DCS_NOT_RUNNING<br>0x80300104        | O Conjunto de Recoletores de Dados não está em execução.                                                                                                  |
| PLA_E_CONFLICT_INCL_EXCL_API<br>0x80300105 | Foi detetado um conflito na lista de APIs de inclusão/exclusão. Não especifique a mesma API simultaneamente na lista de inclusão e na lista de exclusões. |
| PLA_E_NETWORK_EXE_NOT_VALID<br>0x80300106  | O caminho executável que especificou refere-se a uma partilha de rede ou caminho UNC.                                                                     |
| PLA_E_EXE_ALREADY_CONFIGURED<br>0x80300107 | O caminho executável que especificou já está configurado para rastreio de APIs.                                                                           |
| PLA_E_EXE_PATH_NOT_VALID<br>0x80300108     | O caminho executável que especificou não existe. Verifique se o caminho especificado está correto.                                                        |
| PLA_E_DC_ALREADY_EXISTS<br>0x80300109      | O Recoletor de Dados já existe.                                                                                                                           |

| <b>Constante/Valor</b>                            | <b>Descrição</b>                                                                                                                                                                                                                                              |
|---------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PLA_E_DCS_START_WAIT_TIMEOUT<br>0x8030010A        | A espera pela notificação de início do Conjunto de Recolectores de Dados excedeu o tempo limite.                                                                                                                                                              |
| PLA_E_DC_START_WAIT_TIMEOUT<br>0x8030010B         | A espera pelo início do Recolector de Dados excedeu o tempo limite.                                                                                                                                                                                           |
| PLA_E_REPORT_WAIT_TIMEOUT<br>0x8030010C           | A espera pela conclusão da ferramenta de geração de relatórios excedeu o tempo limite.                                                                                                                                                                        |
| PLA_E_NO_DUPLICATES<br>0x8030010D                 | Não são permitidos itens duplicados.                                                                                                                                                                                                                          |
| PLA_E_EXE_FULL_PATH_REQUIRED<br>0x8030010E        | Quando especificar o executável que pretende rastrear, tem de especificar um caminho completo para o executável e não apenas um nome de ficheiro.                                                                                                             |
| PLA_E_INVALID_SESSION_NAME<br>0x8030010F          | O nome de sessão fornecido é inválido.                                                                                                                                                                                                                        |
| PLA_E_PLA_CHANNEL_NOT_ENABLED<br>0x80300110       | O canal do Registo de Eventos Microsoft-Windows-Diagnosis-PLA/Operacional tem de estar ativado para executar esta operação.                                                                                                                                   |
| PLA_E_TASKSCHED_CHANNEL_NOT_ENABLED<br>0x80300111 | O canal do Microsoft-Windows-TaskScheduler tem de estar ativado para executar esta operação.                                                                                                                                                                  |
| PLA_E_RULES_MANAGER_FAILED<br>0x80300112          | Falha na execução do Gestor de Regras.                                                                                                                                                                                                                        |
| PLA_E_CABAPI_FAILURE<br>0x80300113                | Ocorreu um erro ao tentar comprimir ou extrair os dados.                                                                                                                                                                                                      |
| FVE_E_LOCKED_VOLUME<br>0x80310000                 | Esta unidade está bloqueada pela Encriptação de Unidade BitLocker. Tem de desbloquear esta unidade a partir do Painel de Controlo.                                                                                                                            |
| FVE_E_NOT_ENCRYPTED<br>0x80310001                 | A unidade não está encriptada.                                                                                                                                                                                                                                |
| FVE_E_NO_TPM_BIOS<br>0x80310002                   | O BIOS não comunicou corretamente com o TPM. Contacte o fabricante do computador para obter as instruções de atualização do BIOS.                                                                                                                             |
| FVE_E_NO_MBR_METRIC<br>0x80310003                 | O BIOS não comunicou corretamente com o registo de arranque principal (MBR). Contacte o fabricante do computador para obter as instruções de atualização do BIOS.                                                                                             |
| FVE_E_NO_BOOTSECTOR_METRIC<br>0x80310004          | Uma medição de TPM necessária está em falta. Se existir um CD ou DVD de arranque no computador, remova-o, reinicie o computador e ative novamente o BitLocker. Se o problema persistir, certifique-se de que o registo de arranque principal está atualizado. |

| <b>Constante/Valor</b>                      | <b>Descrição</b>                                                                                                                                                                                                                                                                                                                       |
|---------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| FVE_E_NO_BOOTMGR_METRIC<br>0x80310005       | O setor de arranque desta unidade não é compatível com a Encriptação de Unidade BitLocker. Utilize a ferramenta Bootrec.exe no Ambiente de Recuperação do Windows para atualizar ou reparar o gestor de arranque (BOOTMGR).                                                                                                            |
| FVE_E_WRONG_BOOTMGR<br>0x80310006           | O gestor de arranque deste sistema operativo não é compatível com a Encriptação de Unidade BitLocker. Utilize a ferramenta Bootrec.exe no Ambiente de Recuperação do Windows para atualizar ou reparar o gestor de arranque (BOOTMGR).                                                                                                 |
| FVE_E_SECURE_KEY_REQUIRED<br>0x80310007     | É necessário, pelo menos, um protetor de chave seguro para que esta operação seja efetuada.                                                                                                                                                                                                                                            |
| FVE_E_NOT_ACTIVATED<br>0x80310008           | A Encriptação de Unidade BitLocker não está ativada nesta unidade. Ative o BitLocker.                                                                                                                                                                                                                                                  |
| FVE_E_ACTION_NOT_ALLOWED<br>0x80310009      | A Encriptação de Unidade BitLocker não consegue efetuar a ação pedida. Esta condição pode ocorrer quando são emitidos dois pedidos ao mesmo tempo. Aguarde alguns momentos e tente a operação novamente.                                                                                                                               |
| FVE_E_AD_SCHEMA_NOT_INSTALLED<br>0x8031000A | A floresta dos Serviços de Domínio do Active Directory não contém os atributos e as classes necessários para alojar informações de Encriptação de Unidade BitLocker ou do TPM. Contacte o administrador do domínio para verificar se quaisquer extensões de esquema do Active Directory para o BitLocker necessárias foram instaladas. |
| FVE_E_AD_INVALID_DATATYPE<br>0x8031000B     | O tipo de dados obtido a partir do Active Directory não era esperado. As informações de recuperação do BitLocker podem estar em falta ou danificadas.                                                                                                                                                                                  |
| FVE_E_AD_INVALID_DATASIZE<br>0x8031000C     | O tamanho dos dados obtidos a partir do Active Directory não era esperado. As informações de recuperação do BitLocker podem estar em falta ou danificadas.                                                                                                                                                                             |
| FVE_E_AD_NO_VALUES<br>0x8031000D            | O atributo lido a partir do Active Directory não contém quaisquer valores. As informações de recuperação do BitLocker podem estar em falta ou danificadas.                                                                                                                                                                             |
| FVE_E_AD_ATTR_NOT_SET<br>0x8031000E         | O atributo não foi definido. O atributo não foi definido. Verifique se tem sessão iniciada com uma conta de domínio que tenha a capacidade de escrever informações em objetos do Active Directory.                                                                                                                                     |
| FVE_E_AD_GUID_NOT_FOUND<br>0x8031000F       | Não foi possível encontrar o atributo especificado nos Serviços de Domínio do Active Directory. Contacte o administrador do domínio para verificar se quaisquer extensões de esquema do Active Directory para o BitLocker necessárias foram instaladas.                                                                                |
| FVE_E_BAD_INFORMATION<br>0x80310010         | Os metadados do BitLocker para a unidade encriptada não são válidos. Pode tentar reparar a unidade para restaurar o acesso.                                                                                                                                                                                                            |
| FVE_E_TOO_SMALL<br>0x80310011               | Não é possível encriptar a unidade porque esta não tem espaço livre suficiente. Elimine quaisquer dados                                                                                                                                                                                                                                |

| Constante/Valor                              | Descrição                                                                                                                                                                                                                                                                                                                         |
|----------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                              | desnecessários na unidade para criar espaço livre adicional e tente novamente.                                                                                                                                                                                                                                                    |
| FVE_E_SYSTEM_VOLUME<br>0x80310012            | Não é possível encriptar a unidade porque esta contém informações de arranque do sistema. Crie uma partição separada para utilizar como a unidade de sistema que contém as informações de arranque e uma segunda partição para utilizar como unidade de sistema operativo e, em seguida, encripte a unidade do sistema operativo. |
| FVE_E_FAILED_WRONG_FS<br>0x80310013          | Não é possível encriptar a unidade porque o sistema de ficheiros não é suportado.                                                                                                                                                                                                                                                 |
| FVE_E_BAD_PARTITION_SIZE<br>0x80310014       | O sistema de ficheiros é maior do que o tamanho da partição existente na tabela de partições. Esta unidade pode estar danificada ou ter sido adulterada. Para a utilizar com o BitLocker, tem de reformatar a partição.                                                                                                           |
| FVE_E_NOT_SUPPORTED<br>0x80310015            | Não é possível encriptar esta unidade.                                                                                                                                                                                                                                                                                            |
| FVE_E_BAD_DATA<br>0x80310016                 | Os dados não são válidos.                                                                                                                                                                                                                                                                                                         |
| FVE_E_VOLUME_NOT_BOUND<br>0x80310017         | A unidade de dados especificada não está definida para desbloquear automaticamente no computador atual e não pode ser desbloqueada automaticamente.                                                                                                                                                                               |
| FVE_E_TPM_NOT_OWNED<br>0x80310018            | É necessário inicializar o TPM antes de poder utilizar a Encriptação de Unidade BitLocker.                                                                                                                                                                                                                                        |
| FVE_E_NOT_DATA_VOLUME<br>0x80310019          | Não é possível efetuar a operação tentada numa unidade do sistema operativo.                                                                                                                                                                                                                                                      |
| FVE_E_AD_INSUFFICIENT_BUFFER<br>0x8031001A   | A memória intermédia fornecida a uma função é insuficiente para conter os dados devolvidos. Aumente o tamanho da memória intermédia antes de executar a função novamente.                                                                                                                                                         |
| FVE_E_CONV_READ<br>0x8031001B                | Uma operação de leitura falhou ao converter a unidade. A unidade não foi convertida. Ative novamente o BitLocker.                                                                                                                                                                                                                 |
| FVE_E_CONV_WRITE<br>0x8031001C               | Uma operação de escrita falhou ao converter a unidade. A unidade não foi convertida. Ative novamente o BitLocker.                                                                                                                                                                                                                 |
| FVE_E_KEY_REQUIRED<br>0x8031001D             | Este volume necessita de um ou mais protetores de chave do BitLocker. Não é possível eliminar a última chave existente nesta unidade.                                                                                                                                                                                             |
| FVE_E_CLUSTERING_NOT_SUPPORTED<br>0x8031001E | A Encriptação de Unidade BitLocker não suporta configurações de cluster.                                                                                                                                                                                                                                                          |
| FVE_E_VOLUME_BOUND_ALREADY<br>0x8031001F     | A unidade especificada já está configurada para ser automaticamente desbloqueada no computador atual.                                                                                                                                                                                                                             |
| FVE_E_OS_NOT_PROTECTED                       | A unidade do sistema operativo não está a ser protegida pela Encriptação de Unidade BitLocker.                                                                                                                                                                                                                                    |

| Constante/Valor                               | Descrição                                                                                                                                                                                                                                              |
|-----------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 0x80310020                                    |                                                                                                                                                                                                                                                        |
| FVE_E_PROTECTION_DISABLED<br>0x80310021       | A Encriptação de Unidade BitLocker foi suspensa nesta unidade. Todos os protetores de chave BitLocker configurados para esta unidade estão efetivamente desativados e a unidade será desbloqueada automaticamente utilizando uma chave não encriptada. |
| FVE_E_RECOVERY_KEY_REQUIRED<br>0x80310022     | A unidade que está a tentar bloquear não tem protetores de chave disponíveis para encriptação porque a proteção BitLocker está atualmente suspensa. Ative novamente o BitLocker para bloquear esta unidade.                                            |
| FVE_E_FOREIGN_VOLUME<br>0x80310023            | O BitLocker não pode utilizar o TPM para proteger uma unidade de dados. Só é possível utilizar a proteção TPM na unidade do sistema operativo.                                                                                                         |
| FVE_E_OVERLAPPED_UPDATE<br>0x80310024         | Não é possível atualizar os metadados do BitLocker relativos à unidade encriptada porque esta está bloqueada para atualização por outro processo. Repita este processo.                                                                                |
| FVE_E_TPM_SRK_AUTH_NOT_ZERO<br>0x80310025     | Os dados da autorização para o SRK (Storage Root Key) do TPM são diferentes de zero, pelo que são incompatíveis com o BitLocker. Inicialize o TPM antes de tentar utilizá-lo com o BitLocker.                                                          |
| FVE_E_FAILED_SECTOR_SIZE<br>0x80310026        | O algoritmo de encriptação da unidade não pode ser utilizado neste tamanho de setores.                                                                                                                                                                 |
| FVE_E_FAILED_AUTHENTICATION<br>0x80310027     | Não é possível desbloquear a unidade com a chave fornecida. Confirme se forneceu a chave correta e tente novamente.                                                                                                                                    |
| FVE_E_NOT_OS_VOLUME<br>0x80310028             | A unidade especificada não é a unidade do sistema operativo.                                                                                                                                                                                           |
| FVE_E_AUTOUNLOCK_ENABLED<br>0x80310029        | Não é possível desativar a Encriptação de Unidade BitLocker na unidade do sistema operativo até que a funcionalidade de desbloqueio automático tenha sido desativada para as unidades de dados fixas e amovíveis associadas a este computador.         |
| FVE_E_WRONG_BOOTSECTOR<br>0x8031002A          | O setor de arranque da partição do sistema não efetua medições do TPM. Utilize a ferramenta Bootrec.exe no Ambiente de Recuperação do Windows para atualizar ou reparar o setor de arranque.                                                           |
| FVE_E_WRONG_SYSTEM_FS<br>0x8031002B           | As unidades do sistema operativo da Encriptação de Unidade BitLocker têm de estar formatadas com o sistema de ficheiros NTFS para serem encriptadas. Converta a unidade para NTFS e ative o BitLocker.                                                 |
| FVE_E_POLICY_PASSWORD_REQUIRED<br>0x8031002C  | As definições de Política de Grupo necessitam que seja especificada uma palavra-passe antes da encriptação da unidade.                                                                                                                                 |
| FVE_E_CANNOT_SET_FVEK_ENCRYPTED<br>0x8031002D | Não é possível definir o algoritmo de encriptação e a chave da unidade numa unidade previamente encriptada. Para encriptar esta unidade com a Encriptação de Unidade                                                                                   |

| Constante/Valor                                       | Descrição                                                                                                                                                                                                                                                                                                                                                                                                     |
|-------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                       | BitLocker, remova a encriptação anterior e, em seguida, ative o BitLocker.                                                                                                                                                                                                                                                                                                                                    |
| FVE_E_CANNOT_ENCRYPT_NO_KEY<br>0x8031002E             | A Encriptação de Unidade BitLocker não consegue encriptar a unidade especificada, porque não está disponível uma chave de encriptação. Adicione um protetor de chave para encriptar esta unidade.                                                                                                                                                                                                             |
| FVE_E_BOOTABLE_CDDVD<br>0x80310030                    | A Encriptação de Unidade BitLocker detetou suportes multimédia de arranque (CD ou DVD) no computador. Remova o suporte multimédia e reinicie o computador antes de configurar o BitLocker.                                                                                                                                                                                                                    |
| FVE_E_PROTECTOR_EXISTS<br>0x80310031                  | Não é possível adicionar este protetor de chave. Só é permitido um protetor de chave deste tipo para esta unidade.                                                                                                                                                                                                                                                                                            |
| FVE_E_RELATIVE_PATH<br>0x80310032                     | O ficheiro de palavra-passe de recuperação não foi encontrado porque foi especificado um caminho relativo. As palavras-chave de recuperação têm de ser guardadas num caminho totalmente qualificado. As variáveis de ambiente configuradas no computador podem ser utilizadas no caminho.                                                                                                                     |
| FVE_E_PROTECTOR_NOT_FOUND<br>0x80310033               | O protetor de chave especificado não foi encontrado na unidade. O protetor de chave especificado não foi encontrado na unidade. Tente outro protetor de chave.                                                                                                                                                                                                                                                |
| FVE_E_INVALID_KEY_FORMAT<br>0x80310034                | A chave de recuperação fornecida está danificada e não pode ser utilizada para aceder à unidade. Tem de ser utilizado um método de recuperação alternativo, tal como uma palavra-passe de recuperação, um agente de recuperação de dados ou uma versão de cópia de segurança da chave de recuperação para recuperar o acesso à unidade.                                                                       |
| FVE_E_INVALID_PASSWORD_FORMAT<br>0x80310035           | O formato da palavra-passe de recuperação fornecida é inválido. As palavras-passe de recuperação do BitLocker têm 48 dígitos. Verifique se a palavra-passe de recuperação tem o formato correto e tente novamente.                                                                                                                                                                                            |
| FVE_E_FIPS_RNG_CHECK_FAILED<br>0x80310036             | Falha no teste de verificação do gerador de números aleatórios.                                                                                                                                                                                                                                                                                                                                               |
| FVE_E_FIPS_PREVENTS_RECOVERY_PASSWORD<br>0x80310037   | A definição de Política de Grupo que necessita da compatibilidade com FIPS impede a geração ou a utilização pela Encriptação de Unidade BitLocker de uma palavra-passe de recuperação local. Quando trabalha no modo compatível com FIPS, as opções de recuperação do BitLocker podem ser uma chave de recuperação armazenada numa unidade USB ou a recuperação através de um agente de recuperação de dados. |
| FVE_E_FIPS_PREVENTS_EXTERNAL_KEY_EXPORT<br>0x80310038 | A definição de Política de Grupo que necessita da compatibilidade com FIPS impede que a palavra-passe de recuperação seja guardada no Active Directory. Quando trabalha no modo compatível com FIPS, as opções de recuperação do BitLocker podem ser uma chave de recuperação armazenada numa unidade USB ou a recuperação através de um agente de recuperação de                                             |

| <b>Constante/Valor</b>                       | <b>Descrição</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|----------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                              | dados. Verifique a configuração das definições de Política de Grupo.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| FVE_E_NOT_DECRYPTED<br>0x80310039            | A unidade tem de ser totalmente descriptada para concluir esta operação.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| FVE_E_INVALID_PROTECTOR_TYPE<br>0x8031003A   | Não é possível utilizar o protetor de chave especificado para esta operação.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| FVE_E_NO_PROTECTORS_TO_TEST<br>0x8031003B    | Não existem protetores de chave na unidade para efetuar o teste de hardware.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| FVE_E_KEYFILE_NOT_FOUND<br>0x8031003C        | Não é possível localizar a chave de arranque ou a palavra-passe de recuperação do BitLocker no dispositivo USB. Verifique se tem o dispositivo USB correto, se o dispositivo USB está introduzido numa porta USB ativa no computador, reinicie o computador e tente novamente. Se o problema persistir, contacte o fabricante do computador para obter instruções de atualização do BIOS.                                                                                                                                                                           |
| FVE_E_KEYFILE_INVALID<br>0x8031003D          | A chave de arranque ou o ficheiro de palavra-passe de recuperação do BitLocker está danificado ou é inválido. Verifique se tem a chave de arranque ou o ficheiro de palavra-passe de recuperação correto e tente novamente.                                                                                                                                                                                                                                                                                                                                         |
| FVE_E_KEYFILE_NO_VMK<br>0x8031003E           | Não é possível obter a chave de encriptação do BitLocker a partir da chave de arranque ou da palavra-passe de recuperação. Verifique se tem a chave de arranque ou a palavra-passe de recuperação correta e tente novamente.                                                                                                                                                                                                                                                                                                                                        |
| FVE_E_TPM_DISABLED<br>0x8031003F             | O TPM está desativado. O TPM tem de estar ativado, inicializado e tem de ter uma propriedade válida antes de poder ser utilizado com a Encriptação de Unidade BitLocker.                                                                                                                                                                                                                                                                                                                                                                                            |
| FVE_E_NOT_ALLOWED_IN_SAFE_MODE<br>0x80310040 | Não é possível gerir a configuração BitLocker da unidade especificada porque o computador está atualmente a funcionar no Modo de Segurança. Enquanto estiver no Modo de Segurança, a Encriptação de Unidade BitLocker só poderá ser utilizada para fins de recuperação.                                                                                                                                                                                                                                                                                             |
| FVE_E_TPM_INVALID_PCR<br>0x80310041          | O TPM não conseguiu desbloquear a unidade porque as informações de arranque do sistema foram alteradas ou porque não foi fornecido um PIN correto. Confirme se a unidade não foi adulterada e se as alterações às informações de arranque do sistema foram efetuadas por uma origem fidedigna. Depois de confirmar se é seguro aceder à unidade, utilize a consola de recuperação do BitLocker para desbloquear a unidade e, em seguida, suspenda e retome o BitLocker para atualizar as informações de arranque do sistema que o BitLocker associa a esta unidade. |
| FVE_E_TPM_NO_VMK<br>0x80310042               | Não é possível obter a chave de encriptação do BitLocker a partir do TPM.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| FVE_E_PIN_INVALID<br>0x80310043              | Não é possível obter a chave de encriptação do BitLocker a partir do TPM e do PIN.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

| <b>Constante/Valor</b>                                  | <b>Descrição</b>                                                                                                                                                                                                                                     |
|---------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| FVE_E_AUTH_INVALID_APPLICATION<br>0x80310044            | Uma aplicação de arranque foi alterada desde a ativação de Encriptação de Unidade BitLocker.                                                                                                                                                         |
| FVE_E_AUTH_INVALID_CONFIG<br>0x80310045                 | As definições do BCD (Boot Configuration Data) foram alteradas desde a ativação da Encriptação de Unidade BitLocker.                                                                                                                                 |
| FVE_E_FIPS_DISABLE_PROTECTION_NOT_ALLOWED<br>0x80310046 | A definição de Política de Grupo que necessita da compatibilidade com FIPS proíbe a utilização de chaves não encriptadas, o que impede que o BitLocker seja suspenso nesta unidade. Contacte o administrador do domínio para obter mais informações. |
| FVE_E_FS_NOT_EXTENDED<br>0x80310047                     | Esta unidade não pode ser encriptada com a Encriptação de Unidade BitLocker porque o sistema de ficheiros não abrange até ao final da unidade. Crie partições nesta unidade e tente novamente.                                                       |
| FVE_E_FIRMWARE_TYPE_NOT_SUPPORTED<br>0x80310048         | Não é possível ativar a Encriptação de Unidade BitLocker na unidade do sistema operativo. Contacte o fabricante do computador para obter as instruções de atualização do BIOS.                                                                       |
| FVE_E_NO_LICENSE<br>0x80310049                          | Esta versão do Windows não inclui a Encriptação de Unidade BitLocker. Para utilizar a Encriptação de Unidade BitLocker, atualize o sistema operativo.                                                                                                |
| FVE_E_NOT_ON_STACK<br>0x8031004A                        | Não é possível utilizar a Encriptação de Unidade BitLocker porque ficheiros de sistema críticos do BitLocker estão em falta ou danificados. Utilize a Reparação do Arranque do Windows para restaurar estes ficheiros no computador.                 |
| FVE_E_FS_MOUNTED<br>0x8031004B                          | Não é possível bloquear a unidade enquanto esta está a ser utilizada.                                                                                                                                                                                |
| FVE_E_TOKEN_NOT_IMPERSONATED<br>0x8031004C              | O token de acesso associado ao thread atual não é um token representado.                                                                                                                                                                             |
| FVE_E_DRY_RUN_FAILED<br>0x8031004D                      | Não é possível obter a chave de encriptação do BitLocker. Verifique se o TPM está ativado e se a propriedade foi obtida. Se este computador não tiver um TPM, verifique se a unidade USB está introduzida e disponível.                              |
| FVE_E_REBOOT_REQUIRED<br>0x8031004E                     | Tem de reiniciar o computador antes de continuar com a Encriptação de Unidade BitLocker.                                                                                                                                                             |
| FVE_E_DEBUGGER_ENABLED<br>0x8031004F                    | Não é possível encriptar a unidade enquanto a depuração de arranque está ativada. Utilize a ferramenta de linha de comandos bcdedit para desativar a depuração de arranque.                                                                          |
| FVE_E_RAW_ACCESS<br>0x80310050                          | Não foi executada nenhuma ação porque a Encriptação de Unidade BitLocker está no modo de acesso RAW.                                                                                                                                                 |
| FVE_E_RAW_BLOCKED<br>0x80310051                         | A Encriptação de Unidade BitLocker não consegue entrar no modo de acesso RAW para esta unidade porque a unidade está atualmente a ser utilizada.                                                                                                     |

| <b>Constante/Valor</b>                                   | <b>Descrição</b>                                                                                                                                                                                                                |
|----------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| FVE_E_BCD_APPLICATIONS_PATH_INCORRECT<br>0x80310052      | O caminho especificado nos Dados de Configuração de Arranque (BCD) para uma aplicação de integridade protegida por Encriptação de Unidade BitLocker está incorreto. Verifique e corrija as definições de BCD e tente novamente. |
| FVE_E_NOT_ALLOWED_IN_VERSION<br>0x80310053               | Só é possível utilizar a Encriptação de Unidade BitLocker para aprovisionamento limitado ou efeitos de recuperação quando o computador é utilizado em ambientes de pré-instalação ou recuperação.                               |
| FVE_E_NO_AUTO_UNLOCK_MASTER_KEY<br>0x80310054            | A chave mestre de desbloqueio automático não estava disponível na unidade do sistema operativo.                                                                                                                                 |
| FVE_E_MOR_FAILED<br>0x80310055                           | O firmware do sistema não conseguiu ativar a limpeza da memória do sistema quando o computador foi reiniciado.                                                                                                                  |
| FVE_E_HIDDEN_VOLUME<br>0x80310056                        | Não é possível encriptar a unidade oculta.                                                                                                                                                                                      |
| FVE_E_TRANSIENT_STATE<br>0x80310057                      | As chaves de encriptação do BitLocker foram ignoradas porque a unidade estava num estado transitório.                                                                                                                           |
| FVE_E_PUBKEY_NOT_ALLOWED<br>0x80310058                   | Os protetores baseados em chaves públicas não são permitidos nesta unidade.                                                                                                                                                     |
| FVE_E_VOLUME_HANDLE_OPEN<br>0x80310059                   | A Encriptação de Unidade BitLocker já está a efetuar uma operação nesta unidade. Conclua todas as operações antes de continuar.                                                                                                 |
| FVE_E_NO_FEATURE_LICENSE<br>0x8031005A                   | Esta versão do Windows não suporta esta funcionalidade da Encriptação de Unidade BitLocker. Para utilizar esta funcionalidade, atualize o sistema operativo.                                                                    |
| FVE_E_INVALID_STARTUP_OPTIONS<br>0x8031005B              | As definições de Política de Grupo relativas às opções de arranque do BitLocker estão em conflito e não podem ser aplicadas. Contacte o administrador de sistema para obter mais informações.                                   |
| FVE_E_POLICY_RECOVERY_PASSWORD_NOT_ALLOWED<br>0x8031005C | As definições de Política de Grupo não permitem a criação de uma palavra-passe de recuperação.                                                                                                                                  |
| FVE_E_POLICY_RECOVERY_PASSWORD_REQUIRED<br>0x8031005D    | As definições de Política de Grupo exigem a criação de uma palavra-passe de recuperação.                                                                                                                                        |
| FVE_E_POLICY_RECOVERY_KEY_NOT_ALLOWED<br>0x8031005E      | As definições de Política de Grupo não permitem a criação de uma chave de recuperação.                                                                                                                                          |
| FVE_E_POLICY_RECOVERY_KEY_REQUIRED<br>0x8031005F         | As definições de Política de Grupo exigem a criação de uma chave de recuperação.                                                                                                                                                |
| FVE_E_POLICY_STARTUP_PIN_NOT_ALLOWED<br>0x80310060       | As definições de Política de Grupo não permitem a utilização de um PIN durante o arranque. Selecione outra opção de arranque do BitLocker.                                                                                      |

| <b>Constante/Valor</b>                               | <b>Descrição</b>                                                                                                                                                                                |
|------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| FVE_E_POLICY_STARTUP_PIN_REQUIRED<br>0x80310061      | As definições de Política de Grupo exigem a utilização de um PIN durante o arranque. Selecione esta opção de arranque do BitLocker.                                                             |
| FVE_E_POLICY_STARTUP_KEY_NOT_ALLOWED<br>0x80310062   | As definições de Política de Grupo não permitem a utilização de uma chave de arranque. Selecione outra opção de arranque do BitLocker.                                                          |
| FVE_E_POLICY_STARTUP_KEY_REQUIRED<br>0x80310063      | As definições de Política de Grupo exigem a utilização de uma chave de arranque. Selecione esta opção de arranque do BitLocker.                                                                 |
| FVE_E_POLICY_STARTUP_PIN_KEY_NOT_ALLOWED0x80310064   | As definições de Política de Grupo não permitem a utilização de uma chave de arranque e PIN. Selecione outra opção de arranque do BitLocker.                                                    |
| FVE_E_POLICY_STARTUP_PIN_KEY_REQUIRED<br>0x80310065  | As definições de Política de Grupo necessitam da utilização de uma chave de arranque e PIN. Selecione esta opção de arranque do BitLocker.                                                      |
| FVE_E_POLICY_STARTUP_TPM_NOT_ALLOWED<br>0x80310066   | A política de grupo não permite a utilização de apenas TPM durante o arranque. Selecione outra opção de arranque do BitLocker.                                                                  |
| FVE_E_POLICY_STARTUP_TPM_REQUIRED<br>0x80310067      | As definições de Política de Grupo necessitam da utilização de apenas TPM durante o arranque. Selecione esta opção de arranque do BitLocker.                                                    |
| FVE_E_POLICY_INVALID_PIN_LENGTH<br>0x80310068        | O PIN fornecido não satisfaz as necessidades de comprimento mínimo ou máximo.                                                                                                                   |
| FVE_E_KEY_PROTECTOR_NOT_SUPPORTED<br>0x80310069      | O protetor de chave não é suportado pela versão da Encriptação de Unidade BitLocker existente atualmente na unidade. Atualize a unidade para adicionar o protetor de chave.                     |
| FVE_E_POLICY_PASSPHRASE_NOT_ALLOWED<br>0x8031006A    | As definições de Política de Grupo não permitem a criação de uma palavra-passe.                                                                                                                 |
| FVE_E_POLICY_PASSPHRASE_REQUIRED<br>0x8031006B       | As definições de Política de Grupo necessitam da criação de uma palavra-passe.                                                                                                                  |
| FVE_E_FIPS_PREVENTS_PASSPHRASE<br>0x8031006C         | A definição de política de grupo que necessita da compatibilidade com FIPS impediu a geração ou a utilização da palavra-passe. Contacte o administrador do domínio para obter mais informações. |
| FVE_E_OS_VOLUME_PASSPHRASE_NOT_ALLOWED<br>0x8031006D | Não é possível adicionar uma palavra-passe à unidade do sistema operativo.                                                                                                                      |
| FVE_E_INVALID_BITLOCKER_OID<br>0x8031006E            | O identificador de objeto (OID) do BitLocker existente na unidade parece ser inválido ou estar danificado. Utilize manage-BDE para repor o OID nesta unidade.                                   |
| FVE_E_VOLUME_TOO_SMALL<br>0x8031006F                 | A unidade é demasiado pequena para ser protegida utilizando a Encriptação de Unidade BitLocker.                                                                                                 |

| <b>Constante/Valor</b>                                              | <b>Descrição</b>                                                                                                                                                                                                                                                              |
|---------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| FVE_E_DV_NOT_SUPPORTED_ON_FS<br>0x80310070                          | O tipo de unidade de deteção selecionada é incompatível com o sistema de ficheiros existente na unidade. As unidades de deteção BitLocker To Go têm de ser criadas em unidades formatadas com FAT.                                                                            |
| FVE_E_DV_NOT_ALLOWED_BY_GP<br>0x80310071                            | O tipo de unidade de deteção selecionado não é permitido pelas definições de Política de Grupo do computador. Verifique se as definições de Política de Grupo permitem a criação de unidades de deteção para utilização com o BitLocker To Go.                                |
| FVE_E_POLICY_USER_CERTIFICATE_NOT_ALLOWED<br>0x80310072             | As definições de Política de Grupo não permitem a utilização de certificados de utilizador, tais como smart cards, com a Encriptação de Unidade BitLocker.                                                                                                                    |
| FVE_E_POLICY_USER_CERTIFICATE_REQUIRED<br>0x80310073                | As definições de Política de Grupo necessitam que tenha um certificado de utilizador válido, tal como um smart card, para utilização com a Encriptação de Unidade BitLocker.                                                                                                  |
| FVE_E_POLICY_USER_CERT_MUST_BE_HW<br>0x80310074                     | As definições de Política de Grupo exigem a utilização de um protetor de chave baseado em smart card com Encriptação de Unidade BitLocker.                                                                                                                                    |
| FVE_E_POLICY_USER_CONFIGURE_FDVAUTOUNLOCK_NOT_ALLOWED<br>0x80310075 | As definições de Política de Grupo não permitem que unidades de dados fixas protegidas pelo BitLocker sejam automaticamente desbloqueadas.                                                                                                                                    |
| FVE_E_POLICY_USER_CONFIGURE_RDVAUTOUNLOCK_NOT_ALLOWED<br>0x80310076 | As definições de Política de Grupo não permitem que unidades de dados amovíveis protegidas pelo BitLocker sejam automaticamente desbloqueadas.                                                                                                                                |
| FVE_E_POLICY_USER_CONFIGURE_RDV_NOT_ALLOWED<br>0x80310077           | As definições de Política de Grupo não permitem que configure a Encriptação de Unidade BitLocker em unidades de dados amovíveis.                                                                                                                                              |
| FVE_E_POLICY_USER_ENABLE_RDV_NOT_ALLOWED<br>0x80310078              | As definições de Política de Grupo não permitem que ative a Encriptação de Unidade BitLocker em unidades de dados amovíveis. Contacte o administrador de sistema se necessitar de ativar o BitLocker.                                                                         |
| FVE_E_POLICY_USER_DISABLE_RDV_NOT_ALLOWED<br>0x80310079             | As definições de Política de Grupo não permitem que desative a Encriptação de Unidade BitLocker em unidades de dados amovíveis. Contacte o administrador de sistema se necessitar de desativar o BitLocker.                                                                   |
| FVE_E_POLICY_INVALID_PASSPHRASE_LENGTH<br>0x80310080                | A sua palavra-passe não satisfaz as necessidades de comprimento mínimo. Por predefinição, as palavras-passe têm de ter um comprimento mínimo de 8 caracteres. Contacte o administrador de sistema para obter as necessidades de comprimento de palavras-passe da organização. |
| FVE_E_POLICY_PASSPHRASE_TOO_SIMPLE<br>0x80310081                    | A palavra-passe não satisfaz as necessidades de complexidade definidas pelo administrador de sistema. Tente adicionar caracteres maiúsculos e minúsculos, números e símbolos                                                                                                  |

| <b>Constante/Valor</b>                                          | <b>Descrição</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| FVE_E_RECOVERY_PARTITION<br>0x80310082                          | Não é possível encriptar esta unidade porque esta está reservada para as Opções de Recuperação do Sistema do Windows.                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| FVE_E_POLICY_CONFLICT_FDVRK_OFF_AUK_ON<br>0x80310083            | Não é possível aplicar a Encriptação de Unidade BitLocker a esta unidade devido à existência de definições de Política de Grupo em conflito. Não é possível configurar o BitLocker para desbloquear automaticamente unidades de dados fixas quando as opções de recuperação do utilizador estão desativadas. Se pretender que as unidades de dados fixas protegidas pelo BitLocker sejam automaticamente desbloqueadas após a validação da chave, peça ao administrador de sistema para resolver o conflito das definições antes de ativar o BitLocker.         |
| FVE_E_POLICY_CONFLICT_RDVRK_OFF_AUK_ON<br>0x80310084            | Não é possível aplicar a Encriptação de Unidade BitLocker a esta unidade devido à existência de definições de Política de Grupo em conflito. Não é possível configurar o BitLocker para desbloquear automaticamente unidades de dados amovíveis quando as opções de recuperação do utilizador estão desativadas. Se pretender que as unidades de dados amovíveis protegidas pelo BitLocker sejam automaticamente desbloqueadas após a validação da chave, peça ao administrador de sistema para resolver o conflito das definições antes de ativar o BitLocker. |
| FVE_E_NON_BITLOCKER_OID<br>0x80310085                           | O atributo EKU (Utilização de Chave Avançada) do certificado especificado não permite que este seja utilizado para a Encriptação de Unidade BitLocker. O BitLocker não necessita que o certificado tenha um atributo EKU, mas se existir um configurado, tem de ser definido para um OID (identificador de objeto) que corresponda ao OID configurado para o BitLocker.                                                                                                                                                                                         |
| FVE_E_POLICY_PROHIBITS_SELFSIGNED<br>0x80310086                 | Não é possível aplicar a Encriptação de Unidade BitLocker a esta unidade conforme atualmente configurada devido às definições de Política de Grupo. O certificado que fornece para encriptação da unidade é autoassinado. As definições atuais de Política de Grupo não permitem a utilização de certificados autoassinados. Obtenha um novo certificado junto da autoridade de certificação antes de tentar ativar o BitLocker.                                                                                                                                |
| FVE_E_POLICY_CONFLICT_RO_AND_STARTUP_KEY_REQUIRED<br>0x80310087 | Não é possível aplicar a Encriptação BitLocker a esta unidade devido à existência de definições de Política de Grupo em conflito. Quando o acesso de escrita a unidade não protegidas pelo BitLocker é negado, não é possível exigir a utilização de uma chave de arranque USB. Peça ao administrador de sistema para resolver os conflitos de política antes de tentar ativar o BitLocker.                                                                                                                                                                     |
| FVE_E_CONV_RECOVERY_FAILED<br>0x80310088                        | Não é possível aplicar a Encriptação de Unidade BitLocker a esta unidade porque existem definições de Política de Grupo em conflito relativamente às opções de recuperação em unidades do sistema operativo. O armazenamento de informações de recuperação nos Serviços de Domínio do Active Directory não pode ser exigido quando a geração de palavras-passe de recuperação não é permitida. Peça ao administrador de sistema para resolver os conflitos de política antes de tentar ativar o BitLocker.                                                      |

| <b>Constante/Valor</b>                                      | <b>Descrição</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| FVE_E_VIRTUALIZED_SPACE_TOO_BIG<br>0x80310089               | O tamanho de virtualização pedido é demasiado grande.                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| FVE_E_POLICY_CONFLICT_OSV_RP_OFF_ADB_ON<br>0x80310090       | Não é possível aplicar a Encriptação de Unidade BitLocker a esta unidade porque existem definições de Política de Grupo em conflito relativamente às opções de recuperação em unidades do sistema operativo. O armazenamento de informações de recuperação nos Serviços de Domínio do Active Directory não pode ser exigido quando a geração de palavras-passe de recuperação não é permitida. Peça ao administrador de sistema para resolver os conflitos de política antes de tentar ativar o BitLocker. |
| FVE_E_POLICY_CONFLICT_FDV_RP_OFF_ADB_ON<br>0x80310091       | A Encriptação de Unidade BitLocker não pode ser aplicada a esta unidade, uma vez que existem definições da Política de grupo em conflito relativamente às opções de recuperação em unidades de dados fixas. O armazenamento de informações de recuperação nos Serviços de Domínio do Active Directory não pode ser exigido quando a geração de palavras-passe de recuperação não é permitida. Peça ao administrador de sistema para resolver os conflitos de política antes de tentar ativar o BitLocker.  |
| FVE_E_POLICY_CONFLICT_RDV_RP_OFF_ADB_ON<br>0x80310092       | Não é possível aplicar a Encriptação de Unidade BitLocker a esta unidade porque existem definições de Política de Grupo em conflito relativamente às opções de recuperação em unidades de dados amovíveis. O armazenamento de informações de recuperação nos Serviços de Domínio do Active Directory não pode ser exigido quando a geração de palavras-passe de recuperação não é permitida. Peça ao administrador de sistema para resolver os conflitos de política antes de tentar ativar o BitLocker.   |
| FVE_E_NON_BITLOCKER_KU<br>0x80310093                        | O atributo KU (Key Usage) do certificado especificado não permite que este seja utilizado para a Encriptação de Unidade BitLocker. O BitLocker não necessita que um certificado tenha um atributo KU, mas se existir um configurado, tem de ser definido para Cifragem de Chaves ou Correspondência de Chaves.                                                                                                                                                                                             |
| FVE_E_PRIVATEKEY_AUTH_FAILED<br>0x80310094                  | Não foi possível autorizar a chave privada associada ao certificado especificado. A autorização da chave privada não foi fornecida ou a autorização fornecida era inválida.                                                                                                                                                                                                                                                                                                                                |
| FVE_E_REMOVAL_OF_DRA_FAILED<br>0x80310095                   | A remoção do certificado do agente de recuperação de dados tem de ser efetuada utilizando o snap-in Certificados.                                                                                                                                                                                                                                                                                                                                                                                          |
| FVE_E_OPERATION_NOT_SUPPORTED_ON_VISTA_VOLUME<br>0x80310096 | Esta unidade foi encriptada utilizando a versão da Encriptação de Unidade BitLocker incluída com o Windows Vista e o Windows Server 2008, que não suporta identificadores organizacionais. Para especificar identificadores organizacionais para esta unidade, atualize a encriptação da unidade para a versão mais recente utilizando o comando "manage-bde -upgrade".                                                                                                                                    |
| FVE_E_CANT_LOCK_AUTOUNLOCK_ENABLED_VOLUME<br>0x80310097     | Não é possível bloquear a unidade, porque esta é desbloqueada automaticamente neste computador. Remova o protetor de desbloqueio automático para bloquear esta unidade.                                                                                                                                                                                                                                                                                                                                    |

| <b>Constante/Valor</b>                                               | <b>Descrição</b>                                                                                                                                                                                                                                                                                                                                                               |
|----------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| FVE_E_FIPS_HASH_KDF_NOT_ALLOWED<br>0x80310098                        | A Função de Derivação de Chaves SP800-56A para smart cards ECC predefinida do BitLocker não é suportada pelo seu smart card. A definição de Política de Grupo que exige a conformidade com o FIPS impede que o BitLocker utilize qualquer outra função de derivação de chaves para encriptação. Tem de utilizar um smart card compatível com FIPS em ambientes FIPS restritos. |
| FVE_E_ENH_PIN_INVALID<br>0x80310099                                  | Não foi possível obter a chave de encriptação do BitLocker a partir do TPM e do PIN avançado. Experimente utilizar um PIN que contenha apenas numerais.                                                                                                                                                                                                                        |
| FVE_E_INVALID_PIN_CHARS<br>0x8031009A                                | O PIN do TPM pedido contém caracteres inválidos.                                                                                                                                                                                                                                                                                                                               |
| FVE_E_INVALID_DATUM_TYPE<br>0x8031009B                               | As informações de gestão armazenadas na unidade contêm um tipo desconhecido. Se estiver a utilizar uma versão antiga do Windows, tente aceder à unidade a partir da versão mais recente.                                                                                                                                                                                       |
| FVE_E_EFI_ONLY<br>0x8031009C                                         | A funcionalidade só é suportada em sistemas EFI.                                                                                                                                                                                                                                                                                                                               |
| FVE_E_MULTIPLE_NKP_CERTS<br>0x8031009D                               | Foi encontrado mais de um certificado de Protetor de Chave de Rede no sistema.                                                                                                                                                                                                                                                                                                 |
| FVE_E_REMOVAL_OF_NKP_FAILED<br>0x8031009E                            | O certificado de Protetor de Chave de Rede tem de ser removido utilizando o snap-in Certificados.                                                                                                                                                                                                                                                                              |
| FVE_E_INVALID_NKP_CERT<br>0x8031009F                                 | Foi encontrado um certificado inválido no arquivo de certificados de Protetor de Chave de Rede.                                                                                                                                                                                                                                                                                |
| FVE_E_NO_EXISTING_PIN<br>0x803100A0                                  | Esta unidade não está protegida com PIN.                                                                                                                                                                                                                                                                                                                                       |
| FVE_E_PROTECTOR_CHANGE_PIN_MISMATCH<br>0x803100A1                    | Introduza o PIN atual correto.                                                                                                                                                                                                                                                                                                                                                 |
| FVE_E_PROTECTOR_CHANGE_BY_STD_USER_DISALLOWED<br>0x803100A2          | Tem de ter sessão iniciada com a conta de administrador para alterar o PIN ou a palavra-passe. Clique na hiperligação para repor o PIN ou a palavra-passe como administrador.                                                                                                                                                                                                  |
| FVE_E_PROTECTOR_CHANGE_MAX_PIN_CHANGE_ATTEMPTS_REACHED<br>0x803100A3 | O BitLocker desativou alterações de PIN e palavra-passe na sequência de demasiados pedidos falhados. Clique na hiperligação para repor o PIN ou a palavra-passe como administrador.                                                                                                                                                                                            |
| FVE_E_POLICY_PASSPHRASE_REQUIRES_ASCII<br>0x803100A4                 | O administrador de sistema exige que as palavras-passe contenham apenas caracteres ASCII imprimíveis. Isto inclui letras não acentuadas (A-Z, a-z), números (0-9), espaço, sinais aritméticos, pontuação comum, separadores e os símbolos seguintes: # \$ & @ ^ _ ~ .                                                                                                          |
| FVE_E_FULL_ENCRYPTION_NOT_ALLOWED_ON_TP_STORAGE<br>0x803100A5        | A Encriptação de Unidade BitLocker só suporta a encriptação Apenas do Espaço Utilizado em armazenamento com aprovisionamento dinâmico.                                                                                                                                                                                                                                         |

| <b>Constante/Valor</b>                                      | <b>Descrição</b>                                                                                                                      |
|-------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| FVE_E_WIPE_NOT_ALLOWED_ON_TP_STORAGE<br>0x803100A6          | A Encriptação de Unidade BitLocker não suporta a limpeza do espaço livre em armazenamento com aprovisionamento dinâmico.              |
| FVE_E_KEY_LENGTH_NOT_SUPPORTED_BY_EDRIVE<br>0x803100A7      | O comprimento de chave de autenticação necessário não é suportado pela unidade.                                                       |
| FVE_E_NO_EXISTING_PASSPHRASE<br>0x803100A8                  | A unidade não está protegida com palavra-passe.                                                                                       |
| FVE_E_PROTECTOR_CHANGE_PASSPHRASE_MISMATCH<br>0x803100A9    | Introduza a palavra-passe atual correta.                                                                                              |
| FVE_E_PASSPHRASE_TOO_LONG<br>0x803100AA                     | A palavra-passe não pode exceder 256 caracteres.                                                                                      |
| FVE_E_NO_PASSPHRASE_WITH_TPM<br>0x803100AB                  | Não é possível adicionar um protetor de chave de palavra-passe, porque existe um protetor de TPM na unidade.                          |
| FVE_E_NO_TPM_WITH_PASSPHRASE<br>0x803100AC                  | Não é possível adicionar um protetor de chave de TPM, porque existe um protetor de palavra-passe na unidade.                          |
| FVE_E_NOT_ALLOWED_ON_CSV_STACK<br>0x803100AD                | Este comando só pode ser efetuado a partir do nó coordenador do volume CSV especificado.                                              |
| FVE_E_NOT_ALLOWED_ON_CLUSTER<br>0x803100AE                  | Não é possível efetuar este comando num volume quando este faz parte de um cluster.                                                   |
| FVE_E_EDRIVE_NO_FAILOVER_TO_SW<br>0x803100AF                | O BitLocker não reverteu para a utilização de encriptação de software BitLocker devido à configuração de política de grupo.           |
| FVE_E_EDRIVE_BAND_IN_USE<br>0x803100B0                      | A unidade não pode ser gerida pelo BitLocker, porque a funcionalidade de encriptação de hardware da unidade já está a ser utilizada.  |
| FVE_E_EDRIVE_DISALLOWED_BY_GP<br>0x803100B1                 | As definições de Política de Grupo não permitem utilizar encriptação baseada em hardware.                                             |
| FVE_E_EDRIVE_INCOMPATIBLE_VOLUME<br>0x803100B2              | A unidade especificada não suporta encriptação baseada em hardware.                                                                   |
| FVE_E_NOT_ALLOWED_TO_UPGRADE_WHILE_CONVERTING<br>0x803100B3 | Não é possível atualizar o BitLocker durante a encriptação ou desencriptação de um disco.                                             |
| FVE_E_EDRIVE_DV_NOT_SUPPORTED<br>0x803100B4                 | Não são suportados Volumes de Deteção para volumes que utilizem encriptação de hardware.                                              |
| FVE_E_NO_PREBOOT_KEYBOARD_DETECTED<br>0x803100B5            | Nenhum teclado de pré-arranque detetado. O utilizador poderá não conseguir introduzir os dados necessários para desbloquear o volume. |

| <b>Constante/Valor</b>                                                      | <b>Descrição</b>                                                                                                                                                                                                                                                                                      |
|-----------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| FVE_E_NO_PREBOOT_KEYBOARD_OR_WINRE_DETECTED<br>0x803100B6                   | Não foi detetado qualquer teclado de pré-arranque ou Ambiente de Recuperação do Windows. O utilizador poderá não conseguir introduzir os dados necessários para desbloquear o volume.                                                                                                                 |
| FVE_E_POLICY_REQUIRES_STARTUP_PIN_ON_TOUCH_DEVICE<br>0x803100B7             | As definições de Política de Grupo exigem a criação de um PIN de arranque, mas este dispositivo não tem nenhum teclado de pré-arranque disponível. O utilizador poderá não conseguir introduzir os dados necessários para desbloquear o volume.                                                       |
| FVE_E_POLICY_REQUIRES_RECOVERY_PASSWORD_ON_TOUCH_DEVICE<br>0x803100B8       | As definições de Política de Grupo exigem a criação de uma palavra-passe de recuperação, mas este dispositivo não tem um teclado de pré-arranque nem o Ambiente de Recuperação do Windows disponível. O utilizador poderá não conseguir introduzir os dados necessários para desbloquear o volume.    |
| FVE_E_WIPE_CANCEL_NOT_APPLICABLE<br>0x803100B9                              | A limpeza do espaço livre não está a ser efetuada neste momento.                                                                                                                                                                                                                                      |
| FVE_E_SECUREBOOT_DISABLED<br>0x803100BA                                     | O BitLocker não pode utilizar o Arranque Seguro para integridade da plataforma, porque o Arranque Seguro foi desativado.                                                                                                                                                                              |
| FVE_E_SECUREBOOT_CONFIGURATION_INVALID<br>0x803100BB                        | O BitLocker não pode utilizar o Arranque Seguro para integridade da plataforma, porque a configuração de Arranque Seguro não preenche os requisitos do BitLocker.                                                                                                                                     |
| FVE_E_EDRIVE_DRY_RUN_FAILED<br>0x803100BC                                   | O computador não suporta encriptação BitLocker baseada em hardware. Contacte o fabricante do computador para obter atualizações de firmware.                                                                                                                                                          |
| FVE_E_SHADOW_COPY_PRESENT<br>0x803100BD                                     | Não é possível ativar o BitLocker no volume, porque este contém uma Cópia Sombra de Volumes. Remova todas as Cópias Sombra de Volumes antes de encriptar o volume.                                                                                                                                    |
| FVE_E_POLICY_INVALID_ENHANCED_BCD_SETTINGS<br>0x803100BE                    | Não é possível aplicar a Encriptação de Unidade BitLocker a esta unidade, porque a definição de Política de Grupo para Dados de Configuração de Arranque Avançada contém dados inválidos. Peça ao administrador de sistema que resolva esta configuração inválida antes de tentar ativar o BitLocker. |
| FVE_E_EDRIVE_INCOMPATIBLE_FIRMWARE<br>0x803100BF                            | O firmware do PC não é capaz de suportar a encriptação de hardware.                                                                                                                                                                                                                                   |
| FVE_E_PROTECTOR_CHANGE_MAX_PASSPHRASE_CHANGE_ATTEMPTS_REACHED<br>0x803100C0 | O BitLocker desativou alterações de palavra-passe na sequência de demasiados pedidos falhados. Clique na hiperligação para repor a palavra-passe como administrador.                                                                                                                                  |
| FVE_E_PASSPHRASE_PROTECTOR_CHANGE_BY_STD_USER_DISALLOWED<br>0x803100C1      | Tem de ter sessão iniciada com a conta de administrador para alterar a palavra-passe. Clique na hiperligação para repor a palavra-passe como administrador.                                                                                                                                           |
| FVE_E_LIVEID_ACCOUNT_SUSPENDED<br>0x803100C2                                | O BitLocker não consegue guardar a palavra-passe de recuperação, porque a conta Microsoft especificada está Suspensa.                                                                                                                                                                                 |

| <b>Constante/Valor</b>                                 | <b>Descrição</b>                                                                                                                                                                                                      |
|--------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| FVE_E_LIVEID_ACCOUNT_BLOCKED<br>0x803100C3             | O BitLocker não consegue guardar a palavra-passe de recuperação, porque a conta Microsoft especificada está Bloqueada.                                                                                                |
| FVE_E_NOT_PROVISIONED_ON_ALL_VOLUMES<br>0x803100C4     | Este PC não está provisionado para suportar a encriptação do dispositivo. Ative o BitLocker em todos os volumes para estar em conformidade com a política de encriptação do dispositivo.                              |
| FVE_E_DE_FIXED_DATA_NOT_SUPPORTED<br>0x803100C5        | Este PC não pode suportar a encriptação do dispositivo, porque os volumes de dados fixos não encriptados estão presentes.                                                                                             |
| FVE_E_DE_HARDWARE_NOT_COMPLIANT<br>0x803100C6          | Este PC não cumpre os requisitos de hardware para suportar a encriptação do dispositivo.                                                                                                                              |
| FVE_E_DE_WINRE_NOT_CONFIGURED<br>0x803100C7            | Este PC não pode suportar a encriptação do dispositivo, porque o WinRE não está configurado corretamente.                                                                                                             |
| FVE_E_DE_PROTECTION_SUSPENDED<br>0x803100C8            | A proteção está ativada no volume, mas foi suspensa. É provável que esta situação tenha ocorrido por ter sido aplicada uma atualização ao sistema. Volte a tentar depois de reiniciar.                                |
| FVE_E_DE_OS_VOLUME_NOT_PROTECTED<br>0x803100C9         | Este PC não está provisionado para suportar a encriptação do dispositivo.                                                                                                                                             |
| FVE_E_DE_DEVICE_LOCKEDOUT<br>0x803100CA                | O Bloqueio do Dispositivo foi acionado devido a demasiadas tentativas de palavras-passe incorretas.                                                                                                                   |
| FVE_E_DE_PROTECTION_NOT_YET_ENABLED<br>0x803100CB      | A proteção não foi ativada no volume. A ativação da proteção necessita de uma conta ligada. Se já tiver uma conta ligada e estiver a visualizar este erro, consulte o registo de eventos para obter mais informações. |
| FVE_E_INVALID_PIN_CHARS_DETAILED<br>0x803100CC         | O PIN só pode conter números entre 0 e 9.                                                                                                                                                                             |
| FVE_E_DEVICE_LOCKOUT_COUNTER_UNAVAILABLE<br>0x803100CD | O BitLocker não consegue utilizar proteção de repetição de hardware, porque o PC não tem nenhum contador disponível.                                                                                                  |
| FVE_E_DEVICELOCKOUT_COUNTER_MISMATCH<br>0x803100CE     | Falha na validação do estado de bloqueio de dispositivo devido a um erro de correspondência de contador.                                                                                                              |
| FVE_E_BUFFER_TOO_LARGE<br>0x803100CF                   | A memória intermédia de entrada é demasiado grande.                                                                                                                                                                   |

## Glossário

**Ativado** - A ativação ocorre quando o computador tiver sido registado no Dell Server e tiver recebido, pelo menos, um conjunto inicial de políticas.

**Active Directory (AD)** - Um serviço de directório criado pela Microsoft para as redes de domínio Windows.

**Application Data Encryption** - O Application Data Encryption encripta qualquer ficheiro gravado por uma aplicação protegida, utilizando uma substituição de categoria 2. Isto significa que qualquer directório que tenha uma proteção de categoria 2 ou superior, ou qualquer localização que tenha extensões específicas protegidas com categoria 2 ou superior, fará com que a ADE não encripte esses ficheiros.

**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.

**Credenciais em cache** - As credenciais em cache são credenciais adicionadas à base de dados da PBA quando um utilizador é autenticado com êxito no Active Directory. Estas informações sobre o utilizador são mantidas para que o utilizador possa iniciar sessão quando não tem ligação ao Active Directory (por exemplo, quando leva o portátil para casa).

**Encriptação comum** - A chave Comum torna os ficheiros encriptados acessíveis a todos os utilizadores geridos no dispositivo onde foram criados.

**Desativar** - A desativação ocorre quando o SED Manager é desligado na Management Console. Após a desativação do computador, a base de dados da PBA é eliminada e deixa de existir registo dos utilizadores em cache.

**Encryption External Media** - Este serviço dentro do Encryption protege suportes de dados amovíveis e dispositivos de armazenamento externos.

**Código de acesso do Encryption External Media** - Este serviço permite a recuperação de dispositivos protegidos pelo Encryption External Media, caso o utilizador se esqueça da palavra-passe e já não consiga iniciar sessão. Concluir este processo permite ao utilizador repor a palavra-passe definida no suporte de dados.

**Encryption** - Componente que aplica políticas de segurança, quer um endpoint esteja ligado à rede, desligado da rede, seja perdido ou roubado. Ao criar um ambiente de computação fidedigno para endpoints, o 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.

**Endpoint** - Dependendo do contexto, um computador, dispositivo móvel ou suporte de dados externo.

**Chaves de encriptação** - Na maioria dos casos, o Encryption Client utiliza a chave de Utilizador em conjunto com duas chaves de encriptação adicionais. No entanto, existem exceções: Todas as políticas de SDE e a política de Credenciais Seguras do Windows utilizam a chave de SDE. A política de Encriptar ficheiro de paginação do Windows e a política de Ficheiro de hibernação seguro do Windows utilizam a sua própria chave, a General Purpose Key (GPK). A chave Comum torna os ficheiros acessíveis a todos os utilizadores geridos no dispositivo em que foram criados. A chave de Utilizador torna os ficheiros acessíveis apenas ao utilizador que os criou, e apenas no dispositivo em que foram criados. A chave de Roaming de utilizador torna os ficheiros acessíveis apenas ao utilizador que os criou, em qualquer dispositivo Windows (ou Mac) protegido.

**Varrimento de encriptação** - processo de análise das pastas a serem encriptadas 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, da seguinte forma: - Um varrimento de encriptação ocorre 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 política *Analisar ambiente de trabalho ao iniciar sessão* estiver ativada, as pastas especificadas para a encriptação são 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 (utilizador de versos comuns), aciona um varrimento. Adicionalmente, a alternância entre a encriptação ativada e desativada aciona 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 Server. O novo servidor troca de certificados com o Dell Server no decurso da ativação e utiliza o certificado nos eventos de autenticação subsequentes.

Autenticação de Pré-arranque (PBA) - A Autenticação de Pré-arranque funciona como uma extensão da BIOS ou do firmware de arranque e garante um ambiente seguro, à prova de adulteração e externo ao sistema operativo como camada de autenticação fidedigna. A PBA impede a leitura de quaisquer informações a partir do disco rígido, como o sistema operativo, até que o utilizador confirme ter as credenciais corretas.

SED Manager – O SED Manager 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. O SED Manager é um componente de gestão central e redimensionável que lhe permite proteger e gerir os seus dados de forma mais eficaz. O SED Manager assegura que pode administrar a sua empresa de forma mais rápida e fácil.

Utilizador de servidor – Uma conta de utilizador virtual criada pelo Encryption para a gestão das atualizações de políticas e chaves de encriptação no sistema operativo de um servidor. Esta conta de utilizador não corresponde a nenhuma outra conta de utilizador do computador ou do domínio, não tendo um nome de utilizador ou uma palavra-passe que possam ser fisicamente utilizados. Um valor UCID exclusivo é atribuído à conta na Management Console.

System Data Encryption (SDE) - A SDE foi concebida para encriptar o sistema operativo e ficheiros de programas. Para concretizar este objetivo, é necessário que a SDE consiga abrir a respetiva chave durante o arranque do sistema operativo. O seu objetivo é impedir alterações ou ataques offline ao sistema operativo por um atacante. A SDE não se destina à encriptação de dados do utilizador. A encriptação de chave Comum e de Utilizador destina-se a dados confidenciais do utilizador, uma vez que estes requerem uma palavra-passe do utilizador para desbloquear as chaves de encriptação. As políticas de SDE não encriptam os ficheiros de que o sistema operativo necessita para iniciar o processo de arranque. As políticas SDE não requerem uma autenticação de pré-arranque, nem interferem, de modo algum, com o Registo de Arranque Principal. Quando o computador arranca, os ficheiros encriptados estão disponíveis antes de qualquer utilizador iniciar sessão (para ativar as ferramentas de cópia de segurança e recuperação, SMS e gestão de patches). Ao desativar a SDE, é iniciada a desencriptação automática de todos os diretórios e ficheiros encriptados pela SDE para os utilizadores aplicáveis, independentemente de outros valores de política de SDE, tais como as Regras de encriptação SDE.

TPM (Trusted Platform Module) – O TPM é um chip de segurança com três funções principais: armazenamento seguro, medição e atestados. O cliente Encryption utiliza o TPM para a sua função de armazenamento seguro. O TPM pode também fornecer contentores encriptados para o cofre do software.

Encriptação de utilizador – A chave de Utilizador torna os ficheiros acessíveis apenas ao utilizador que os criou, e apenas no dispositivo onde foram criados. Quando executar o Dell Server Encryption, a encriptação de Utilizador é convertida para encriptação Comum. É aberta uma exceção aos dispositivos de suporte de dados amovíveis; ao serem inseridos num servidor que tenha a encriptação instalada, os ficheiros são encriptados com a chave de roaming de utilizador.