Encryption

Requisitos do sistema v10.1

Notas, avisos e advertências

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

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

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

2018 - 11

Rev. A01

Índice

1

Introdução

Este documento lista os requisitos do Dell Encryption.

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

Entre em contato com o Dell ProSupport

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

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

Quando telefonar, tenha em mãos a Etiqueta de serviço ou Código de serviço expresso, para nos ajudar a garantir que possamos direcioná-lo rapidamente ao especialista técnico correto.

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

Requisitos

Todos os clientes

Estes requisitos se aplicam a todos os clientes. Os requisitos apresentados em outras seções se aplicam a clientes específicos.

- As práticas recomendadas de TI devem ser seguidas durante a implementação. Isso inclui, sem limitações, ambientes de teste controlados para testes iniciais e implantações escalonadas para os usuários.
- A conta de usuário que executa a instalação/upgrade/desinstalação precisa ser a de um usuário Admin local ou de domínio, que pode ser temporariamente atribuída por uma ferramenta de implementação, como o Microsoft SMS ou o Dell KACE. Não há suporte para um usuário que não é administrador mas possui privilégios elevados.
- Faça backup de todos os dados importantes antes de iniciar a instalação/desinstalação.
- Não realize alterações no computador, incluindo a inserção ou a remoção de unidades externas (USB), durante a instalação.
- Verifique se a porta de saída 443 está disponível para se comunicar com o Servidor de gerenciamento de segurança/Servidor de gerenciamento de segurança virtual se os clientes do instalador mestre forem qualificados usando o Dell Digital Delivery (DDD). A funcionalidade de habilitação não funcionará se a porta 443 estiver bloqueada por qualquer motivo. O DDD não será usado se a instalação for feita usando instaladores filhos.
- Verifique periodicamente www.dell.com/support para obter a documentação e recomendações técnicas mais recentes.

Todos os clientes - Pré-requisitos

- O Microsoft .Net Framework 4.5.2 (ou superior) é necessário para os clientes do instalador mestre e do instalador filho do . O instalador *não* instala o componente Microsoft .Net Framework.

  Todos os computadores enviados da fábrica da Dell são pré-instalados com a versão completa do Microsoft .Net Framework 4.5.2 (ou posterior). No entanto, se você não estiver realizando a instalação em um hardware da Dell ou estiver fazendo a atualização do cliente em equipamentos mais antigos da Dell, será necessário verificar qual versão do Microsoft .Net está instalada e atualizar a versão **antes de instalar o cliente** a fim de evitar falhas de atualização/instalação. Para verificar a versão do Microsoft .Net instalado, siga estas instruções no computador de instalação: http://msdn.microsoft.com/en-us/library/hh925568(v=vs.110).aspx. Para instalar o Microsoft .Net Framework 4.5.2, visite https://www.microsoft.com/en-us/download/details.aspx?id=42643.
- Os drivers e o firmware dos leitores de impressão digital, do ControlVault e dos cartões inteligentes (conforme mostrado a seguir) não estão incluídos nos arquivos executáveis do instalador mestre ou do instalador filho do . Os drivers e o firmware precisam ser mantidos atualizados e podem ser obtidos por download acessando o site http://www.dell.com/support e selecionando o modelo do computador. Faça download dos drivers e firmware adequados com base em seu hardware de autenticação.

  – ControlVault
  – NEXT Biometrics Fingerprint Driver
  – Driver 495 do leitor de impressão digital Validity
  – Driver de cartão inteligente O2Micro

Todos os clientes - Hardware

- A tabela a seguir detalha o hardware de computador suportado.

Hardware
– Processador Intel Pentium ou AMD

Hardware

- 110 MB de espaço disponível em disco
- 512 MB de RAM

NOTA: O espaço livre em disco adicional é necessário para criptografar os arquivos no endpoint. Este tamanho varia com base nas políticas e tamanho da unidade.

Todos os clientes - Localização

- Os clientes do Encryption e Gerenciador BitLocker são compatíveis com interfaces de usuário de vários idiomas (MUI) e estão localizados nos idiomas a seguir.

Suporte a idiomas

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

Cliente Encryption

- O computador cliente precisa ter conectividade de rede para realizar a ativação.
- Para reduzir o tempo inicial de criptografia, execute o Assistente de Limpeza de Disco do Windows para remover arquivos temporários e todos os outros dados desnecessários.
- Desative o modo de suspensão durante a varredura inicial de criptografia para impedir que um computador não supervisionado entre em modo de suspensão. Nem a criptografia nem a descriptografia podem ocorrer em um computador em modo de suspensão.
- O cliente Encryption não suporta configurações de inicialização dupla, pois existe a possibilidade de criptografar arquivos de sistema do outro sistema operacional e isto pode interferir na sua operação.
- O instalador mestre não oferece suporte a atualizações de componentes anteriores à versão v8.0. Extraia os instaladores filho do instalador mestre e faça upgrade do 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 soluções similares para implementar o cliente Encryption. Para obter instruções sobre como instalar o cliente Encryption em uma imagem corporativa, consulte http://www.dell.com/support/article/us/en/19/SLN304039.
- O Encryption Client foi testado e é compatível com McAfee, o cliente da Symantec, Kaspersky e MalwareBytes. Há exclusões inseridas no código em vigor para esses fornecedores de antivírus a fim de evitar incompatibilidades entre a varredura do antivírus e a criptografia. O cliente Encryption também foi testado com o Kit de ferramentas de experiência de mitigação aprimorada da Microsoft.

  Se sua organização usa um fornecedor de antivírus que não está na lista, consulte http://www.dell.com/support/article/us/en/19/SLN288353 ou entre em contato com o Dell ProSupport para obter ajuda.
- O TPM é usado para selar a GPK. Entretanto, se estiver executando o cliente Encryption, limpe o TPM no BIOS antes de instalar um novo sistema operacional no computador cliente.
- Não há suporte para upgrade de sistema operacional instalado quando o cliente Encryption está instalado. Desinstale e descriptografe o cliente Encryption, faça o upgrade para o novo sistema operacional e depois reinstale o cliente Encryption.

  Além disso, não há suporte para reinstalação de sistema operacional. Para reinstalar o sistema operacional, faça um backup do computador de destino, formate o computador, instale o sistema operacional e, depois, faça a recuperação dos dados criptografados seguindo os procedimentos de recuperação estabelecidos.

Pré-requisitos do cliente Encryption

- O instalador mestre instala o Microsoft Visual C++ 2012 Update 4 se ele não estiver instalado no computador. **Quando estiver usando o instalador filho**, você precisará instalar esse componente antes de instalar o cliente Encryption.

Pré-requisito
– Visual C++ 2012 Update 4 ou Redistributable Package mais recente (x86 e x64) – Visual C++ 2015 Update 3 ou Redistributable Package mais recente (x86 e x64)

Hardware do cliente Encryption

- A tabela a seguir detalha o hardware suportado.

Hardware integrado opcional
– TPM 1.2 ou 2.0

Sistemas operacionais do cliente Encryption

- A tabela a seguir detalha os sistemas operacionais suportados.

Sistemas operacionais Windows (32 e 64 bits)
– Windows 7 SP1: Enterprise, Professional, Ultimate – Windows Embedded Standard 7 com modelo de compatibilidade de aplicativo (sem suporte para criptografia de hardware) – Windows 8: Enterprise, Pro – Windows 8.1 Update 0-1: Enterprise Edition, Pro Edition – Windows Embedded 8.1 Industry Enterprise (sem suporte para criptografia de hardware) – Windows 10: Education, Enterprise, Pro Version 1607 (Atualização de Aniversário/Redstone 1) até a versão 1803 (April 2018 Update/Redstone 4) – VMWare Workstation 12.5 e mais recentes

NOTA:
Sem suporte para o modo UEFI em Windows 7, Windows Embedded Standard 7 ou Windows Embedded 8.1 Industry Enterprise.

Os sistemas operacionais do Encryption External Media

- A seguinte tabela detalha os sistemas operacionais suportados ao acessar mídias protegidas pelo Encryption External Media.

NOTA:
A mídia externa precisa ter aproximadamente 55 MB disponíveis, além de espaço livre na mídia igual ao maior arquivo a ser criptografado para hospedar o Encryption External Media.

Sistemas operacionais Windows suportados para acessar mídia protegida por Encryption External Media (32 e 64 bits)
– Windows 7 SP1: Enterprise, Professional, Ultimate

Sistemas operacionais Windows suportados para acessar mídia protegida por Encryption External Media (32 e 64 bits)

- Windows 8: Enterprise, Pro, Consumer
- Windows 8.1 Update 0-1: Enterprise Edition, Pro Edition
- Windows 10: Education, Enterprise, Pro Version 1607 (Atualização de Aniversário/Redstone 1) até a versão 1803 (April 2018 Update/Redstone 4)

Sistemas operacionais Mac suportados para acessar mídias protegidas por Encryption External Media (kernels de 64 bits)

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

Cliente Server Encryption

O Server Encryption é voltado para uso em computadores que funcionam no modo de servidor, especialmente servidores de arquivo.

- O Server Encryption é compatível apenas com o Encryption Enterprise e o Endpoint Security Suite Enterprise.
- O Server Encryption fornece o seguinte:
  - Há suporte para criptografia de software
  - Criptografia de mídia removível
  - Controle de porta

    NOTA:
    O servidor precisa oferecer suporte para controles de porta.

    As políticas de sistema de controle de porta de servidor afetam as mídias removíveis em servidores protegidos, controlando, por exemplo, o acesso e o uso das portas USB do servidor por dispositivos USB. A política de porta USB se aplica a portas USB externas. O recurso de portas USB internas não é afetado pela política de portas USB. Se a política de porta USB for desativada, o teclado e o mouse USB do cliente não funcionam e o usuário não consegue usar o computador, a menos que uma conexão de área de trabalho remota seja configurada antes da política ser aplicada.

O Server Encryption é voltado para uso em:

- Servidores de arquivo com unidades locais
- Máquinas virtuais (VM) executando um sistema operacional de servidor ou sistema operacional que não seja de servidor, mas atue como um servidor de arquivos simples
- Configurações compatíveis:
  - Servidores equipados com unidades RAID 5 ou 10; RAID 0 (particionamento) e RAID 1 (espelhamento) são suportadas de forma independente entre si.
  - Servidores equipados com unidades RAID de múltiplos TBs
  - Servidores equipados com unidades que podem ser trocadas sem desligar o computador
  - O Server Encryption é validado por provedores de antivírus líderes do setor. Exclusões no código de programação estão em vigor para esses fornecedores de antivírus, para impedir incompatibilidade entre a varredura do antivírus e a criptografia. Se sua organização usa um fornecedor de antivírus que não está na lista, consulte o artigo do banco de conhecimento SLN298707 ou entre em contato com o Dell ProSupport para obter ajuda.

Não suportado

O Server Encryption não é voltado para uso em:

- Servidores Servidor de gerenciamento de segurança / Servidor de gerenciamento de segurança virtual ou que executam bancos de dados para o Servidor de gerenciamento de segurança / Servidor de gerenciamento de segurança virtual .
- O Server Encryption não é compatível com o Encryption Personal.

- O Server Encryption não é suportado com cliente do SED Management ou do Gerenciador BitLocker.
- O Server Encryption não é suportado em servidores que fazem parte de sistemas de arquivos distribuídos (DFS).
- Não há suporte para migração de ou para o Server Encryption. Upgrades do Encryption External Media para o Server Encryption exigem que os produtos anteriores sejam desinstalados completamente antes da instalação do Server Encryption.
- Hosts de máquinas virtuais (um host de VM normalmente contém múltiplas VMs guest)
- Controladores de domínio
- Servidores Exchange
- Servidores que hospedam bancos de dados (SQL, Sybase, SharePoint, Oracle, MySQL, Exchange etc.)
- Servidores que usam qualquer uma das tecnologias a seguir:
  - Sistemas de arquivos resilientes
  - Sistemas de arquivos fluidos
  - Espaços de armazenamento Microsoft
  - Soluções de armazenamento de rede SAN/NAS
  - Dispositivos conectados por iSCSI
  - Software de desduplicação
  - Desduplicação de hardware
  - RAIDs divididos (múltiplos volumes em um único RAID)
  - Unidades SED (RAID e não RAID)
  - Logon automático (Windows OS 7, 8/8.1) para quiosques
  - Microsoft Storage Server 2012
- O Server Encryption não suporta configurações de inicialização dupla, pois existe a possibilidade de criptografar arquivos de sistema do outro sistema operacional e isto pode interferir na sua operação.
- Não há suporte para reinstalações de sistema operacional. Para reinstalar o sistema operacional, faça um backup do computador de destino, formate o computador, instale o sistema operacional e recupere os dados criptografados seguindo os procedimentos de recuperação estabelecidos. Para obter mais informações sobre como recuperar dados criptografados, consulte *Recovery Guide* (Guia de recuperação).

Hardware do cliente Server Encryption

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

Sistemas operacionais do cliente Server Encryption

A tabela a seguir detalha os sistemas operacionais suportados.

Sistemas operacionais (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 a versão 1803 (April 2018 Update/ Redstone 4)

Sistemas operacionais 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 (Server Core não é suportado)
- Windows Server 2012 R2: Standard Edition, Essentials Edition, Datacenter Edition (Server Core não é suportado)
- Windows Server 2016: Standard Edition, Essentials Edition, Datacenter Edition (Server Core não é suportado)

Sistemas operacionais suportados com o modo UEFI

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

NOTA:

Em um computador com suporte a UEFI, após selecionar **Reiniciar** no menu principal, o computador reinicia e, em seguida, mostra uma das duas telas de login possíveis. A tela de login mostrada é determinada por diferenças na arquitetura da plataforma do computador.

Os sistemas operacionais do Encryption External Media

A seguinte tabela detalha os sistemas operacionais suportados ao acessar mídias protegidas pelo Encryption External Media.

NOTA:

A mídia externa precisa ter aproximadamente 55 MB disponíveis, além de espaço livre na mídia igual ao maior arquivo a ser criptografado para hospedar o Encryption External Media.

Sistemas operacionais Windows suportados para acessar mídia protegida por 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 a versão 1803 (April 2018 Update/ Redstone 4)

Sistemas operacionais de servidor suportados

- Windows Server 2012 R2

Sistemas operacionais Mac suportados para acessar mídias protegidas por 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