Dell Data Protection | Encryption

Guia de instalação avançada do Enterprise Edition v8.13

Notas, avisos e advertências

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

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

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

Guia de instalação avançada do Enterprise Edition

2017 - 04

Rev. A01

Índice

1

Introdução

Este guia descreve como instalar e configurar o cliente Encryption, o cliente de gerenciamento de SED, o Advanced Authentication e o BitLocker Manager.

Todas as informações sobre as políticas e suas descrições podem ser encontradas no AdminHelp.

Antes de começar

1 Instale o EE Server/VE Server antes de implantar clientes. Localize o guia correto conforme mostrado abaixo, siga as instruções descritas e retorne para este guia.

- *Guia de instalação e migração do DDP Enterprise Server*
- *Guia de Instalação e de Início Rápido do DDP Enterprise Server – Virtual Edition*

Verifique se as políticas estão definidas conforme desejado. Procure através do AdminHelp, disponível a partir do **?** no canto direito da tela. O AdminHelp é uma ajuda no nível de página desenvolvida para ajudar você a definir e modificar políticas e compreender as suas opções com o EE Server/VE Server.

2 Leia completamente o capítulo Requisitos deste documento.

3 Implemente os clientes para os usuários finais.

Usar este guia

Use este guia na seguinte ordem.

- Consulte Requisitos para obter os pré-requisitos do cliente, as informações sobre o hardware e o software do computador, as limitações e as modificações especiais de registro necessárias para os recursos.
- Caso seja necessário, consulte Configuração de pré-instalação da Senha de uso único, da UEFI da SED e do BitLocker.
- Se os seus clientes forem habilitados usando o Dell Digital Delivery (DDD), consulte Definir GPO no controlador de domínio para ativar a habilitação.
- Se for instalar os clientes usando o instalador mestre do , consulte:
  - Instalar de forma interativa usando o instalador mestre do

    ou
  - Instalar por linha de comando usando o instalador mestre do
- Se for instalar os clientes usando os instaladores filhos, os arquivos executáveis do instalador filho precisam ser extraídos do instalador mestre do . Consulte Extrair os instaladores filhos do instalador mestre e retorne aqui.
  - Instale os instaladores filhos por linha de comando:
    - Instalar drivers - faça download dos drivers e firmware adequados com base em seu hardware de autenticação.
    - Instalar o cliente Encryption - use estas instruções ao instalar o cliente Encryption, que é o componente que impõe a política de segurança, se um computador está conectado à rede, desconectado da rede, perdido ou roubado.
    - Instalar os clientes do SED Management e do Advanced Authentication - use estas instruções para instalar o software de criptografia das unidades de criptografia automática (SED - Self-Encrypting Drive). Embora as SEDs forneçam sua própria criptografia, elas carecem de uma plataforma para gerenciar a criptografia e as políticas. Com o gerenciamento de SED, todas as

políticas, armazenamento e recuperação de chaves de criptografia estão disponíveis a partir de um único console, o que reduz o risco de ter computadores desprotegidos em caso de perda ou de acesso não autorizado.

O cliente Advanced Authentication gerencia múltiplos métodos de autenticação, incluindo a PBA para SEDs, Login único (SSO - Single Sign-On) e credenciais de usuários, como impressões digitais e senhas. Além disso,, fornece os recursos do Advanced Authentication para acessar sites e aplicativos.

- Instalar o cliente BitLocker Manager - use estas instruções para instalar o cliente BitLocker Manager, projetado para melhorar a segurança das implementações do BitLocker e simplificar e reduzir o custo de propriedade.

  NOTA:
  A *maioria* dos instaladores filhos podem ser instalados interativamente; porém, as instalações não são descritas neste guia.

- Consulte Cenários mais utilizados para obter os scripts da maioria dos cenários comumente usados.

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 Data Protection.

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

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

Para obter os números de telefone fora dos Estados Unidos, consulte 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 EE Server/VE Server se os clientes do instalador mestre do forem habilitados 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 posterior) é necessário para o instalador mestre e os clientes secundários do instalador. 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, acesse https://www.microsoft.com/en-us/download/details.aspx?id=42643.
- Os drivers e o firmware para o ControlVault, leitores de impressão digital e cartões inteligentes (conforme mostrado abaixo) não estão incluídos nos arquivos executáveis do instalador filho nem do instalador mestre . 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

  No caso de instalação em hardware que não seja da Dell, faça download dos drivers e do firmware atualizados no site do fornecedor. As instruções de instalação dos drivers do ControlVault são fornecidas em Atualização dos drivers e firmware Dell ControlVault.

Todos os clientes - Hardware

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

Hardware

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

Todos os clientes - Suporte a idiomas

- Os clientes Encryption e BitLocker Manager são compatíveis com interfaces de usuário multi-idiomas (MUI) e suportam os 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)

- Os clientes da unidade de criptografia automática (SED - Self-Encrypting Drive) e do Advanced Authentication são compatíveis com interfaces de usuário multi-idiomas (MUI) e suportam os idiomas a seguir. O Modo UEFI e a Autenticação de pré-inicialização não são suportados em russo, em chinês tradicional e em chinês simplificado.

Suporte a idiomas

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

Cliente Encryption

- O computador cliente 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. Consulte Extrair os instaladores filhos do instalador mestre para obter instruções de extração.
- 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/SLN298707 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 do instala o Microsoft Visual C++ 2012 Update 4 caso não esteja 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)

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 SP0-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 • VMWare Workstation 5.5 e mais recentes

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

Sistemas operacionais do External Media Shield (EMS)

- A seguinte tabela detalha os sistemas operacionais suportados para acesso a mídias protegidas pelo EMS.

  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 EMS.

  NOTA:
  O Windows XP só é suportado ao usar o EMS Explorer.

Sistemas operacionais Windows suportados para acessar mídia protegida por EMS (32 e 64 bits)

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

Sistemas operacionais Mac suportados para acessar mídias protegidas por EMS (kernels de 64 bits)

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

Cliente do 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 Enterprise Edition e o Endpoint Security Suite Enterprise.
- O Server Encryption fornece o seguinte:
  - Há suporte para criptografia de software
  - Criptografia de armazenamento 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 mídias removíveis em servidores protegidos e controlam, por exemplo, acesso e uso das portas USB do servidor por dispositivos USB. A política de portas 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 funcionarão e o usuário não conseguirá 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 foi testado e é compatível com clientes McAfee VirusScan, Symantec, Kaspersky Anti-Virus e MalwareBytes Anti-Malware. 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:

- Dell Data Protection Server ou servidores executando banco de dados do Dell Data Protection Server
- O Server Encryption não é compatível com Endpoint Security Suite, Personal Edition ou Security Tools.
- O Server Encryption não é suportado com cliente do SED Management ou do BitLocker Manager.
- Não há suporte para migração de ou para o Server Encryption. Upgrades do External Media Edition 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)
  - Login 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 upgrade local de sistema operacional no Server Encryption. Para atualizar o sistema operacional, desinstale e descriptografe o Server Encryption, faça a atualização para o novo sistema operacional e então reinstale o Server Encryption.

  Além disso, não há suporte para reinstalações de sistema operacional. Caso queira 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. Para obter mais informações sobre como recuperar dados criptografados, consulte o *Guia de Recuperação*.

Pré-requisitos do cliente do Server Encryption

- Você precisa instalar este componente antes de instalar o cliente do Server Encryption.

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

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 SP0-SP1: Home, Enterprise, Professional, Ultimate
- Windows 8.0: Enterprise, Pro
- Windows 8.1 - Windows 8.1 Update 1: Enterprise Edition, Pro Edition
- Windows 10: Education Edition, Enterprise Edition, Pro Edition

Sistemas operacionais de servidor suportados

- Windows Server 2008 SP2: Standard Edition, Datacenter Edition com e sem Hyper-V, Enterprise Edition com e sem Hyper-V, Foundation Server Edition
- Windows Server 2008 R2 SP1: Standard Edition, Datacenter Edition com e sem Hyper-V, Enterprise Edition com e sem Hyper-V, Foundation Edition, Webserver Edition
- Windows Server 2012: Standard Edition, Essentials Edition, Foundation Edition, Datacenter Edition
- Windows Server 2012 R2: Standard Edition, Essentials Edition, Foundation Edition, Datacenter Edition
- Windows Server 2016: Standard Edition, Essentials Edition, Datacenter Edition

Sistemas operacionais suportados com o modo UEFI

- Windows 8: Enterprise, Pro
- Windows 8.1 - Windows 8.1 Update 1: Enterprise Edition, Pro Edition
- Windows 10: Education Edition, Enterprise Edition, Pro Edition

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.

Sistemas operacionais do External Media Shield (EMS)

A seguinte tabela detalha os sistemas operacionais suportados para acesso a mídias protegidas pelo EMS.

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 EMS.

NOTA:

O Windows XP só é suportado ao usar o EMS Explorer.

Sistemas operacionais Windows suportados para acessar mídia protegida por EMS (32 e 64 bits)

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

Sistemas operacionais de servidor suportados

- Windows Server 2008 SP1 ou posterior
- Windows Server 2012 R2

Sistemas operacionais Mac suportados para acessar mídias protegidas por EMS (kernels de 64 bits)

- OS X Mavericks 10.9.5
- OS X Yosemite 10.10.5
- OS X El Capitan 10.11.4 e 10.11.5

Cliente SED

- O computador precisa ter uma conexão de rede cabeada para instalar satisfatoriamente o SED Management.
- IPv6 não é compatível.
- Esteja preparado para desligar e reiniciar o computador após você aplicar políticas e estar pronto para iniciar a aplicação delas.
- Computadores equipados com unidades de criptografia automática não podem ser usados com placas de HCA. Há incompatibilidades que impedem o provisionamento do HCA. A Dell não comercializa computadores com unidades de criptografia automática que oferecem suporte ao módulo de HCA. Esta configuração não-suportada seria uma configuração de reposição.
- Se o computador destinado para criptografia estiver equipado com uma unidade de criptografia automática, certifique-se de que a opção *O usuário precisa mudar a senha no próximo login* do Active Directory esteja desativada. A Autenticação de pré-inicialização não é compatível com essa opção do Active Directory.
- A DELL recomenda que você não altere o método de autenticação depois que a PBA tiver sido ativada. Se for necessário mudar para um método de autenticação diferente, você precisará:

  - Remova todos os usuários da PBA.

  ou

  - Desative a PBA, altere o método de autenticação e ative novamente a PBA.

  IMPORTANTE:
  Em função da natureza do RAID e das SEDs, o gerenciamento de SED não suporta o RAID. O problema de *RAID=On* com SEDs é que o RAID exige acesso ao disco para ler e gravar dados relacionados ao RAID em um alto setor não disponível em uma SED bloqueada desde o início e não consegue aguardar para ler esses dados até o usuário ter feito login. Altere a operação de SATA no BIOS de *RAID=On* para *AHCI* para resolver o problema. Se o sistema operacional não tiver os drivers de controlador AHCI pré-instalados, o sistema mostrará a tela azul quando alterado de *RAID=On* para *AHCI*.
- O SED Management não é suportado com Server Encryption.

Drivers OPAL

- As SEDs compatíveis com OPAL suportadas exigem drivers da tecnologia Intel Rapid Storage atualizados, localizados em http://www.dell.com/support.

Pré-requisitos do Cliente de SED

- O instalador mestre do instalará o Microsoft Visual C++2010 SP1 **e** o Microsoft Visual C++ 2012 Update 4 caso ainda não estejam instalados no computador. **Quando estiver usando o instalador filho**, você precisará instalar esses componentes antes de instalar o gerenciamento de SED.

Pré-requisitos
• Visual C++ 2010 SP1 ou Redistributable Package mais recente (x86 e x64) • Visual C++ 2012 Update 4 ou Redistributable Package mais recente (x86 e x64)

Hardware do cliente SED

SEDs compatíveis com OPAL

- Para obter a lista mais atualizada de SEDs compatíveis com Opal suportadas com o SED Management, consulte este artigo da base de conhecimento: http://www.dell.com/support/article/us/en/19/SLN296720.

Modelos de computadores Dell compatíveis com UEFI

- A tabela a seguir detalha os modelos de computador Dell compatíveis com UEFI.

Modelos de computador Dell - Suporte para UEFI

- Latitude 5280
- Latitude 5480
- Latitude 5580
- Latitude 7370
- Latitude E5270
- Latitude E5470
- Latitude E5570
- Latitude E7240
- Latitude E7250
- Latitude E7260
- Latitude E7265
- Latitude E7270
- Latitude E7275
- Latitude E7280
- Latitude E7350
- Latitude E7440
- Latitude E7450
- Latitude E7460
- Latitude E7470
- Latitude E7480
- Latitude 12 Rugged Extreme
- Latitude 12 Rugged Tablet (Modelo 7202)
- Latitude 14 Rugged Extreme
- Precision M3510
- Precision M4800
- Precision M5510
- Precision M5520
- Precision M6800
- Precision M7510
- Precision M7520
- Precision M7710
- Precision M7720
- Precision T3420
- Precision T3620
- Precision T7810
- Optiplex 3040 Micro, Minitorre, Fator de forma pequeno
- Optiplex 3046
- OptiPlex 3050 All-In-One
- OptiPlex 3050 Tower, Small Form Factor, Micro
- Optiplex 5040 Minitorre, Fator de forma pequeno
- OptiPlex 5050 Tower, Small Form Factor, Micro
- OptiPlex 7020
- Optiplex 7040 Micro, Minitorre, Fator de forma pequeno
- OptiPlex 7050 Tower, Small Form Factor, Micro
- Optiplex 3240 All-In-One
- OptiPlex 5250 All-In-One
- Optiplex 7440 All-In-One
- OptiPlex 7450 All-In-One
- OptiPlex 9020 Micro
- Venue Pro 11 (Modelos 5175/5179)
- Venue Pro 11 (Modelo 7139)

Modelos de computador Dell - Suporte para UEFI

- Latitude 14 Rugged

> **NOTA:**
> Os recursos de autenticação são compatíveis com o modo UEFI nesses computadores com Windows 8, Windows 8.1 e Windows 10 com SEDs compatíveis com Opal qualificadas. Outros computadores com Windows 7, Windows 8, Windows 8.1 e Windows 10 oferecem suporte para o modo de inicialização preexistente.

Teclados internacionais

- A tabela a seguir mostra os teclados internacionais compatíveis com Autenticação de pré-inicialização em UEFI e computadores não compatíveis com UEFI.

Suporte a teclado internacional - UEFI

- DE-CH - Alemão da Suíça
- DE-FR - Francês da Suíça

Suporte a teclado internacional - Non-UEFI

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

Sistemas operacionais do Cliente de SED

- A tabela a seguir detalha os sistemas operacionais suportados.

Sistemas operacionais Windows (32 e 64 bits)

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

  > **NOTA:**
  > O modo de inicialização herdada é suportado no Windows 7. O UEFI não é suportado no Windows 7.

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

Cliente Advanced Authentication

- Ao usarem o Advanced Authentication, os usuários estarão protegendo o acesso ao computador com o uso de credenciais de autenticação avançadas que são gerenciadas e inscritas usando o Security Tools. O Security Tools se tornará o gerenciador principal das credenciais de autenticação para login no Windows, incluindo, senha, impressão digital e cartões inteligentes do Windows. Senha com imagem, código numérico e impressão digital inscrita usando o sistema operacional da Microsoft não serão reconhecidos durante o login no Windows

  Para continuar usando o sistema operacional Microsoft para gerenciar as credenciais de usuário, não instale ou desinstale o Security Tools.
- O recurso de Senha de uso único (OTP – One-time Password) do Security Tools exige que um TPM esteja presente, ativado e possua um proprietário. O OTP não é suportado com TPM 2.0 . Para limpar e definir a propriedade do TPM, consulte https://technet.microsoft.com.

- Uma SED não exige um TPM para fornecer autenticação avançada ou criptografia.

Hardware do cliente de autenticação avançada

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

Leitores de cartões inteligentes e de impressão digital

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

Cartões sem contato

- Cartões sem contato que usam leitores de cartões sem contato integrados em laptops Dell específicos

Cartões inteligentes

- Cartões inteligentes PKCS #11 usando o cliente ActivIdentity

  NOTA:
  O cliente ActivIdentity não é pré-carregado e precisa ser instalado separadamente.

- Cartões CSP
- Cartões de acesso comum (CACs)
- Cartões Classe B/SIPR Net

- A tabela a seguir detalha os modelos de computador Dell com suporte para cartões SIPR Net.

Modelos de computador Dell - Suporte para cartão Classe B/SIPR Net

- Latitude E6440
- Latitude E6540
- Precision M2800
- Precision M4800
- Precision M6800
- Latitude 14 Rugged Extreme
- Latitude 12 Rugged Extreme
- Latitude 14 Rugged

Sistemas operacionais do cliente de autenticação avançada

Sistemas operacionais Windows

- A tabela a seguir detalha os sistemas operacionais suportados.

Sistemas operacionais Windows (32 e 64 bits)

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

NOTA: O modo UEFI não é suportado no Windows 7.

Sistemas operacionais de dispositivos móveis

- Os seguintes sistemas operacionais móveis são suportados com o recurso de Senha de uso único do Security Tools.

Sistemas operacionais Android

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

Sistemas operacionais iOS

- iOS 7.x
- iOS 8.x

Sistemas operacionais Windows Phone

- Windows Phone 8.1
- Windows 10 Mobile

Cliente BitLocker Manager

- Considere a revisão dos Requisitos do Microsoft BitLocker caso o BitLocker ainda não esteja implementado no ambiente,
- Verifique se a partição de PBA já está configurada. Se o BitLocker Manager for instalado antes de a partição de PBA ser configurada, o BitLocker não poderá ser ativado e o BitLocker Manager não ficará operacional. Consulte Configuração de pré-instalação para configurar uma partição de PBA de BitLocker.
- O teclado, o mouse e os componentes de vídeo precisam estar diretamente conectados ao computador. Não use um interruptor KVM para gerenciar os periféricos, visto que ele pode interferir na capacidade do computador de identificar corretamente o hardware.
- Ligue e ative o TPM. O BitLocker Manager assumirá a propriedade do TPM e não exigirá uma reinicialização. Entretanto, se uma posse do TPM já existir, o BitLocker Manager iniciará o processo de configuração de criptografia (nenhuma reinicialização será necessária). A questão é que o TPM precisa ter um “proprietário” e estar ativado.
- O cliente BitLocker Manager usará os algoritmos validados aprovados para AES FIPS se o modo FIPS estiver ativado para a configuração de segurança GPO "Criptografia do sistema: usar algoritmos em conformidade com FIPS para criptografia, função hash ou assinatura" no dispositivo e você gerenciar esse dispositivo via nosso produto. Nós não forçamos este modo como padrão para clientes criptografados com o BitLocker porque a Microsoft agora sugere que os clientes não usem criptografia validada para FIPS devido aos diversos problemas com compatibilidade de aplicativos, recuperação e criptografia de mídia: http://blogs.technet.com.
- O BitLocker Manager não é suportado com o Server Encryption.

Pré-requisitos do cliente BitLocker Manager

- O instalador mestre do instalará o Microsoft Visual C++2010 SP1 **e** o Microsoft Visual C++ 2012 Update 4 caso ainda não estejam instalados no computador. **Quando estiver usando o instalador filho**, você precisará instalar esses componentes antes de instalar o BitLocker Manager.

Pré-requisitos

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

Sistemas operacionais do cliente BitLocker Manager

- A tabela a seguir detalha os sistemas operacionais suportados.

Sistemas operacionais Windows

- Windows 7 SP0-SP1: Enterprise, Ultimate (32 e 64 bits)
- Windows 8: Enterprise (64 bits)

Sistemas operacionais Windows

- Windows 8.1: Enterprise Edition, Pro Edition (64 bits)
- Windows 10: Education, Enterprise, Pro
- Windows Server 2008 R2: Standard Edition, Enterprise Edition (64 bits)
- Windows Server 2012
- Windows Server 2012 R2: Standard Edition, Enterprise Edition (64 bits)
- Windows Server 2016

Opções de autenticação

- As seguintes opções de autenticação exigem hardware específico: impressões digitais, cartões inteligentes, cartões sem contato, cartões classe B/SIPR Net e autenticação em computadores UEFI. As opções a seguir precisam de configurações: cartões inteligentes com autenticação do Windows, cartões inteligentes com autenticação de pré-inicialização e senha de uso único. As tabelas a seguir mostram as opções de autenticação disponíveis pelo sistema operacional, quando os requisitos de hardware e configuração são atendidos.

Cliente Encryption

Não UEFI

	PBA					Autenticação do Windows				
	Senha	**Impressão digital**	**Cartão inteligente de contato**	**OTP**	**Cartão SIPR**	**Senha**	**Impressão digital**	**Cartão inteligente**	**OTP**	**Cartão SIPR**
Windows 7 SP0-SP1						X	X[2]	X[2]	X[1]	X[2]
Windows 8						X	X[2]	X[2]	X[1]	X[2]
Windows 8.1 Upgrade 0-1						X	X[2]	X[2]	X[1]	X[2]
Windows 10						X	X[2]	X[2]	X[1]	X[2]

1. Disponível quando instalado com o Instalador Mestre ou com o pacote Advanced Authentication ao usar instaladores filhos.

2. Disponível quando os drivers de autenticação forem baixados do site support.dell.com.

UEFI

	PBA - em computadores Dell compatíveis					Autenticação do Windows				
	Senha	**Impressão digital**	**Cartão inteligente de contato**	**OTP**	**Cartão SIPR**	**Senha**	**Impressão digital**	**Cartão inteligente**	**OTP**	**Cartão SIPR**
Windows 7 SP0-SP1										
Windows 8						X	X[2]	X[2]	X[1]	X[2]
Windows 8.1 Upgrade 0-1						X	X[2]	X[2]	X[1]	X[2]
Windows 10						X	X[2]	X[2]	X[1]	X[2]

UEFI

	PBA - em computadores Dell compatíveis					Autenticação do Windows				
	Senha	**Impressão digital**	**Cartão inteligente de contato**	**OTP**	**Cartão SIPR**	**Senha**	**Impressão digital**	**Cartão inteligente**	**OTP**	**Cartão SIPR**

1. Disponível quando instalado com o Instalador Mestre ou com o pacote Advanced Authentication ao usar instaladores filhos.

2. Disponível quando os drivers de autenticação forem baixados do site support.dell.com.

Cliente SED

Não UEFI

	PBA					Autenticação do Windows				
	Senha	**Impressão digital**	**Cartão inteligente de contato**	**OTP**	**Cartão SIPR**	**Senha**	**Impressão digital**	**Cartão inteligente**	**OTP**	**Cartão SIPR**
Windows 7 SP0-SP1	X[2]		X[2 3]			X	X[3]	X[3]	X[1]	X[3]
Windows 8	X[2]		X[2 3]			X	X[3]	X[3]	X[1]	X[3]
Windows 8.1	X[2]		X[2 3]			X	X[3]	X[3]	X[1]	X[3]
Windows 10	X[2]		X[2 3]			X	X[3]	X[3]	X[1]	X[3]

1. Disponível quando instalado com o Instalador Mestre ou com o pacote Advanced Authentication ao usar instaladores filhos.

2. Disponível quando os drivers de autenticação forem baixados do site support.dell.com.

3. Disponível com uma SED com OPAL suportada.

UEFI

	PBA - em computadores Dell compatíveis					Autenticação do Windows				
	Senha	**Impressão digital**	**Cartão inteligente de contato**	**OTP**	**Cartão SIPR**	**Senha**	**Impressão digital**	**Cartão inteligente**	**OTP**	**Cartão SIPR**
Windows 7										
Windows 8	X[4]					X	X[2]	X[2]	X[1]	X[2]
Windows 8.1	X[4]					X	X[2]	X[2]	X[1]	X[2]
Windows 10	X[4]					X	X[2]	X[2]	X[1]	X[2]

1. Disponível quando instalado com o Instalador Mestre ou com o pacote Advanced Authentication ao usar instaladores filhos.

2. Disponível quando os drivers de autenticação forem baixados do site support.dell.com.

4. Disponível com uma SED OPAL compatível em computadores com UEFI suportados.

Gerenciador BitLocker

Não UEFI

	PBA [5]					Autenticação do Windows				
	Senha	**Impressão digital**	**Cartão inteligente de contato**	**OTP**	**Cartão SIPR**	**Senha**	**Impressão digital**	**Cartão inteligente**	**OTP**	**Cartão SIPR**
Windows 7						X	X[2]	X[2]	X[1]	X[2]
Windows 8						X	X[2]	X[2]	X[1]	X[2]
Windows 8.1						X	X[2]	X[2]	X[1]	X[2]
Windows 10						X	X[2]	X[2]	X[1]	X[2]
Windows Server 2008 R2 (64 bits)						X		X[2]		

1. Disponível quando instalado com o Instalador Mestre ou com o pacote Advanced Authentication ao usar instaladores filhos.

2. Disponível quando os drivers de autenticação forem baixados do site support.dell.com.

5. O PIN de pré-inicialização do BitLocker é gerenciado através da funcionalidade da Microsoft.

UEFI

	PBA[5] - em computadores Dell compatíveis					Autenticação do Windows				
	Senha	**Impressão digital**	**Cartão inteligente de contato**	**OTP**	**Cartão SIPR**	**Senha**	**Impressão digital**	**Cartão inteligente**	**OTP**	**Cartão SIPR**
Windows 7										
Windows 8						X	X[2]	X[2]	X[1]	X[2]
Windows 8.1						X	X[2]	X[2]	X[1]	X[2]
Windows 10						X	X[2]	X[2]	X[1]	X[2]
Windows Server 2008 R2 (64 bits)						X		X[2]		

1. Disponível quando instalado com o Instalador Mestre ou com o pacote Advanced Authentication ao usar instaladores filhos.

2. Disponível quando os drivers de autenticação forem baixados do site support.dell.com.

5. O PIN de pré-inicialização do BitLocker é gerenciado através da funcionalidade da Microsoft.

3

Configurações de registro

- Esta seção detalha todas as configurações de registro aprovadas pelo Dell ProSupport para computadores **clientes** locais, independentemente do motivo para a configuração do registro. Se uma configuração de registro envolve dois produtos, ela será apresentada na lista de cada categoria.
- Essas alterações no registro devem ser feitas apenas por administradores e podem não ser adequadas ou podem não funcionar em todos os cenários.

Configurações de registro do cliente Encryption

- Se um certificado autoassinado for usado no Dell Server for Enterprise Edition for Windows, a validação de confiança do certificado precisa permanecer desativada no computador cliente (a validação de confiança é *desativada* por padrão com o Enterprise Edition for Windows). Antes de *ativar* a validação de confiança no computador cliente, os seguintes requisitos precisam ser atendidos.
  - Um certificado assinado por uma autoridade raiz, como EnTrust ou Verisign, precisa ser importado para o EE Server/VE Server.
  - A cadeia completa de confiança do certificado precisa ser armazenada no Microsoft keystore no computador do cliente.
  - Para *ativar* a validação de confiança para EE para Windows, altere o valor da seguinte entrada no registro para 0 no computador cliente.

    [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 usar cartões inteligentes com a autenticação do Windows, o seguinte valor de registro precisará ser configurado no computador cliente:

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

  "MSSmartcardSupport"=dword:1
- Para criar um arquivo de log do Agente de remoção do Encryption, crie a seguinte entrada no Registro no computador que você deseja descriptografar. Consulte (Opcional) Criar um arquivo de log do Agente de remoção de criptografia.

  [HKLM\Software\Credant\DecryptionAgent]

  "LogVerbosity"=dword:2

  0: nenhum registro em log

  1: registra os erros que impedem a execução do Serviço

  2: registra os erros que impedem a descriptografia de dados completa (nível recomendado)

  3: registra as informações sobre todos os volumes e arquivos de descriptografia

  5: registra as informações de depuração

- Por padrão, o ícone da bandeja de sistema será mostrado durante a instalação. Use a seguinte configuração de registro para ocultar o ícone da bandeja de sistema para todos os usuários gerenciados em um computador após a instalação original. Crie ou modifique a configuração do registro como indicado abaixo:

  [HKLM\Software\CREDANT\CMGShield]

  "HIDESYSTRAYICON"=dword:1
- Por padrão, todos os arquivos temporários no diretório c:\windows\temp são automaticamente apagados durante a instalação. A exclusão dos arquivos temporários acelera a criptografia inicial e ocorre antes da varredura de criptografia inicial.

  Entretanto, se a sua organização usa um aplicativo de terceiro que exige que a estrutura de arquivos dentro do diretório \temp seja preservada, você deve evitar esta exclusão.

  Para desativar a exclusão de arquivo temporário, crie ou modifique a configuração de registro da seguinte forma:

  [HKLM\SOFTWARE\CREDANT\CMGShield]

  "DeleteTempFiles"=REG_DWORD:0

  Não apagar os arquivos temporários aumenta o tempo da criptografia inicial.
- O cliente Encryption mostra o prompt de *duração de cada atraso para atualização de política* por cinco minutos de cada vez. Se o usuário não responder ao prompt, o próximo atraso será iniciado. O prompt de atraso final inclui uma contagem regressiva e uma barra de progresso, e é exibido até que o usuário responda, ou o atraso final expirar e o logout ou reinicialização necessários ocorra.

  Você pode alterar o comportamento do prompt de usuário para iniciar ou atrasar a criptografia, para impedir o processamento de criptografia após não obter nenhuma resposta do usuário. Para fazer isso, configure o registro com o seguinte valor:

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

  "SnoozeBeforeSweep"=DWORD:1

  Nenhum valor diferente de zero alterará o comportamento para suspensão. Sem nenhuma interação do usuário, o processamento de criptografia será atrasado até o número de atrasos permitidos configurável. O processamento da criptografia começará quando o atraso final expirar.

  Calcule o máximo possível de atrasos da seguinte forma (um atraso máximo envolveria o usuário nunca responder a um prompt de atraso, cada um do qual é exibido por 5 minutos):

  (NÚMERO DE ATRASOS DE ATUALIZAÇÃO DE POLÍTICA PERMITIDOS × DURAÇÃO DE CADA ATRASO DE ATUALIZAÇÃO DE POLÍTICA) + (5 MINUTOS × [NÚMERO DE ATRASOS DE ATUALIZAÇÃO DE POLÍTICA PERMITIDOS - 1])
- Use a seguinte configuração de registro para que o cliente Encryption pesquise o EE Server/VE Server a fim de obter uma atualização forçada de política. Crie ou modifique a configuração do registro como indicado abaixo:

  [HKLM\SOFTWARE\Credant\CMGShield\Notify]

  "PingProxy"=DWORD value:1

  A configuração de registro desaparecerá automaticamente ao terminar.
- Use as seguintes configurações de registro para permitir que o cliente Encryption envie um inventário otimizado ao EE Server/VE Server, envie um inventário completo ao EE Server/VE Server ou envie um inventário completo de todos os usuários ativados ao EE Server/VE Server.

  - Enviar um inventário otimizado ao EE Server/VE Server:

    Crie ou modifique a configuração do registro como indicado abaixo:

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

    "OnlySendInvChanges"=REG_DWORD:1

Se não houver uma entrada presente, o inventário otimizado será enviado ao EE Server/VE Server.

- Enviar um inventário completo ao EE Server/VE Server:

  Crie ou modifique a configuração do registro como indicado abaixo:

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

  "OnlySendInvChanges"=REG_DWORD:0

  Se não houver uma entrada presente, o inventário otimizado será enviado ao EE Server/VE Server.

- Enviar um inventário completo de todos os usuários ativados

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

  "RefreshInventory"=REG_DWORD:1

  Essa entrada é apagada do registro logo após ser processada. O valor é salvo no cofre, de modo que mesmo que o computador seja reinicializado antes de ocorrer o upload do inventário, o cliente Encryption ainda processará essa solicitação no próximo upload de inventário bem-sucedido.

  Essa entrada substitui o valor de registro OnlySendInvChanges.

- Ativação dividida é um recurso que permite dividir as ativações de clientes ao longo de um período de tempo definido a fim de atenuar a carga do EE Server/VE Server durante uma implementação em massa. As ativações são atrasadas com base nos períodos de tempo gerados algoritmicamente para fornecer uma distribuição regular dos tempos de ativação.

  Para usuários que exigem uma ativação através de VPN, uma configuração de ativação dividida no cliente pode ser necessária, a fim de atrasar a ativação inicial o suficiente para permitir que o cliente VPN estabeleça uma conexão de rede.

  IMPORTANTE:
  Configure a Ativação dividida apenas com a assistência do Dell ProSupport. Uma configuração inadequada do intervalo de tempo pode resultar em um grande número de clientes tentando entrar em contato com o EE Server/VE Server de uma vez, criando, possivelmente, sérios problemas de desempenho.

  Essas entradas de registro exigem que o computador seja reinicializado para que as atualizações sejam aplicadas.

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

    Ativa ou desativa a Ativação dividida

    Desativada=0 (padrão)

    Ativada=1

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

    O período de tempo em segundos do intervalo de ativação. Use essa configuração para sobrepor o período de tempo em segundos do intervalo de ativação. Há 25.200 segundos disponíveis para a divisão das ativações em um período de sete horas. A configuração padrão é de 86.400 segundos, o que representa uma repetição diária.

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

    O intervalo dentro da repetição, ACTIVATION_SLOT_CALREPEAT, para todo o intervalo de tempo de ativação. Apenas um intervalo é permitido. Essa configuração deve ser igual a 0,<CalRepeat>. Um deslocamento igual a 0 pode produzir resultados inesperados. O configuração padrão é 0,86400. Para configurar uma repetição a cada sete horas, use a configuração 0,25200. CALREPEAT é ativado quando um usuário faz o login.

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

    O número de períodos de ativação que podem ser perdidos antes de o computador tentar ativar no próximo login do usuário cuja ativação foi dividida. Se a ativação falhar durante essa tentativa imediata, o cliente retomará as tentativas de ativação dividida. Se a

ativação falhar devido a uma falha de rede, a ativação será tentada após a reconexão da rede, mesmo que o valor em MISSTHRESHOLD não tenha excedido. Se um usuário fizer o logout antes de o tempo de ativação ser atingido, um novo intervalo será atribuído no próximo login.

- [HKCU/Software/CREDANT/ActivationSlot] (dados por usuário)

  O tempo adiado para tentar a ativação dividida, o qual é definido quando o usuário faz o login na rede pela primeira vez depois de habilitar a ativação dividida. O período de ativação é recalculado para cada tentativa de ativação.

- [HKCU/Software/CREDANT/SlotAttemptCount] (dados por usuário)

  Número de tentativas falhas ou perdidas, quando o período de tempo chega e a ativação é tentada, mas falha. Assim que esse número atingir o valor definido em ACTIVATION_SLOT_MISSTHRESHOLD, o computador tentará uma ativação imediata depois de se conectar à rede.

- Para detectar usuários não gerenciados no computador cliente, configure o seguinte valor de registro no computador cliente:

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

  "UnmanagedUserDetected"=DWORD value:1

  Detectar usuários não gerenciados nesse computador = 1

  Não detectar usuários não gerenciados nesse computador = 0

- O acesso à mídia externa criptografada com o External Media Edition pode ser restrito a computadores com acesso ao EE Server/VE Server que produziram as chaves de criptografia com as quais a mídia foi criptografada.

  Este recurso é ativado configurando-se o seguinte registro:

  [HKLM\SYSTEM\CurrentControlSet\Services\EMS]

  "EnterpriseUsage"=dword:0

  Off (default)=0

  Acesso de Arquivo restrito a Empresa=1

  Se este valor for alterado após a criptografia dos arquivos na mídia externa, os arquivos serão recriptografados com base no valor de chave do registro atualizado quando a mídia for conectada ao computador no qual a configuração de registro foi atualizada.

- Para habilitar a reativação automática silenciosa no caso raro de um usuário ficar desativado, o valor do registro a seguir precisa ser definido no computador cliente.

  [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CMGShield]

  "AutoReactivation"=dword:00000001

  0 = Desativado (padrão)

  1 = Ativado

- O System Data Encryption (SDE) é forçado com base no valor da política para as Regras de Criptografia do SDE. Diretórios adicionais são protegidos por padrão quando a política Criptografia do SDE Ativada é selecionada. Para obter mais informações, pesquise as "Regras de Criptografia do SDE" no AdminHelp. Quando o cliente Encryption estiver processando uma atualização de política que inclui uma política do SDE ativa, o diretório de perfil do usuário atual é criptografado por padrão com a chave SDUser (uma chave do usuário) em vez da chave SDE (uma chave do dispositivo). A chave SDUser também é usada para criptografar arquivos ou pastas que são copiados (não movidos) em um diretório do usuário que não é criptografado com o SDE.

  Para desativar a chave SDUser e usar a chave do SDE para criptografar esses diretórios do usuário, crie a seguinte entrada do registro no computador:

  [HKEY_LOCAL_MACHINE\SOFTWARE\Credant\CMGShield]

  "EnableSDUserKeyUsage"=dword:00000000

Se esta chave do registro não estiver presente ou estiver configurada para qualquer outro valor diferente de 0, a chave SDUser será usada para criptografar esses diretórios do usuário.

Para obter mais informações sobre SDUser, consulte www.dell.com/support/article/us/en/19/SLN304916

- Como configurar a entrada do registro, EnableNGMetadata, se ocorrerem problemas relacionados às atualizações da Microsoft em computadores com dados criptografados por chave comum ou ao criptografar, descriptografar ou descompactar vários arquivos de uma pasta.

  Defina a entrada do registro EnableNGMetadata no seguinte local:

  [HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\CmgShieldFFE]

  "EnableNGMetadata" = dword:1

  0 = Desativado (padrão)

  1 = Ativado
- O recurso de ativação fora de domínio pode ser ativado entrando em contato com o Dell ProSupport e solicitando instruções.

Configurações de registro do cliente SED

- Para configurar o intervalo de repetição que será usado quando o EE Server/VE Server estiver indisponível para se comunicar com o cliente de SED, adicione o valor de registro a seguir.

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

  "CommErrorSleepSecs"=dword:300

  Esse valor é o tempo em segundos que o cliente de SED irá esperar para tentar entrar em contato com o EE Server/VE Server caso esteja indisponível para se comunicar com o cliente de SED. O padrão é 300 segundos (5 minutos).
- Se um certificado autoassinado for usado no EE Server/VE Server para gerenciamento de SED, a validação de confiança de SSL/TLS precisa permanecer desativada no computador cliente (a validação de confiança de SSL/TLS é *desativada* por padrão com o gerenciamento de SED). Antes de *ativar* a validação de confiança de SSL/TLS no computador cliente, os seguintes requisitos precisam ser atendidos.
  - Um certificado assinado por uma autoridade raiz, como EnTrust ou Verisign, precisa ser importado para o EE Server/VE Server.
  - A cadeia completa de confiança do certificado precisa ser armazenada no Microsoft keystore no computador do cliente.
  - Para *ativar* a validação de confiança de SSL/TLS para gerenciamento de SED, altere o valor da seguinte entrada no registro para 0 no computador cliente.

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

    "DisableSSLCertTrust"=DWORD:0

    0 = Ativado

    1 = Desativado
- Para usar cartões inteligentes com a autenticação do Windows, o seguinte valor de registro precisará ser configurado no computador cliente:

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

  "MSSmartcardSupport"=dword:1
- Para usar cartões inteligentes com Autenticação de pré-inicialização, o seguinte valor de registro precisa ser configurado no computador do cliente. Configure também a política Método de autenticação para Cartão inteligente no Console de gerenciamento remoto e confirme a alteração.

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

"MSSmartcardSupport"=dword:1

- Para determinar se a PBA está ativada, verifique se o seguinte valor está definido:

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

  "PBAIsActivated"=DWORD (32-bit):1

  O valor 1 significa que a PBA está ativada. O valor 0 significa que a PBA não está ativada.
- Para definir o intervalo no qual o cliente de SED tentará entrar em contato com o EE Server/VE Server quando ele estiver indisponível para se comunicar com o cliente de SED, configure o seguinte valor no computador cliente:

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

  "CommErrorSleepSecs"=DWORD Value:300

  Esse valor é o tempo em segundos que o cliente de SED irá esperar para tentar entrar em contato com o EE Server/VE Server caso esteja indisponível para se comunicar com o cliente de SED. O padrão é 300 segundos (5 minutos).
- O host do Security Server pode ser alterado do local de instalação original, se necessário. As informações de host são lidas pelo computador cliente toda vez que ocorre uma mudança de política. Altere o valor de registro a seguir no computador cliente:

  [HKLM\SYSTEM\CurrentControlSet\services\DellMgmtAgent]

  "ServerHost"=REG_SZ:<newname>.<organization>.com
- A porta do Security Server pode ser alterada do local de instalação original, se necessário. Esse valor é lido pelo computador cliente toda vez que ocorre uma mudança de política. Altere o valor de registro a seguir no computador cliente:

  [HKLM\SYSTEM\CurrentControlSet\services\DellMgmtAgent]

  ServerPort=REG_SZ:8888
- O URL do Security Server pode ser alterado do local de instalação original, se necessário. Esse valor é lido pelo computador cliente toda vez que ocorre uma mudança de política. Altere o valor de registro a seguir no computador cliente:

  [HKLM\SYSTEM\CurrentControlSet\services\DellMgmtAgent]

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

Configurações de registro do cliente Advanced Authentication

- Se você **não** quiser que o cliente Advanced Authentication (Security Tools) altere os serviços associados aos cartões inteligentes e dispositivos biométricos para um tipo de inicialização "automática", desative o recurso de inicialização de serviço. Desativar esse recurso também cancela avisos associados aos serviços necessários que não estão em execução.

  Quando **desativado**, o Security Tools não tentará iniciar estes serviços:

  - SCardSvr – Gerencia o acesso a cartões inteligentes lidos pelo computador. Se esse serviço for interrompido, este computador será incapaz de ler cartões inteligentes. Se esse serviço for desativado, quaisquer serviços que dependerem explicitamente dele não serão iniciados.
  - SCPolicySvc – Permite que o sistema seja configurado para bloquear a área de trabalho do usuário após a remoção do cartão inteligente.
  - WbioSrvc – O serviço biométrico do Windows oferece aos aplicativos de clientes a capacidade de capturar, comparar, manipular e armazenar dados biométricos sem obter acesso direto a nenhum hardware biométrico nem amostras. O serviço é hospedado em um processo privilegiado de SVCHOST.

    Por padrão, se a chave de registro não existir ou se o valor estiver definido como 0, esse recurso é ativado.

    [HKLM\SOFTWARE\DELL\Dell Data Protection]

SmartCardServiceCheck=REG_DWORD:0

0 = Ativado

1 = Desativado

- Para usar cartões inteligentes com a autenticação do Windows, o seguinte valor de registro precisará ser configurado no computador cliente:

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

  "MSSmartcardSupport"=dword:1

- Para usar cartões inteligentes com o recurso SED Preboot Authentication, o seguinte valor de registro precisará ser configurado no computador cliente equipado com uma SED.

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

  "MSSmartcardSupport"=dword:1

  Configure a política Método de autenticação para Cartão inteligente no Console de gerenciamento remoto e confirme a alteração.

Configurações de registro do cliente BitLocker Manager

- Se um certificado autoassinado for usado no EE Server/VE Server para o BitLocker Manager, a validação de confiança de SSL/TLS precisa permanecer desativada no computador cliente (a validação de confiança de SSL/TLS é *desativada* por padrão com o BitLocker Manager). Antes de *ativar* a validação de confiança de SSL/TLS no computador cliente, os seguintes requisitos precisam ser atendidos.
  - Um certificado assinado por uma autoridade raiz, como EnTrust ou Verisign, precisa ser importado para o EE Server/VE Server.
  - A cadeia completa de confiança do certificado precisa ser armazenada no Microsoft keystore no computador do cliente.
  - Para *ativar* a validação de confiança de SSL/TLS para o BitLocker Manager, altere o valor da seguinte entrada no registro para 0 no computador cliente.

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

    "DisableSSLCertTrust"=DWORD:0

    0 = Ativado

    1 = Desativado

4

Instalar usando o instalador mestre do

- Parâmetros e opções de linha de comando fazem distinção entre maiúsculas e minúsculas.
- Para instalar usando portas que não são as portas padrão, use os instaladores filhos em vez do instalador mestre.
- Os arquivos de log do instalador mestre do estão localizados em **C:\ProgramData\Dell\Dell Data Protection\Installer.**
- Oriente os usuários a consultar o documento e os arquivos de ajuda a seguir para obter ajuda com o aplicativo:
  - Consulte a *Ajuda de criptografia Dell* para aprender como usar o recurso do cliente Encryption. Acesse a ajuda em **<Diretório de instalação>:\Program Files\Dell\Dell Data Protection\Encryption\Help**.
  - Consulte a *Ajuda EMS* para aprender sobre os recursos do External Media Shield. Acesse a ajuda em **<Diretório de instalação>:\Program Files\Dell\Dell Data Protection\Encryption\EMS**.
  - Consulte a *Ajuda do Security Tools* para aprender como usar os recursos de Advanced Authentication, . Acesse a ajuda em **<Diretório de instalação>:\Program Files\Dell\Dell Data Protection\Security Tools \Help**.
- Os usuários devem atualizar suas políticas, clicando com o botão direito no ícone do Dell Data Protection na bandeja do sistema e selecionando **Verificar se há atualizações de políticas** depois de a instalação terminar.
- O instalador mestre instala todo o conjunto de produtos. Há dois métodos de instalação usando o instalador mestre do . Escolha um dos métodos a seguir.
  - Instalar de forma interativa usando o instalador mestre do

  ou
  - Instalar por linha de comando usando o instalador mestre do

Instalar de forma interativa usando o instalador mestre do

- O instalador mestre do pode ser localizado em:
  - **support.dell.com** - Se necessário, baixe o software de support.dell.com e, em seguida, extraia os instaladores filhos do instalador mestre do .
  - **Sua conta de FTP na Dell** - Localize o kit de instalação em DDP-Enterprise-Edition-8.x.x.xxx.zip
- Use essas instruções para instalar o Dell Enterprise Edition interativamente usando o instalador mestre . Este método pode ser usado para instalar o conjunto de produtos no computador de uma vez.

1. Localize **DDPSetup.exe** na mídia de instalação da Dell. Copie-o para o computador local.
2. Clique duas vezes em para iniciar o instalador. Isso pode levar vários minutos.
3. Clique em **Avançar** na caixa de diálogo de Boas-vindas.
4. Leia o contrato de licença, aceite os termos e condições e clique em **Avançar**.
5. Selecione **Enterprise Edition** e clique em **Avançar**.

   Marque a caixa de seleção Somente External Media Edition se pretende instalar somente a External Media Edition
6. No campo **Enterprise Server Name** (Nome do Enterprise Server), digite o nome de host totalmente qualificado do EE Server/VE Server que gerenciará o usuário de destino, como server.organization.com.

   No campo **Device Server URL** (URL do Device Server), digite o URL do Device Server (Security Server) com o qual o cliente se comunicará.

   Caso a versão do seu EE Server seja anterior à versão 7.7, o formato será https://server.organization.com:**8081**/xapi.

Caso o seu EE Server seja v7.7 ou mais recente, o formato será https://server.organization.com:**8443**/xapi**/** (incluindo a barra final).

Clique em **Avançar**.

7 Clique em **Avançar** para instalar o produto no local padrão **C:\Program Files\Dell\Dell Data Protection\. A Dell recomenda instalar somente no local padrão**, pois podem ocorrer problemas ao instalar em outros locais.

8 Selecione os componentes a serem instalados.

A opção *Security Framework* instala a estrutura de segurança subjacente e o Security Tools, o cliente de autenticação avançada que gerencia múltiplos métodos de autenticação, incluindo PBA e credenciais como impressões digitais e senhas.

A *Advanced Authentication* (Autenticação avançada) instala os arquivos e serviços necessários para a Autenticação avançada. .

A opção *Encryption* instala o cliente Encryption, o qual impõe a política de segurança, esteja o computador conectado ou não à rede, seja perdido ou roubado.

A opção *BitLocker Manager* instala o cliente do BitLocker Manager, projetado para aprimorar a segurança das implantações do BitLocker simplificando e reduzindo o custo de propriedade através do gerenciamento centralizado das políticas de criptografia do BitLocker.

Clique em **Avançar** quando terminar de selecionar.

9 Clique em **Instalar** para iniciar a instalação. A instalação tomará alguns minutos.

10 Selecione **Sim, quero reiniciar meu computador agora** e clique em **Concluir**.

A instalação está concluída.

Instalar por linha de comando usando o instalador mestre do

- As opções precisam ser especificadas primeiro em uma instalação de linha de comando. Outros parâmetros vão dentro de um argumento que é passado para a opção /v.

Opções

- A tabela a seguir descreve as opções que podem ser usadas com o instalador mestre do .

Opção	Descrição
-y -gm2	Pré-extração do instalador mestre do . As opções -y e -gm2 precisam ser usadas juntas. Não as separe.
/s	Instalação silenciosa
/z	Passa as variáveis para o .msi dentro de DDPSetup.exe

Parâmetros

- A tabela a seguir descreve os parâmetros que podem ser usados com o instalador mestre do .

Parâmetro	Descrição
SUPPRESSREBOOT	Suprime a reinicialização automática após a conclusão da instalação. Pode ser usado no modo SILENCIOSO.
Servidor	Especifica a URL do EE Server/VE Server.
InstallPath	Especifica o caminho da instalação. Pode ser usado no modo SILENCIOSO.
FEATURES	Especifica os componentes que podem ser instalados no modo SILENCIOSO.

Parâmetro	Descrição
	DE = ***Somente*** Drive Encryption (cliente Encryption) EME = somente External Media Edition BLM = BitLocker Manager SED = Gerenciamento de unidade de criptografia automática (EMAgent/Manager, Drivers PBA/GPE)
BLM_ONLY=1	Precisa ser usado em conjunto com o uso de FEATURES=BLM na linha de comando para excluir o plugin de gerenciamento de SED.

Exemplo de linha de comando

- Os parâmetros de linha de comando diferenciam letras maiúsculas de minúsculas.
- Este exemplo instala todos os componentes usando o instalador mestre do em portas padrão, de forma silenciosa, no local padrão **C:\Program Files\Dell\Dell Data Protection**, e o configura para usar o EE Server/VE Server especificado.

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

- Este exemplo instala o gerenciamento de SED e External Media Edition usando o instalador mestre em portas padrão, de forma silenciosa, com reinicialização suprimida, no local padrão **C:\Program Files\Dell\Dell Data Protection**, e o configura para usar o EE Server/VE Server especificado.

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

- Este exemplo instala o gerenciamento de SED e External Media Edition usando o instalador mestre em portas padrão, de forma silenciosa, com reinicialização suprimida, no local padrão **C:\Program Files\Dell\Dell Data Protection**, e o configura para usar o EE Server/VE Server especificado.

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

- Este exemplo instala o gerenciamento de SED e External Media Edition usando o instalador mestre em portas padrão, de forma silenciosa, no local padrão **C:\Program Files\Dell\Dell Data Protection**, e o configura para usar o EE Server/VE Server especificado.

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

- Este exemplo instala o cliente Encryption e BitLocker Manager (sem o plug-in gerenciamento de SED), usando o instalador mestre em portas padrão, de forma silenciosa, no local padrão **C:\Program Files\Dell\Dell Data Protection**, e o configura para usar o EE Server/VE Server especificado.

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

- Este exemplo instala o BitLocker Manager (com o plug-in gerenciamento de SED) e External Media Edition usando o instalador mestre em portas padrão, de forma silenciosa, com reinicialização suprimida, no local padrão **C:\Program Files\Dell\Dell Data Protection**, e o configura para usar o EE Server/VE Server especificado.

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

- Este exemplo instala o BitLocker Manager (sem o plug-in de gerenciamento de SED) e External Media Edition usando o instalador mestre em portas padrão, de forma silenciosa, com reinicialização suprimida, no local padrão **C:\Program Files\Dell\Dell Data Protection **, e o configura para usar o EE Server/VE Server especificado.

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

Desinstalar usando o instalador mestre do

- Cada componente precisa ser desinstalado separadamente, seguido pela desinstalação do instalador mestre do . Os clientes precisam ser desinstalados em uma **ordem específica para evitar falhas de desinstalação**.
- Siga as instruções em Extrair os instaladores filhos do instalador mestre do para obter os instaladores filhos.
- Certifique-se de usar, para a desinstalação, a mesma versão do instalador mestre do (e, por consequência, dos clientes) usada para a instalação.
- Esse capítulo direciona você para outros capítulos que contêm instruções *detalhadas* sobre como desinstalar os instaladores filho. Este capítulo explica **apenas** a última etapa, que desinstala o instalador mestre do .
- Desinstale os clientes na seguinte ordem.

  a Desinstalar o cliente Encryption.

  b Desinstalar SED e clientes de autenticação avançada.

  c Desinstalar o BitLocker Manager Client.

  O pacote de drivers não precisa ser desinstalado.
- Prossiga para Desinstalar o instalador mestre do .

Desinstalar o instalador mestre do

Agora que todos os clientes individuais foram desinstalados, o instalador mestre do pode ser desinstalado.

Desinstalação por linha de comando

- O exemplo a seguir desinstala silenciosamente o instalador mestre do .

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

  Reinicie o computador ao terminar.

Instalar usando os instaladores filhos

- Para instalar cada cliente individualmente, os arquivos executáveis filhos precisam primeiro ser extraídos do instalador mestre do , como mostrado em Extrair os instaladores filhos do instalador mestre do .
- Os exemplos de comandos incluídos nesta seção presumem que eles sejam executados a partir de C:\extracted.
- Parâmetros e opções de linha de comando fazem distinção entre maiúsculas e minúsculas.
- Lembre-se de cercar um valor que contenha um ou mais caracteres especiais, como um espaço em branco na linha de comando, com aspas como caractere de escape.
- Use esses instaladores para instalar os clientes usando uma instalação com scripts, arquivos em lote ou qualquer outra tecnologia push disponível para sua organização.
- A reinicialização foi suprimida nos exemplos de instalação por linha de comando. Entretanto, uma eventual reinicialização é necessária. Não será possível iniciar a criptografia até o computador ser reinicializado.
- Arquivos de log: o Windows cria arquivos de log de instalação do instalador filho exclusivos para o usuário logado em %temp%, localizados em C:\Users\<UserName>\AppData\Local\Temp.

  Se você decidir adicionar um arquivo de log distinto quando executar o instalador, verifique se o arquivo de log tem um nome único, pois os arquivos de log de instalador filho não são acrescidos. O comando .msi padrão pode ser usado para criar um arquivo de log usando /l*v C:\<qualquer diretório>\<qualquer nome de arquivo de log>.log.
- Todos os instaladores filhos usam as mesmas opções de exibição e opções .msi básicas, exceto onde indicado, para as instalações por linha de comando. As opções precisam ser especificadas antes. A opção /v é necessária e utiliza um argumento. Outros parâmetros vão dentro de um argumento que é passado para a opção /v.

  Opções de exibição podem ser especificadas no final do argumento passado para a opção /v para obter o comportamento esperado. Não use /q e /qn na mesma linha de comando. Use apenas ! e - depois de /qb.

Switch	Significado
/v	Passa as variáveis para o .msi dentro de setup.exe. O conteúdo deve estar sempre entre aspas e com texto sem formatação.
/s	Modo silencioso
/x	Modo Desinstalar
/a	Instalação administrativa (copiará todos os arquivos dentro do .msi)

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

Opção	Significado
/q	Não há caixa de diálogo de andamento, reinicia-se após a conclusão do processo
/qb	Caixa de diálogo de andamento com o botão **Cancelar**, solicita a reinicialização
/qb-	Caixa de diálogo de andamento com o botão **Cancelar**, reinicia-se após a conclusão do processo

Opção	Significado
/qb!	Caixa de diálogo de andamento sem o botão **Cancelar**, solicita a reinicialização
/qb!-	Caixa de diálogo de andamento sem o botão **Cancelar**, reinicia-se após a conclusão do processo
/qn	Sem interface do usuário
/norestart	Suprime a reinicialização

- Oriente os usuários a consultar o documento e os arquivos de ajuda a seguir para obter ajuda com o aplicativo:
  - Consulte a *Ajuda de criptografia Dell* para aprender como usar o recurso do cliente Encryption. Acesse a ajuda em **<Install dir>:\Program Files\Dell\Dell Data Protection\Encryption\Help**.
  - Consulte a *Ajuda EMS* para aprender sobre os recursos do External Media Shield. Acesse a ajuda em **<Install dir>:\Program Files\Dell\Dell Data Protection\Encryption\EMS**.
  - Consulte a *Ajuda do Console do DDP* para aprender como usar os recursos de Advanced Authentication,. Acesse a ajuda em **<Install dir>:\Program Files\Dell\Dell Data Protection\Security Tools \Help**.

Instalar drivers

- Os drivers e o firmware para o ControlVault, leitores de impressão digital e cartões inteligentes não estão incluídos nos arquivos executáveis do instalador filho nem do instalador mestre 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

  No caso de instalação em hardware que não seja da Dell, faça download dos drivers e do firmware atualizados no site do fornecedor.

Instalar o cliente Encryption

- Analise os Requisitos do cliente Encryption caso sua organização esteja usando um certificado assinado por uma autoridade raiz, como EnTrust ou Verisign. É necessário fazer uma mudança na configuração do registro do computador cliente para permitir a validação do certificado.
- Os usuários devem atualizar suas políticas, clicando com o botão direito no ícone do Dell Data Protection na bandeja do sistema e selecionando **Verificar se há atualizações de políticas** depois de a instalação terminar.
- O instalador do cliente Encryption está disponível:
  - **support.dell.com** - Se necessário, baixe o software de support.dell.com e, em seguida, extraia os instaladores filhos do instalador mestre do . Após a extração, localize o arquivo em **C:\extracted\Encryption**.
  - **Da sua conta de FTP da Dell** - Localize o kit de instalação em DDP-Enterprise-Edition-8.x.x.xxx.zip e, em seguida, Extraia os instaladores filhos do instalador mestre do . Após a extração, localize o arquivo em **C:\extracted\Encryption**.

Instalação por linha de comando

- A tabela a seguir detalha os parâmetros disponíveis para a instalação.

Parâmetros
SERVERHOSTNAME=<Nome do servidor> (FQDN do Dell Server para reativação)
POLICYPROXYHOSTNAME=<RGKName> (FQDN of the default Policy Proxy)
MANAGEDDOMAIN=<Meu domínio> (Domínio a ser usado pelo dispositivo)
DEVICESERVERURL=<Nome do servidor do dispositivo/Nome do servidor de segurança> (URL usado para ativação, normalmente inclui o nome do servidor, porta e xapi)
GKPORT=<Nova porta GK> (Porta de gatekeeper)
MACHINEID=<Nome da máquina> (Nome do computador)
RECOVERYID=<ID de recuperação> (ID de recuperação)
REBOOT=ReallySuppress (Null ativa a reinicialização automática, ReallySuppress desativa a reinicialização)
HIDEOVERLAYICONS=1 (0 ativa ícones de sobreposição, 1 desativa os ícones de sobreposição)
HIDESYSTRAYICON=1 (0 ativa o ícone systray, 1 desativa o ícone systray)
EME=1 (Instala o External Media Edition)

Para obter uma lista de opções de .msi e opções de exibição básicas que podem ser usadas em linhas de comando, consulte Instalar usando os instaladores filhos.

- A tabela a seguir exibe detalhes de parâmetros opcionais relacionados à ativação.

Parâmetros
SLOTTEDACTIVATON=1 (0 desativa ativações atrasadas/programadas, 1 ativa ativações atrasadas/programadas)
SLOTINTERVAL=30,300 (programa ativações por meio do parâmetro x,x, no qual o primeiro valor é o menor limite de programação e o segundo é o limite máximo, tudo em segundos)
CALREPEAT=300 (DEVE corresponder ou exceder o limite máximo definido em SLOTINTERVAL. Número de segundos que o cliente Encryption aguarda antes de gerar uma tentativa de ativação com base no SLOTINTERVAL.)

Exemplo de linha de comando

- O exemplo a seguir instala o cliente com os parâmetros padrão (cliente Encryption e Encrypt for Sharing (Criptografar para compartilhamento), nenhuma caixa de diálogo, nenhuma barra de andamento, reinicialização automática, no local padrão **C:\Program Files\Dell\Dell Data Protection**).

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

- Substitua `DEVICESERVERURL=https://server.organization.com:`**8081/xapi** (sem a barra final) se a versão do seu EE Server for anterior à 7.7.
- O exemplo a seguir instala o cliente Encryption e Encrypt for Sharing (Criptografar para compartilhamento), oculta o ícone da bandeja de sistema do DDP, oculta os ícones de sobreposição, nenhuma caixa de diálogo, nenhuma barra de andamento, suprime a reinicialização, no local padrão **C:\Program Files\Dell\Dell Data Protection.**

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

```
server.organization.com:8443/xapi/ HIDESYSTRAYICON=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" DEVICESERVERURL="https://server.organization.com:8443/xapi/"
HIDESYSTRAYICON="1" HIDEOVERLAYICONS="1"
```

- Substitua `DEVICESERVERURL=https://server.organization.com:`**8081/xapi** (sem a barra final) se a versão do seu EE Server for anterior à 7.7.

- **Exemplo de linha de comando para instalar apenas o External Media Edition (EME)**

- Instalação silenciosa, nenhuma barra de andamento, reinicialização automática, no local padrão **C:\Program Files\Dell\Dell Data Protection.**

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

- Substitua `DEVICESERVERURL=https://server.organization.com:`**8081/xapi** (sem a barra final) se a versão do seu EE Server for anterior à 7.7.

- Instalação silenciosa, sem reinicialização, no local padrão **C:\Program Files\Dell\Dell Data Protection**)

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

- Substitua `DEVICESERVERURL=https://server.organization.com:`**8081/xapi** (sem a barra final) se a versão do seu EE Server for anterior à 7.7.

> **NOTA:**
> Embora a caixa Sobre no cliente mostre informações sobre o número da versão do software, ela não mostra se um cliente completo está instalado ou se é EME apenas. Para localizar essas informações, acesse **C:\ProgramData\Dell\Dell Data Protection\Encryption\CMGShield.log** e encontre a seguinte entrada:
>
> [<date/timestamp> DeviceInfo: < >] ***Shield Information - SM=External Media Only***, SB=DELL, UNF=FQUN, last sweep={0, 0}

Exemplo de linha de comando para converter o External Media Edition para a versão Shield completa

- A descriptografia não é necessária ao converter o Media Edition para uma versão Shield completa.

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

Comando MSI:

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

- Substitua `DEVICESERVERURL=https://server.organization.com:`**8081/xapi** (sem a barra final) se a versão do seu EE Server for anterior à 7.7.

- **Exemplo de linha de comando para instalar em Deferred Activation**
- O exemplo a seguir instala o cliente com Deferred Activation no local padrão C:\Program Files\Dell\Dell Data Protection

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

Comando MSI:

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

- O exemplo a seguir instala o cliente com Deferred Activation e com parâmetros padrão (cliente Encryption, Criptografar para compartilhamento, nenhuma caixa de diálogo, nenhuma barra de andamento, nenhuma reinicialização, nenhum ícone de sobreposição de criptografia, instalado no local padrão C:\Program Files\Dell\Dell Data Protection).

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

Comando MSI:

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

NOTA:
Alguns clientes mais antigos podem precisar de caracteres de escape, como "\", ao redor dos valores de parâmetros. Por exemplo:

```
DDPE_XXbit_setup.exe /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"
```

Instalar o cliente Server Encryption

Há dois métodos disponíveis para instalar o Server Encryption. Escolha um dos métodos a seguir:

- Instalar o Server Encryption de forma interativa

  NOTA:
  O Server Encryption pode ser instalado de forma interativa apenas em computadores com sistemas operacionais de servidor. A instalação em computadores com sistemas operacionais que não são de servidor precisa ser realizada através da linha de comando, com o parâmetro SERVERMODE=1 especificado.

- Instalar o Server Encryption usando a linha de comando

Conta de usuário virtual

- Como parte da instalação, uma **conta de usuário virtual do servidor** é criada para uso exclusivo do Server Encryption. A autenticação DPAPI e senha são desativadas para que apenas o usuário virtual do servidor possa acessar as chaves de criptografia no computador.

Antes de começar

- A conta de usuário que realiza a instalação precisa ser um usuário de domínio ou local com permissões de nível de administrador.
- Para anular o requisito de que um administrador de domínio ative um Server Encryption ou para executar o Server Encryption em servidores que não são de domínio ou em múltiplos servidores, defina no arquivo application.properties a propriedade ssos.domainadmin.verify como falso. O arquivo é armazenado nos seguintes caminhos de arquivo, baseado no DDP Server que você está usando:

  Dell Enterprise Server - *<pasta de instalação>*/Security Server/conf/application.properties

  Virtual Edition - /opt/dell/server/security-server/conf/application.properties

- O servidor precisa oferecer suporte para controles de porta.

  As políticas de sistema de controle de porta de servidor afetam mídias removíveis em servidores protegidos e controlam, por exemplo, acesso e uso das portas USB do servidor por dispositivos USB. A política de portas 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 funcionarão e o usuário não conseguirá usar o computador, a menos que uma conexão de área de trabalho remota seja configurada antes da política ser aplicada.
- Para ativar satisfatoriamente o Server Encryption, o computador precisa ter conectividade de rede.
- Quando o módulo TPM (Trusted Platform Module - Módulo de plataforma confiável) está disponível, ele é usado para selar a chave GPK no hardware da Dell. Se não houver um módulo TPM disponível, o Server Encryption usa a API de proteção de dados da Microsoft (DPAPI) para proteger a chave para finalidades gerais.

  NOTA:
  Quando você for instalar um novo sistema operacional em um computador Dell com TPM executando o Server Encryption, desmarque o TPM no BIOS. Consulte https://technet.microsoft.com/en-us/library/cc749022%28v=ws.10%29.aspx#BKMK_S2 para obter instruções.

Extrair o instalador filho

- O Server Encryption precisa apenas de um dos instaladores encontrados no instalador mestre. Para instalar o Server Encryption, primeiro você precisa extrair o instalador filho do cliente do Encryption, o **DDPE_xxbit_setup.exe**, do instalador mestre. Consulte Extrair os instaladores filhos do instalador mestre.

Instalar o Server Encryption de forma interativa

- Use estas instruções para instalar o Server Encryption de forma interativa. Esse instalador inclui os componentes necessários para a criptografia de software.

1 Localize o arquivo **DDPE_XXbit_setup.exe** na pasta C:\extracted\Encryption. Copie-o para o computador local.
2 Se estiver instalando o Server Encryption em um servidor, clique duas vezes no arquivo **DDPE_XXbit_setup.exe** para abrir o instalador.

   NOTA:
   Quando o Server Encryption for instalado em um computador que executa um sistema operacional de servidor, como o Windows Server 2012 R2, o instalador instala o Encryption, por padrão, no modo Servidor.

3 Na caixa de diálogo Bem-vindo, clique em **Avançar**.
4 Na tela Contrato de licença, leia o contrato de licença, concorde com os termos e clique em **Avançar**.
5 Clique em **Avançar** para instalar o Server Encryption no local padrão.

   NOTA:
   A Dell recomenta instalar no local padrão. Não é recomendado realizar sua instalação em um local diferente do padrão, seja em um diretório diferente, na unidade D ou em uma unidade USB.

6 Clique em **Avançar** para ir para a caixa de diálogo **Tipo de gerenciamento**.
7 No campo Nome do Dell Enterprise Server, digite o nome de host totalmente qualificado do Dell Enterprise Server ou Virtual Edition que gerenciará o usuário de destino (por exemplo, *server.organization.com*).
8 Digite o nome do domínio no campo **Domínio gerenciado** (exemplo, organização) e clique em **Avançar**.
9 Clique em **Avançar** para ignorar a caixa de diálogo **Informações do Dell Policy Proxy** preenchida automaticamente.
10 Clique em **Avançar** para ignorar a caixa de diálogo **Informações do Dell Device Server** preenchida automaticamente.
11 Clique em **Instalar** para iniciar a instalação.
   A instalação pode levar vários minutos.
12 Clique em Concluir na caixa de diálogo **Configuração concluída**.

A instalação está concluída.

NOTA:
O arquivo de log da instalação está localizado no diretório %temp% da conta, em **C:\Users\<nome do usuário>\AppData\Local\Temp**. Para localizar o arquivo de log do instalador, procure por um nome de arquivo que comece com as letras MSI e termine com a extensão .log. O arquivo deve ter uma marca de hora/data que corresponda ao horário no qual você executou o instalador.

NOTA:
Como parte da instalação, uma **conta de usuário virtual do servidor** é criada para uso exclusivo do Server Encryption. A autenticação DPAPI e senha são desativadas para que apenas o usuário virtual do servidor possa acessar as chaves de criptografia no computador.

13 Reinicie o computador.

IMPORTANTE: Escolha a opção Adiar reinicialização somente se você precisar de tempo para salvar seu trabalho e encerrar aplicativos em execução.

Instalar o Server Encryption usando a linha de comando

Cliente do Server Encryption - localize o instalador em C:\extracted\Encryption

- Use **DDPE_xxbit_setup.exe** para instalar ou fazer upgrade usando uma instalação com scripts, arquivos de lotes ou qualquer outra tecnologia push disponível para sua organização.

Switches

A tabela a seguir detalha os switches disponíveis para a instalação.

Switch	Significado
/v	Passa variáveis para o .msi dentro de DDPE_XXbit_setup.exe
/a	Instalação administrativa
/s	Modo silencioso

Parâmetros

A tabela a seguir detalha os parâmetros disponíveis para a instalação.

Componente	Arquivo de log	Parâmetros de linha de comando
Todos	/l*v [caminhocompleto] [nomedoarquivo].log *	SERVERHOSTNAME=<nome do servidor de gerenciamento>
		SERVERMODE=1
		POLICYPROXYHOSTNAME=<Nome RGK>
		MANAGEDDOMAIN=<Meu domínio>
		DEVICESERVERURL=<Nome do servidor de ativação>
		GKPORT=<Nova porta GK>
		MACHINEID=<Nome da máquina>

Componente	Arquivo de log	Parâmetros de linha de comando
		RECOVERYID=<ID de recuperação>
		REBOOT=ReallySuppress
		HIDEOVERLAYICONS=1
		HIDESYSTRAYICON=1
		EME=1

NOTA:
Embora a reinicialização possa ser suprimida, uma reinicialização eventual será necessária. Não será possível iniciar a criptografia até o computador ser reinicializado.

Opções

A tabela a seguir detalha as opções de exibição que podem ser especificadas ao final do argumento passado para o switch /v.

Opção	Significado
/q	Não há caixa de diálogo de andamento, reinicia-se após a conclusão do processo
/qb	Caixa de diálogo de andamento com o botão **Cancelar**, solicita a reinicialização
/qb-	Caixa de diálogo de andamento com o botão **Cancelar**, reinicia-se após a conclusão do processo
/qb!	Caixa de diálogo de andamento sem o botão **Cancelar**, solicita a reinicialização
/qb!-	Caixa de diálogo de andamento sem o botão **Cancelar**, reinicia-se após a conclusão do processo
/qn	Sem interface do usuário

NOTA:
Não use **/q** e **/qn** na mesma linha de comando. Use apenas **!** e - depois de **/qb**.

- O parâmetro de linha de comando, SERVERMODE=1, só é seguido durante novas instalações. O parâmetro é ignorado para desinstalações.
- Não é recomendado realizar sua instalação em um local diferente do padrão, seja em um diretório diferente, em uma unidade diferente da unidade C: ou em uma unidade USB. A Dell recomenta instalar no local padrão.
- Cerque um valor que contenha um ou mais caracteres especiais, como um espaço em branco, com aspas com caractere de escape.
- O URL do Dell Activation Server (DEVICESERVERURL) faz distinção entre maiúsculas e minúsculas.

Exemplo de instalação por linha de comando

- O exemplo a seguir instala o cliente do Server Encryption com os parâmetros padrão (cliente do Server Encryption, instalação silenciosa, Encrypt for Sharing, sem caixa de diálogo, sem barra de andamento, reinicialização automática, instalado no local padrão de C:\Arquivos de Programas\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 seguinte exemplo instala o cliente do Server Encryption com um arquivo de log e parâmetros padrão (cliente do Server Encryption, instalação silenciosa, criptografar para compartilhamento, sem caixa de diálogo, sem barra de andamento, sem reinicialização, instalado no local padrão de **C:\Arquivos de Programas\Dell\Dell Data Protection\Encryption)** e especifica um nome personalizado de arquivo de log terminado com um número (DDP_ssos-090.log) que deve ser incrementado se a linha de comando for executada mais de uma vez no mesmo servidor.

  ```
  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/ /l*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/" /l*v
  DDP_ssos-090.log /norestart/qn"
  ```

  Para especificar um local para o log diferente do local padrão onde o arquivo executável está localizado, forneça o caminho completo no comando. Por exemplo, **/l*v C:\Logs\DDP_ssos-090.log** criará logs de instalação em uma pasta **C:\Logs**.

Reinicie o computador.

Depois da instalação, reinicie o computador. O computador precisa ser reiniciado assim que possível.

IMPORTANTE:

Escolha a opção **Adiar reinicialização** somente se você precisar de tempo para salvar seu trabalho e encerrar aplicativos em execução.

Ativar o Server Encryption

- O servidor precisa estar conectado à rede da sua organização.
- Verifique se o nome do computador no servidor é o nome do endpoint que você quer ver no Remote Management Console.
- Para que a ativação inicial ocorra, é preciso que um usuário interativo em tempo real faça login no servidor com credenciais de administrador de domínio no mínimo uma vez. O usuário conectado pode ser de qualquer tipo, domínio ou não domínio, conectado por desktop remoto ou usuário interativo no servidor, no entanto, a ativação precisa das credenciais de administrador de domínio.
- Seguindo a reinicialização após a instalação, a caixa de diálogo Ativação é mostrada. O administrador precisa digitar as credenciais de administrador de domínio com um nome de usuário no formato UPN (User Principal Name - Nome principal do usuário). O cliente do Server Encryption não é ativado automaticamente.
- Durante a ativação inicial, uma conta de usuário virtual do servidor é criada. 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 atribuído ao computador um ID de computador único, as chaves de criptografia são criadas e agregadas, e uma relação é estabelecida entre o pacote de chaves de criptografia e o usuário virtual do servidor. O pacote de chaves de criptografia associa as políticas e chaves de criptografia ao novo usuário virtual do servidor para criar uma relação permanente entre os dados criptografados, o computador específico e o usuário virtual do servidor. Depois da ativação do dispositivo, o usuário virtual do servidor aparece no Remote Management Console como SERVER-USER@*<nome de servidor totalmente qualificado>*. Para obter mais informações sobre a ativação, consulte Ativação em um sistema operacional de servidor.

NOTA:

Se você renomear o servidor após a ativação, seu nome de exibição não será alterado no Remote Management Console. Entretanto, se o cliente do Server Encryption for ativado novamente depois de alterar o nome do servidor, o novo nome do servidor aparecerá no Remote Management Console.

Uma caixa de diálogo Ativação é mostrada uma vez após cada reinicialização para solicitar que o usuário ative o Server Encryption. Se a ativação ainda não foi concluída, execute este procedimento:

1 Faça login no servidor diretamente no servidor ou usando uma conexão de área de trabalho remota.

2 Clique com o botão direito no ícone do Encryption  na bandeja do sistema e clique em **Sobre**.

3 Verifique se o Encryption está sendo executado no modo Servidor.

4 Selecione **Ativar Encryption** no menu.

5 Digite o nome de usuário de um administrador de domínio no formato UPN e a senha e clique em **Ativar**. Essa é a mesma caixa de diálogo de ativação que aparece toda vez que um sistema não ativado é reiniciado.

O DDP Server emite uma chave de criptografia para o ID do computador, cria a **conta de usuário virtual do servidor**, cria uma chave de criptografia para a conta de usuário, agrupa as chaves de criptografia e cria a relação entre o pacote de criptografia e a conta de usuário virtual do servidor.

6 Clique em **Fechar**.

Após a ativação, a criptografia será iniciada.

7 Depois de terminar a varredura da criptografia, reinicie o computador para processar todos os arquivos que estavam anteriormente em uso. Essa é uma etapa importante para fins de segurança.

> **NOTA:**
> Se a política *Credenciais seguras do Windows* estiver definida como Verdadeiro, o Server Encryption criptografa os arquivos da pasta **\Windows\system32\config**, incluindo as credenciais do Windows. Os arquivos na pasta **\Windows \system32\config** são criptografados mesmo que a política *Criptografia SDE ativada* esteja **Não selecionada**. Por padrão, a política *Credenciais seguras do Windows* é **Selecionada**.

> **NOTA:**
> Depois de reiniciar o computador, a autenticação do material de chave Comum *sempre* exige a chave Computador do servidor protegido. O DDP Server retorna uma chave de desbloqueio para acessar as políticas e chaves de criptografia no cofre. As chaves e as políticas são voltadas ao servidor, não ao usuário. Sem a chave Computador do servidor, a chave de criptografia de arquivo Comum não pode ser desbloqueada e o computador não pode receber atualizações de política.

Confirmar a ativação

No console local, abra a caixa de diálogos Sobre para confirmar que o Server Encryption está instalado, autenticado e no modo Servidor. Se o Shield ID estiver **vermelho**, a criptografia ainda não foi ativada.

Usuário virtual do servidor

- No Remote Management Console, um servidor protegido pode ser encontrado sob o nome do computador. Além disso, cada servidor protegido tem sua própria conta de usuário virtual do servidor. Toda conta possui um nome de usuário estático e um nome de computador único.
- A conta de usuário virtual do servidor só é usada pelo Server Encryption e, em outros casos, é transparente para a operação do servidor protegido. O usuário virtual do servidor é associado com o pacote de chaves de criptografia e o Policy Proxy.
- Após a ativação, a conta de usuário virtual do servidor é a conta de usuário que é ativada e associada ao servidor.
- Após a ativação da conta de usuário virtual do servidor, todas as notificações de login/log off do servidor serão ignoradas. Em vez disso, durante a inicialização, o computador autentica automaticamente com o usuário virtual do servidor e depois baixa a chave Computador do Dell Data Protection Server.

Instalar clientes SED Management e Advanced Authentication

- O cliente SED é necessário para a Advanced Authentication em v8.x.
- Analise os Requisitos do cliente SED caso sua organização esteja usando um certificado assinado por uma autoridade raiz, como EnTrust ou Verisign. Será necessário alterar a configuração de registro no computador cliente para ativar a validação de confiança de SSL/TLS.

- Os usuários fazem login na PBA usando suas credenciais do Windows.
- Os instaladores dos clientes SED e Advanced Authentication estão disponíveis em:
  - **support.dell.com** - Se necessário, baixe o software de support.dell.com e, em seguida, extraia os instaladores filhos do instalador mestre do . Após a extração, localize o arquivo em **C:\extracted\Security Tools** e **C:\extracted\Security Tools\Authentication**.
  - **Da sua conta de FTP da Dell** - Localize o kit de instalação em DDP-Enterprise-Edition-8.x.x.xxx.zip e, em seguida, Extraia os instaladores filhos do instalador mestre do . Após a extração, localize o arquivo em **C:\extracted\Security Tools** e **C:\extracted \Security Tools\Authentication**.

Instalação por linha de comando

- A tabela a seguir detalha os parâmetros disponíveis para a instalação.

Parâmetros
CM_EDITION=1 <gerenciamento remoto>
INSTALLDIR=<altera o destino da instalação>
SERVERHOST=<securityserver.organization.com>
SERVERPORT=8888
SECURITYSERVERHOST=<securityserver.organization.com>
SECURITYSERVERPORT=8443
ARPSYSTEMCOMPONENT=1 <nenhuma entrada na lista de programas do Painel de controle>

Para obter uma lista de opções de .msi e opções de exibição básicas que podem ser usadas em linhas de comando, consulte Instalar usando os instaladores filhos.

Exemplo de linha de comando

\Security Tools

- O exemplo a seguir instala a SED gerenciada remotamente (instalação silenciosa, nenhuma reinicialização, nenhuma entrada na lista de programas do Painel de controle, no local padrão 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"
```

Em seguida:

\Security Tools\Authentication

- O exemplo a seguir instala o Advanced Authentication (instalação silenciosa, nenhuma reinicialização)

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

Instalar o cliente BitLocker Manager

- Analise os Requisitos do cliente BitLocker Manager caso sua organização esteja usando um certificado assinado por uma autoridade raiz, como EnTrust ou Verisign. Será necessário alterar a configuração de registro no computador cliente para ativar a validação de confiança de SSL/TLS.
- Os instaladores do cliente BitLocker Manager podem ser localizados em:
  - **support.dell.com** - Se necessário, baixe o software de support.dell.com e, em seguida, extraia os instaladores filhos do instalador mestre do . Após a extração, localize o arquivo em **C:\extracted\Security Tools**.

- **Da sua conta de FTP da Dell** - Localize o kit de instalação em DDP-Enterprise-Edition-8.x.x.xxx.zip e, em seguida, Extraia os instaladores filhos do instalador mestre do . Após a extração, localize o arquivo em **C:\extracted\Security Tools**.

Instalação por linha de comando

- A tabela a seguir detalha os parâmetros disponíveis para a instalação.

Parâmetros
CM_EDITION=1 <gerenciamento remoto>
INSTALLDIR=<altera o destino da instalação>
SERVERHOST=<securityserver.organization.com>
SERVERPORT=8888
SECURITYSERVERHOST=<securityserver.organization.com>
SECURITYSERVERPORT=8443
FEATURE=BLM <instalar apenas o BitLocker Manager>
FEATURE=BLM,SED <instalar o BitLocker Manager com SED>
ARPSYSTEMCOMPONENT=1 <nenhuma entrada na lista de programas do Painel de controle>

Para obter uma lista de opções de .msi e opções de exibição básicas que podem ser usadas em linhas de comando, consulte Instalar usando os instaladores filhos.

Exemplo de linha de comando

- O exemplo a seguir instala apenas o BitLocker Manager (instalação silenciosa, nenhuma reinicialização, nenhuma entrada na lista de programas do Painel de controle, no local padrão **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 a seguir instala o BitLocker Manager com SED (instalação silenciosa, nenhuma reinicialização, nenhuma entrada na lista de programas do Painel de controle, no local padrão **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"
```

Desinstalar usando os instaladores filhos

- Para desinstalar cada cliente individualmente, os arquivos executáveis filhos precisam primeiro ser extraídos do instalador mestre do , como mostrado em Extrair os instaladores filhos do instalador mestre do . Como alternativa, execute uma instalação administrativa para extrair o .msi.
- Certifique-se de que as mesmas versões dos clientes usadas na instalação sejam usadas na desinstalação.
- Parâmetros e opções de linha de comando fazem distinção entre maiúsculas e minúsculas.
- Lembre-se de cercar um valor que contenha um ou mais caracteres especiais, como um espaço em branco na linha de comando, com aspas como caractere de escape. Os parâmetros de linha de comando diferenciam letras maiúsculas de minúsculas.
- Use esses instaladores para desinstalar os clientes usando uma instalação com scripts, arquivos em lote ou qualquer outra tecnologia push disponível para sua organização.
- Arquivos de log: o Windows cria arquivos de log de desinstalação do instalador filho exclusivos para o usuário logado em %temp%, localizados em **C:\Users\<UserName>\AppData\Local\Temp.**

  Se você decidir adicionar um arquivo de log distinto quando executar o instalador, verifique se o arquivo de log tem um nome único, pois os arquivos de log de instalador filho não são acrescidos. O comando padrão .msi pode ser usado para criar um arquivo de log usando /l **C:\<qualquer diretório>\<qualquer nome de arquivo de log>.log**. A Dell não recomenda usar "/l*v" (registro em log detalhado) em uma desinstalação por linha de comando, pois o nome de usuário e a senha são gravados no arquivo de log.
- Todos os instaladores filho usam as mesmas opções de exibição e opções .msi básicas, exceto onde indicado, para desinstalações de linha de comando. As opções precisam ser especificadas antes. A opção /v é necessária e utiliza um argumento. Outros parâmetros vão dentro de um argumento que é passado para a opção /v.

  Opções de exibição podem ser especificadas no final do argumento passado para a opção /v para obter o comportamento esperado. Não use /q e /qn na mesma linha de comando. Use apenas ! e - depois de /qb.

Switch	Significado
/v	Passa as variáveis para o .msi dentro de setup.exe. O conteúdo deve estar sempre entre aspas e com texto sem formatação.
/s	Modo silencioso
/x	Modo Desinstalar
/a	Instalação administrativa (copiará todos os arquivos dentro do .msi)

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

Opção	Significado
/q	Não há caixa de diálogo de andamento, reinicia-se após a conclusão do processo
/qb	Caixa de diálogo de andamento com o botão **Cancelar**, solicita a reinicialização
/qb-	Caixa de diálogo de andamento com o botão **Cancelar**, reinicia-se após a conclusão do processo
/qb!	Caixa de diálogo de andamento sem o botão **Cancelar**, solicita a reinicialização

Opção	Significado
/qb!-	Caixa de diálogo de andamento sem o botão **Cancelar**, reinicia-se após a conclusão do processo
/qn	Sem interface do usuário

Desinstalar o cliente Encryption e Server Encryption

- Para reduzir o tempo de descriptografia, execute o assistente de Limpeza de Disco do Windows para remover arquivos temporários e outros dados desnecessários.
- Planeje realizar a descriptografia durante a noite, se possível.
- Desative o modo de suspensão para impedir que um computador sem supervisão entre em modo de suspensão. A descriptografia não pode ocorrer em um computador em modo de suspensão.
- Feche todos os processos e aplicativos para reduzir as falhas de descriptografia devido a arquivos bloqueados.
- Depois que a desinstalação estiver concluída e a descriptografia estiver em execução, desative toda a conectividade de rede. Caso contrário, novas políticas que reativem a criptografia poderão ser adquiridas.
- Siga seu processo existente para descriptografar dados, como emitir uma atualização de política.
- O Windows e o EME Shields atualizam o EE Server/VE Server para mudar o status para *Desprotegido* no início de um processo de desinstalação do Shield. Entretanto, caso o cliente não consiga entrar em contato com o EE Server/VE Server, independentemente do motivo, o status não poderá ser atualizado. Nesse caso, você precisará *Remover o endpoint* manualmente no Remote Management Console. Caso sua organização use esse fluxo de trabalho para fins de conformidade, a Dell recomenda que você verifique se a opção *Desprotegido* foi configurada conforme esperado, seja no Remote Management Console ou no Compliance Reporter.

Processo

- **Antes de iniciar o processo de desinstalação**, consulte (Opcional) Criar um arquivo de log do Agente de remoção de criptografia. Este arquivo de log é útil para solucionar problemas de uma operação de desinstalação/descriptografia. Se você não pretende descriptografar arquivos durante o processo de desinstalação, não é necessário criar um arquivo de log do Agente de remoção de criptografia.
- O Key Server (e o EE Server) precisa ser configurado antes da desinstalação no caso do uso da opção **Fazer download de chaves do servidor do Encryption Removal Agent**. Consulte Configurar o Key Server para desinstalação do cliente Encryption ativado no EE Server para obter instruções. Não é necessário realizar nenhuma ação antes disso se o cliente a ser desinstalado estiver ativado em um VE Server, uma vez que o VE Server não usa o Key Server.
- Você precisa usar o Dell Administrative Utility (CMGAd) antes de iniciar o Encryption Removal Agent se estiver usando a opção **Importar chaves de um arquivo do Encryption Removal Agent**. Esse utilitário é usado para obter o pacote de chaves de criptografia. Consulte Usar o Administrative Download Utility (CMGAd) para obter instruções. O utilitário pode ser encontrado na mídia de instalação Dell.
- Execute o WSScan para garantir que todos os dados sejam descriptografados após a conclusão da desinstalação, mas antes de reiniciar o computador. Consulte Usar WSScan para obter instruções.
- Periodicamente Verificar o status do Agente de remoção de criptografia. A descriptografia de dados ainda estará em andamento se o serviço Encryption Removal Agent ainda estiver no painel Serviços.

Desinstalação por linha de comando

- Once extracted from the master installer, the Encryption client installer can be located at **C:\extracted\Encryption \DDPE_XXbit_setup.exe**.
- A tabela a seguir detalha os parâmetros disponíveis para a desinstalação.

Parâmetro	Seleção
CMG_DECRYPT	Propriedade para selecionar o tipo de instalação do Encryption Removal Agent:

Parâmetro	Seleção
	3 - Use o pacote LSARecovery 2 - Use o material de chave forense previamente baixado 1 - Fazer download das chaves do Dell Server 0 - Não instalar o Agente de remoção de criptografia
CMGSILENTMODE	Propriedade de desinstalação silenciosa: 1 - Silenciosa 0 - Não silenciosa
Propriedades necessárias	
DA_SERVER	FQHN para o EE Server que hospeda a sessão de negociação.
DA_PORT	Porta no EE Server para solicitação (o padrão é 8050).
SVCPN	Nome de usuário, no formato UPN, ao qual o serviço do Key Server está conectado no EE Server.
DA_RUNAS	Contexto do nome de usuário no formato compatível com SAM em que a solicitação de extração de chave será feita. Esse usuário precisa estar na lista do Key Server no EE Server.
DA_RUNASPWD	Senha do usuário runas.
FORENSIC_ADMIN	A conta de administrador forense no Dell Server, que pode ser usada para solicitações forenses para desinstalações ou chaves.
FORENSIC_ADMIN_PWD	A senha da conta de administrador forense.
Propriedades opcionais	
SVCLOGONUN	Nome de usuário no formato UPN para login no serviço Encryption Removal Agent como parâmetro.
SVCLOGONPWD	Senha para login como usuário.

- O exemplo a seguir desinstala silenciosamente o cliente Encryption e faz download das chaves de criptografia do EE Server.

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

  Comando MSI:

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

  Reinicie o computador ao terminar.

- O exemplo a seguir desinstala silenciosamente o cliente Encryption e faz download das chaves de criptografia usando 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 ao terminar.

IMPORTANTE:

A Dell recomenda as seguintes ações quando você usar uma senha de administrador forense na linha de comando:

1. Criar uma conta de Administrador forense no Console de gerenciamento remoto para fazer a desinstalação silenciosa.
2. Usar uma senha temporária para essa conta que seja exclusiva dessa conta e desse período.
3. Após o término da desinstalação silenciosa, remova a conta temporária da lista de administradores ou altere sua senha.

NOTA:

Alguns clientes mais antigos podem precisar de caracteres de escape, como "\", ao redor dos valores de parâmetros. Por exemplo:

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

Desinstalar External Media Edition

Once extracted from the master installer, the Encryption client installer can be located at C:\extracted\Encryption \DDPE_XXbit_setup.exe.

Desinstalação por linha de comando

Execute um comando de linha de comando semelhante ao seguinte:

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

Reinicie o computador ao terminar.

Desinstalar clientes SED e Advanced Authentication

- É preciso ter uma conexão de rede com o EE Server/VE Server para desativar o recurso PBA.

Processo

- Desative o PBA, o que vai remover todos os dados de PBA do computador e desbloquear as chaves da SED.
- Desinstalar o cliente SED.
- Desinstalar o cliente de autenticação avançada.

Desativar o PBA

1. Como um administrador Dell, faça login no Remote Management Console.
2. No painel esquerdo, clique em > **Proteger e gerenciar endpoints**.
3. Selecione o Tipo de endpoint apropriado.
4. Selecione Mostrar >*Visível*, *Oculto* ou *Todos*.
5. Se você souber o nome de host do computador, digite-o no campo Nome de host (há suporte para caracteres curinga). Você pode deixar o campo em branco para ver todos os computadores. Clique em **Pesquisar**.

Se você não souber o nome de host, navegue pela lista para localizar o computador.

Um computador ou uma lista de computadores é mostrado com base em seu filtro de pesquisa.

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

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

8 Selecione **Unidades de criptografia automática** no menu **Categoria de política**.

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

10 Clique em **Salvar**.

11 No painel à esquerda, clique em **Ações** > **Confirmar políticas**.

12 Clique em **Aplicar alterações**.

Aguarde a política ser propagada a partir do EE Server/VE Server para o computador de destino para fazer a desativação.

Desinstale os clientes de autenticação e SED após o PBA ser desativado.

Desinstalar o cliente de SED e os clientes Advanced Authentication

Desinstalação por linha de comando

- Depois de extraído do instalador mestre do , o instalador do cliente SED pode ser localizado em C:\extracted\Security Tools \EMAgent_XXbit_setup.exe.
- Depois de extraído do instalador mestre do , o instalador do cliente SED pode ser encontrado em C:\extracted\Security Tools \Authentication\<x64/x86>\setup.exe.
- O exemplo a seguir desinstala silenciosamente o cliente SED.

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

  Desligue e reinicie o computador ao terminar.

Em seguida:

- O exemplo a seguir desinstala silenciosamente o cliente de autenticação avançada.

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

  Desligue e reinicie o computador ao terminar.

Desinstalar o cliente BitLocker Manager

Desinstalação por linha de comando

- Depois de extraído do instalador mestre do , o instalador do cliente BitLocker pode ser localizado em C:\extracted\Security Tools \EMAgent_XXbit_setup.exe.
- O exemplo a seguir desinstala silenciosamente o cliente BitLocker Manager.

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

  Reinicie o computador ao terminar.

8

Cenários mais utilizados

- Para instalar cada cliente individualmente, os arquivos executáveis filhos precisam primeiro ser extraídos do instalador mestre do , como mostrado em Extrair os instaladores filhos do instalador mestre do .
- O cliente de SED é necessário para o Advanced Authentication na v8.x, e é por isso que ele faz parte da linha de comando nos exemplos a seguir.
- Parâmetros e opções de linha de comando fazem distinção entre maiúsculas e minúsculas.
- Lembre-se de cercar um valor que contenha um ou mais caracteres especiais, como um espaço em branco na linha de comando, com aspas como caractere de escape.
- Use esses instaladores para instalar os clientes usando uma instalação com scripts, arquivos em lote ou qualquer outra tecnologia push disponível para sua organização.
- A reinicialização foi suprimida nos exemplos de instalação por linha de comando. Entretanto, uma eventual reinicialização é necessária. Não será possível iniciar a criptografia até o computador ser reinicializado.
- Arquivos de log: o Windows cria arquivos de log de instalação do instalador filho exclusivos para o usuário logado em %temp%, localizados em **C:\Users\<UserName>\AppData\Local\Temp.**

  Se você decidir adicionar um arquivo de log distinto quando executar o instalador, verifique se o arquivo de log tem um nome único, pois os arquivos de log de instalador filho não são acrescidos. O comando .msi padrão pode ser usado para criar um arquivo de log usando /l*v **C:\<any directory>\<any log file name>.log**.
- Todos os instaladores filhos usam as mesmas opções de exibição e opções .msi básicas, exceto onde indicado, para as instalações por linha de comando. As opções precisam ser especificadas antes. A opção /v é necessária e utiliza um argumento. Outros parâmetros vão dentro de um argumento que é passado para a opção /v.

  Opções de exibição podem ser especificadas no final do argumento passado para a opção /v para obter o comportamento esperado. Não use /q e /qn na mesma linha de comando. Use apenas ! e - depois de /qb.

Switch	Significado
/v	Passa as variáveis para o .msi dentro do *.exe
/s	Modo silencioso
/i	Modo de instalação

Opção	Significado
/q	Não há caixa de diálogo de andamento, reinicia-se após a conclusão do processo
/qb	Caixa de diálogo de andamento com o botão **Cancelar**, solicita a reinicialização
/qb-	Caixa de diálogo de andamento com o botão **Cancelar**, reinicia-se após a conclusão do processo
/qb!	Caixa de diálogo de andamento sem o botão **Cancelar**, solicita a reinicialização
/qb!-	Caixa de diálogo de andamento sem o botão **Cancelar**, reinicia-se após a conclusão do processo
/qn	Sem interface do usuário

- Oriente os usuários a consultar o documento e os arquivos de ajuda a seguir para obter ajuda com o aplicativo:
  - Consulte a *Ajuda de criptografia Dell* para aprender como usar o recurso do cliente Encryption. Acesse a ajuda em **<Install dir>:\Program Files\Dell\Dell Data Protection\Encryption\Help**.
  - Consulte a *Ajuda EMS* para aprender sobre os recursos do External Media Shield. Acesse a ajuda em **<Install dir>:\Program Files\Dell\Dell Data Protection\Encryption\EMS**.
  - Consulte a *Ajuda do Security Tools* para aprender como usar os recursos de Advanced Authentication, . Acesse a ajuda em **<Install dir>:\Program Files\Dell\Dell Data Protection\Security Tools \Help**.

Cliente Encryption e Advanced Authentication

- O exemplo a seguir instala a SED gerenciada remotamente (instalação silenciosa, nenhuma reinicialização, nenhuma entrada na lista de programas do Painel de controle, no local padrão **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"
  ```

  Em seguida:
- O exemplo a seguir instala a Advanced Authentication (instalação silenciosa, nenhuma reinicialização, no local padrão **C:\Program Files\Dell\Dell Data Protection\Authentication**).

  ```
  setup.exe /s /v"/norestart /qn ARPSYSTEMCOMPONENT=1"
  ```
- O exemplo a seguir instala o cliente Encryption com os parâmetros padrão (cliente Encryption, Encrypt for Sharing, nenhuma caixa de diálogo, nenhuma barra de andamento, nenhuma reinicialização, no local padrão **C:\Program Files\Dell\Dell Data Protection**).

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

  Substitua `DEVICESERVERURL=https://server.organization.com:` **8081/xapi** (sem a barra final) se a versão do seu EE Server for anterior à 7.7.

Cliente SED (incluindo Advanced Authentication) e cliente Encryption

- O exemplo a seguir instala os drivers para Pilha de software confiável (TSS, Trusted Software Stack) para o TPM e hotfixes da Microsoft no local especificado, não cria uma entrada na lista de programas do Painel de controle e suprime a reinicialização.

  Esses drivers precisam ser instalados ao instalar o cliente Encryption.

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

  Em seguida:
- O exemplo a seguir instala a SED gerenciada remotamente (instalação silenciosa, nenhuma reinicialização, nenhuma entrada na lista de programas do Painel de controle, instalada no local padrão **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"
  ```

  Em seguida:
- O exemplo a seguir instala a Advanced Authentication (instalação silenciosa, nenhuma reinicialização, no local padrão **C:\Program Files\Dell\Dell Data Protection\Authentication**).

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

  Em seguida:

- O exemplo a seguir instala o cliente com os parâmetros padrão (cliente Encryption, Criptografar para compartilhamento, nenhuma caixa de diálogo, nenhuma barra de andamento, nenhuma reinicialização, instalado no local padrão **C:\Program Files\Dell\Dell Data Protection**).

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

  Substitua `DEVICESERVERURL=https://server.organization.com:`**8081/xapi** (sem a barra final) se a versão do seu EE Server for anterior à 7.7.

Cliente SED (incluindo Advanced Authentication) e External Media Shield

- O exemplo a seguir instala a SED gerenciada remotamente (instalação silenciosa, sem reinicialização, nenhuma entrada na lista de programas do Painel de controle, no local padrão **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"
  ```

  Em seguida:

- O exemplo a seguir instala a Advanced Authentication (instalação silenciosa, sem reinicialização, no local padrão **C:\Program Files\Dell\Dell Data Protection\Authentication**).

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

  Em seguida:

- O exemplo a seguir instala apenas o EMS (instalação silenciosa, sem reinicialização, no local padrão **C:\Program Files\Dell\Dell Data Protection**).

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

  Substitua `DEVICESERVERURL=https://server.organization.com:`**8081/xapi** (sem a barra final) se a versão do seu EE Server for anterior à 7.7.

BitLocker Manager e External Media Shield

- O exemplo a seguir instala o BitLocker Manager (instalação silenciosa, nenhuma reinicialização, nenhuma entrada na lista de programas do Painel de controle, no local padrão **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 a seguir instala apenas o EMS (instalação silenciosa, nenhuma reinicialização e instalado no local padrão **C:\Program Files\Dell\Dell Data Protection**).

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

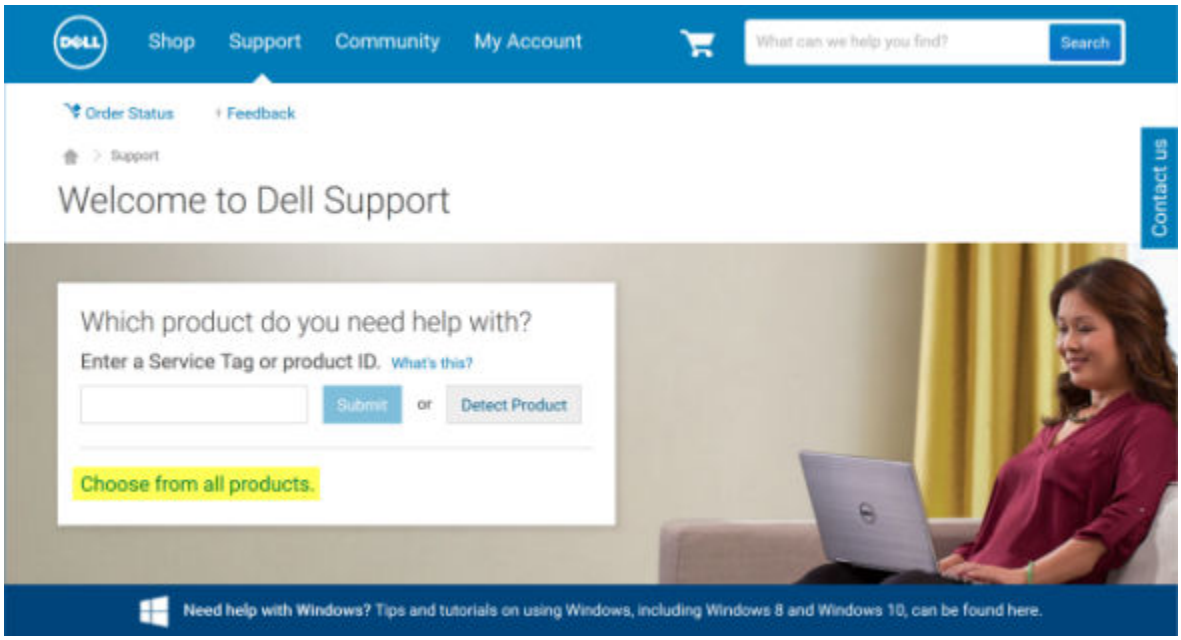
Substitua `DEVICESERVERURL=https://server.organization.com:`**8081/xapi** (sem a barra final) se a versão do seu EE Server for anterior à 7.7.

Faça o download do software

Esta seção detalha as informações sobre como obter o software em dell.com/support. Se você já tiver o software, você pode ignorar esta seção.

Acesse dell.com/support para começar.

1 Na página Suporte Dell, selecione **Escolha entre todos os produtos**.



2 Selecione **Software e segurança** da lista de produtos.

3 Selecione **Soluções de segurança de ponto de extremidade** na seção *Software e segurança*.
Depois de fazer essa seleção uma vez, o site se lembrará.

4 Selecione o produto Dell Data Protection.
Exemplos:

Dell Encryption

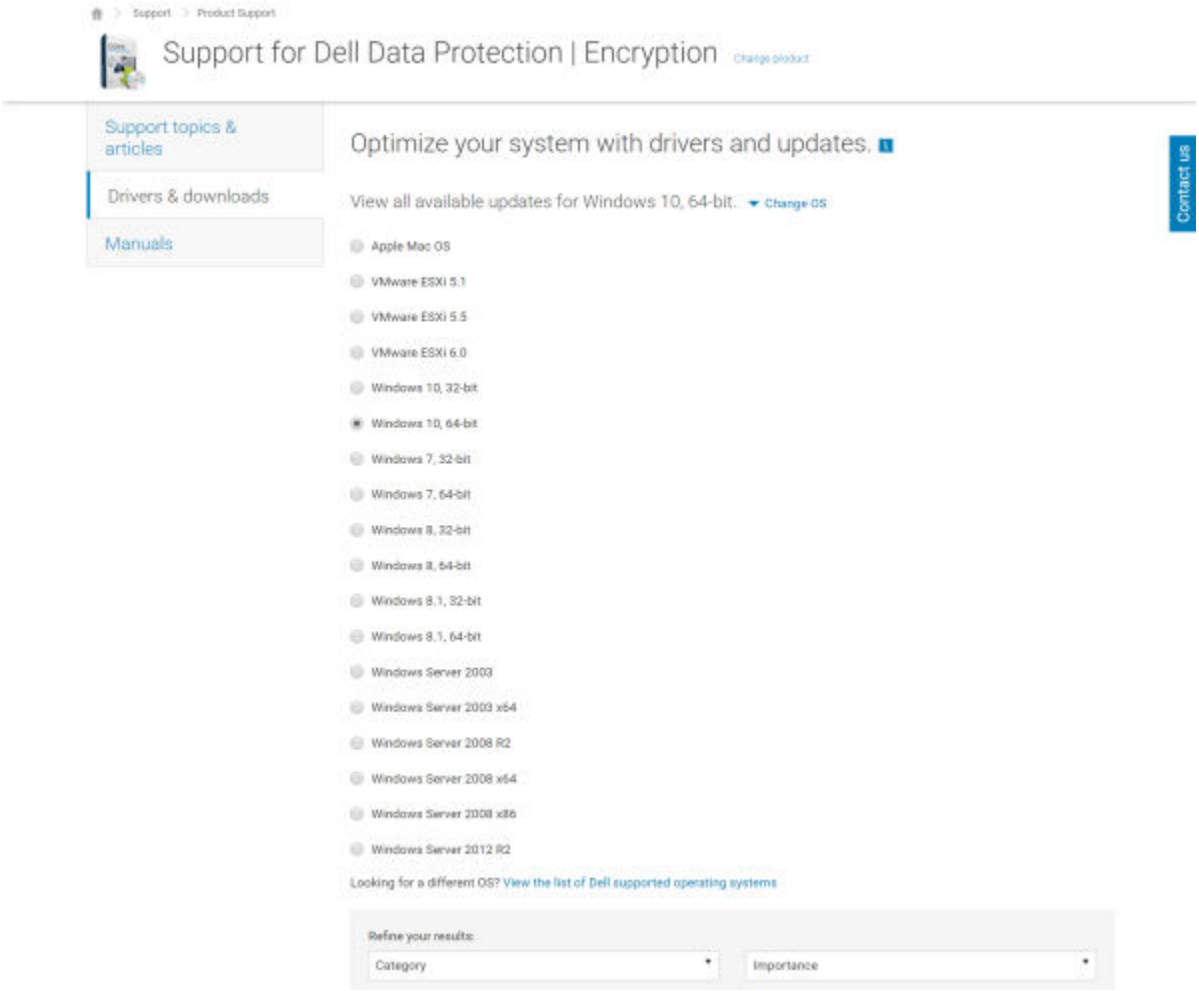
Dell Endpoint Security Suite

Dell Endpoint Security Suite Enterprise

5 Selecione **Drivers e downloads**.

6 Selecione o tipo de sistema operacional do cliente desejado.

7 Selecione **Dell Data Protection (4 arquivos)** no resultado. A sequência descrita acima é apenas um exemplo, por isso, pode ser um pouco diferente. Por exemplo, pode ser que não haja 4 arquivos para você escolher.



8 Selecione **Fazer download de arquivo** ou **Adicionar à lista de download nº XX**.

Configuração de pré-instalação para senha de uso único, SED UEFI e BitLocker

Inicializar o TPM

- É preciso ser membro do grupo de administradores locais ou ter função equivalente.
- O computador precisa estar equipado com BIOS e módulo TPM compatíveis.

Essa tarefa é necessária se você estiver usando uma senha de uso único (OTP).

- Siga as instruções disponíveis em http://technet.microsoft.com/en-us/library/cc753140.aspx.

Configuração de pré-instalação para computadores com UEFI

Ativar a conectividade de rede durante a Autenticação de pré-inicialização em computadores com UEFI

Para a autenticação de pré-inicialização ser bem-sucedida em um computador com firmware de UEFI, o recurso PBA precisa ter conectividade de rede. Por padrão, os computadores com firmware de UEFI não têm conectividade de rede até que o sistema operacional seja carregado, o que ocorre após o modo de PBA.

O procedimento a seguir ativa a conectividade de rede durante a PBA para computadores habilitados para UEFI. Como as etapas de configuração variam de um modelo de computador com UEFI para outro, o procedimento a seguir é apenas um exemplo.

1 Inicialize na configuração de firmware de UEFI.
2 Pressione F2 continuamente durante a inicialização até aparecer uma mensagem no canto superior direito da tela, similar a "preparando o menu da inicialização a ser executada uma única vez".
3 Digite a senha de administrador do BIOS, se for solicitado.

> **NOTA:**
> Em geral, você não verá esse prompt se este for um computador novo, visto que a senha do BIOS ainda não foi configurada.

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

> **NOTA:**
> Computadores *sem* firmware de UEFI não precisam dessa configuração.

Desativar ROMs de opção preexistentes

Verifique se a configuração de **Ativar ROMs de opção preexistentes** está desativada no BIOS.

1 Reinicie o computador.
2 Quando a reinicialização começar, pressione **F12** repetidamente para abrir as configurações de inicialização do computador com UEFI.
3 Pressione a seta para baixo, realce a opção **Configurações do BIOS** e pressione **Enter**.
4 Selecione **Configurações** > **Geral** > **Opções avançadas de inicialização**.
5 Desmarque a caixa de seleção **Ativar ROMs de opção preexistentes** e clique em **Aplicar**.

Configuração de pré-instalação para configurar uma partição de PBA de BitLocker

- Você precisa 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 assumirá a propriedade do TPM (uma reinicialização não será necessária). Entretanto, se a posse do TPM já existir, o BitLocker Manager iniciará o processo de configuração de criptografia. A questão é que o TPM precisa ter um "dono".
- Pode ser necessário particionar o disco manualmente. Consulte a descrição da Microsoft para a Ferramenta de preparação de unidade BitLocker para obter mais informações.
- Use o comando BdeHdCfg.exe para criar a partição de PBA. O parâmetro padrão indica que a ferramenta de linha de comando seguirá o mesmo processo do assistente de Configuração do BitLocker.

```
BdeHdCfg -target default
```

DICA:
Para conhecer mais opções disponíveis para o comando BdeHdCfg, consulte Referência de parâmetros de BdeHdCfg.exe da Microsoft.

Configurar GPO no controlador de domínio para ativar direitos

- Se os seus clientes forem habilitados no Dell Digital Delivery (DDD), siga estas instruções para definir o GPO no controlador de domínio para ativar a habilitação (esse pode não ser o mesmo servidor que executa o EE Server/VE Server).
- A estação de trabalho precisa ser membro do OU em que o GPO é aplicado.

> **NOTA:**
> Verifique se a porta de saída 443 está disponível para se comunicar com o EE Server/VE Server. Se a porta 443 estiver bloqueada por qualquer motivo, a funcionalidade de habilitação não funcionará.

1. No Controlador de domínio, para gerenciar os clientes, clique em **Iniciar** > **Ferramentas administrativas** > **Gerenciamento de política de grupo**.
2. Clique com o botão direito na OU (Organizational unit - unidade organizacional) em que a política deverá ser aplicada e selecione **Criar um GPO neste domínio** e **Vinculá-lo aqui...**.
3. Digite um nome para o novo GPO, selecione "nenhum" para o Source Starter GPO (GPO de iniciador de origem) e clique em **OK**.
4. Clique com o botão direito no GPO que foi criado e selecione **Editar**.
5. O Editor de gerenciamento de política de grupo é carregado. Acesse **Configuração do computador** > **Preferências** > **Configurações do Windows** > **Registro**.
6. Clique com o botão direito no Registro e selecione **Novo** > **Registry Item (Item de registro)**. Complete o seguinte:

   Action: Create

   Hive: HKEY_LOCAL_MACHINE

   Key Path: SOFTWARE\Dell\Dell Data Protection

   Value name: Server

   Value type: REG_SZ

   Value data: <Endereço IP do EE Server/VE Server>
7. Clique em **OK**.
8. Faça logout e depois login na estação de trabalho ou execute **gpupdate /force** para aplicar a política de grupo.

Extrair os instaladores filhos do instalador mestre do

- Para instalar cada cliente individualmente, extraia os arquivos executáveis filhos do instalador.
- O instalador mestre do não é um *desinstalador* mestre. Cada cliente precisa ser desinstalado individualmente, seguido pela desinstalação do instalador mestre do . Use esse processo para extrair os clientes do instalador mestre do para que possam ser usados para desinstalação.

1 A partir da mídia de instalação da Dell, copie o arquivo para o computador local.

2 Abra um prompt de comando no mesmo local em que se encontra o arquivo **DDPSetup.exe** e digite:

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

O caminho de extração não pode ter mais de 63 caracteres.

Antes de começar a instalação, certifique-se de que todos os pré-requisitos foram atendidos e que todos os softwares necessários foram instalados para cada instalador filho que você planeja instalar. Consulte Requisitos para obter detalhes.

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

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

- Esta seção explica como configurar os componentes para uso com autenticação/autorização Kerberos usando um EE Server. O VE Server não usa o Key Server.

  O Servidor de chaves é um serviço que escuta os clientes conectarem em um soquete. Assim que um cliente se conecta, uma conexão segura é negociada, autenticada e criptografada usando APIs Kerberos (se uma conexão segura não puder ser negociada, o cliente será desconectado).

  Em seguida, o Servidor de chaves verifica com o Security Server (anteriormente conhecido como Device Server) se o usuário que está executando o cliente tem permissão para acessar as chaves. Este acesso é concedido no Remote Management Console através de domínios individuais.
- Se a autorização/autenticação do Kerberos for usada, então o servidor que contém o componente do Servidor de chaves terá de fazer parte do domínio afetado.
- Uma vez que o VE Server não usa o Key Server, a desinstalação típica é afetada. Quando um cliente Encryption ativado em um VE Server é desinstalado, a recuperação de chave forense padrão através do Security Server é usada, em vez do método Kerberos do Key Server. Consulte Desinstalação por linha de comando para obter mais informações.

Painel Serviços - Adicionar usuário da conta de domínio

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

2 Clique com o botão direito no Key Server e selecione **Propriedades**.

3 Selecione a guia Login e, em seguida, a opção **Esta conta:**.

  No campo *Esta conta:*, adicione o usuário da domínio de domínio. Este usuário do domínio precisa ter no mínimo direitos de administrador local na pasta do servidor de chaves (ele precisar poder gravar no arquivo de configuração do servidor de chaves, e poder gravar no arquivo log.txt.).

  Digite e confirme a senha para o usuário de domínio.

  Clique em **OK**

4 Reinicie o serviço do Key Server (deixe o painel Serviços aberto para continuar a operação).

5 Navegue até <Diretório de instalação do servidor de chaves> log.txt para verificar se o serviço foi iniciado corretamente.

Arquivo de configuração do servidor de chaves - Adicionar usuário para comunicação com o EE Server

1 Navegue até <Diretório de instalação do servidor de chaves>.

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

3 Vá para <add key="user" value="superadmin" /> e altere o valor "superadmin" para o nome do usuário apropriado (você também pode deixar como "superadmin").

O formato "superadmin" pode ser qualquer método que puder autenticar no EE Server. O nome de conta SAM, UPN ou domínio \nome de usuário são aceitáveis. Qualquer método que puder autenticar no EE Server é aceitável porque a validação é necessária para essa conta de usuário de autorização em relação ao Active Directory.

Por exemplo, em um ambiente multidomínio, a simples digitação de um nome de conta SAM, como "jdoe", provavelmente falhará, pois o EE Server não poderá autenticar "jdoe" porque não conseguirá encontrar "jdoe". Em um ambiente multi-domínio, o UPN é recomendado, apesar do formato domínio\nome de usuário ser aceitável. Em um ambiente de domínio único, o nome da conta SAM é aceitável.

4 Vá até <add key="epw" value="<valor criptografado da senha>" /> e altere "epw" para "senha". Depois altere "<valor criptografado da senha>" para a senha do usuário na etapa 3. Esta senha será criptografada novamente quando o EE Server for reiniciado.

Se estiver usando "superadmin" na etapa 3 e a senha superadmin não for "changeit", ela precisará ser alterada aqui. Salve e feche o arquivo.

Exemplo de arquivo de configuração

<?xml version="1.0" encoding="utf-8" ?>

<configuration>

<appSettings>

<add key="port" value="8050" /> [porta TCP à qual o servidor de chaves Dell escutará. O padrão é 8050.]

<add key="maxConnections" value="2000" /> [número de conexões ativas de soquete que o Servidor de chaves Dell permitirá]

<add key="url" value="https://keyserver.domain.com:8443/xapi/" /> [Dell Device Server URL (o formato é 8081/xapi para um pré-v7.7 EE Enterprise Server)]

<add key="verifyCertificate" value="false" /> [o valor true verifica certificados/definir para false para não verificar ou se estiver usando certificados autoassinado]

<add key="user" value="superadmin" /> [Nome de usuário usado para se comunicar com o Servidor de dispositivo Dell. Este usuário precisa ter a função de administrador selecionada no Console de gerenciamento remoto. O formato "superadmin" pode ser qualquer método que puder autenticar no EE Server. O nome de conta SAM, UPN ou domínio\nome de usuário são aceitáveis. Qualquer método que puder autenticar no EE Server é aceitável porque a validação é necessária para essa conta de usuário de autorização em relação ao Active Directory. Por exemplo, em um ambiente multidomínio, a simples digitação de um nome de conta SAM, como "jdoe", provavelmente falhará, pois o EE Server não poderá autenticar "jdoe" porque não conseguirá encontrar "jdoe". Em um ambiente multi-domínio, o UPN é recomendado, apesar do formato domínio\nome de usuário ser aceitável. Em um ambiente de domínio único, o nome da conta SAM é aceitável.]

<add key="cacheExpiration" value="30" /> [Com que frequência (em segundos) o Service deve verificar para ver quem está autorizado a pedir as chaves. O serviço mantém um cache e registra quantos tempo tem. Assim que o cache for mais velho do que o valor, ele obterá uma nova lista. Quando um usuário se conecta, o servidor de chaves precisa baixar os usuários autorizados do Security Server. Se não houver um cache desses usuários ou a lista não foi baixada nos últimos "x" segundos, ela será baixada novamente. Não há sondagem, mas esse valor configura o quão obsoleta a lista pode se tornar antes de ser atualizada quando for necessária.]

<add key="epw" value="valor criptografado da senha" /> [Senha usada para se comunicar com o servidor de segurança. Se senha superadmin tiver sido alterada, ela precisará ser alterada aqui.]

</appSettings>

</configuration>

Painel Serviços - Reiniciar o serviço do servidor de chaves

1 Volte para o painel Serviços (Iniciar > Executar... > services.msc > OK).
2 Reinicie o serviço do Key Server.
3 Navegue até <Diretório de instalação do servidor de chaves> log.txt para verificar se o serviço foi iniciado corretamente.
4 Feche o painel Serviços.

Remote Management Console - Adicionar administrador forense

1 Se necessário, faça login no Remote Management Console.
2 Clique em **Populações** > **Domínios**.
3 Selecione o domínio adequado.
4 Clique na guia **Key Server**.
5 No campo Account (Conta), adicione o usuário que realizará as atividades de administrador. O formato é DOMÍNIO\Nome de usuário. Clique em **Adicionar conta**.
6 Clique em **Usuários** no menu à esquerda. Na caixa de pesquisa, procure o nome de usuário adicionado na Etapa 5. Clique em **Search** (Pesquisar).
7 Assim que o usuário correto for localizado, clique na guia **Admin**.
8 Selecione **Administrador forense** e clique em **Atualizar**.

Agora os componentes estão configurados para a autorização/autenticação do Kerberos.

Usar o utilitário de download administrativo (CMGAd)

- Este utilitário possibilita fazer download de um pacote de materiais de chaves para uso em um computador não conectado a um EE Server/VE Server.
- O utilitário usa um dos métodos a seguir para fazer download de um pacote de chaves, dependendo do parâmetro de linha de comando passado ao aplicativo:
  - Forensic Mode (Modo forense) - Usado se "-f" for incluído na linha de comando ou se nenhum parâmetro de linha de comando for usado.
  - Admin Mode (Modo administrativo) - Usado se "-a" for incluído na linha de comando.

    Os arquivos de log podem ser encontrados em C:\ProgramData\CmgAdmin.log

Usar o utilitário de download administrativo no modo forense

1 Clique duas vezes em **cmgad.exe** para abrir o utilitário ou abra um prompt de comando onde o CMGAd está localizado e digite **`cmgad.exe -f`** (ou **`cmgad.exe`**).

2 Digite as informações a seguir (alguns campos podem já estar preenchidos).

URL do servidor de dispositivos: URL do Security Server (Device Server) totalmente qualificado. O formato é https://securityserver.domain.com:8443/xapi/. Caso o seu EE Server seja pré-v7.7, o formato é https://deviceserver.domain.com:8081/xapi (número de porta diferente, sem a barra).

Administrador da Dell: nome do administrador com credenciais de administrador forense (habilitado no Remote Management Console), por exemplo, jdoe

Senha: senha do administrador forense

MCID: ID da máquina, por exemplo, machineID.domain.com

DCID: Oito primeiros dígitos da ID Shield de 16 dígitos

> **DICA:**
> Normalmente, especificar o MCID *ou* DCID é suficiente. No entanto, se você souber ambos, é útil digitar os dois. Cada parâmetro contém diferentes informações sobre o cliente e o computador cliente.

Clique em **Next** (Avançar).

3 No campo Passphrase: (Senha:), digite uma senha para proteger o arquivo de download. A senha deve ter no mínimo oito caracteres e conter pelo menos um caractere alfabético e um numérico. Confirme a senha.

Aceite o nome e o local padrão onde o arquivo será salvo ou clique em ... para selecionar um local diferente.

Clique em **Next** (Avançar).

Uma mensagem indicando que o material de chave foi desbloqueado corretamente é mostrada. Os arquivos estão acessíveis agora.

4 Clique em **Concluir** quando terminar.

Usar o utilitário de download administrativo no modo administrativo

O VE Server não usa o Key Server, de forma que o modo administrativo não pode ser usado para obter um pacote de chaves de um VE Server. Use o modo forense para obter um pacote de chaves se o cliente estiver ativado em um VE Server.

1 Abra um prompt de comando onde o CMGAd está localizado e digite **`cmgad.exe -a`**.

2 Digite as informações a seguir (alguns campos podem já estar preenchidos).

Servidor: nome de Host totalmente qualificado do Key Server, por exemplo, keyserver.domain.com

Número da porta: a porta padrão é 8050

Conta de servidor: o usuário de domínio com o qual o Key Server está sendo executado. O formato é domínio\nome de usuário. O usuário de domínio executando o utilitário precisa estar autorizado a fazer download no Key Server

MCID: ID da máquina, por exemplo, machineID.domain.com

DCID: oito primeiros dígitos da ID Shield de 16 dígitos

> **DICA:**
> Normalmente, especificar o MCID *ou* DCID é suficiente. No entanto, se você souber ambos, é útil digitar os dois. Cada parâmetro contém diferentes informações sobre o cliente e o computador cliente.

Clique em **Next** (Avançar).

3 No campo Passphrase: (Senha:), digite uma senha para proteger o arquivo de download. A senha deve ter no mínimo oito caracteres e conter pelo menos um caractere alfabético e um numérico.

Confirme a senha.

Aceite o nome e o local padrão onde o arquivo será salvo ou clique em ... para selecionar um local diferente.

Clique em **Next** (Avançar).

Uma mensagem indicando que o material de chave foi desbloqueado corretamente é mostrada. Os arquivos estão acessíveis agora.

4 Clique em **Concluir** quando terminar.

Configurar o Server Encryption

Ativar o Server Encryption

NOTA:
O Server Encryption converte a criptografia do usuário para criptografia comum.

1 Faça login como administrador Dell no Dell Remote Management Console.

2 Selecione **Grupo de endpoints** (ou **Endpoint**), procure o endpoint ou grupo de endpoints que você quer ativar, selecione **Políticas de segurança** e, em seguida, selecione a categoria de políticas **Server Encryption**.

3 Defina as seguintes políticas:

- Server Encryption - **Selecione** para ativar a Server Encryption e políticas relacionadas.
- Criptografia SDE ativada - **Selecione** para ativar a Criptografia SDE.
- Criptografia ativada - **Selecione** para ativar a Criptografia comum.
- Proteger Credenciais do Windows - Esta política é **Selecionada** por padrão.

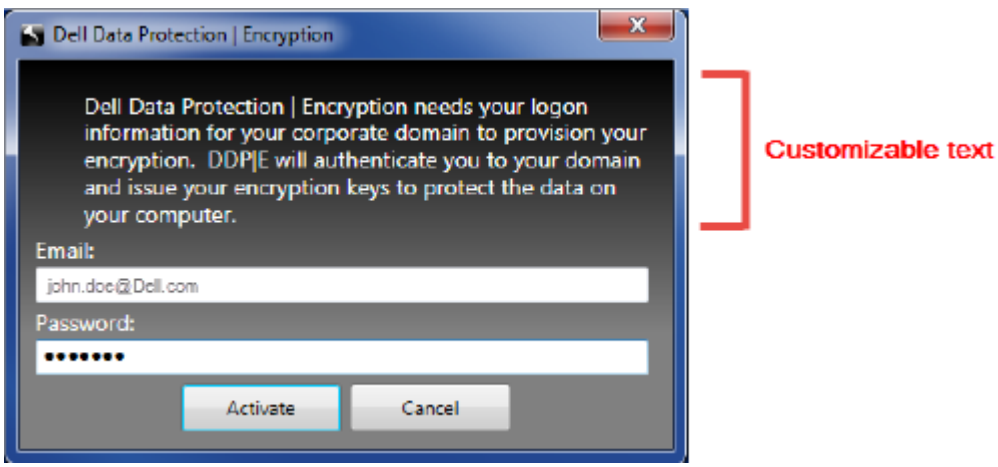
  Quando a política *Proteger Credenciais do Windows* estiver definida como **Selecionada** (o padrão), todos os arquivos na pasta \Windows\system32\config são criptografados, incluindo as credenciais do Windows. Para evitar que as credenciais do Windows sejam criptografadas, defina a política *Proteger Credenciais do Windows* como **Não selecionado**. A criptografia das credenciais do Windows ocorre de forma independente à configuração da política *Criptografia SDE ativada*.

4 Salve e confirme as políticas.

Personalizar caixa de diálogo Login de ativação

A caixa de diálogo de login de ativação é mostrada:

- Quando um usuário não gerenciado faz login.
- Quando o usuário seleciona a opção Ativar Dell Encryption no menu do ícone do Encryption, situado na bandeja do sistema.



Definir políticas EMS do Server Encryption

O ***computador de criptografia de origem*** é o computador que criptografa originalmente um dispositivo removível. Quando o computador de origem é um ***servidor protegido*** (ou seja, um servidor com Server Encryption instalado e ativado) e o servidor protegido primeiro detecta a presença de um dispositivo removível, o usuário é solicitado a criptografar o dispositivo removível.

- As políticas EMS controlam o acesso de mídias removíveis ao servidor, à autenticação, à criptografia e muito mais.
- As políticas de controle de porta afetam as mídias removíveis em servidores protegidos, por exemplo, controlando o acesso e o uso das portas USB do servidor por dispositivos USB.

As políticas de criptografia de mídias removíveis podem ser encontradas no Remote Management Console, no grupo de tecnologia *Server Encryption*.

Server Encryption e mídia externa

Quando a política *EMS Criptografar mídia externa* do servidor protegido estiver **Selecionada**, a mídia externa é criptografada. O Server Encryption vincula o dispositivo ao servidor protegido, com a chave Máquina e ao usuário, com a chave Roaming de usuário do usuário/proprietário do dispositivo removível. Todos os arquivos adicionados ao dispositivo removível serão então criptografados com essas mesmas chaves, independentemente do computador ao qual ele está conectado.

NOTA:
O Server Encryption converte a criptografia de usuário para a criptografia comum, exceto em dispositivos removíveis. Em dispositivos removíveis, a criptografia é realizada com a chave Roaming de usuário associada computador.

Quando o usuário não concorda em criptografar o dispositivo removível, o acesso do usuário ao dispositivo pode ser definido como *bloqueado* quando usado no servidor protegido, *Somente leitura* quando usado no servidor protegido ou *Acesso completo*. As políticas do servidor protegido determinam o nível de acesso em um dispositivo removível desprotegido.

As atualizações de política ocorrem quando o dispositivo removível é reinserido no servidor protegido de origem.

Autenticação e mídias externas

As políticas do servidor protegido determinam o recurso de autenticação.

Depois que um dispositivo removível for criptografado, apenas seu proprietário/usuário pode acessá-lo no servidor protegido. Outros usuários não poderão acessar os arquivos criptografados na mídia removível.

A autenticação automática local permite que a mídia removível protegida seja autenticada automaticamente quando inserida no servidor protegido quando o proprietário da mídia estiver conectado. Quando a autenticação automática estiver desativada, o proprietário/usuário deve autenticar para acessar o dispositivo removível protegido.

Quando o computador de criptografia de origem de um dispositivo removível for um servidor protegido, o usuário/proprietário precisará sempre fazer login no dispositivo removível quando o estiver usando em computadores que não sejam de origem, independentemente das configurações de política EMS definidas nos outros computadores.

Consulte o AdminHelp para obter informações sobre o controle de porta do Server Encryption e as políticas EMS.

Suspender uma instância do servidor criptografado

A suspensão de um servidor criptografado impede o acesso a dados criptografados após uma reinicialização. O usuário do servidor virtual não pode ser suspenso. Em vez disso, a chave Máquina do Server Encryption é suspensa.

NOTA:
Suspender o endpoint de um servidor não suspende o servidor imediatamente. A suspensão ocorre na próxima vez que a chave for solicitada, normalmente na próxima reinicialização do servidor.

IMPORTANTE:

Tome cuidado. Suspender uma instância do servidor criptografado pode causar instabilidade, conforme as configurações de política e caso a suspensão do servidor protegido ocorra enquanto ele estiver desconectado da rede.

Pré-requisitos

- Direitos de administrador de Suporte Técnico, atribuídos no Remote Management Console, são necessários para suspender um endpoint.
- O administrador precisa estar conectado ao Remote Management Console.

No painel esquerdo do Remote Management Console, clique em **Populações** > **Endpoints**.

Pesquise ou selecione um nome de host e, em seguida, clique na guia **Detalhes e ações**.

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

NOTA:

Clique no botão **Reintegrar** para permitir que o Server Encryption acesse os dados criptografados no servidor após sua reinicialização.

Configurar o Deferred Activation

O Enterprise Edition com Deferred Activation se diferencia da ativação do Enterprise Edition de duas formas:

Políticas de criptografia baseadas em dispositivo

As políticas de criptografia do Enterprise Edition são baseadas em usuário, já as políticas de criptografia do Enterprise Edition com Deferred Activation são baseadas em dispositivo. A criptografia de usuário é convertida para a criptografia Comum. Esta diferença permite que o usuário use um dispositivo pessoal em um domínio da organização, enquanto a organização mantém a segurança gerenciando centralmente as políticas de criptografia.

Ativação

Com o Enterprise Edition, a ativação é automática. Ao instalar o Enterprise Edition com Deferred Activation, a ativação automática é desativada. Em vez disso, o usuário escolhe se deseja ativar a criptografia e quando ativá-la.

IMPORTANTE:
Antes que um usuário deixe a organização permanentemente, e enquanto seu endereço de e-mail ainda estiver ativo, ele deverá executar o Encryption Removal Agent e desinstalar o cliente Encryption do seu computador pessoal.

Personalizar o Deferred Activation

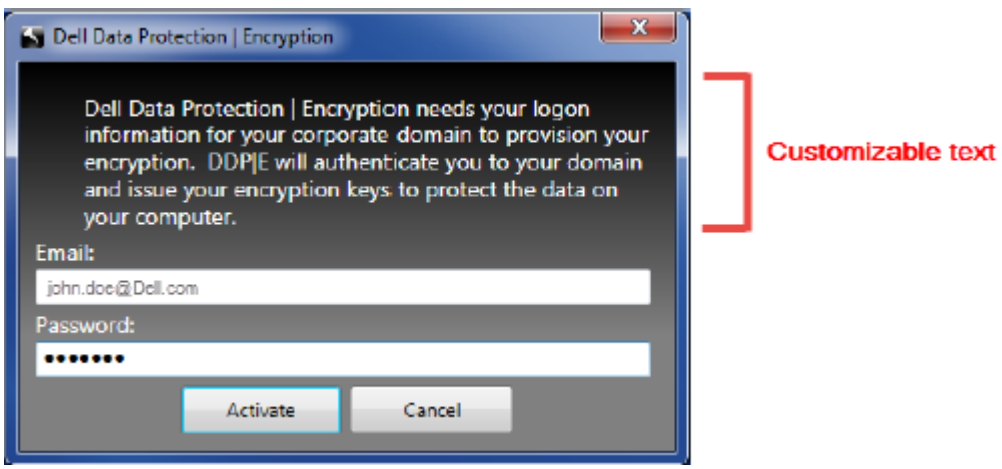
Estas tarefas do lado do cliente permitem a personalização do Deferred Activation.

- Adicionar um aviso à caixa de diálogo Login de ativação
- Desativar a reativação automática (opcional)

Adicionar um aviso à caixa de diálogo Login de ativação

A caixa de diálogo Login de ativação é exibida:

- Quando um usuário não gerenciado faz log in.
- Quando o usuário decide ativar a criptografia e seleciona Ativar Encryption a partir do menu de ícone de bandeja do sistema do Encryption.



Preparar o computador para a instalação

Se os dados estiverem criptografados com um produto que não seja da Dell, antes de instalar o cliente Encryption, descriptografe os dados usando o software de criptografia existente e, então, desinstale o software de criptografia existente. Se o computador não reiniciar automaticamente, reinicie-o.

Criar uma senha do Windows

A Dell recomenda fortemente que uma senha do Windows seja criada (se ela ainda não existir) para proteger o acesso aos dados criptografados. Criar uma senha para o computador impede que outras pessoas façam login na sua conta de usuário sem a sua senha.

Desinstalar versões anteriores do cliente Encryption

Antes de desinstalar uma versão anterior do cliente Encryption, interrompa ou pause uma varredura de criptografia, caso seja necessário.

Se o computador estiver executando uma versão do Dell Encryption anterior à v8.6, desinstale o cliente Encryption da linha de comando. Para obter instruções, consulte *Desinstalar o cliente Encryption e Server Encryption*.

NOTA:
Se você planeja instalar a versão mais recente do cliente Encryption logo após a desinstalação, não será necessário executar o Encryption Removal Agent para descriptografar os arquivos.

Para atualizar uma versão anterior do cliente Encryption instalado com Deferred Activation, use o utilitário Control Panel/Uninstall a Program (Painel de controle/Desinstalar um programa). Este método de desinstalação é possível mesmo se OPTIN estiver desativado.

NOTA:
Se nenhum usuário tiver sido anteriormente ativado, o cliente Encryption limpa a configuração OPTIN da caixa SDE já que a configuração foi deixada por uma instalação anterior. O cliente Encryption bloqueia Deferred Activations se os usuários forem anteriormente ativados, mas o sinalizador OPTIN não estiver definido na caixa SDE.

Como instalar o cliente Encryption com Deferred Activation

Para instalar o cliente Encryption com Deferred Activation, instale o cliente Encryption usando o parâmetro OPTIN=1. Para obter mais informações sobre a instalação do cliente usando o parâmetro OPTIN=1, consulte Como instalar o cliente Encryption.

Como ativar o cliente Encryption com Deferred Activation

- A ativação associa um usuário do domínio a uma conta de usuário local e um computador específico.
- Diversos usuários podem ser ativados no mesmo computador, desde que eles usem contas locais exclusivas e tenham endereços de e-mail de domínio exclusivos.
- Um usuário pode ativar o cliente Encryption apenas uma vez por conta de domínio.

Antes de ativar o cliente Encryption:

- Faça login na conta local que você usa com mais frequência. Os dados associados a essa conta são os dados que serão criptografados.
- Conecte-se à rede da sua organização.

1 Clique com o botão direito no ícone do Encryption  na bandeja do sistema e clique em **Sobre**.

2 Selecione **Ativar criptografia** no menu.

3 Digite seu endereço de e-mail de domínio e senha e clique em **Ativar**.

> **NOTA:**
> Endereços de e-mail fora do domínio da empresa ou pessoais não poderão ser usados para ativação.

4 Clique em **Fechar**.

O Dell Server combina o pacote de chave de criptografia com as credenciais do usuário e com o ID exclusivo do computador (ID da máquina), criando uma relação indissolúvel entre o pacote de chave, o computador especificado e o usuário.

5 Reinicie o computador para que a varredura de criptografia seja iniciada.

> **NOTA:**
> O Console de gerenciamento local, acessível a partir do ícone da bandeja do sistema, mostra as políticas enviadas pelo servidor, não a política efetiva.

Solucionar problemas do Deferred Activation

Solucionar problemas de ativação

Problema: Não é possível acessar determinados arquivos e pastas

A incapacidade de acessar determinados arquivos e pastas é um sintoma de estar conectado com uma conta diferente daquela em que o usuário foi ativado.

A caixa de diálogo Login de ativação é exibida automaticamente mesmo que o usuário já tenha sido ativado.

Possível solução

Saia e faça login novamente com as credenciais da conta ativada. Então, tente acessar os arquivos mais uma vez.

Raramente, o cliente Encryption não consegue autenticar o usuário. Se esse for o caso, a caixa de diálogo Login de ativação solicitará que o usuário insira as credenciais para autenticar e acessar as chaves de criptografia. Para usar o recurso de reativação automática, as chaves de registro *AutoReactivation* e *AutoPromptForActivation* DEVEM estar ativadas. Embora o recurso seja ativado por padrão, ele pode ser desativado manualmente. Para obter mais informações, consulte Desativar a reativação automática.

Mensagem de erro: Falha na autenticação do servidor

O servidor não foi capaz de autenticar o endereço de e-mail e a senha.

Possíveis soluções

- Use o endereço de e-mail associado à organização. Endereços de e-mail pessoais não poderão ser usados para ativação.
- Digite novamente o endereço de e-mail e a senha e certifique-se de que não existem erros tipográficos.
- Peça ao administrador para verificar se a conta de e-mail está ativa e não está bloqueada.
- Peça ao administrador para redefinir a senha de domínio do usuário.

Mensagem de erro: Erro de conexão de rede

Não houve uma conexão entre o cliente Encryption e o Dell Server.

Possíveis soluções

- Conecte-se diretamente à rede da organização e tente ativar novamente.
- Se o acesso por VPN for necessário para conectar-se à rede, verifique a conexão 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 usuário digitou no instalador ficam armazenados no registro. Verifique a precisão dos dados em [HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield] e [HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield\Servlet]

- Desconecte e reconecte:

  Desconecte o computador da rede.

  Reconecte-o à rede.

  Reinicie o computador.

  Tente conectar-se à rede novamente.

Mensagem de erro: Servidor preexistente não suportado

O Encryption não pode ser ativado em um servidor preexistente. A versão do Dell Server precisa ser 9.1 ou posterior.

Possível solução

- Verifique o URL do Dell Server para garantir que corresponde ao URL fornecido pelo administrador.

  O URL e outros dados que o usuário digitou no instalador ficam armazenados no registro.
- Verifique a precisão dos dados em [HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield] e [HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield\Servlet]

Mensagem de erro: Usuário de domínio já ativado

Um segundo usuário se conectou ao computador local e tentou ativar uma conta de domínio que já foi ativada.

Um usuário pode ativar o cliente Encryption apenas uma vez por conta de domínio.

Possível solução

Descriptografe e desinstale o cliente Encryption enquanto estiver conectado como o segundo usuário ativado.

Mensagem de erro: Erro geral do servidor

Ocorreu um erro no servidor.

Possível solução

O administrador deve verificar os registros do servidor para garantir que os serviços estão em execução.

O usuário deve tentar ativar mais tarde.

Ferramentas

CMGad

Use o utilitário CMGAd antes de iniciar o Encryption Removal Agent para obter o pacote de chave de criptografia. O utilitário CMGAd e suas instruções estão localizados na mídia de instalação Dell (Dell-Offline-Admin-XXbit-8.x.x.xxx.zip)

Arquivos de log

Em **C:\ProgramData\Dell\Dell Data Protection\Encryption**, procure um arquivo de log chamado **CmgSysTray**.

Procure a frase "Manual activation result".

O código de erro está na mesma linha, seguido por "status =". O status indica o erro.

Solução de problemas

Todos os clientes - solução de problemas

- Os arquivos de log do instalador mestre do **stão localizados em** C:\ProgramData\Dell\Dell Data Protection\Installer.
- O Windows cria **arquivos de log de desinstalação do instalador filho** exclusivos para o usuário logado em %temp%, localizados em **C:\Users\<UserName>\AppData\Local\Temp.**
- O Windows cria arquivos de log referentes a pré-requisitos do cliente, como Visual C++, para o usuário logado em %temp%, localizados em **C:\Users\<UserName>\AppData\Local\Temp. Por exemplo, C:\Users\<NomeDoUsuário>\AppData\Local\Temp \dd_vcredist_amd64_20160109003943.log**
- Siga as instruções em http://msdn.microsoft.com para verificar a versão do Microsoft .Net instalada no computador onde será feita a instalação.

  Acesse https://www.microsoft.com/en-us/download/details.aspx?id=30653 para baixar a versão completa do Microsoft .Net Framework 4.5.
- Consulte *Dell Data Protection | Security Tools Compatibility* se o computador onde será feita a instalação tem (ou já teve) o Dell Access instalado. O DDP|A não é compatível com esse conjunto de produtos.

Solução de problemas do cliente Encryption e Server Encryption

Upgrade para a Atualização de Aniversário do Windows 10

Para fazer o upgrade para a versão Atualização de Aniversário do Windows 10, siga as instruções no seguinte artigo: http://www.dell.com/support/article/us/en/19/SLN298382.

Ativação em um sistema operacional de servidor

Quando o Encryption estiver instalado em um sistema operacional de servidor, a ativação exige duas fases de ativação: ativação inicial e ativação do dispositivo.

Solução de problemas da ativação inicial

A ativação inicial falha quando:

- Um UPN válido não pode ser construído usando as credenciais fornecidas.
- As credenciais não são encontradas no vault empresarial.
- As credenciais usadas para ativar não são as credenciais do administrador do domínio.

Mensagem de erro: Nome de usuário desconhecido ou senha incorreta

O nome de usuário ou a senha não correspondem.

Possível solução: Tente fazer login novamente, garantindo que você digite o nome de usuário e a senha corretamente.

Mensagem de erro: A ativação falhou porque a conta de usuário não tem direitos de administrador de domínio.

As credenciais usadas para ativar não têm direitos de administrador de domínio ou o nome de usuário do administrador não estava no formato UPN.

Possível solução: Na caixa de diálogo Ativação, digite as credenciais para um administrador de domínio, no formato UPN.

Mensagens de erro: Não foi possível estabelecer uma conexão com o servidor.

ou

`The operation timed out.`

O Server Encryption não conseguiu se comunicar usando a porta 8449 por HTTPS com o DDP Security Server.

Possíveis soluções

- Conecte-se diretamente à rede e tente ativar novamente.
- Caso esteja conectado por VPN, tente se conectar diretamente à rede e tente ativar novamente.
- Verifique o URL do DDP Server para garantir que corresponde ao URL fornecido pelo administrador. O URL e outros dados que o usuário digitou no instalador ficam armazenados no registro. 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-se à rede.

Mensagem de erro: Falha na ativação porque o servidor não foi capaz de atender a esta solicitação.

Possíveis soluções

- O Server Encryption não pode ser ativado em um servidor preexistente; a versão do DDP Server precisa ser 9.1 ou superior. Se necessário, faça upgrade de seu DDP Server para a versão 9.1 ou superior.
- Verifique o URL do DDP Server para garantir que corresponde ao URL fornecido pelo administrador. O URL e outros dados que o usuário digitou no instalador ficam armazenados no registro.
- 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 a seguir ilustra uma ativação inicial bem-sucedida.

O processo de ativação inicial do Server Encryption precisa de um usuário ativo para acessar o servidor. O usuário pode ser de qualquer tipo: usuário de domínio ou não, conectado por área de trabalho remota ou interativo, mas ele precisa ter acesso às credenciais do administrador do domínio.

A caixa de diálogo Ativação mostra quando uma das duas opções a seguir ocorre:

- Um novo usuário (não gerenciado) faz login no computador.
- Quando um novo usuário clica com o botão direito no ícone do cliente Encryption na bandeja do sistema e seleciona Activate Dell Encryption (Ativar Dell Encryption).

O processo de ativação inicial ocorre da seguinte forma:

1 O usuário faz login.
2 Ao detectar um novo usuário (não gerenciado), a caixa de diálogo Ativar é mostrada. O usuário clica em **Cancelar**.
3 O usuário abre a caixa Sobre do Server Encryption para confirmar que ele está sendo executado no modo de servidor.
4 O usuário clica com o botão direito no ícone do cliente Encryption na bandeja do sistema e seleciona **Activate Dell Encryption (Ativar Dell Encryption)**.
5 O usuário digita as credenciais do administrador no domínio na caixa de diálogo Ativar.

NOTA:
A necessidade de credenciais do administrador do domínio é uma medida de segurança que impede que um Server Encryption seja implementado em outros ambientes de servidor que não sejam compatíveis com ele. Para desativar a necessidade de credenciais do administrador do domínio, consulte Antes de começar.

6 O DDP Server verifica as credenciais no vault empresarial (Active Directory ou equivalente) para confirmar que as credenciais sejam do administrador do domínio.

7 Um UPN é construído usando as credenciais.

8 Com o UPN, um DDP Server cria uma nova conta de usuário para o usuário de servidor virtual, e armazena as credenciais no vault do DDP Server.

A **conta de usuário de servidor virtual** é para uso exclusivo do cliente Encryption. Ela será usada para autenticar com o servidor, para lidar com chaves de criptografia comuns e para receber atualizações de política.

NOTA:
A autenticação DPAPI e de senha são desativadas para esta conta de forma que *somente* o usuário do servidor virtual possa acessar as chaves de criptografia no computador. Esta conta não corresponde a nenhuma outra conta de usuário no computador ou no domínio.

9 Quando a ativação for bem-sucedida, o usuário reinicia o computador, que dá início à segunda parte da ativação, a autenticação e a ativação do dispositivo.

Solucionar problemas de autenticação e ativação do dispositivo

A ativação do dispositivo falha quando:

- A ativação inicial falhou.
- Não foi possível estabelecer uma conexão com o servidor.
- Não foi possível validar o certificado de confiança.

Depois da ativação, quando o computador é reiniciado, o Server Encryption faz login automaticamente como o usuário do servidor virtual, solicitando a chave Computador do DDP Enterprise Server. Isso ocorre mesmo antes de qualquer usuário poder fazer login.

- Abra a caixa de diálogo Sobre para confirmar que o Server Encryption está autenticado e no modo Servidor.
- Se o Shield ID estiver vermelho, a criptografia ainda não foi ativada.
- No Remote Management Console, a versão de um servidor com o Server Encryption instalado é listada como *Shield para Server*.
- Se a obtenção da chave Computador falhar devido a um problema de rede, o Server Encryption se registrará para notificações de rede com o sistema operacional.
- Se a obtenção da chave Computador falhar:
  - O login de usuário do servidor virtual ainda ocorrerá satisfatoriamente.
  - Configure a política *Intervalo de nova tentativa após falha de rede* para realizar tentativas de obtenção de chave em um intervalo programado.

    Consulte AdminHelp, disponível no Remote Management Console, para obter detalhes sobre a política *Intervalo de nova tentativa após falha*.

Processo de autenticação e ativação do dispositivo

O diagrama a seguir ilustra a ativação do dispositivo e autenticação bem-sucedida.

1 Quando reinicializado após uma ativação inicial bem-sucedida, um computador com Server Encryption autentica automaticamente usando a conta de usuário de servidor virtual e executa o cliente Encryption no modo de servidor.

2 O computador verifica seu estado de ativação do dispositivo com o DDP Server:

- Se o computador não tiver sido previamente ativado no dispositivo, o DDP Server atribui ao computador um MCID, um DCID e um certificado de confiança, e armazena todas as informações no vault do DDP Server.

- Se o computador tiver sido previamente ativado pelo dispositivo, o DDP Server verifica o certificado de confiança.

3 Depois que o DDP Server atribui o certificado de confiança ao servidor, ele pode acessar suas chaves de criptografia.

4 A ativação do dispositivo ocorre com sucesso.

> **NOTA:**
> Quando o cliente Encryption está sendo executado no modo de servidor, ele precisa ter acesso ao mesmo certificado usado para a ativação do dispositivo para acessar as chaves de criptografia.

(Opcional) Criar um arquivo de log do Agente de remoção de criptografia

- Antes de iniciar o processo de desinstalação, você terá a opção de criar um arquivo de log do Agente de remoção de criptografia. Este arquivo de log é útil para solucionar problemas de uma operação de desinstalação/descriptografia. Se você não pretende descriptografar arquivos durante o processo de desinstalação, não é necessário criar esse arquivo de log.
- O arquivo de log do Agente de remoção de criptografia não será criado até que o serviço Agente de remoção de criptografia seja concluído, o que não acontece até o computador ser reiniciado. Quando o cliente tiver sido desinstalado com êxito e o computador estiver totalmente descriptografado, o arquivo de log será apagado permanentemente.
- O caminho do arquivo de log é **C:\ProgramData\Dell\Dell Data Protection\Encryption.**
- Crie a seguinte entrada de registro no computador que você pretende descriptografar.

  [HKLM\Software\Credant\DecryptionAgent]

  "LogVerbosity"=dword:2

  0: nenhum registro em log

  1: registra os erros que impedem a execução do Serviço

  2: registra os erros que impedem a descriptografia de dados completa (nível recomendado)

  3: registra as informações sobre todos os volumes e arquivos de descriptografia

  5: registra as informações de depuração

Localizar a versão do TSS

- O TSS é um componente que faz interface com o TPM. Para localizar a versão do TSS, acesse (local padrão) **C:\Program Files\Dell \Dell Data Protection\Drivers\TSS\bin > tcsd_win32.exe**. Clique com o botão direito no arquivo e selecione **Propriedades**. Verifique a versão do arquivo na guia **Detalhes**.

Interações de EMS e PCS

Para garantir que a mídia não está como somente leitura e a porta não está bloqueada

A política EMS - Acesso a mídia não protegida interage com a política Sistema de controle de portas - Classe de armazenamento: Controle de unidade externa. Se você pretende definir a política EMS - Acesso a mídia não protegida como *Acesso completo*, verifique se a política Classe de armazenamento: Controle de unidade externa também está definida como *Acesso completo*, para garantir que a mídia não esteja definida para somente leitura e que a porta não esteja bloqueada.

Para criptografar dados gravados em CD/DVD:

- Defina Criptografar mídia externa (EMS) = Verdadeiro.

- Defina Excluir criptografia de CD/DVD (EMS) = Falso.
- Definir Subclasse de armazenamento: Controle de unidade óptica = UDF somente.

Usar WSScan

- O WSScan permite que você garanta que todos os dados sejam descriptografados ao desinstalar o cliente Encryption, bem como visualizar o status de criptografia e identificar arquivos não criptografados que devem ser criptografados.
- Privilégios do administrador são necessários para executar este utilitário.

Execute o WSScan

1 Copie o WSScan.exe da mídia de instalação Dell para o computador Windows a ser verificado.

2 Inicie uma linha de comando no local acima e digite **wsscan.exe** no prompt de comando. O WSScan é aberto.

3 Clique em **Avançado**.

4 Selecione o tipo de unidade a ser analisada no menu suspenso: *Todas as unidades*, *Unidades fixas*, *Unidades removíveis* ou *CDROM/DVDROM*.

5 Selecione o tipo de relatório de criptografia desejado no menu suspenso: *Arquivos criptografados*, *Arquivos não criptografados*, *Todos os arquivos* ou *Arquivos não criptografados em violação*:

- *Arquivos criptografados* - Para garantir que todos os dados sejam descriptografados ao desinstalar o cliente Encryption. Siga seu processo existente para descriptografar dados, como emitir uma atualização de política de descriptografia. Após descriptografar os dados, mas antes de fazer uma reinicialização, execute o WSScan para garantir que todos os dados sejam descriptografados.
- *Arquivos não criptografados* - Para identificar os arquivos não criptografados, com uma indicação se os arquivos devem ser criptografados (S/N).
- *Todos os arquivos* - Para mostrar uma lista de todos os arquivos criptografados e não criptografados, com a indicação se os arquivos devem ser criptografados (S/N).
- *Arquivos não criptografados em violação* - Para identificar os arquivos não criptografados que devem ser criptografados.

6 Clique em **Pesquisar**.

OU

1 Clique em **Avançado** para alternar a exibição para **Simples** para verificar uma pasta específica.

2 Acesse Configurações de varredura e digite o caminho da pasta no campo **Caminho de pesquisa**. Se este campo for usado, a seleção na caixa suspensa será ignorada.

3 Se você não quiser gravar a saída de WSScan em um arquivo, desmarque a caixa de seleção **Saída para arquivo**.

4 Se quiser, altere o caminho padrão e o nome do arquivo em *Caminho*.

5 Selecione **Adicionar a arquivo existente** se você não deseja substituir nenhum arquivo de saída WSScan existente.

6 Escolha o formato de saída:

- Selecione Formato de relatório para obter uma lista de estilo de relatório de saída verificada. Este é o formato padrão.
- Selecione "Arquivo delimitado por valor" para gerar um arquivo que pode ser importado para um aplicativo de planilha. O delimitador padrão é "|", embora ele possa ser alterado para até 9 caracteres alfanuméricos, de espaço ou pontuação.
- Selecione a opção 'Valores entre aspas' para incluir cada valor entre aspas duplas.
- Selecione 'Arquivo de largura fixa' para gerar um arquivo não delimitado que contenha uma linha contínua de informações de comprimento fixo sobre cada arquivo criptografado.

7 Clique em **Pesquisar**.

Clique em **Parar pesquisa** para parar sua pesquisa. Clique em **Clear** (Apagar) para apagar as mensagens mostradas.

Uso da linha de comando do WSScan

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

Switch	Significado
Unidade	Unidade a ser verificada. Se não for especificada, o padrão é todos os discos rígidos fixos locais. Pode ser uma unidades de rede mapeada.
-ta	Verifica todas as unidades
-tf	Verifica as unidades fixas (padrão)
-tr	Verifica as unidades removíveis
-tc	Verifica os CDROMs/DVDROMs
-s	Operação silenciosa
-o	Caminho do arquivo de saída
-A	Acrescenta ao arquivo de saída. O comportamento padrão trunca o arquivo de saída.
-f	Especificador do formato de relatório (Relatório, Fixo, Delimitado)
-r	Executa o WSScan sem privilégios de administrador. **Alguns arquivos podem não ser visíveis se esse modo for usado.**
-u	Inclui arquivos descriptografados no arquivo de saída. Essa chave é posicional: o "u" precisa vir primeiro, o "a" deve vir em segundo (ou ser omitido), o "-" ou o "v" precisam vir por último.
-u-	Inclui apenas arquivos descriptografados no arquivo de saída.
-ua	Relata também arquivos descriptografados, mas usa todas as políticas de usuário para mostrar o campo "deve".
-ua-	Relata apenas arquivos descriptografados, mas usa todas as políticas de usuário para mostrar o campo "deve".
-uv	Reporta apenas arquivos descriptografados que violam política (É=Não / Deve=S)
-uav	Reporta apenas arquivos descriptografados que violam política (É=Não / Deve=S), usando todas as políticas de usuário.
-d	Especifica o que usar como separador de valor para saída delimitada
-q	Especifica que valores devem estar aspas para saída delimitada
-e	Inclui campos de criptografia estendida na saída delimitada
-x	Exclui um diretório da verificação. Múltiplas exclusões são permitidas.
-y	Tempo de suspensão (em milissegundos) entre diretórios. Essa opção faz com que as verificações sejam mais lentas, mas, potencialmente, torna a CPU mais responsiva.

Saída de WSScan

As informações de WSScan sobre arquivos criptografados contêm as seguintes informações.

Exemplo de saída:

[2015-07-28 07:52:33] SysData.07vdlxrsb._SDENCR_: "c:\temp\Dell - test.log" ainda é criptografado em AES256

Saída	Significado
Marca de data/hora	A data e hora em que o arquivo foi verificado.
Tipo de criptografia	O tipo de criptografia usada para criptografar o arquivo. **SysData:** chave de criptografia do SDE. **Usuário:** chave de criptografia do usuário. **Comum:** chave de criptografia comum. O WSScan não mostra arquivos que foram criptografados com o recurso Criptografar para compartilhamento.
KCID	A identificação do computador-chave. Como mostrado no exemplo acima, "**7vdlxrsb**" Se você estiver verificando uma unidade de rede mapeada, o relatório de verificação não retornará um KCID.
UCID	O ID do usuário. Como mostrado no exemplo acima, "**_SDENCR_**" O UCID é compartilhado por todos os usuários do computador.
Arquivo	O caminho do arquivo criptografado. Como mostrado no exemplo acima, "**c:\temp\Dell - test.log**"
Algoritmo	O algoritmo de criptografia que está sendo usado para criptografar o arquivo. Como mostrado no exemplo acima, "**ainda é criptografado em AES256**" Rijndael 128 Rijndael 256 AES 128 AES 256 3DES

Usar o WSProbe

O Utilitário de sondagem é para uso com todas as versões do cliente Encryption, com exceção das políticas de EMS. Use o Utilitário de sondagem para:

- Verificar ou agendar uma verificação de um computador criptografado. O Utilitário de sondagem segue a política Prioridade da verificação de estações de trabalho.
- Desativar temporariamente ou reativar a Lista de criptografia de dados de aplicativos do usuário atual.
- Adicionar ou remover nomes de processos na lista privilegiada.
- Solucionar problemas conforme instruído pelo Dell ProSupport.

Abordagens para a criptografia de dados

Se você for especificar políticas para criptografar dados em dispositivos Windows, você pode usar uma das abordagens a seguir:

- A primeira abordagem é aceitar o comportamento padrão do cliente. Se você especificar pastas em Pastas criptografadas comuns ou em Pastas criptografadas do usuário, ou se selecionar as opções Criptografar "Meus documentos", Criptografar pastas pessoais do Outlook, Criptografar arquivos temporários, Criptografar arquivos temporários da Internet ou Criptografar arquivo de paginação do Windows, os arquivos impactados serão criptografados ao serem criados ou (depois de serem criados por um usuário não gerenciado) quando um usuário gerenciado fizer login. O cliente também verifica as pastas especificadas nessas políticas ou relacionadas a elas quanto à possível criptografia/descriptografia quando uma pasta é renomeada ou quando o cliente recebe alterações para essas políticas.
- Você pode também configurar Examinar a estação de trabalho no login para Verdadeiro. Se Examinar a estação de trabalho no login for Verdadeiro, quando um usuário fizer login, o cliente comparará como os arquivos nas pastas criptografadas atualmente e anteriormente estão criptografados em relação às políticas do usuário, e fará todas as alterações necessárias.
- Para criptografar os arquivos que atendem aos seus critérios de criptografia, mas que foram criados antes de as políticas de criptografia entrarem em vigor, sem influenciar o desempenho das verificações regulares, você pode usar este utilitário para verificar ou agendar uma verificação do computador.

Pré-requisitos

- O dispositivo Windows com o qual você quer trabalhar precisa estar criptografado.
- O usuário com o qual você quer trabalhar precisa estar conectado.

Usar o Utilitário de sondagem

O WSProbe.exe está disponível na mídia de instalação.

Sintaxe

```
wsprobe [path]

wsprobe [-h]

wsprobe [-f path]

wsprobe [-u n] [-x process_names] [-i process_names]
```

Parâmetros

Parâmetro	Para
caminho	Opcionalmente, especifique um determinado caminho no dispositivo que você quer verificar quanto à possível criptografia/descriptografia. Se você não especificar um caminho, o utilitário verificará todas as pastas relacionadas com as suas políticas de criptografia.
-h	Mostra a Ajuda da linha de comando.
-f	Solucionar problemas conforme instruído pelo Dell ProSupport
-u	Desativa temporariamente ou reativa a Lista de criptografia de dados de aplicativos do usuário. Essa lista estará ativa apenas se a opção Criptografia ativada estiver selecionada para o usuário atual. Especifique 0 para desativar ou 1 para reativar. A política atual em vigor para o usuário será restabelecida no próximo login.
-x	Adiciona nomes de processos à lista privilegiada. Os nomes de processos do computador e do instalador nessa lista, além daqueles que você adicionar usando esse parâmetro ou HKLM \Software\CREDANT\CMGShield\EUWPrivilegedList, serão ignorados se estiverem especificados na Lista de criptografia de dados de aplicativos. Separe os nomes de processos com vírgulas. Se sua lista incluir um ou mais espaços, coloque a lista entre aspas duplas.
-i	Remove os nomes de processos anteriormente adicionados à lista privilegiada (não é possível remover nomes de processos embutidos no código). Separe os nomes de processos com vírgulas. Se sua lista incluir um ou mais espaços, coloque a lista entre aspas duplas.

Verificar o status do agente de remoção de criptografia

O Agente de remoção de criptografia mostra o status na área de descrição do painel Serviços (Iniciar > Executar... > services.msc > OK) da seguinte maneira. Atualize periodicamente o Serviço (realce o Serviço > clique com o botão direito > Atualizar) para atualizar seu status.

- **Aguardando a desativação de SDE** – O cliente Encryption ainda está instalado, ainda está configurado, ou ambos. A descriptografia não iniciará até o cliente Encryption ser desinstalado.
- **Varredura inicial** – o serviço está realizando uma varredura inicial, calculando o número de arquivos e bytes criptografados. A varredura inicial ocorre uma vez.
- **Varredura de descriptografia** – o serviço está descriptografando arquivos e possivelmente solicitando a descriptografia de arquivos bloqueados.
- **Descriptografar na reinicialização (parcial)** – a varredura de descriptografia está concluída e alguns arquivos bloqueados (mas não todos) precisam ser descriptografados na próxima reinicialização.
- **Descriptografar na reinicialização** – a varredura de descriptografia está concluída e todos os arquivos bloqueados precisam ser descriptografados na próxima reinicialização.
- **Não foi possível descriptografar todos os arquivos** – a varredura de descriptografia está concluída, mas não foi possível descriptografar todos os arquivos. Esse status significa que uma das seguintes situações ocorreu:
  - Não foi possível agendar os arquivos bloqueados para descriptografia porque eles eram muito grandes ou ocorreu um erro durante a solicitação para desbloqueá-los.
  - Ocorreu um erro de entrada/saída durante a descriptografia de arquivos.
  - Não foi possível descriptografar os arquivos por política.
  - Os arquivos estão marcados como se devessem ser criptografados.
  - Ocorreu um erro durante a varredura de descriptografia.
  - Em todos os casos, um arquivo de log é criado (se o registro em log estiver configurado) quando LogVerbosity=2 (ou superior) é definido. Para solucionar o problema, defina o detalhamento do log como 2 e reinicie o serviço Agente de remoção de criptografia para forçar outra varredura de descriptografia. Consulte (Opcional) Criar um arquivo de log do Agente de remoção de criptografia para obter instruções.
- **Concluída** – A varredura de descriptografia está concluída. O Serviço, o executável, o driver e o executável do driver ficam agendados para serem apagados na próxima reinicialização.

Solução de problemas do cliente SED

Usar a política Código de acesso inicial

- Essa política é usada para fazer login em um computador quando o acesso à rede está indisponível. Ou seja, o acesso ao EE Server/VE Server e ao AD não está disponível a ambos. Use a política *Código de acesso inicial* apenas se for absolutamente necessário. A Dell não recomenda esse método para fazer login. O uso da política *Initial Access Code* (Código de acesso inicial) não oferece o mesmo nível de segurança que o método de autenticação normal de login usando nome de usuário, domínio e senha.

  Além de ser um método menos seguro de login, se um usuário final for ativado usando a política *Initial Access Code* (Código de acesso inicial), não haverá no EE Server/VE Server nenhum registro desse usuário sendo ativado nesse computador. Por outro lado, não existe nenhuma possibilidade de gerar um Código de resposta a partir do EE Server/VE Server para o usuário final se ele não digitar a senha correta e responder às perguntas de autoajuda corretamente.
- O *Código de acesso inicial* pode ser usado apenas **uma** vez, imediatamente após a ativação. Após um usuário final ter feito login, o *Código de acesso inicial* não estará disponível novamente. O primeiro login de domínio que ocorre após o *código de acesso inicial* ser inserido é armazenado em cache, e o campo de entrada *Initial Access Code* não será mostrado novamente.
- O *Código de acesso inicial* será mostrado **apenas** nas seguintes circunstâncias:
  - O usuário nunca foi ativado no PBA.
  - O cliente não tem conectividade com a rede nem com o EE Server/VE Server.

Usar o Código de acesso inicial

1 Defina um valor para a política de **Código de acesso inicial** no Console de gerenciamento remoto.
2 Salve e confirme a política.
3 Inicie o computador local.
4 Digite o **Código de acesso inicial** quando a tela Código de acesso for mostrada.
5 Clique na **seta azul**.
6 Clique em **OK** quando a tela de notificação legal for mostrada.
7 Faça login no Windows com as credenciais do usuário para este computador. Essas credenciais precisam ser parte do domínio.
8 Após fazer login, abra o Console de segurança e verifique se o usuário de PBA foi criado corretamente.

   Clique em **Log** no menu superior e procure a mensagem *Usuário de PBA criado para <domínio\nome de usuário*, que indica que o processo foi bem-sucedido.
9 Desligue e reinicie o computador.
10 Na tela de login, informe o nome de usuário, o domínio e a senha anteriormente usados para login no Windows.

   É preciso que o formato de nome de usuário seja igual ao usado na criação do usuário de PBA. Portanto, se você usou o formato domínio/nome de usuário, será preciso digitar o domínio/nome de usuário no campo Username (Nome de usuário).
11 (Gerenciador Credant apenas) Responda aos prompts de pergunta e resposta.

   Clique na **seta azul**.
12 Clique em **Login** quando a tela de notificação legal for mostrada.

   O Windows agora é iniciado, e o computador pode ser usado como de costume.

Criar um arquivo de log de PBA para solucionar problemas

- Pode ser necessário um arquivo de log de PBA para solucionar problemas de PBA, como:
  - O ícone de conexão de rede não está visível, mas você sabe que há conectividade da rede. O arquivo de log contém informações de DHCP para resolver o problema.
  - Você não consegue ver o ícone de conexão do DDP EE Server/VE Server. O arquivo de log contém informações para ajudar o diagnóstico de problemas de conectividade do EE Server/VE Server.
  - A autenticação falha mesmo com a digitação das credenciais corretas. O arquivo de log usado com os logs do EE Server/VE Server pode ajudar a diagnosticar o problema.

Capturar logs ao fazer a inicialização na PBA (PBA herdada)

1 Crie uma pasta em uma unidade USB e a nomeie **\CredantSED**, no nível da raiz da unidade USB.
2 Crie um arquivo com o nome actions.txt e coloque-o na pasta **\CredantSED**.
3 Em actions.txt, adicione a linha:

```
get environment
```

4 Salve e feche o arquivo.

   Não insira a unidade USB com o computador desligado. Se a unidade USB já estiver inserida durante o estado de desligamento, retire-a.
5 Ligue o computador e faça login na PBA. Insira a unidade USB no computador onde os logs serão coletados durante essa etapa.
6 Após inserir a unidade USB, aguarde de 5 a 10 segundos e retire a unidade.

   Um arquivo credpbaenv.tgz será gerado na pasta **\CredantSED** que contem os arquivos de log necessários.

Capturar logs ao fazer a inicialização na PBA (PBA UEFI)

1 Crie um arquivo chamado **PBAErr.log** na raiz da unidade USB.
2 Insira a unidade USB **antes** de ligar o computador.

3 Remova a unidade USB **após** reproduzir o problema para o qual os logs são necessários.

O arquivo de log PBAErr.log será atualizado e gravado em tempo real.

Drivers Dell ControlVault

Atualização dos drivers e firmware Dell ControlVault

- Os drivers e firmware Dell ControlVault instalados de fábrica nos computadores Dell estão desatualizados e precisam ser atualizados. Siga o procedimento adiante e na ordem em que ele é apresentado.
- Se uma mensagem de erro for mostrada durante a instalação do cliente solicitando que você saia do instalador para atualizar os drivers do Dell ControlVault, você pode desconsiderar completamente essa mensagem para continuar a instalação do cliente. Os drivers (e firmware) Dell ControlVault podem ser atualizados após a instalação do cliente ser concluída.

Download dos drivers mais recentes

1 Vá para support.dell.com.
2 Selecione o modelo do seu computador.
3 Selecione **Drivers e Downloads**.
4 Selecione o **Sistema operacional** do computador em questão.
5 Expanda a categoria **Segurança**.
6 Faça o download e salve os drivers Dell ControlVault.
7 Faça o download e salve o firmware Dell ControlVault.
8 Copie os drivers e o firmware nos computadores de destino, se necessário.

Instale o driver Dell ControlVault.

1 Navegue até a pasta na qual você fez o download do arquivo de instalação do driver.
2 Clique duas vezes no driver Dell ControlVault para abrir o arquivo executável autoextraível.

> **DICA:**
> Instale o driver primeiro. O nome de arquivo do driver *quando este documento foi criado* é ControlVault_Setup_2MYJC_A37_ZPE.exe.

3 Clique em **Continue** (Continuar) para começar.
4 Clique em **OK** para descompactar os arquivos do driver no local padrão **C:\Dell\Drivers\<Nova pasta>**.
5 Clique em **Sim** para criar uma nova pasta.
6 Clique em **Ok** quando for mostrada a mensagem de que a descompactação foi bem-sucedida.
7 A pasta que contém os arquivos deve ser mostrada após a extração. Se ela não for mostrada, navegue até à pasta na qual você extraiu os arquivos. Neste caso, a pasta é **JW22F**.
8 Clique duas vezes em **CVHCI64.MSI** para abrir o instalador de drivers. [este exemplo é **CVHCI64.MSI** neste modelo (CVHCI para um computador de 32 bits)].
9 Clique em **Avançar** na tela de Boas-vindas.
10 Clique em **Avançar** para instalar os drivers no local padrão **C:\Program Files\Broadcom Corporation\Broadcom USH Host Components\.**
11 Selecione a opção **Concluir** e clique em **Avançar**.
12 Clique em **Instalar** para iniciar a instalação dos drivers.
13 Opcionalmente marque a caixa para mostrar o arquivo de log do instalador. Clique em **Concluir** para sair do assistente.

Verificação da instalação de drivers

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

Instalação do firmware Dell ControlVault

1 Navegue até a pasta na qual você fez o download do arquivo de instalação do firmware.
2 Clique duas vezes no firmware Dell ControlVault para abrir o arquivo executável autoextraível.
3 Clique em **Continuar** para começar.
4 Clique em **OK** para descompactar os arquivos do driver no local padrão **C:\Dell\Drivers\<Nova pasta>**.
5 Clique em **Sim** para criar uma nova pasta.
6 Clique em **Ok** quando for mostrada a mensagem de que a descompactação foi bem-sucedida.
7 A pasta que contém os arquivos deve ser mostrada após a extração. Se ela não for mostrada, navegue até à pasta na qual você extraiu os arquivos. Selecione a pasta **firmware**.
8 Clique duas vezes em **ushupgrade.exe** para abrir o instalador do firmware.
9 Clique em **Iniciar** para começar o upgrade do firmware.

> **IMPORTANTE:**
> Se estiver fazendo o upgrade de uma versão mais antiga do firmware, será solicitado que você digite a senha de administrador. Digite `Broadcom` como a senha e clique em **Enter** se essa caixa de diálogo for mostrada.

Várias mensagens de status serão mostradas.

10 Clique em **Reiniciar** para concluir o upgrade do firmware.

A atualização dos drivers e firmware Dell ControlVault foi concluída.

Computadores com UEFI

Solucionar problemas de conexão de rede

- Para a autenticação de pré-inicialização ser bem-sucedida em um computador com firmware de UEFI, o modo de PBA precisa ter conectividade de rede. Por padrão, os computadores com firmware de UEFI não têm conectividade de rede até que o sistema operacional seja carregado, o que ocorre após o modo de PBA. Se o procedimento para computador descrito em Configuração de pré-instalação para computadores com UEFI for bem-sucedido e configurado adequadamente, o ícone de conexão de rede aparecerá na tela de autenticação de pré-inicialização quando o computador estiver conectado à rede.

- Verifique o cabo de rede para ver se ele está conectado ao computador caso o ícone da conexão de rede ainda não apareça durante a autenticação de pré-inicialização. Reinicie o computador para reiniciar o modo de PBA se o cabo não estava conectado ou se estava solto.

TPM e BitLocker

Códigos de erro do TPM e BitLocker

Constante/Valor	Descrição
TPM_E_ERROR_MASK 0x80280000	Esta é uma máscara de erro para conversão de erros de hardware de TPM em erros de win.
TPM_E_AUTHFAIL 0x80280001	Falha de autenticação.
TPM_E_BADINDEX 0x80280002	O índice de um PCR, DIR ou outro registro está incorreto.
TPM_E_BAD_PARAMETER 0x80280003	Um ou mais parâmetros são inválidos.
TPM_E_AUDITFAILURE 0x80280004	Uma operação foi concluída com êxito, mas a auditoria dessa operação falhou.
TPM_E_CLEAR_DISABLED 0x80280005	O sinalizador de desabilitação de limpeza está definido e todas as operações limpas agora requerem acesso físico.
TPM_E_DEACTIVATED 0x80280006	Ative o TPM.
TPM_E_DISABLED 0x80280007	Habilite o TPM.
TPM_E_DISABLED_CMD 0x80280008	O comando de destino foi desabilitado.
TPM_E_FAIL 0x80280009	A operação falhou.
TPM_E_BAD_ORDINAL 0x8028000A	O ordinal era desconhecido ou estava inconsistente.
TPM_E_INSTALL_DISABLED 0x8028000B	A capacidade de instalar um proprietário está desabilitada.
TPM_E_INVALID_KEYHANDLE 0x8028000C	Não é possível interpretar o identificador de chave.

Constante/Valor	Descrição
TPM_E_KEYNOTFOUND 0x8028000D	O identificador de chave aponta para uma chave inválida.
TPM_E_INAPPROPRIATE_ENC 0x8028000E	Esquema de criptografia inaceitável.
TPM_E_MIGRATEFAIL 0x8028000F	Falha na autorização de migração.
TPM_E_INVALID_PCR_INFO 0x80280010	Não foi possível interpretar as informações de PCR.
TPM_E_NOSPACE 0x80280011	Não há espaço para carregar a chave.
TPM_E_NOSRK 0x80280012	Não há conjunto de Chaves de Raiz de Armazenamento (SRK).
TPM_E_NOTSEALED_BLOB 0x80280013	Um blob criptografado é inválido ou não foi criado por este TPM.
TPM_E_OWNER_SET 0x80280014	O TPM já tem um proprietário.
TPM_E_RESOURCES 0x80280015	O TPM não tem recursos internos suficientes para executar a ação solicitada.
TPM_E_SHORTRANDOM 0x80280016	Uma cadeia de caracteres aleatória era pequena demais.
TPM_E_SIZE 0x80280017	O TPM não tem espaço para executar a operação.
TPM_E_WRONGPCRVAL 0x80280018	O valor de PCR nomeado não corresponde ao valor de PCR atual.
TPM_E_BAD_PARAM_SIZE 0x80280019	O argumento paramSize para o comando tem o valor incorreto
TPM_E_SHA_THREAD 0x8028001A	Não existe nenhum thread SHA-1.
TPM_E_SHA_ERROR 0x8028001B	Não é possível prosseguir com o cálculo porque o thread SHA-1 existente já encontrou um erro.

Constante/Valor	Descrição
TPM_E_FAILEDSELFTEST 0x8028001C	O dispositivo de hardware de TPM relatou uma falha durante autoteste interno. Tente reiniciar o computador para solucionar o problema. Se o problema continuar, talvez seja necessário substituir o hardware de TPM ou a placa-mãe.
TPM_E_AUTH2FAIL 0x8028001D	Falha na autorização para a segunda chave em uma função de duas chaves.
TPM_E_BADTAG 0x8028001E	O valor da marca enviada a um comando é inválido.
TPM_E_IOERROR 0x8028001F	Erro de E/S ao transmitir informações ao TPM.
TPM_E_ENCRYPT_ERROR 0x80280020	Problema no processo de criptografia.
TPM_E_DECRYPT_ERROR 0x80280021	O processo de descriptografia não foi concluído.
TPM_E_INVALID_AUTHHANDLE 0x80280022	Identificador inválido usado.
TPM_E_NO_ENDORSEMENT 0x80280023	O TPM não possui uma Chave de Endosso (EK) instalada.
TPM_E_INVALID_KEYUSAGE 0x80280024	O uso de uma chave não é permitido.
TPM_E_WRONG_ENTITYTYPE 0x80280025	O tipo de entidade enviado não é permitido.
TPM_E_INVALID_POSTINIT 0x80280026	O comando foi recebido na sequência incorreta em relação a TPM_Init e TPM_Startup subsequente.
TPM_E_INAPPROPRIATE_SIG 0x80280027	Os dados assinados não podem incluir informações adicionais de DER.
TPM_E_BAD_KEY_PROPERTY 0x80280028	Não há suporte para as propriedades principais em TPM_KEY_PARMs deste TPM.
TPM_E_BAD_MIGRATION 0x80280029	As propriedades de migração desta chave estão incorretas.
TPM_E_BAD_SCHEME 0x8028002A	O esquema de assinatura ou criptografia desta chave está incorreto ou não é permitido nessa situação.

Constante/Valor	Descrição
TPM_E_BAD_DATASIZE 0x8028002B	O tamanho do parâmetro de dados (ou blob) é inválido ou está inconsistente com a chave referenciada.
TPM_E_BAD_MODE 0x8028002C	Um parâmetro de modo é inválido, como capArea ou subCapArea para TPM_GetCapability, o parâmetro phsicalPresence para TPM_PhysicalPresence ou migrationType para TPM_CreateMigrationBlob.
TPM_E_BAD_PRESENCE 0x8028002D	Os bits de physicalPresence ou physicalPresenceLock têm o valor incorreto.
TPM_E_BAD_VERSION 0x8028002E	O TPM não pode executar esta versão do recurso.
TPM_E_NO_WRAP_TRANSPORT 0x8028002F	O TPM não permite sessões de transporte com invólucros.
TPM_E_AUDITFAIL_UNSUCCESSFUL 0x80280030	Falha na construção de auditoria de TPM e o comando subjacente também estava retornando um código de falha.
TPM_E_AUDITFAIL_SUCCESSFUL 0x80280031	Falha na construção de auditoria de TPM e o comando subjacente estava retornando êxito.
TPM_E_NOTRESETABLE 0x80280032	Tentativa de redefinir um registro PCR que não tem o atributo que pode ser redefinido.
TPM_E_NOTLOCAL 0x80280033	Tentativa de redefinir um registro PCR que requer que a localidade e o modificador de localidade não façam parte do transporte de comando.
TPM_E_BAD_TYPE 0x80280034	Blob de criação de identidade digitado incorretamente.
TPM_E_INVALID_RESOURCE 0x80280035	Tipo de recurso identificado no contexto ao salvar não correspondente ao recurso real.
TPM_E_NOTFIPS 0x80280036	O TPM está tentando executar um comando disponível apenas no modo FIPS.
TPM_E_INVALID_FAMILY 0x80280037	O comando está tentando usar uma identificação de família inválida.
TPM_E_NO_NV_PERMISSION 0x80280038	Permissão para manipular o armazenamento NV não disponível.
TPM_E_REQUIRES_SIGN 0x80280039	A operação requer um comando assinado.

Constante/Valor	Descrição
TPM_E_KEY_NOTSUPPORTED 0x8028003A	Operação incorreta para carregar chave NV.
TPM_E_AUTH_CONFLICT 0x8028003B	O blob NV_LoadKey requer autorização do proprietário e do blob.
TPM_E_AREA_LOCKED 0x8028003C	A área NV está bloqueada e não é gravável.
TPM_E_BAD_LOCALITY 0x8028003D	A localidade está incorreta para a operação tentada.
TPM_E_READ_ONLY 0x8028003E	A área NV é somente leitura e não é possível gravar nela.
TPM_E_PER_NOWRITE 0x8028003F	Não há proteção contra gravação na área NV.
TPM_E_FAMILYCOUNT 0x80280040	O valor de contagem da família não corresponde.
TPM_E_WRITE_LOCKED 0x80280041	A área NV já foi gravada.
TPM_E_BAD_ATTRIBUTES 0x80280042	Conflito de atributos da área NV.
TPM_E_INVALID_STRUCTURE 0x80280043	A marca e a versão da estrutura são inválidas ou inconsistentes.
TPM_E_KEY_OWNER_CONTROL 0x80280044	A chave está sob o controle do Proprietário de TPM e só pode ser removida por ele.
TPM_E_BAD_COUNTER 0x80280045	Identificador de contador incorreto.
TPM_E_NOT_FULLWRITE 0x80280046	A gravação da área não está completa.
TPM_E_CONTEXT_GAP 0x80280047	O intervalo entre as contagens de contexto salvo é muito grande.
TPM_E_MAXNVWRITES 0x80280048	O número máximo de gravações NV sem proprietário foi ultrapassado.

Constante/Valor	Descrição
TPM_E_NOOPERATOR 0x80280049	Não há valor de AuthData definido.
TPM_E_RESOURCEMISSING 0x8028004A	O recurso apontado pelo contexto não está carregado.
TPM_E_DELEGATE_LOCK 0x8028004B	A delegação de administração está bloqueada.
TPM_E_DELEGATE_FAMILY 0x8028004C	Tentativa de gerenciar uma família, sem ser a família delegada.
TPM_E_DELEGATE_ADMIN 0x8028004D	O gerenciamento de tabela de delegação não está habilitado.
TPM_E_TRANSPORT_NOTEXCLUSIVE 0x8028004E	Um comando foi executado fora de uma sessão de transporte exclusiva.
TPM_E_OWNER_CONTROL 0x8028004F	Tentativa de salvar em contexto uma chave controlada de remoção de proprietário.
TPM_E_DAA_RESOURCES 0x80280050	O comando DAA não tem recursos disponíveis para execução.
TPM_E_DAA_INPUT_DATA0 0x80280051	Falha na verificação de consistência no parâmetro DAA inputData0.
TPM_E_DAA_INPUT_DATA1 0x80280052	Falha na verificação de consistência no parâmetro DAA inputData1.
TPM_E_DAA_ISSUER_SETTINGS 0x80280053	Falha na verificação de consistência em DAA_issuerSettings.
TPM_E_DAA_TPM_SETTINGS 0x80280054	Falha na verificação de consistência em DAA_tpmSpecific.
TPM_E_DAA_STAGE 0x80280055	O processo atômico indicado pelo comando DAA enviado não é o processo esperado.
TPM_E_DAA_ISSUER_VALIDITY 0x80280056	A verificação de validade do emissor detectou uma inconsistência.
TPM_E_DAA_WRONG_W 0x80280057	Falha na verificação de consistência em w.

Constante/Valor	Descrição
TPM_E_BAD_HANDLE 0x80280058	O identificador está incorreto.
TPM_E_BAD_DELEGATE 0x80280059	A delegação não está correta.
TPM_E_BADCONTEXT 0x8028005A	O blob de contexto é inválido.
TPM_E_TOOMANYCONTEXTS 0x8028005B	Contextos demais armazenados pelo TPM.
TPM_E_MA_TICKET_SIGNATURE 0x8028005C	Falha na validação da assinatura da autoridade de migração.
TPM_E_MA_DESTINATION 0x8028005D	Destino de migração não autenticado.
TPM_E_MA_SOURCE 0x8028005E	Origem de migração incorreta.
TPM_E_MA_AUTHORITY 0x8028005F	Autoridade de migração incorreta.
TPM_E_PERMANENTEK 0x80280061	Tentativa de revogar o EK que não é revogável.
TPM_E_BAD_SIGNATURE 0x80280062	Assinatura inválida de tíquete CMK.
TPM_E_NOCONTEXTSPACE 0x80280063	Não há espaço na lista de contexto para contextos adicionais.
TPM_E_COMMAND_BLOCKED 0x80280400	O comando foi bloqueado.
TPM_E_INVALID_HANDLE 0x80280401	O identificador especificado não foi encontrado.
TPM_E_DUPLICATE_VHANDLE 0x80280402	O TPM retornou um identificador duplicado e é necessário reenviar o comando.
TPM_E_EMBEDDED_COMMAND_BLOCKED 0x80280403	O comando no transporte estava bloqueado.

Constante/Valor	Descrição
TPM_E_EMBEDDED_COMMAND_UNSUPPORTED 0x80280404	Não há suporte para o comando no transporte.
TPM_E_RETRY 0x80280800	O TPM está ocupado demais para responder ao comando imediatamente, mas é possível reenviar o comando mais tarde.
TPM_E_NEEDS_SELFTEST 0x80280801	SelfTestFull não foi executado.
TPM_E_DOING_SELFTEST 0x80280802	O TPM está executando atualmente um autoteste completo.
TPM_E_DEFEND_LOCK_RUNNING 0x80280803	O TPM está se defendendo de ataques de dicionário e está em um período de tempo limite.
TBS_E_INTERNAL_ERROR 0x80284001	Erro de software interno detectado.
TBS_E_BAD_PARAMETER 0x80284002	Um ou mais parâmetros de entrada são inválidos.
TBS_E_INVALID_OUTPUT_POINTER 0x80284003	Um ponteiro de saída especificado é inválido.
TBS_E_INVALID_CONTEXT 0x80284004	O identificador de contexto especificado não se refere a um contexto válido.
TBS_E_INSUFFICIENT_BUFFER 0x80284005	Um buffer de saída especificado é pequeno demais.
TBS_E_IOERROR 0x80284006	Erro ao comunicar-se com o TPM.
TBS_E_INVALID_CONTEXT_PARAM 0x80284007	Um ou mais parâmetros de contexto são inválidos.
TBS_E_SERVICE_NOT_RUNNING 0x80284008	O serviço TBS não está em execução e não foi possível iniciá-lo.
TBS_E_TOO_MANY_TBS_CONTEXTS 0x80284009	Não foi possível criar um novo contexto porque há muitos contextos abertos.
TBS_E_TOO_MANY_RESOURCES 0x8028400A	Não foi possível criar um novo recurso virtual porque há muitos recursos virtuais abertos.

Constante/Valor	Descrição
TBS_E_SERVICE_START_PENDING 0x8028400B	O serviço TBS foi iniciado, mas ainda não está em execução.
TBS_E_PPI_NOT_SUPPORTED 0x8028400C	Não há suporte para a interface de presença física.
TBS_E_COMMAND_CANCELED 0x8028400D	O comando foi cancelado.
TBS_E_BUFFER_TOO_LARGE 0x8028400E	O buffer de entrada ou saída é muito grande.
TBS_E_TPM_NOT_FOUND 0x8028400F	Dispositivo de segurança de TPM compatível não encontrado neste computador.
TBS_E_SERVICE_DISABLED 0x80284010	O serviço TBS foi desabilitado.
TBS_E_NO_EVENT_LOG 0x80284011	Nenhum log de evento TCG disponível.
TBS_E_ACCESS_DENIED 0x80284012	O chamador não possui os direitos apropriados para executar a operação solicitada.
TBS_E_PROVISIONING_NOT_ALLOWED 0x80284013	A ação de provisionamento de TPM não é permitida pelos sinalizadores especificados. Para obter êxito no provisionamento, uma dentre várias ações podem ser necessárias. A ação do console de gerenciamento de TPM (tpm.msc) para tornar o TPM Pronto pode ajudar. Para obter mais informações, consulte a documentação do método WMI do Win32_Tpm 'Provision'. (As ações que podem ser necessárias são, dentre outras: importar o valor Autorização de Proprietário de TPM no sistema, chamar o método WMI do Win32_Tpm para provisionar o TPM e especificar TRUE para 'ForceClear_Allowed' ou 'PhysicalPresencePrompts_Allowed' (conforme indicado pelo valor retornado nas Informações Adicionais) ou habilitar o TPM no BIOS do sistema.)
TBS_E_PPI_FUNCTION_UNSUPPORTED 0x80284014	A Interface de Presença Física deste firmware não dá suporte para o método solicitado.
TBS_E_OWNERAUTH_NOT_FOUND 0x80284015	O valor OwnerAuth de TPM solicitado não foi encontrado.
TBS_E_PROVISIONING_INCOMPLETE 0x80284016	O provisionamento de TPM não foi concluído. Para obter mais informações sobre como concluir o provisionamento, chame o método WMI do Win32_Tpm para provisionar o TPM ('Provision') e verifique as Informações retornadas.
TPMAPI_E_INVALID_STATE 0x80290100	O buffer de comando não está no estado correto.

Constante/Valor	Descrição
TPMAPI_E_NOT_ENOUGH_DATA 0x80290101	O buffer de comando não contém dados suficientes para atender à solicitação.
TPMAPI_E_TOO_MUCH_DATA 0x80290102	O buffer de comando não pode conter mais dados.
TPMAPI_E_INVALID_OUTPUT_POINTER 0x80290103	Um ou mais parâmetros de saída eram NULL ou inválidos.
TPMAPI_E_INVALID_PARAMETER 0x80290104	Um ou mais parâmetros de entrada são inválidos.
TPMAPI_E_OUT_OF_MEMORY 0x80290105	Não havia memória suficiente disponível para atender à solicitação.
TPMAPI_E_BUFFER_TOO_SMALL 0x80290106	O buffer especificado era pequeno demais.
TPMAPI_E_INTERNAL_ERROR 0x80290107	Erro interno detectado.
TPMAPI_E_ACCESS_DENIED 0x80290108	O chamador não possui os direitos apropriados para executar a operação solicitada.
TPMAPI_E_AUTHORIZATION_FAILED 0x80290109	As informações de autorização especificadas eram inválidas.
TPMAPI_E_INVALID_CONTEXT_HANDLE 0x8029010A	O identificador de contexto especificado não era válido.
TPMAPI_E_TBS_COMMUNICATION_ERROR 0x8029010B	Erro ao comunicar-se com o TBS.
TPMAPI_E_TPM_COMMAND_ERROR 0x8029010C	O TPM retornou um resultado inesperado.
TPMAPI_E_MESSAGE_TOO_LARGE 0x8029010D	A mensagem era grande demais para o esquema de codificação.
TPMAPI_E_INVALID_ENCODING 0x8029010E	A codificação no blob não foi reconhecida.
TPMAPI_E_INVALID_KEY_SIZE 0x8029010F	O tamanho da chave não é válido.

Constante/Valor	Descrição
TPMAPI_E_ENCRYPTION_FAILED 0x80290110	Falha na operação de criptografia.
TPMAPI_E_INVALID_KEY_PARAMS 0x80290111	A estrutura de parâmetros principal não era válida
TPMAPI_E_INVALID_MIGRATION_AUTHORIZATION_BLOB 0x80290112	Os dados fornecidos solicitados não parecem constituir um blob de autorização de migração válido.
TPMAPI_E_INVALID_PCR_INDEX 0x80290113	O índice PCR especificado era inválido
TPMAPI_E_INVALID_DELEGATE_BLOB 0x80290114	Os dados fornecidos não parecem ser um blob de delegação válido.
TPMAPI_E_INVALID_CONTEXT_PARAMS 0x80290115	Um ou mais dos parâmetros de contexto especificados não era válido.
TPMAPI_E_INVALID_KEY_BLOB 0x80290116	Os dados fornecidos não parecem ser um blob de chave válido
TPMAPI_E_INVALID_PCR_DATA 0x80290117	Os dados PCR especificados eram inválidos.
TPMAPI_E_INVALID_OWNER_AUTH 0x80290118	O formato dos dados de autenticação de proprietário era inválido.
TPMAPI_E_FIPS_RNG_CHECK_FAILED 0x80290119	O número aleatório gerado não passou na verificação FIPS RNG.
TPMAPI_E_EMPTY_TCG_LOG 0x8029011A	O Log de Eventos TCG não contém dados.
TPMAPI_E_INVALID_TCG_LOG_ENTRY 0x8029011B	Uma entrada no Log de Eventos TCG foi inválida.
TPMAPI_E_TCG_SEPARATOR_ABSENT 0x8029011C	Um Separador TCG não foi detectado.
TPMAPI_E_TCG_INVALID_DIGEST_ENTRY 0x8029011D	Um valor de resumo em uma entrada de log TCG não correspondeu os dados de hash.
TPMAPI_E_POLICY_DENIES_OPERATION 0x8029011E	A operação solicitada foi bloqueada pela política de TPM atual. Entre em contato com o administrador de sistema para obter assistência.

Constante/Valor	Descrição
TBSIMP_E_BUFFER_TOO_SMALL 0x80290200	O buffer especificado era pequeno demais.
TBSIMP_E_CLEANUP_FAILED 0x80290201	Não foi possível limpar o contexto.
TBSIMP_E_INVALID_CONTEXT_HANDLE 0x80290202	O identificador de contexto especificado é inválido.
TBSIMP_E_INVALID_CONTEXT_PARAM 0x80290203	Foi especificado um parâmetro de contexto inválido.
TBSIMP_E_TPM_ERROR 0x80290204	Erro ao comunicar-se com o TPM
TBSIMP_E_HASH_BAD_KEY 0x80290205	Nenhuma entrada com a chave especificada foi encontrada.
TBSIMP_E_DUPLICATE_VHANDLE 0x80290206	O identificador virtual especificado corresponde a um identificador virtual em uso.
TBSIMP_E_INVALID_OUTPUT_POINTER 0x80290207	O ponteiro para o local de identificador retornado era NULL ou inválido
TBSIMP_E_INVALID_PARAMETER 0x80290208	Um ou mais parâmetros são inválidos
TBSIMP_E_RPC_INIT_FAILED 0x80290209	Não foi possível inicializar o subsistema RPC.
TBSIMP_E_SCHEDULER_NOT_RUNNING 0x8029020A	O agendador TBS não está em execução.
TBSIMP_E_COMMAND_CANCELED 0x8029020B	O comando foi cancelado.
TBSIMP_E_OUT_OF_MEMORY 0x8029020C	Não havia memória suficiente para atender à solicitação
TBSIMP_E_LIST_NO_MORE_ITEMS 0x8029020D	A lista especificada está vazia ou a iteração alcançou o fim da lista.
TBSIMP_E_LIST_NOT_FOUND 0x8029020E	O item especificado não foi encontrado na lista.

Constante/Valor	Descrição
TBSIMP_E_NOT_ENOUGH_SPACE 0x8029020F	O TPM não tem espaço suficiente para carregar o recurso solicitado.
TBSIMP_E_NOT_ENOUGH_TPM_CONTEXTS 0x80290210	Há muitos contextos de TPM em uso.
TBSIMP_E_COMMAND_FAILED 0x80290211	Falha no comando de TPM.
TBSIMP_E_UNKNOWN_ORDINAL 0x80290212	O TBS não reconhece o ordinal especificado.
TBSIMP_E_RESOURCE_EXPIRED 0x80290213	O recurso solicitado não está mais disponível.
TBSIMP_E_INVALID_RESOURCE 0x80290214	O tipo de recurso não corresponde.
TBSIMP_E_NOTHING_TO_UNLOAD 0x80290215	Não foi possível descarregar nenhum recurso.
TBSIMP_E_HASH_TABLE_FULL 0x80290216	Não é possível adicionar nenhuma entrada nova à tabela de hash.
TBSIMP_E_TOO_MANY_TBS_CONTEXTS 0x80290217	Não foi possível criar um novo contexto TBS porque há muitos contextos abertos.
TBSIMP_E_TOO_MANY_RESOURCES 0x80290218	Não foi possível criar um novo recurso virtual porque há muitos recursos virtuais abertos.
TBSIMP_E_PPI_NOT_SUPPORTED 0x80290219	Não há suporte para a interface de presença física.
TBSIMP_E_TPM_INCOMPATIBLE 0x8029021A	O TBS não é compatível com a versão do TPM encontrada no sistema.
TBSIMP_E_NO_EVENT_LOG 0x8029021B	Nenhum log de evento TCG disponível.
TPM_E_PPI_ACPI_FAILURE 0x80290300	Um erro geral foi detectado durante a tentativa de aquisição da resposta da BIOS a um comando de Presença Física.
TPM_E_PPI_USER_ABORT 0x80290301	O usuário não confirmou a solicitação de operação de TPM.

Constante/Valor	Descrição
TPM_E_PPI_BIOS_FAILURE 0x80290302	A falha na BIOS impediu a execução bem-sucedida da operação de TPM solicitada (por exemplo, solicitação de operação de TPM inválida, erro de comunicação da BIOS com o TPM).
TPM_E_PPI_NOT_SUPPORTED 0x80290303	A BIOS não oferece suporte à interface de presença física.
TPM_E_PPI_BLOCKED_IN_BIOS 0x80290304	O comando Presença Física foi bloqueado pelas configurações atuais do BIOS. Talvez o proprietário do sistema possa reconfigurar as configurações do BIOS para permitir o comando.
TPM_E_PCP_ERROR_MASK 0x80290400	Esta é uma máscara de erro para conversão de erros de Provedor de Criptografia de Plataforma em erros de win.
TPM_E_PCP_DEVICE_NOT_READY 0x80290401	O Dispositivo de Criptografia de Plataforma não está pronto atualmente. Ele precisa ser totalmente provisionado para se tornar operacional.
TPM_E_PCP_INVALID_HANDLE 0x80290402	O identificador fornecido para o Provedor de Criptografia de Plataforma é inválido.
TPM_E_PCP_INVALID_PARAMETER 0x80290403	Um parâmetro fornecido para o Provedor de Criptografia de Plataforma é inválido.
TPM_E_PCP_FLAG_NOT_SUPPORTED 0x80290404	Um sinalizador fornecido para o Provedor de Criptografia de Plataforma não tem suporte.
TPM_E_PCP_NOT_SUPPORTED 0x80290405	A operação solicitada não tem suporte para o Provedor de Criptografia de Plataforma.
TPM_E_PCP_BUFFER_TOO_SMALL 0x80290406	O buffer é pequeno demais para conter todos os dados. Nenhuma informação foi gravada no buffer.
TPM_E_PCP_INTERNAL_ERROR 0x80290407	Erro interno inesperado no Provedor de Criptografia de Plataforma.
TPM_E_PCP_AUTHENTICATION_FAILED 0x80290408	Falha da autorização ao usar um objeto do provedor.
TPM_E_PCP_AUTHENTICATION_IGNORED 0x80290409	O Dispositivo de Criptografia de Plataforma ignorou a autorização para o objeto do provedor para reduzir ataques de dicionário.
TPM_E_PCP_POLICY_NOT_FOUND 0x8029040A	A política referenciada não foi encontrada.
TPM_E_PCP_PROFILE_NOT_FOUND 0x8029040B	O perfil referenciado não foi encontrado.

Constante/Valor	Descrição
TPM_E_PCP_VALIDATION_FAILED 0x8029040C	A validação não foi bem-sucedida.
PLA_E_DCS_NOT_FOUND 0x80300002	Conjunto de Coletores de Dados não encontrado.
PLA_E_DCS_IN_USE 0x803000AA	O Conjunto de Coletores de Dados ou uma de suas dependências já está em uso.
PLA_E_TOO_MANY_FOLDERS 0x80300045	Não é possível iniciar o Conjunto de Coletores de Dados porque há muitas pastas.
PLA_E_NO_MIN_DISK 0x80300070	Não há espaço livre em disco suficiente para iniciar o Conjunto de Coletores de Dados.
PLA_E_DCS_ALREADY_EXISTS 0x803000B7	O Conjunto de Coletores de Dados já existe.
PLA_S_PROPERTY_IGNORED 0x00300100	O valor da propriedade será ignorado.
PLA_E_PROPERTY_CONFLICT 0x80300101	Conflito de valor de propriedade.
PLA_E_DCS_SINGLETON_REQUIRED 0x80300102	A configuração atual deste Conjunto de Coletores de Dados requer que ele contenha exatamente um Coletor de Dados.
PLA_E_CREDENTIALS_REQUIRED 0x80300103	Uma conta de usuário é necessária para confirmar as propriedades do Conjunto de Coletores de Dados atual.
PLA_E_DCS_NOT_RUNNING 0x80300104	O Conjunto de Coletores de Dados não está em execução.
PLA_E_CONFLICT_INCL_EXCL_API 0x80300105	Conflito detectado na lista de APIs de inclusão/exclusão. Não especifique a mesma API nas listas de inclusão e exclusão.
PLA_E_NETWORK_EXE_NOT_VALID 0x80300106	O caminho executável especificado refere-se a um compartilhamento de rede ou caminho UNC.
PLA_E_EXE_ALREADY_CONFIGURED 0x80300107	O caminho executável especificado já está configurado para o rastreamento de API.
PLA_E_EXE_PATH_NOT_VALID 0x80300108	O caminho executável especificado não existe. Verifique se esse caminho está correto.

Constante/Valor	Descrição
PLA_E_DC_ALREADY_EXISTS 0x80300109	O Coletor de Dados já existe.
PLA_E_DCS_START_WAIT_TIMEOUT 0x8030010A	O tempo limite da espera pela notificação de inicialização do Coletor de Dados acabou.
PLA_E_DC_START_WAIT_TIMEOUT 0x8030010B	O tempo limite da espera pela inicialização do Coletor de Dados acabou.
PLA_E_REPORT_WAIT_TIMEOUT 0x8030010C	O tempo limite da espera pela conclusão da ferramenta de geração de relatório acabou.
PLA_E_NO_DUPLICATES 0x8030010D	Itens duplicados não são permitidos.
PLA_E_EXE_FULL_PATH_REQUIRED 0x8030010E	Ao especificar o executável que você deseja rastrear, primeiro especifique um caminho completo para ele e não apenas um nome de arquivo.
PLA_E_INVALID_SESSION_NAME 0x8030010F	O nome de sessão fornecido é inválido.
PLA_E_PLA_CHANNEL_NOT_ENABLED 0x80300110	O canal de Log de Eventos Microsoft-Windows-Diagnosis-PLA/Operational deve ser habilitado para a execução desta operação.
PLA_E_TASKSCHED_CHANNEL_NOT_ENABLED 0x80300111	O canal de Log de Eventos Microsoft-Windows-TaskScheduler deve ser habilitado para a execução desta operação.
PLA_E_RULES_MANAGER_FAILED 0x80300112	Falha na execução do Gerenciador de Regras.
PLA_E_CABAPI_FAILURE 0x80300113	Erro ao tentar compactar ou extrair os dados.
FVE_E_LOCKED_VOLUME 0x80310000	Essa unidade está bloqueada pela Criptografia de Unidade de Disco BitLocker. É necessário desbloquear essa unidade a partir do Painel de controle.
FVE_E_NOT_ENCRYPTED 0x80310001	Esta unidade não está criptografada.
FVE_E_NO_TPM_BIOS 0x80310002	O BIOS não se comunicou corretamente com o TPM. Contate o fabricante do computador para obter instruções de atualização de BIOS.
FVE_E_NO_MBR_METRIC 0x80310003	O BIOS não se comunicou corretamente com o Registro Mestre de Inicialização (MBR). Contate o fabricante do computador para obter instruções de atualização de BIOS.

Constante/Valor	Descrição
FVE_E_NO_BOOTSECTOR_METRIC 0x80310004	Uma avaliação obrigatória de TPM está faltando. Se houver um CD ou DVD inicializável no computador, remova-o, reinicie o computador e ative o BitLocker novamente. Se o problema continuar, certifique-se de que o registro mestre de inicialização esteja atualizado.
FVE_E_NO_BOOTMGR_METRIC 0x80310005	O setor de inicialização desta unidade não é compatível com Criptografia de Unidade de Disco BitLocker. Use a ferramenta Bootrec.exe no Ambiente de Recuperação do Windows para atualizar ou reparar o gerenciador de inicialização (BOOTMGR).
FVE_E_WRONG_BOOTMGR 0x80310006	O gerente de inicialização deste sistema operacional não é compatível com Criptografia de Unidade de Disco BitLocker. Use a ferramenta Bootrec.exe no Ambiente de Recuperação do Windows para atualizar ou reparar o gerenciador de inicialização (BOOTMGR).
FVE_E_SECURE_KEY_REQUIRED 0x80310007	Pelo menos um protetor de chave segura é obrigatório para que esta operação seja realizada.
FVE_E_NOT_ACTIVATED 0x80310008	A Criptografia de Unidade de Disco BitLocker não está habilitada nesta unidade. Ative o BitLocker.
FVE_E_ACTION_NOT_ALLOWED 0x80310009	A Criptografia de Unidade de Disco BitLocker não pôde realizar a ação solicitada. Essa condição poderá ocorrer quando duas solicitações forem emitidas ao mesmo tempo. Espere alguns segundos e tente novamente.
FVE_E_AD_SCHEMA_NOT_INSTALLED 0x8031000A	A floresta de Serviços de Domínio do Active Directory não contém as classes e os atributos necessários para hospedar informações de Criptografia de Unidade de Disco BitLocker ou TPM. Contate o administrador do seu domínio para verificar se há extensões de esquema do Active Directory do BitLocker instaladas.
FVE_E_AD_INVALID_DATATYPE 0x8031000B	O tipo de dados obtido do Active Directory não era o esperado. As informações de recuperação do BitLocker podem estar faltando ou danificadas.
FVE_E_AD_INVALID_DATASIZE 0x8031000C	O tamanho de dados obtido do Active Directory não era o esperado. As informações de recuperação do BitLocker podem estar faltando ou danificadas.
FVE_E_AD_NO_VALUES 0x8031000D	O atributo de leitura do Active Directory não contém valores. As informações de recuperação do BitLocker podem estar faltando ou danificadas.
FVE_E_AD_ATTR_NOT_SET 0x8031000E	O atributo não foi definido. Verifique se você está conectado com uma conta de domínio que tem capacidade de gravar informações em objetos do Active Directory.
FVE_E_AD_GUID_NOT_FOUND 0x8031000F	O atributo especificado não pode ser localizado no Active Directory Domain Services. Contate o administrador do seu domínio para verificar se há extensões de esquema do Active Directory do BitLocker instaladas.
FVE_E_BAD_INFORMATION 0x80310010	Os metadados de BitLocker da unidade criptografada não são válidos. Você pode tentar reparar a unidade para restaurar o acesso.

Constante/Valor	Descrição
FVE_E_TOO_SMALL 0x80310011	A unidade não pode ser criptografada porque não possui espaço livre suficiente. Exclua os dados desnecessários na unidade para criar mais espaço livre e tente novamente.
FVE_E_SYSTEM_VOLUME 0x80310012	Não é possível criptografar a unidade porque ela contém informações de inicialização do sistema. Crie uma partição separada para usar como a unidade do sistema que contém as informações de inicialização e uma segunda partição para usar como a unidade do sistema operacional e, em seguida, criptografar a unidade do sistema operacional.
FVE_E_FAILED_WRONG_FS 0x80310013	A unidade não pode ser criptografada porque não há suporte ao sistema de arquivos.
FVE_E_BAD_PARTITION_SIZE 0x80310014	O tamanho do sistema de arquivos é superior ao tamanho de partição da tabela de partição. Esta unidade pode estar corrompida ou foi violada. Para usá-la com o BitLocker, é necessário reformatar a partição.
FVE_E_NOT_SUPPORTED 0x80310015	Não é possível criptografar a unidade.
FVE_E_BAD_DATA 0x80310016	Dados inválidos.
FVE_E_VOLUME_NOT_BOUND 0x80310017	A unidade de dados especificada não é definida para desbloquear automaticamente o computador atual e não pode ser desbloqueada automaticamente.
FVE_E_TPM_NOT_OWNED 0x80310018	Você precisa inicializar o TPM antes de usar a Criptografia de Unidade de Disco BitLocker.
FVE_E_NOT_DATA_VOLUME 0x80310019	A operação não pode ser executada em uma unidade do sistema operacional.
FVE_E_AD_INSUFFICIENT_BUFFER 0x8031001A	O buffer fornecido a uma função era insuficiente para conter os dados retornados. Aumente o tamanho de buffer antes de executar a função novamente.
FVE_E_CONV_READ 0x8031001B	Falha na operação de leitura ao converter a unidade. A unidade não foi convertida. Habilite novamente o BitLocker.
FVE_E_CONV_WRITE 0x8031001C	Falha na operação de gravação ao converter a unidade. A unidade não foi convertida. Habilite novamente o BitLocker.
FVE_E_KEY_REQUIRED 0x8031001D	São necessários um ou mais protetores de chave BitLocker. Não é possível excluir a última chave nesta unidade.
FVE_E_CLUSTERING_NOT_SUPPORTED 0x8031001E	Configurações de cluster não são compatíveis com a Criptografia de Unidade de Disco BitLocker.

Constante/Valor	Descrição
FVE_E_VOLUME_BOUND_ALREADY 0x8031001F	A unidade especificada já está configurada para ser automaticamente desbloqueada no computador atual.
FVE_E_OS_NOT_PROTECTED 0x80310020	A unidade do sistema operacional não está protegida pela Criptografia de Unidade de Disco BitLocker.
FVE_E_PROTECTION_DISABLED 0x80310021	A Criptografia de Unidade de Disco BitLocker foi suspensa nesta unidade. Todos os protetores de chave BitLocker configurados para esta unidade estão efetivamente desabilitados e a unidade será automaticamente desbloqueada usando uma chave descriptografada (limpa).
FVE_E_RECOVERY_KEY_REQUIRED 0x80310022	A unidade que você está tentando bloquear não tem protetores de chave disponíveis para criptografia porque a proteção BitLocker está atualmente suspensa. Reabilite o BitLocker para bloquear essa unidade.
FVE_E_FOREIGN_VOLUME 0x80310023	O BitLocker não pode usar o TPM para proteger uma unidade de dados. A proteção do TPM pode ser usada apenas com a unidade do sistema operacional.
FVE_E_OVERLAPPED_UPDATE 0x80310024	Os metadados do BitLocker da unidade criptografada não podem ser atualizados porque ela foi bloqueada para atualização por outro processo. Tente novamente.
FVE_E_TPM_SRK_AUTH_NOT_ZERO 0x80310025	Os dados de autorização de SRK (System Root Key) do TPM não são zero e, portanto, são incompatíveis com BitLocker. Inicialize o TPM antes de tentar usá-lo com o BitLocker.
FVE_E_FAILED_SECTOR_SIZE 0x80310026	O algoritmo de criptografia da unidade não pode ser usado neste tamanho de setor.
FVE_E_FAILED_AUTHENTICATION 0x80310027	A unidade não pode ser desbloqueada com a chave fornecida. Confirme se você forneceu a chave correta e tente novamente.
FVE_E_NOT_OS_VOLUME 0x80310028	A unidade especificada não é a unidade do sistema operacional.
FVE_E_AUTOUNLOCK_ENABLED 0x80310029	A Criptografia de Unidade de Disco BitLocker não pode ser desativada na unidade do sistema operacional enquanto o recurso de desbloqueio automático estiver desabilitado para as unidades de dados fixas e unidades de dados removíveis associadas a este computador.
FVE_E_WRONG_BOOTSECTOR 0x8031002A	O setor de inicialização da partição do sistema não executa avaliações de TPM. Use a ferramenta Bootrec.exe no Ambiente de Recuperação do Windows para atualizar ou reparar o setor de inicialização.
FVE_E_WRONG_SYSTEM_FS 0x8031002B	O sistema operacional da Criptografia de Unidade de Disco BitLocker deve ser formatado com o sistema de arquivos NTFS, a fim de ser criptografado. Converta a unidade em NTFS e, em seguida, ative o BitLocker.
FVE_E_POLICY_PASSWORD_REQUIRED	As configurações de Política de Grupo exigem que uma senha de recuperação seja especificada antes de criptografar a unidade.

Constante/Valor	Descrição
0x8031002C	
FVE_E_CANNOT_SET_FVEK_ENCRYPTED 0x8031002D	O algoritmo de criptografia de unidade e chave não podem ser definidos em uma unidade criptografada anteriormente. Para criptografar essa unidade com a Criptografia de Unidade de Disco BitLocker, remova a criptografia anterior e, em seguida, ative o BitLocker.
FVE_E_CANNOT_ENCRYPT_NO_KEY 0x8031002E	A Criptografia de Unidade de Disco BitLocker não pode criptografar a unidade especificada porque uma chave de criptografia não está disponível. Adicione um protetor de chave para criptografar essa unidade.
FVE_E_BOOTABLE_CDDVD 0x80310030	A Criptografia de Unidade de Disco BitLocker detectou uma mídia inicializável (CD ou DVD) no computador. Remova a mídia e reinicie o computador.
FVE_E_PROTECTOR_EXISTS 0x80310031	Esse protetor de chave não pode ser adicionado. Apenas um protetor de chave desse tipo é permitido para essa unidade.
FVE_E_RELATIVE_PATH 0x80310032	O arquivo de senha de recuperação não foi localizado porque um caminho relativo foi especificado. As senhas de recuperação devem ser salvas em um caminho totalmente qualificado. As variáveis de ambiente configuradas no computador podem ser usadas no caminho.
FVE_E_PROTECTOR_NOT_FOUND 0x80310033	O protetor de chave especificado não foi encontrado na unidade. Tente outro protetor de chave.
FVE_E_INVALID_KEY_FORMAT 0x80310034	A chave de recuperação fornecida está corrompida e não pode ser usada para acessar a unidade. Um método de recuperação alternativo, como a senha de recuperação, um agente de recuperação de dados ou uma versão de backup da chave de recuperação deve ser usado para recuperar o acesso à unidade.
FVE_E_INVALID_PASSWORD_FORMAT 0x80310035	O formato da senha de recuperação é inválido. As senhas de recuperação do BitLocker são de 48 dígitos. Verifique se a senha de recuperação está no formato correto e, em seguida, tente novamente.
FVE_E_FIPS_RNG_CHECK_FAILED 0x80310036	Falha no teste de verificação do gerador de número aleatório.
FVE_E_FIPS_PREVENTS_RECOVERY_PASSWORD 0x80310037	A configuração de Política de Grupo exigindo conformidade com FIPS impede uma senha de recuperação local de ser gerada ou usada pela Criptografia de Unidade de Disco BitLocker. Ao operar em modo de conformidade com FIPS, as opções de recuperação do BitLocker podem ser uma chave de recuperação armazenada em uma unidade USB ou recuperação através de um agente de recuperação de dados.
FVE_E_FIPS_PREVENTS_EXTERNAL_KEY_EXPORT 0x80310038	A configuração de Diretiva de Grupo exigindo conformidade com FIPS impede uma senha de recuperação de ser salva no Active Directory. Ao operar em modo de conformidade com FIPS, as opções de recuperação do BitLocker podem ser uma chave de recuperação armazenada em uma unidade USB ou recuperação através de um agente de recuperação de dados. Verifique as configurações de Diretiva de Grupo.

Constante/Valor	Descrição
FVE_E_NOT_DECRYPTED 0x80310039	A unidade deve ser totalmente descriptografada para concluir esta operação.
FVE_E_INVALID_PROTECTOR_TYPE 0x8031003A	O protetor de chave especificado não pode ser usado para esta operação.
FVE_E_NO_PROTECTORS_TO_TEST 0x8031003B	Não há nenhum protetor de chave na unidade para executar o teste de hardware.
FVE_E_KEYFILE_NOT_FOUND 0x8031003C	A senha de recuperação ou chave de inicialização do BitLocker não pode ser localizada no dispositivo USB. Verifique se você tem o dispositivo USB correto, se o dispositivo USB está conectado ao computador em uma porta USB ativa, reinicie o computador e, em seguida, tente novamente. Se o problema persistir, contate o fabricante do computador para obter instruções de atualização de BIOS.
FVE_E_KEYFILE_INVALID 0x8031003D	A chave de inicialização BitLocker ou o arquivo de senha de recuperação está corrupto ou inválido. Verifique se você tem a senha de recuperação ou chave de inicialização correta e tente novamente.
FVE_E_KEYFILE_NO_VMK 0x8031003E	Não é possível obter a chave de criptografia BitLocker da chave de inicialização ou da senha de recuperação. Verifique se você tem a senha de recuperação ou chave de inicialização correta e tente novamente.
FVE_E_TPM_DISABLED 0x8031003F	O TPM está desabilitado. Para ser usado com a Criptografia de Unidade de Disco BitLocker, o TPM deve ser habilitado, inicializado e ter propriedade válida.
FVE_E_NOT_ALLOWED_IN_SAFE_MODE 0x80310040	A configuração do BitLocker da unidade especificada não pode ser gerenciada porque este computador está atualmente operando no Modo de Segurança. A Criptografia da Unidade BitLocker só pode ser usada para fins de recuperação no modo de segurança.
FVE_E_TPM_INVALID_PCR 0x80310041	O TPM não conseguiu desbloquear a unidade porque as informações de inicialização do sistema foram alteradas ou não foi fornecido um PIN corretamente. Verifique se a unidade não foi alterada e se as alterações feitas nas informações de inicialização do sistema foram causadas por uma fonte confiável. Depois de verificar se a unidade oferece acesso seguro, use o console de recuperação do BitLocker para desbloquear a unidade e, em seguida, suspenda e continue o BitLocker para atualizar as informações de inicialização do sistema que o BitLocker associa a essa unidade.
FVE_E_TPM_NO_VMK 0x80310042	Não é possível obter a chave de criptografia BitLocker do TPM.
FVE_E_PIN_INVALID 0x80310043	Não é possível obter a chave de criptografia BitLocker do TPM e do PIN.
FVE_E_AUTH_INVALID_APPLICATION 0x80310044	O aplicativo de inicialização foi alterado desde a habilitação da Criptografia de Unidade de Disco BitLocker.

Constante/Valor	Descrição
FVE_E_AUTH_INVALID_CONFIG 0x80310045	As configurações de BCD (Dados de Configuração de Inicialização) foram alteradas desde a habilitação da Criptografia de Unidade de Disco BitLocker.
FVE_E_FIPS_DISABLE_PROTECTION_NOT_ALLOWED 0x80310046	A configuração de diretiva de grupo que requer conformidade com FIPS proíbe o uso de chaves não criptografadas, o que impede que o BitLocker seja suspenso nessa unidade. Para obter mais informações, contate o administrador do domínio.
FVE_E_FS_NOT_EXTENDED 0x80310047	Esta unidade não pode ser criptografada pela Criptografia de Unidade de Disco BitLocker porque o sistema de arquivos não se estende até o final da unidade. Faça a repartição desta unidade e tente novamente.
FVE_E_FIRMWARE_TYPE_NOT_SUPPORTED 0x80310048	Não é possível habilitar a Criptografia de Unidade de Disco BitLocker nesta unidade do sistema operacional. Contate o fabricante do computador para obter instruções de atualização de BIOS.
FVE_E_NO_LICENSE 0x80310049	Esta versão não inclui a Criptografia de Unidade de Disco BitLocker. Para usar essa criptografia, atualize o sistema operacional.
FVE_E_NOT_ON_STACK 0x8031004A	A Criptografia de Unidade de Disco BitLocker não pode ser usada porque os arquivos de sistema críticos do BitLocker estão faltando ou estão corrompidos. Use o Reparo de Inicialização do Windows para restaurar arquivos.
FVE_E_FS_MOUNTED 0x8031004B	A unidade não pode ser bloqueada quando a unidade estiver em uso.
FVE_E_TOKEN_NOT_IMPERSONATED 0x8031004C	O token de acesso associado ao thread atual não é um token de representação.
FVE_E_DRY_RUN_FAILED 0x8031004D	Não é possível obter a chave de criptografia BitLocker. Verifique se o TPM está habilitado e a propriedade foi obtida. Se este computador não tiver um TPM, verifique se a unidade USB foi inserida e está disponível.
FVE_E_REBOOT_REQUIRED 0x8031004E	É necessário reiniciar o seu computador antes de continuar com a Criptografia de Unidade de Disco BitLocker.
FVE_E_DEBUGGER_ENABLED 0x8031004F	A criptografia de unidade não pode ocorrer enquanto a depuração de inicialização estiver habilitada. Use a ferramenta da linha de comando bcdedit para desativar a depuração de inicialização.
FVE_E_RAW_ACCESS 0x80310050	Nenhuma ação foi executada porque a Criptografia de Unidade de Disco BitLocker está no modo de acesso bruto.
FVE_E_RAW_BLOCKED 0x80310051	A Criptografia de Unidade de Disco BitLocker não pode entrar no modo de acesso bruto para esta unidade porque a unidade está atualmente em uso.
FVE_E_BCD_APPLICATIONS_PATH_INCORRECT 0x80310052	O caminho especificado no BCD (Dados de Configuração da Inicialização) para um aplicativo de integridade protegida de Criptografia de Unidade de Disco BitLocker está incorreto. Verifique e corrija as configurações de BCD e tente novamente.

Constante/Valor	Descrição
FVE_E_NOT_ALLOWED_IN_VERSION 0x80310053	A Criptografia de Unidade de Disco BitLocker poderá ser usada somente para fins de recuperação ou provisionamento limitado quando o computador estiver sendo executado em ambientes de pré-instalação ou recuperação.
FVE_E_NO_AUTOUNLOCK_MASTER_KEY 0x80310054	A chave mestra de desbloqueio automático não estava disponível na unidade do sistema operacional.
FVE_E_MOR_FAILED 0x80310055	O firmware do sistema não conseguiu habilitar a limpeza da memória do sistema quando o computador foi reiniciado.
FVE_E_HIDDEN_VOLUME 0x80310056	A unidade oculta não pode ser criptografada.
FVE_E_TRANSIENT_STATE 0x80310057	As chaves de criptografia do BitLocker foram ignoradas, pois a unidade estava em um estado transitório.
FVE_E_PUBKEY_NOT_ALLOWED 0x80310058	Chave pública com base em protetores não permitida nesta unidade.
FVE_E_VOLUME_HANDLE_OPEN 0x80310059	A Criptografia de Unidade de Disco BitLocker já está realizando uma operação nesta unidade. Conclua todas as operações antes de continuar.
FVE_E_NO_FEATURE_LICENSE 0x8031005A	Esta versão do Windows não dá suporte a este recurso de Criptografia de Unidade de Disco BitLocker. Para usá-lo, atualize o sistema operacional.
FVE_E_INVALID_STARTUP_OPTIONS 0x8031005B	As configurações de Política de Grupo para opções de inicialização do BitLocker estão em conflito e não podem ser aplicadas. Entre em contato com o administrador do sistema para obter mais informações.
FVE_E_POLICY_RECOVERY_PASSWORD_NOT_ALLOWED 0x8031005C	As configurações de Política de Grupo não permitem a criação de uma senha de recuperação.
FVE_E_POLICY_RECOVERY_PASSWORD_REQUIRED 0x8031005D	As configurações de Política de Grupo requerem a criação de uma senha de recuperação.
FVE_E_POLICY_RECOVERY_KEY_NOT_ALLOWED 0x8031005E	As configurações de Política de Grupo não permitem a criação de uma chave de recuperação.
FVE_E_POLICY_RECOVERY_KEY_REQUIRED 0x8031005F	As configurações de Política de Grupo requerem a criação de uma chave de recuperação.
FVE_E_POLICY_STARTUP_PIN_NOT_ALLOWED 0x80310060	As configurações de Política de Grupo não permitem o uso de um PIN na inicialização. Escolha outra opção de inicialização do BitLocker.
FVE_E_POLICY_STARTUP_PIN_REQUIRED	As configurações de Política de Grupo requerem o uso de um PIN na inicialização. Escolha esta opção de inicialização do BitLocker.

Constante/Valor	Descrição
0x80310061	
FVE_E_POLICY_STARTUP_KEY_NOT_ALLOWED 0x80310062	As configurações de política de grupo não permitem o uso de uma chave de inicialização. Escolha outra opção de inicialização do BitLocker.
FVE_E_POLICY_STARTUP_KEY_REQUIRED 0x80310063	As configurações de Política de Grupo requerem o uso de uma chave de inicialização. Escolha esta opção de inicialização do BitLocker.
FVE_E_POLICY_STARTUP_PIN_KEY_NOT_ALLOWED0x80310064	As configurações de política de grupo não permitem o uso de uma chave de inicialização e PIN. Escolha outra opção de inicialização do BitLocker.
FVE_E_POLICY_STARTUP_PIN_KEY_REQUIRED 0x80310065	As configurações de Política de Grupo requerem o uso de uma chave de inicialização e PIN. Escolha esta opção de inicialização do BitLocker.
FVE_E_POLICY_STARTUP_TPM_NOT_ALLOWED 0x80310066	A política de grupo não permite o uso de apenas TPM na inicialização. Escolha outra opção de inicialização do BitLocker.
FVE_E_POLICY_STARTUP_TPM_REQUIRED 0x80310067	As configurações de Política de Grupo requerem o uso de apenas TPM na inicialização. Escolha esta opção de inicialização do BitLocker.
FVE_E_POLICY_INVALID_PIN_LENGTH 0x80310068	O PIN fornecido não atende aos requisitos mínimos ou máximos de comprimento de senha.
FVE_E_KEY_PROTECTOR_NOT_SUPPORTED 0x80310069	O protetor de chave não é compatível com a versão de Criptografia de Unidade de Disco BitLocker atualmente na unidade. Atualize a unidade para adicionar o protetor de chave.
FVE_E_POLICY_PASSPHRASE_NOT_ALLOWED 0x8031006A	As configurações de Política de Grupo não permitem a criação de uma senha.
FVE_E_POLICY_PASSPHRASE_REQUIRED 0x8031006B	As configurações de Política de Grupo requerem a criação de uma senha.
FVE_E_FIPS_PREVENTS_PASSPHRASE 0x8031006C	A configuração de política de grupo que requer conformidade com FIPS impediu a geração ou o uso de senhas. Para obter mais informações, contate o administrador do domínio.
FVE_E_OS_VOLUME_PASSPHRASE_NOT_ALLOWED 0x8031006D	Uma senha não pode ser adicionada à unidade do sistema operacional.
FVE_E_INVALID_BITLOCKER_OID 0x8031006E	O identificador de objeto (OID) do BitLocker na unidade parece ser inválido ou corrompido. Use manage-BDE para redefinir o OID nesta unidade.
FVE_E_VOLUME_TOO_SMALL 0x8031006F	A unidade é muito pequena para ser protegida usando a Criptografia de Unidade de Disco BitLocker.

Constante/Valor	Descrição
FVE_E_DV_NOT_SUPPORTED_ON_FS 0x80310070	O tipo de unidade de descoberta selecionado é incompatível com o sistema de arquivos na unidade. As unidades de descoberta BitLocker To Go devem ser criadas em unidades formatadas FAT.
FVE_E_DV_NOT_ALLOWED_BY_GP 0x80310071	O tipo de unidade de descoberta selecionado não é permitido pelas configurações de Política de Grupo da máquina. Verifique se as configurações de Política de Grupo permitem a criação de unidades de descoberta para uso com o BitLocker To Go.
FVE_E_POLICY_USER_CERTIFICATE_NOT_ALLOWED 0x80310072	As configurações de Política de Grupo não permitem que certificados de usuário, como cartões inteligentes, sejam usados com a Criptografia de Unidade de Disco BitLocker.
FVE_E_POLICY_USER_CERTIFICATE_REQUIRED 0x80310073	As configurações de Política de Grupo exigem o uso de um certificado de usuário válido, como um cartão inteligente, com a Criptografia de Unidade de Disco BitLocker.
FVE_E_POLICY_USER_CERT_MUST_BE_HW 0x80310074	As configurações de Política de Grupo exigem o uso de um protetor de chave baseado em um cartão inteligente, com a Criptografia de Unidade de Disco BitLocker.
FVE_E_POLICY_USER_CONFIGURE_FDV_AUTOUNLOCK_NOT_ALLOWED 0x80310075	As configurações de Política de Grupo não permitem que unidades de dados fixas protegidas pelo BitLocker sejam desbloqueadas automaticamente.
FVE_E_POLICY_USER_CONFIGURE_RDV_AUTOUNLOCK_NOT_ALLOWED 0x80310076	As configurações de Política de Grupo não permitem que unidades de dados removíveis protegidas pelo BitLocker sejam desbloqueadas automaticamente.
FVE_E_POLICY_USER_CONFIGURE_RDV_NOT_ALLOWED 0x80310077	As configurações de Política de Grupo não permitem que você configure a Criptografia de Unidade de Disco BitLocker em unidades de dados removíveis.
FVE_E_POLICY_USER_ENABLE_RDV_NOT_ALLOWED 0x80310078	As configurações de Política de Grupo não permitem que você ative a Criptografia de Unidade de Disco BitLocker em unidades de dados removíveis. Entre em contato com o administrador do sistema se precisar ativar o BitLocker.
FVE_E_POLICY_USER_DISABLE_RDV_NOT_ALLOWED 0x80310079	As configurações de Política de Grupo não permitem que você desative a Criptografia de Unidade de Disco BitLocker em unidades de dados removíveis. Entre em contato com o administrador do sistema se precisar desativar o BitLocker.
FVE_E_POLICY_INVALID_PASSPHRASE_LENGTH 0x80310080	A senha não corresponde aos requisitos de comprimento mínimo de senha. Por padrão, as senhas devem ter, pelo menos, oito caracteres de comprimento. Verifique com o administrador do sistema quanto ao requisito de comprimento de senha na sua empresa.
FVE_E_POLICY_PASSPHRASE_TOO_SIMPLE 0x80310081	Sua senha não atende os requisitos de complexidade definidos pelo administrador do sistema. Tente adicionar caracteres maiúsculos e minúsculos, números e símbolos.
FVE_E_RECOVERY_PARTITION 0x80310082	A unidade não pode ser criptografada porque ela está reservada para as Opções de Recuperação de Sistema do Windows.
FVE_E_POLICY_CONFLICT_FDV_RK_OFF_AUK_ON	A Criptografia de Unidade de Disco BitLocker não pode ser aplicada nesta unidade devido a conflito de configurações de Política de

Constante/Valor	Descrição
0x80310083	Grupo. O BitLocker não pode ser configurado para desbloquear automaticamente unidades de dados fixas quando as opções de recuperação de usuário estiverem desabilitadas. Se você quiser que as unidades de dados fixas protegidas pelo BitLocker sejam automaticamente desbloqueadas após a validação de chave, solicite ao seu administrador de sistema que resolva o conflito de configurações antes de habilitar o BitLocker.
FVE_E_POLICY_CONFLICT_RDV_RK_OFF_AUK_ON 0x80310084	A Criptografia de Unidade de Disco BitLocker não pode ser aplicada nesta unidade devido a conflito de configurações de Política de Grupo. O BitLocker não pode ser configurado para desbloquear automaticamente unidades de dados removíveis quando as opções de recuperação de usuário estão desabilitadas. Para que as unidades de dados removíveis protegidas pelo BitLocker sejam automaticamente desbloqueadas após a validação de chave, peça ao seu administrador de sistema para resolver o conflito nas configurações antes de habilitar o BitLocker.
FVE_E_NON_BITLOCKER_OID 0x80310085	O atributo Uso Avançado de Chave (EKU) do certificado especificado não permite que ele seja usado para Criptografia de Unidade de Disco BitLocker. O BitLocker não requer que um certificado tenha um atributo EKU, mas se ele estiver configurado deverá ser um identificador de objeto (OID) que corresponda ao OID configurado para BitLocker.
FVE_E_POLICY_PROHIBITS_SELFSIGNED 0x80310086	A Criptografia de Unidade de Disco BitLocker não pode ser aplicada nesta unidade devido a conflito de configurações de Política de Grupo. O certificado que você forneceu para a criptografia de dados é autoassinado. As configurações atuais de Política de Grupo não permitem o uso de certificados autoassinados. Obtenha um novo certificado da sua autoridade de certificação antes de tentar habilitar o BitLocker.
FVE_E_POLICY_CONFLICT_RO_AND_STARTUP_KEY_REQUIRED 0x80310087	A Criptografia de Unidade de Disco BitLocker não pode ser aplicada nesta unidade devido a conflito de configurações de Política de Grupo. Quando o acesso para gravação a unidades não protegidas pelo BitLocker for negado, o uso de uma chave de inicialização USB não pode ser exibido. Solicite ao seu administrador de sistema que resolva os conflitos de política antes de tentar habilitar o BitLocker.
FVE_E_CONV_RECOVERY_FAILED 0x80310088	A Criptografia de Unidade de Disco BitLocker não pode ser aplicada nesta unidade devido a conflito de configurações de Política de Grupo para opções de recuperação em unidades do sistema operacional. Armazenar informações de recuperação para Active Directory Domain Services não pode ser exigido quando a geração de senhas de recuperação não é permitida. Solicite ao seu administrador de sistema que resolva os conflitos de política antes de tentar habilitar o BitLocker.
FVE_E_VIRTUALIZED_SPACE_TOO_BIG 0x80310089	O tamanho solicitado da virtualização é muito grande.
FVE_E_POLICY_CONFLICT_OSV_RP_OFF_ADB_ON 0x80310090	A Criptografia de Unidade de Disco BitLocker não pode ser aplicada nesta unidade devido a conflito de configurações de Política de Grupo para opções de recuperação em unidades do sistema operacional. Armazenar informações de recuperação para Active Directory Domain Services não pode ser exigido quando a geração de senhas de recuperação não é permitida. Solicite ao seu administrador de sistema que resolva os conflitos de política antes de tentar habilitar o BitLocker.

Constante/Valor	Descrição
FVE_E_POLICY_CONFLICT_FDV_RP_OFF_ADB_ON 0x80310091	A Criptografia de Unidade de Disco BitLocker não pode ser aplicada nesta unidade devido a conflito de configurações de Política de Grupo para opções de recuperação em unidades de dados fixas. Armazenar informações de recuperação para Active Directory Domain Services não pode ser exigido quando a geração de senhas de recuperação não é permitida. Solicite ao seu administrador de sistema que resolva os conflitos de política antes de tentar habilitar o BitLocker.
FVE_E_POLICY_CONFLICT_RDV_RP_OFF_ADB_ON 0x80310092	A Criptografia de Unidade de Disco BitLocker não pode ser aplicada nesta unidade devido a conflito de configurações de Política de Grupo para opções de recuperação em unidades de dados removíveis. Armazenar informações de recuperação para Active Directory Domain Services não pode ser exigido quando a geração de senhas de recuperação não é permitida. Solicite ao seu administrador de sistema que resolva os conflitos de política antes de tentar habilitar o BitLocker.
FVE_E_NON_BITLOCKER_KU 0x80310093	O atributo Uso de Chave (KU) do certificado especificado não permite que ele seja usado para Criptografia de Unidade de Disco BitLocker. O BitLocker não requer que um certificado tenha um atributo KU, mas se ele estiver configurado deverá ser definido para ser como Codificação de Chaves ou Acordo de chave.
FVE_E_PRIVATEKEY_AUTH_FAILED 0x80310094	A chave privada associada ao certificado especificado não pode ser autorizada. A autorização da chave privada não foi fornecida ou a autorização fornecida era inválida.
FVE_E_REMOVAL_OF_DRA_FAILED 0x80310095	A remoção do certificado do agente de recuperação de dados deve ser feita com o snap-in Certificados.
FVE_E_OPERATION_NOT_SUPPORTED_ON_VISTA_VOLUME 0x80310096	Esta unidade foi criptografada usando a versão da Criptografia de Unidade de Disco BitLocker incluída no Windows Vista e no Windows Server 2008, que não aceita identificadores organizacionais. Para especificar identificadores organizacionais para essa unidade, atualize a criptografia da unidade para a última versão usando o comando "manage-bde -upgrade".
FVE_E_CANT_LOCK_AUTOUNLOCK_ENABLED_VOLUME 0x80310097	A unidade não pode ser bloqueada porque ela foi desbloqueada automaticamente neste computador. Remova o protetor de desbloqueio automático para bloquear essa unidade.
FVE_E_FIPS_HASH_KDF_NOT_ALLOWED 0x80310098	A Função de Derivação de Chaves BitLocker SP800-56A padrão para cartões inteligentes ECC não é aceita por seu cartão inteligente. A configuração de Política de Grupo que exige conformidade com FIPS impede que o BitLocker use qualquer outra função de derivação de chaves para criptografia. É necessário usar um cartão inteligente compatível com FIPS em ambientes restritos para FIPS.
FVE_E_ENH_PIN_INVALID 0x80310099	Não foi possível obter a chave de criptografia BitLocker do TPM e do PIN avançado. Tente usar um PIN que contenha apenas numerais.
FVE_E_INVALID_PIN_CHARS 0x8031009A	O PIN do TPM solicitado contém caracteres inválidos.
FVE_E_INVALID_DATUM_TYPE 0x8031009B	As informações de gerenciamento armazenadas na unidade continham um tipo desconhecido. Se você estiver usando uma

Constante/Valor	Descrição
	versão antiga do Windows, tente acessar a unidade usando a última versão.
FVE_E_EFI_ONLY 0x8031009C	Somente há suporte a este recurso em sistemas EFI.
FVE_E_MULTIPLE_NKP_CERTS 0x8031009D	Mais de um certificado de Protetor de Chave de Rede foi encontrado no sistema.
FVE_E_REMOVAL_OF_NKP_FAILED 0x8031009E	A remoção do certificado de Protetor de Chave de Rede precisa ser feita usando o snap-in Certificados.
FVE_E_INVALID_NKP_CERT 0x8031009F	Um certificado inválido foi encontrado no repositório de certificados de Protetor de Chave de Rede.
FVE_E_NO_EXISTING_PIN 0x803100A0	Esta unidade não está protegida com um PIN.
FVE_E_PROTECTOR_CHANGE_PIN_MISMATCH 0x803100A1	Digite o PIN atual correto.
FVE_E_PROTECTOR_CHANGE_BY_STD_USER_DISALLOWED 0x803100A2	Você precisa estar conectado com uma conta de administrador para alterar o PIN ou a senha. Clique no link para redefinir o PIN ou a senha como um administrador.
FVE_E_PROTECTOR_CHANGE_MAX_PIN_CHANGE_ATTEMPTS_REACHED 0x803100A3	O BitLocker desabilitou alterações de PIN e senha após muitas falhas de solicitação. Clique no link para redefinir o PIN ou a senha como um administrador.
FVE_E_POLICY_PASSPHRASE_REQUIRES_ASCII 0x803100A4	O administrador de sistema exige que as senhas contenham somente caracteres ASCII imprimíveis. Isso inclui letras sem acento (A–Z, a–z), números (0–9), espaço, sinais aritméticos, pontuação comum, separadores e os seguintes símbolos: # $ & @ ^ _ ~ .
FVE_E_FULL_ENCRYPTION_NOT_ALLOWED_ON_TP_STORAGE 0x803100A5	A Criptografia de Unidade de Disco BitLocker só dá suporte ao modo de criptografia somente espaço usado em armazenamento com provisionamento dinâmico.
FVE_E_WIPE_NOT_ALLOWED_ON_TP_STORAGE 0x803100A6	A Criptografia de Unidade de Disco BitLocker não dá suporte para apagar espaço livre em armazenamento com provisionamento dinâmico.
FVE_E_KEY_LENGTH_NOT_SUPPORTED_BY_EDRIVE 0x803100A7	A unidade não dá suporte ao comprimento de chave de autenticação obrigatório.
FVE_E_NO_EXISTING_PASSPHRASE 0x803100A8	Esta unidade não está protegida com uma senha.
FVE_E_PROTECTOR_CHANGE_PASSPHRASE_MISMATCH 0x803100A9	Digite a senha atual correta.

Constante/Valor	Descrição
FVE_E_PASSPHRASE_TOO_LONG 0x803100AA	A senha não pode ter mais de 256 caracteres.
FVE_E_NO_PASSPHRASE_WITH_TPM 0x803100AB	Um protetor de chave de senha não pode ser adicionado porque existe um protetor de TPM na unidade.
FVE_E_NO_TPM_WITH_PASSPHRASE 0x803100AC	Um protetor de chave de TPM não pode ser adicionado porque existe um protetor de senha na unidade.
FVE_E_NOT_ALLOWED_ON_CSV_STACK 0x803100AD	Este comando só pode ser executado do nó coordenador para o volume CSV especificado.
FVE_E_NOT_ALLOWED_ON_CLUSTER 0x803100AE	Este comando não pode ser executado em um volume quando ele faz parte de um cluster.
FVE_E_EDRIVE_NO_FAILOVER_TO_SW 0x803100AF	O BitLocker não reverteu para o uso da criptografia de software BitLocker devido à configuração das políticas de grupo.
FVE_E_EDRIVE_BAND_IN_USE 0x803100B0	A unidade não pode ser gerenciada pelo BitLocker porque o recurso de criptografia de hardware da unidade já está sendo usado.
FVE_E_EDRIVE_DISALLOWED_BY_GP 0x803100B1	As configurações de Política de Grupo não permitem o uso de criptografia baseada em hardware.
FVE_E_EDRIVE_INCOMPATIBLE_VOLUME 0x803100B2	A unidade especificada não dá suporte a criptografia baseada em hardware.
FVE_E_NOT_ALLOWED_TO_UPGRADE_WHILE_CONVERTING 0x803100B3	O BitLocker não pode ser atualizado durante a criptografia ou descriptografia de disco.
FVE_E_EDRIVE_DV_NOT_SUPPORTED 0x803100B4	Os Volumes de Descoberta não têm suporte para volumes que usam criptografia de hardware.
FVE_E_NO_PREBOOT_KEYBOARD_DETECTED 0x803100B5	Não foi detectado nenhum teclado de pré-inicialização. O usuário não pode fornecer os dados necessários para desbloquear o volume.
FVE_E_NO_PREBOOT_KEYBOARD_OR_WINRE_DETECTED 0x803100B6	Não foi detectado nenhum teclado de pré-inicialização ou Ambiente de Recuperação do Windows. O usuário não pode fornecer os dados necessários para desbloquear o volume.
FVE_E_POLICY_REQUIRES_STARTUP_PIN_ON_TOUCH_DEVICE 0x803100B7	As configurações de Política de Grupo exigem a criação de um PIN de inicialização, mas um teclado de pré-inicialização não está disponível neste dispositivo. O usuário não pode fornecer os dados necessários para desbloquear o volume.
FVE_E_POLICY_REQUIRES_RECOVERY_PASSWORD_ON_TOUCH_DEVICE	As configurações de Política de Grupo exigem a criação de uma senha de recuperação, mas nem um teclado de pré-inicialização, nem o Ambiente de Recuperação do Windows estão disponíveis

Constante/Valor	Descrição
0x803100B8	neste dispositivo. O usuário não pode fornecer os dados necessários para desbloquear o volume.
FVE_E_WIPE_CANCEL_NOT_APPLICABLE 0x803100B9	O espaço livre não está sendo apagado.
FVE_E_SECUREBOOT_DISABLED 0x803100BA	O BitLocker não pode usar a Inicialização Segura para garantir a integridade da plataforma porque a Inicialização Segura foi desabilitada.
FVE_E_SECUREBOOT_CONFIGURATION_INVALID 0x803100BB	O BitLocker não pode usar a Inicialização Segura para garantir a integridade da plataforma porque a configuração da Inicialização Segura não atende aos requisitos do BitLocker.
FVE_E_EDRIVE_DRY_RUN_FAILED 0x803100BC	O computador não dá suporte à criptografia baseada em hardware BitLocker. Consulte as atualizações de firmware junto ao fabricante do computador.
FVE_E_SHADOW_COPY_PRESENT 0x803100BD	O BitLocker não pode ser habilitado no volume porque ele contém uma Cópia de Sombra de Volume. Remova todas as Cópias de Sombra de Volume antes de criptografar o volume.
FVE_E_POLICY_INVALID_ENHANCED_BCD_SETTINGS 0x803100BE	A Criptografia de Unidade de Disco BitLocker Drive não pode ser aplicada a esta unidade porque a configuração de Política de Grupo para os Dados de Configuração de Inicialização Aprimorados contém dados inválidos. Peça ao administrador de sistema para corrigir essa configuração inválida antes de tentar habilitar o BitLocker.
FVE_E_EDRIVE_INCOMPATIBLE_FIRMWARE 0x803100BF	O firmware deste computador não dá suporte para criptografia de hardware.
FVE_E_PROTECTOR_CHANGE_MAX_PASSPHRASE_CHANGE_ATTEMPTS_REACHED 0x803100C0	O BitLocker desabilitou alterações de senha após muitas falhas de solicitação. Clique no link para redefinir a senha como um administrador.
FVE_E_PASSPHRASE_PROTECTOR_CHANGE_BY_STD_USER_DISALLOWED 0x803100C1	Você precisa estar conectado com uma conta de administrador para alterar a senha. Clique no link para redefinir a senha como um administrador.
FVE_E_LIVEID_ACCOUNT_SUSPENDED 0x803100C2	O BitLocker não pode salvar a senha de recuperação porque a conta da Microsoft especificada foi Suspensa.
FVE_E_LIVEID_ACCOUNT_BLOCKED 0x803100C3	O BitLocker não pode salvar a senha de recuperação porque a conta da Microsoft especificada foi Bloqueada.
FVE_E_NOT_PROVISIONED_ON_ALL_VOLUMES 0x803100C4	Este PC não está provisionado para dar suporte à criptografia de dispositivo. Habilite BitLocker em todos os volumes para atender à política de criptografia de dispositivo.
FVE_E_DE_FIXED_DATA_NOT_SUPPORTED 0x803100C5	Este PC não pode dar suporte à criptografia de dispositivo porque volumes de dados fixos não criptografados estão presentes.

Constante/Valor	Descrição
FVE_E_DE_HARDWARE_NOT_COMPLIANT 0x803100C6	Este PC não atende aos requisitos de hardware para dar suporte à criptografia de dispositivo.
FVE_E_DE_WINRE_NOT_CONFIGURED 0x803100C7	Este PC não pode dar suporte à criptografia de dispositivo porque o WinRE não está configurado corretamente.
FVE_E_DE_PROTECTION_SUSPENDED 0x803100C8	A proteção está habilitada no volume, mas foi suspensa. Isso provavelmente ocorreu devido a uma atualização que está sendo aplicada ao sistema. Tente novamente após uma reinicialização.
FVE_E_DE_OS_VOLUME_NOT_PROTECTED 0x803100C9	Este PC não está provisionado para dar suporte à criptografia de dispositivo.
FVE_E_DE_DEVICE_LOCKEDOUT 0x803100CA	Bloqueio de Dispositivo disparado devido a muitas tentativas de senha incorreta.
FVE_E_DE_PROTECTION_NOT_YET_ENABLED 0x803100CB	A proteção não foi habilitada no volume. Para habilitar a proteção, é necessária uma conta conectada. Se você já tem uma conta conectada e está vendo este erro, consulte o log de eventos para obter mais informações.
FVE_E_INVALID_PIN_CHARS_DETAILED 0x803100CC	O PIN só pode conter números de 0 a 9.
FVE_E_DEVICE_LOCKOUT_COUNTER_UNAVAILABLE 0x803100CD	O BitLocker não pode usar proteção contra reprodução de hardware porque nenhum contador está disponível no seu PC.
FVE_E_DEVICELOCKOUT_COUNTER_MISMATCH 0x803100CE	Falha na validação de estado de Bloqueio de Dispositivo devido a incompatibilidade do contador.
FVE_E_BUFFER_TOO_LARGE 0x803100CF	O buffer de entrada é muito grande.

18

Glossário

Ativar - a ativação ocorre quando o computador é registrado com o Dell Enterprise Server/VE e recebe pelo menos um conjunto inicial de políticas.

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

Advanced Authentication – O produto Advanced Authentication oferece opções totalmente integradas de leitor de impressões digitais, cartão inteligente e cartão inteligente sem contato. O Advanced Authentication ajuda a gerenciar esses diversos métodos de autenticação de hardware, oferece suporte para login com unidades de criptografia automática, SSO e gerencia credenciais e senhas de usuário. Além disso, o Advanced Authentication pode ser usado para acessar não apenas computadores, mas também qualquer site, SaaS ou aplicativo. Depois que os usuários registram suas credenciais, o Advanced Authentication permite o uso dessas credenciais para fazer login no dispositivo e realizar a troca de senha.

Criptografia de dados de aplicativo - Criptografa qualquer arquivo salvo por um aplicativo protegido, usando uma substituição de categoria 2. Isso significa que qualquer diretório que possua uma proteção de categoria 2 ou superior, ou qualquer local que possua extensões específicas protegidas com categoria 2 ou superior, fará com que a ADE não criptografe esses arquivos.

BitLocker Manager – O Windows BitLocker foi projetado para ajudar a proteger computadores Windows ao criptografar os dados e os arquivos do sistema operacional. Para melhorar a segurança das implantações do BitLocker e simplificar e reduzir o custo de propriedade, a Dell fornece um console de gerenciamento único e central que trata de muitas preocupações de segurança e oferece uma abordagem integrada para gerenciar a criptografia em outras plataformas diferentes do BitLocker, sejam elas físicas, virtuais ou na nuvem. O BitLocker Manager oferece suporte para criptografia por BitLocker para sistemas operacionais, unidades fixas e BitLocker To Go. O BitLocker Manager permite que você integre perfeitamente o BitLocker às suas necessidades de criptografia existentes e gerencie o BitLocker com mínimo esforço ao mesmo tempo em que aperfeiçoa a segurança e a conformidade. O BitLocker Manager fornece gerenciamento integrado para recuperação de chaves, gerenciamento e imposição de políticas, gerenciamento de TPM automatizado, conformidade FIPS e relatórios de conformidade.

Credenciais em cache - As credenciais em cache são aquelas adicionadas ao banco de dados de PBA quando um usuário é autenticado no Active Directory. Essas informações sobre o usuário são mantidas para que ele possa fazer login quando não tiver uma conexão com o Active Directory (por exemplo, ao levar o notebook dele para casa).

Criptografia comum – A chave Comum torna os arquivos criptografados acessíveis a todos os usuários gerenciados no dispositivo em que os arquivos foram criados.

Desativar - A desativação ocorre quando o gerenciamento de SED é definido como Desligado no Remote Management Console. Quando o computador é desativado, o banco de dados de PBA é removido, e não haverá mais nenhum registro de usuário em cache.

EMS - External Media Shield - Esse serviço do cliente Dell Encryption aplica políticas à mídia removível e aos dispositivos de armazenamento externo.

Código de acesso do EMS - Esse serviço do Dell Enterprise Server/VE permite a recuperação de dispositivos protegidos pelo External Media Shield em que o usuário se esquece da senha e não consegue mais fazer login. A conclusão desse processo permite ao usuário redefinir a senha configurada na mídia removível ou dispositivo de armazenamento externo.

Cliente Encryption - O cliente Encryption é o componente presente no dispositivo que impõe as políticas de segurança, independentemente de o endpoint estar conectado ou não à rede e de ter sido perdido ou roubado. Criando um ambiente de computação confiável para endpoints, o cliente Encryption opera como uma camada acima do sistema operacional do dispositivo e fornece autenticação imposta de forma sistemática, criptografia e autorização, para maximizar a proteção de informações confidenciais.

Ponto de extremidade - um computador ou dispositivo de hardware móvel que é gerenciado pelo Dell Enterprise Server/VE.

Chaves de criptografia – Na maioria dos casos, o cliente Encryption usa a chave de usuário e mais duas chaves de criptografia adicionais. Entretanto, existem exceções: todas as políticas do SDE e a política Proteger credenciais do Windows usam a chave do SDE. As políticas Criptografar arquivo de paginação do Windows e Proteger arquivo de hibernação do Windows usam suas próprias chaves, a Chave de uso geral (GPK - General Purpose Key). A chave Comum torna os arquivos acessíveis a todos os usuários gerenciados no dispositivo em que foram criados. A chave Usuário torna os arquivos acessíveis apenas para o usuário que os criou, apenas no dispositivo em que foram criados. A chave Roaming de usuário torna os arquivos acessíveis apenas ao usuário que os criou, em qualquer dispositivo protegido do Windows (ou Mac).

Limpeza de criptografia – Uma limpeza de criptografia é o processo de verificar as pastas a serem criptografadas em um ponto de extremidade gerenciado para garantir que os arquivos contidos nelas estejam no estado de criptografia adequado. As operações habituais de criação de arquivo e alteração de nome não acionam uma varredura de criptografia. É importante entender quando uma varredura de criptografia pode ocorrer e o que pode influenciar os tempos de varredura resultantes, da seguinte forma: - Uma varredura de criptografia ocorrerá após o recebimento inicial de uma política com criptografia ativada. Isso pode ocorrer imediatamente após a ativação se sua política tiver criptografia ativada. - Se a política "Verificar estação de trabalho no login" estiver ativada, as pastas especificadas para criptografia serão verificadas toda vez que o usuário fizer login. - Uma varredura pode ser acionada novamente por certas mudanças de política subsequentes. Qualquer mudança de política relacionada à definição das pastas de criptografia, algoritmos de criptografia e uso de chave de criptografia (comum x usuário) ativará uma limpeza. Além disso, alternar entre a ativação e a desativação da criptografia acionará uma varredura de criptografia.

Chave Computador – Quando a criptografia está instalada em um servidor, a chave Computador protege as chaves de política e criptografia de arquivo de um servidor. A chave Computador é armazenada no Dell Enterprise Server/VE. O novo servidor troca certificados com o DDP Server durante a ativação e utiliza o certificado para eventos de autenticação subsequentes.

Senha de uso único (OTP) - Uma senha de uso único só pode ser usada uma vez e é válida apenas por um período limitado de tempo. A OTP exige que o TPM esteja presente, ativado e possua um proprietário. Para ativar a Senha de uso único, um dispositivo móvel é emparelhado com o computador usando o Security Console e o aplicativo Security Tools Mobile. O aplicativo Security Tools Mobile gera no dispositivo móvel a senha utilizada para fazer login no computador na tela de login do Windows. Conforme a política, o recurso de OTP pode ser usado para recuperar o acesso ao computador em caso de vencimento ou esquecimento da senha, desde que a OTP não tenha sido usada para o login no computador. O recurso de OTP pode ser usado para autenticação ou para recuperação, mas não para ambos. A segurança da Senha de uso único é superior a de alguns outros métodos de autenticação, pois a senha gerada pode ser utilizada apenas uma vez e vence em pouco tempo.

PBA (Preboot Authentication, Autenticação de pré-inicialização) – O recurso de PBA serve como uma extensão do BIOS ou do firmware de inicialização e garante um ambiente seguro e à prova de falsificação externo ao sistema operacional, como uma camada de autenticação confiável. A PBA impede a leitura de qualquer informação do disco rígido, como o sistema operacional, até o usuário confirmar que tem as credenciais corretas.

SED Management – O SED Management fornece uma plataforma para gerenciar com segurança as SEDs (self-encrypting drives, unidades de criptografia automática). Embora as SEDs forneçam sua própria criptografia, elas carecem de uma plataforma para gerenciar a criptografia e as políticas disponíveis. O SED Management é um componente central e escalonável de gerenciamento, que permite proteger e gerenciar seus dados com mais eficácia. O SED Management garante que você possa administrar sua empresa de forma mais rápida e descomplicada.

Usuário de servidor – Uma conta de usuário virtual criada pelo Dell Server Encryption com o objetivo de processar chaves de criptografia e atualizações de política. Essa conta de usuário não corresponde a nenhuma outra no computador nem no domínio e não tem nome de usuário ou senha que podem ser usados fisicamente. A conta recebe um valor de UCID exclusivo no Remote Management Console do Dell Enterprise Server/VE.

System Data Encryption (SDE) - O SDE foi projetado para criptografar arquivos do sistema operacional e de programas. Para atingir este objetivo, o SDE precisa ser capaz de abrir sua chave enquanto o sistema operacional estiver sendo inicializado. A intenção é evitar que um invasor altere ou ataque o sistema operacional off-line. O SDE não se destina a dados de usuário. Criptografia comum e de chave de usuário são destinadas a dados confidenciais do usuário, pois exigem uma senha de usuário para desbloquear as chaves de criptografia. As políticas de SDE não criptografam os arquivos necessários para que o sistema operacional comece o processo de inicialização. As políticas de SDE não exigem autenticação de pré-inicialização e não interferem no Registro mestre de inicialização de nenhuma forma. Quando o computador é inicializado, os arquivos criptografados ficam disponíveis antes de qualquer usuário fazer login (para ativar ferramentas de backup e recuperação, SMS e gerenciamento de patches). Desativar a criptografia SDE aciona a descriptografia automática de todos os

arquivos e diretórios criptografados do SDE para os usuários relevantes, independentemente de outras políticas de SDE, como, por exemplo, Regras de criptografia SDE.

Módulo TPM (Trusted Platform Module - Módulo de plataforma confiável) – É um chip de segurança com três funções principais: armazenamento seguro, medição e confirmação. O cliente Encryption usa o TPM para sua função de armazenamento seguro. O TPM pode também fornecer recipientes criptografados para o vault de software. O TPM é também necessário para uso com o BitLocker Manager e o recurso de Senha de uso único.

Criptografia de usuário – A chave Usuário torna os arquivos acessíveis apenas para o usuário que os criou, apenas no dispositivo em que foram criados. Ao executar o Dell Server Encryption, a criptografia de usuário é convertida para criptografia comum. Uma exceção é feita para dispositivos de mídia externos: quando inseridos em um servidor com o Encryption instalado, os arquivos são criptografados com a chave de roaming de usuário.