

Encryption

Requisitos do sistema v10.1



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

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

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

© 2012-2018 Dell Inc. Todos os direitos reservados. Dell, EMC e outras marcas comerciais pertencem à Dell Inc ou às suas subsidiárias. Outras marcas comerciais podem pertencer aos seus respectivos proprietários. Marcas comerciais e marcas comerciais registradas utilizadas no Dell Encryption, Endpoint Security Suite Enterprise e no conjunto de aplicações de documentos Data Guardian: Dell™ e o logótipo Dell, Dell Precision™, OptiPlex™, ControlVault™, Latitude™, XPS® e KACE™ são marcas comerciais da Dell Inc. Cylance®, CylancePROTECT® e o logótipo Cylance são marcas comerciais registradas da Cylance, Inc. nos EUA e noutros países. McAfee® e o logótipo da McAfee são marcas comerciais ou marcas comerciais registradas da McAfee, Inc. nos Estados Unidos e noutros países. Intel®, Pentium®, Intel Core Inside Duo®, Itanium® e Xeon® são marcas comerciais registradas da Intel Corporation nos EUA e noutros países. Adobe®, Acrobat®, e Flash® são marcas registradas da Adobe Systems Incorporated. Authen Tec® e Eikon® são marcas comerciais registradas da Authen Tec. AMD® é marca registada da Advanced Micro Devices, Inc. Microsoft®, Windows® e Windows Server®, Internet Explorer®, Windows Vista®, Windows 7®, Windows 10®, Active Directory®, Access®, BitLocker®, BitLocker To Go®, Excel®, Hyper-V®, Outlook®, PowerPoint®, Word®, OneDrive®, SQL Server® e Visual C++® são marcas comerciais ou marcas comerciais registradas da Microsoft Corporation nos Estados Unidos e/ou noutros países. VMware® é marca registada ou marca comercial da VMware, Inc. nos Estados Unidos ou noutros países. Box® é marca registada da Box. DropboxSM é uma marca de serviço da Dropbox, Inc. Google™, Android™, Google™ Chrome™, Gmail™ e Google™ Play são marcas comerciais ou marcas comerciais registradas da Google Inc. nos Estados Unidos e noutros países. Apple®, App StoreSM, Apple Remote Desktop™, Boot Camp™, FileVault™, iPad®, iPhone®, iPod®, iPod touch®, iPod shuffle® e iPod nano®, Macintosh® e Safari® são marcas de serviço, marcas comerciais ou marcas comerciais registradas da Apple, Inc. nos Estados Unidos e/ou noutros países. EnCase™ e Guidance Software® são marcas comerciais ou marcas registradas da Guidance Software. Entrust® é marca registada da Entrust®, Inc. nos Estados Unidos e noutros países. Mozilla® Firefox® é uma marca comercial registada da Mozilla Foundation nos Estados Unidos e/ou noutros países. iOS® é uma marca comercial ou marca comercial registada da Cisco Systems, Inc. nos Estados Unidos e outros países e é utilizada sob licença. Oracle® e Java® são marcas registradas da Oracle e/ou suas afiliadas. Travelstar® é marca registada da HGST, Inc. nos Estados Unidos e noutros países. UNIX® é marca registada da The Open Group. VALIDITY™ é uma marca comercial da Validity Sensors, Inc. nos Estados Unidos e noutros países. VeriSign® e outras marcas similares são marcas comerciais ou marcas comerciais registradas da VeriSign, Inc. ou respetivas filiais ou subsidiárias nos Estados Unidos e noutros países e licenciadas à Symantec Corporation. KVM on IP® é marca registada da Video Products. Yahoo!® é marca registada da Yahoo! Inc. Bing® é uma marca comercial registada da Microsoft Inc. Ask® é uma marca registada da IAC Publishing, LLC. Os outros nomes podem ser marcas comerciais dos respetivos proprietários.

2018 - 11

1 Introdução.....	4
Contacte o Dell ProSupport.....	4
2 Requisitos.....	5
Todos os clientes.....	5
Todos os clientes - Pré-requisitos.....	5
Todos os clientes - Hardware.....	5
Todos os clientes - Localização.....	6
Cliente de encriptação.....	6
Pré-requisitos do Encryption Client.....	7
Hardware do Encryption Client.....	7
Sistemas operativos do Encryption Client.....	7
Sistemas operativos do Encryption External Media.....	7
Server Encryption Client.....	8
Hardware do Server Encryption Client.....	9
Sistemas operativos do Server Encryption Client.....	9
Sistemas operativos do Encryption External Media.....	10

Introdução

Este documento apresenta os requisitos do Dell Encryption.

Para aceder a toda a documentação do Dell Encryption, consulte www.dell.com/support/home/us/en/04/product-support/product/dell-data-protection-encryption/manuals.

Contacte o Dell ProSupport

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

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

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

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

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, que poderá ser atribuído temporariamente por uma ferramenta de implementação, como o Microsoft SMS ou Dell KACE. Não são suportados utilizadores não administradores com privilégios elevados.
- Realize uma cópia de segurança de todos os dados importantes antes de iniciar a instalação/desinstalação.
- Não realize alterações no computador, incluindo inserir ou remover unidades externas (USB) durante a instalação.
- Se os clientes do instalador principal estiverem autorizados a utilizar o Dell Digital Delivery (DDD), certifique-se de que a porta de saída 443 está disponível para comunicar com o Security Management Server/Security Management Server Virtual. A funcionalidade de elegibilidade não funcionará se a porta 443 estiver bloqueada (por qualquer motivo). O DDD não é utilizado se a instalação for efetuada utilizando os instaladores subordinados.
- Assegure-se de verificar periodicamente a página www.dell.com/support para procurar a documentação mais atual e Conselhos técnicos.

Todos os clientes - Pré-requisitos

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

Todos os computadores enviados da fábrica da Dell são previamente equipados com a versão completa do Microsoft .Net Framework 4.5.2 (ou posterior). No entanto, se não instalar em hardware Dell ou se atualizar o cliente num hardware Dell mais antigo, deve verificar qual a versão do Microsoft .Net instalada e atualizar a versão, **antes de instalar o cliente** para impedir falhas na instalação/atualização. Para verificar a versão instalada do Microsoft .Net, siga estas instruções no computador onde pretende efetuar a instalação: [http://msdn.microsoft.com/en-us/library/hh925568\(v=vs.110\).aspx](http://msdn.microsoft.com/en-us/library/hh925568(v=vs.110).aspx). Para instalar o Microsoft .Net Framework 4.5.2, aceda a <https://www.microsoft.com/en-us/download/details.aspx?id=42643>.

- Os controladores e firmware do ControlVault, leitores de impressão digital e smart cards (conforme abaixo ilustrado) 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

Todos os clientes - Hardware

- A tabela seguinte apresenta o hardware de computador suportado.

Hardware

- Processador Intel Pentium ou AMD
- 110 MB de espaço livre em disco
- 512 MB de RAM

NOTA: É necessário espaço livre em disco adicional para encriptar os ficheiros no ponto final. Este tamanho varia de acordo com as políticas e do tamanho da unidade.

Todos os clientes - Localização

- Os clientes Encryption e BitLocker Manager estão em conformidade com a norma MUI (Multilingual User Interface - Interface de utilizador multilíngue) e estão localizados nos seguintes idiomas.

Suporte de idiomas

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

Cliente de encriptação

- O computador cliente deve ter conectividade de rede para ativar.
- 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.
- Desative o modo de suspensão durante o varrimento de encriptação inicial para impedir a suspensão do computador caso este se encontre sem supervisão. A encriptação não é possível num computador em suspensão (tal como não é possível a desencriptação).
- O cliente Encryption não suporta configurações de duplo arranque, uma vez que é possível encriptar ficheiros de sistema do outro sistema operativo, o que poderia interferir com o respetivo funcionamento.
- O 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.
- O cliente Encryption agora suporta o modo Audit. O modo Audit permite que os administradores implementem o cliente Encryption como parte da imagem corporativa, em vez de usar um SCCM de terceiros ou uma solução similar para implementar o cliente Encryption. Para instruções sobre como instalar o cliente Encryption numa imagem corporativa, consulte <http://www.dell.com/support/article/us/en/19/SLN304039>.
- O cliente Encryption foi sujeito a testes e é compatível com McAfee, com o cliente Symantec, Kaspersky e MalwareBytes. Existem exclusões implementadas para estes fornecedores de produtos anti-vírus, para evitar incompatibilidades entre a monitorização anti-vírus e a encriptação. O cliente Encryption foi também testado com o Microsoft Enhanced Mitigation Experience Toolkit.

Se a sua organização utilizar um antivírus de um fornecedor não indicado na lista, consulte <http://www.dell.com/support/article/us/en/19/SLN288353> ou contacte o Dell ProSupport para obter assistência.

- O TPM é utilizado para selar o GPK. Assim, se o cliente Encryption Client for executado, limpe o TPM no BIOS antes de proceder à instalação de um novo sistema operativo no computador cliente.
- Não é suportada a atualização de versão do sistema operativo com o cliente Encryption instalado. Desinstale e desencripte o cliente Encryption, atualize para o novo sistema operativo e, em seguida, reinstale o cliente Encryption.

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

Pré-requisitos do Encryption Client

- O instalador principal instala o Microsoft Visual C++ 2012 Update 4, se este ainda não estiver instalado no computador. **Quando utilizar o instalador subordinado**, é necessário instalar este componente antes de instalar o cliente Encryption.

Pré-requisito

- Visual C++ 2012 Update 4 ou Redistributable Package posterior (x86 e x64)
- Visual C++ 2015 Update 3 ou Redistributable Package posterior (x86 e x64)

Hardware do Encryption Client

- A tabela seguinte indica o hardware suportado.

Hardware opcional incorporado

- TPM 1.2 ou 2.0

Sistemas operativos do Encryption Client

- A tabela seguinte apresenta os sistemas operativos suportados.

Sistemas operativos Windows (32 e 64 bits)

- Windows 7 SP1: Enterprise, Professional, Ultimate
- Windows Embedded Standard 7 com modelo de Compatibilidade entre Aplicações (a encriptação do hardware não é suportada)
- Windows 8: Enterprise, Pro
- Windows 8.1 Atualização 0-1: Enterprise Edition, Pro Edition
- Windows Embedded 8.1 Industry Enterprise (a encriptação do hardware não é suportada)
- Windows 10: Education, Enterprise, Pro Version 1607 (Atualização de Aniversário/Redstone 1) até à versão 1803 (Atualização de abril de 2018/Redstone 4)
- VMware Workstation 12.5 e posterior



NOTA:

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

Sistemas operativos do Encryption External Media

- A tabela seguinte indica os sistemas operativos compatíveis ao aceder a suportes de dados protegidos pelo Encryption External Media.



NOTA:

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.

Sistemas operativos Windows compatíveis para aceder a suportes de dados protegidos pelo Encryption External Media (32 e 64 bits)

- Windows 7 SP1: Enterprise, Professional, Ultimate
- Windows 8: Enterprise, Pro, Consumer

Sistemas operativos Windows compatíveis para aceder a suportes de dados protegidos pelo Encryption External Media (32 e 64 bits)

- Windows 8.1 Atualização 0-1: Enterprise Edition, Pro Edition
- Windows 10: Education, Enterprise, Pro Version 1607 (Atualização de Aniversário/Redstone 1) até à versão 1803 (Atualização de abril de 2018/Redstone 4)

Sistemas operativos Mac compatíveis para aceder a suportes de dados protegidos pelo Encryption External Media (kernels de 64 bits)

- macOS Sierra 10.12.4 e 10.12.5
- macOS High Sierra 10.13.5 - 10.13.6
- macOS Mojave 10.14

Server Encryption Client

O Server Encryption destina-se a ser utilizado em computadores no modo de servidor, principalmente os servidores de ficheiros.

- O Server Encryption apenas é compatível com o Encryption Enterprise e com o Endpoint Security Suite Enterprise.
- O Server Encryption oferece o seguinte:
 - A encriptação do software
 - Encriptação de suportes de dados amovíveis
 - Controlo de portas

NOTA:

O servidor terá de suportar controlo de portas.

As políticas de 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 por parte dos 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 Server Encryption destina-se a ser utilizado em:

- 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 (repartição) 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. Se a sua organização utilizar um antivírus de um fornecedor não indicado na lista, consulte o artigo KB [SLN298707](#) ou [contacte o Dell ProSupport](#) para obter assistência.

Não Suportado

O Server Encryption não se destina a ser utilizado em:

- Security Management Servers/Security Management Server Virtuals ou servidores a executar bases de dados para Security Management Servers/Security Management Server Virtual.
- O Server Encryption não é compatível com o Encryption Personal.

- O Server Encryption não é suportado com o cliente SED Management ou BitLocker Manager.
- O Server Encryption não é suportado em servidores que fazem parte de sistemas de ficheiros distribuídos (DFS).
- A migração para ou a partir do Server Encryption não é suportada. As atualizações do Encryption External Media para o Server Encryption requerem a desinstalação completa do produto ou produtos anteriores antes de instalar o Server Encryption.
- 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 eliminação de duplicados
 - Eliminação de duplicados de hardware
 - RAIDs divididos (múltiplos volumes num único RAID)
 - Unidades SED (RAIDs e Não-RAID)
 - Início de sessão automático (Windows 7, 8/8.1) para quiosques
 - Início de sessão automático (Windows OS 7, 8/8.1) para quiosques
- O Server 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.
- 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 *Recovery Guide (Guia de recuperação)*.

Hardware do Server Encryption Client

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

Sistemas operativos do Server Encryption Client

A tabela seguinte apresenta os sistemas operativos suportados.

Sistemas operativos (32 e 64 bits)

- Windows 7 SP1: Enterprise, Professional, Ultimate
- Windows 8.0: Enterprise, Pro
- Windows 8.1: Enterprise, Pro
- Windows 10: Education, Enterprise, Pro Version 1607 (Atualização de Aniversário/Redstone 1) até à versão 1803 (Atualização de abril de 2018/Redstone 4)

Sistemas Operativo de Servidor Suportados

- Windows Server 2008 R2 SP1: Standard Edition, Datacenter Edition, Enterprise Edition, Webserver Edition
- Windows Server 2012: Standard Edition, Essentials Edition, Datacenter Edition (o Server Core não é suportado)
- Windows Server 2012 R2: Standard Edition, Essentials Edition, Datacenter Edition (o Server Core não é suportado)
- Windows Server 2016: Standard Edition, Essentials Edition, Datacenter Edition (o Server Core não é suportado)

Sistemas operativos suportados com modo UEFI

- Windows 8: Enterprise, Pro
- Windows 8.1: Enterprise, Pro
- Windows 10: Education, Enterprise, Pro Version 1607 (Atualização de Aniversário/Redstone 1) até à versão 1803 (Atualização de abril de 2018/Redstone 4)

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.

Sistemas operativos do Encryption External Media

A tabela seguinte indica os sistemas operativos compatíveis ao aceder a suportes de dados protegidos pelo Encryption External Media.

NOTA:

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.

Sistemas operativos Windows compatíveis para aceder a suportes de dados protegidos pelo Encryption External Media (32 e 64 bits)

- Windows 7 SP1: Enterprise, Professional, Ultimate
- Windows 8: Enterprise, Pro, Consumer
- Windows 8.1 Enterprise, Pro
- Windows 10: Education, Enterprise, Pro Version 1607 (Atualização de Aniversário/Redstone 1) até à versão 1803 (Atualização de abril de 2018/Redstone 4)

Sistemas Operativo de Servidor Suportados

- Windows Server 2012 R2

Sistemas operativos Mac compatíveis para aceder a suportes de dados protegidos pelo Encryption External Media (kernels de 64 bits)

- macOS Sierra 10.12.6
- macOS High Sierra 10.13.5 – 10.13.6
- macOS Mojave 10.14