Dell Encryption Personal

Installation Guide v11.9

January 2024
Rev. A01

DELL Technologies

Notas, avisos e advertências

NOTA: NOTA fornece informações importantes para ajudar você a usar melhor o computador.

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, lesões corporais ou risco de morte.

Contents

1

Visão geral

Este guia presume que o Advanced Authentication foi instalado com o Encryption Personal.

Encryption Personal

O Encryption Personal tem como objetivo proteger os dados no seu computador, mesmo em caso de perda ou roubo.

Para preservar a segurança dos seus dados sigilosos, o Encryption Personal criptografa os dados no seu computador Windows. Sempre é possível acessar os dados quando você estiver logado no computador, mas usuários não autorizados não têm acesso a esses dados protegidos. Dados sempre permanecem criptografados na unidade de disco, mas, como a criptografia ocorre em segundo plano, não é preciso mudar a maneira de trabalhar com os aplicativos e dados.

Normalmente, o aplicativo descriptografa os dados à medida que você trabalha com eles. Ocasionalmente, é possível que um aplicativo tente acessar um arquivo enquanto o aplicativo está fazendo sua criptografia ou descriptografia. Se isso acontecer, após um ou dois segundos, uma caixa de diálogo é exibida com a opção de aguardar ou cancelar a criptografia/descriptografia. Se você optar por esperar, o aplicativo liberará o arquivo assim que a operação for concluída (geralmente, em alguns segundos).

Advanced Authentication

O Data Security Console é a interface que guia os usuários pelo processo de configuração de suas credenciais de PBA e perguntas para autorrecuperação, com base na política definida pelo administrador local.

Consulte Configurar as definições do administrador do Advanced Authentication e consulte o *Dell Data Security Console User Guide* (Guia do usuário do Data Security Console) para saber como usar a autenticação avançada.

Entre em contato com o Dell ProSupport for Software

Ligue para 877-459-7304, extensão 4310039 para obter suporte por telefone 24x7, para o seu produto Dell.

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

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

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

2

Requisitos

Esses requisitos detalham tudo que é necessário para a instalação do Encryption Personal.

Criptografia

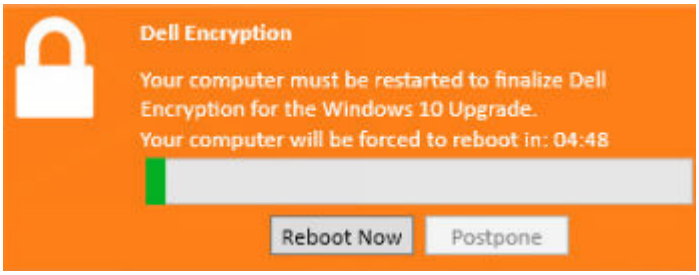
- O Encryption Personal requer uma qualificação para a instalação bem-sucedida. A qualificação é fornecida quando você compra o Encryption Personal. Dependendo de como você compra o Encryption Personal, poderá instalar manualmente a qualificação, usando as instruções simples que a acompanham. Você também pode inserir a qualificação na linha de comando. Se o Encryption Personal for instalado usando o Dell Digital Delivery, a instalação da qualificação será executada pelo serviço do Dell Digital Delivery. (Os mesmos binários são usados para Encryption Enterprise e Encryption Personal. O código de direito informa ao instalador a versão a ser instalada.
- As contas Microsoft e Office 365 são compatíveis ao executar o Encryption Personal v11.0 ou posterior no Windows 10.
- Para ativar uma conta do Microsoft Live com o Encryption Personal, consulte o artigo da base de conhecimento 124722.
- É necessário usar uma senha do Windows (se ela ainda não existir) para proteger o acesso aos seus dados criptografados. Criar uma senha para o seu computador impede que outras pessoas façam login na sua conta de usuário sem a sua senha. O Encryption Personal não será ativado se a senha não for criada.
- O Dell Encryption não pode receber upgrade para v10.7.0 a partir de versões anteriores à v8.16.0. Os endpoints que executam versões anteriores à v8.16.0 devem fazer upgrade para v8.16.0 e, em seguida, fazer upgrade para v10.7.0.
- O Dell Encryption usa os conjuntos de instrução de criptografia da Intel, o Integrated Performance Primitives (IPP). Para obter mais informações, consulte o artigo da base de conhecimento 126015.

1. Vá para o Painel de Controle do Windows (**Iniciar** > **Painel de Controle**).
2. Clique no ícone **Contas de usuário**.
3. Clique em **Criar uma senha para sua conta**.
4. Digite a senha e digite-a novamente.
5. Opcionalmente, adicione uma dica de senha.
6. Clique em **Criar senha**.
7. Reinicie o computador.

- 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. 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/upgrade.
- Não realize alterações no computador, incluindo a inserção ou a remoção de unidades externas (USB), durante a instalação/desinstalação/upgrade.
- Para reduzir o tempo de criptografia inicial (bem como o tempo de descriptografia, se estiver desinstalando), 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 Encryption Client 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. Se tiver perguntas ou preocupações, entre em contato com o Dell ProSupport.
- O Encryption Client agora suporta o modo Audit. O modo Audit permite que os administradores implementem o Encryption Client como parte da imagem corporativa, em vez de usar um SCCM de terceiros ou soluções similares para implementar o Encryption Client. Para obter instruções sobre como instalar o cliente Encryption em uma imagem corporativa, consulte o artigo da base de conhecimento 129990.
- O TPM é usado para selar a Chave de uso geral. Portanto, se estiver executando o cliente Encryption, limpe o TPM no BIOS antes de instalar um novo sistema operacional no computador de destino.

- O client Encryption é testado e compatível com vários antivírus populares baseados em assinatura e com várias soluções antivírus orientadas por IA, inclusive McAfee Virus Scan Enterprise, McAfee Endpoint Security, Symantec Endpoint Protection, CylancePROTECT, CrowdStrike Falcon, Carbon Black Defense e muitos outros. Exclusões codificadas são incluídas por padrão para muitos provedores de antivírus a fim de evitar incompatibilidades entre a varredura e a criptografia do antivírus.

  Se sua organização usa um provedor antivírus não listado ou enfrenta algum problema de compatibilidade, consulte o artigo da KB 126046 ou entre em contato com o Dell ProSupport para obter assistência na validação da configuração de interoperação entre suas soluções de software e as soluções Dell Data Security.
- Não há suporte para reinstalação do 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.
- Verifique periodicamente dell.com/support para obter a documentação e recomendações técnicas mais recentes.
- Seguindo o upgrade do recurso do Windows 10, é **necessário** reiniciar para finalizar o Dell Encryption. A mensagem a seguir é exibida na área de notificações após os upgrades do recurso do Windows 10:



Pré-requisitos

- O Microsoft .Net Framework 4.5.2 (ou posterior) é necessário para os instaladores mestre e filho. O instalador não instala o componente Microsoft .Net Framework.

  NOTA: .Net Framework 4,6 (ou posterior) é necessário ao executar o modo FIPS.

- O instalador mestre instala os pré-requisitos a seguir, se eles ainda não estiverem instalados no computador. **Quando estiver usando o instalador filho**, será necessário instalar esse componente antes de instalar o Encryption.

Pré-requisito
○ Visual C++ 2012 Update 4 ou Redistributable Package mais recente (x86 ou x64) ○ Visual C++ 2017 Update 3 ou Redistributable Package mais recente (x86 ou x64) ○ Os aplicativos e pacotes de instalação autenticados com certificados SHA1 funcionarão, mas um erro será exibido no endpoint durante a instalação ou execução do aplicativo sem essas atualizações instaladas

Hardware

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

Hardware
○ Processador Intel Pentium ou AMD ○ 110 MB de espaço em disco disponível ○ 512 MB de RAM **NOTA:** O espaço em disco livre adicional é necessário para criptografar os arquivos no endpoint. Este tamanho varia com base nas políticas e capacidade da unidade.

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

Hardware integrado opcional
○ TPM 1.2 ou 2.0

Sistemas operacionais

- A tabela a seguir detalha os sistemas operacionais compatíveis.

Sistemas operacionais Windows (32 e 64 bits)
○ Windows 10: Education, Enterprise, Pro v1909-v22H2 (Atualização de novembro de 2019/19H2 - Atualização de novembro de 2022/22H2) **Nota:** OEMs e ODMs não são enviados com Windows 10 v2004 (Atualização de maio de 2020/20H1 e posterior) com arquitetura de 32 bits. Para obter mais informações, acesse https://docs.microsoft.com/windows-hardware/design/minimum/minimum-hardware-requirements-overview. ▪ Windows 10 2019 LTSC ▪ Windows 10 2021 LTSC ○ Windows 11: Enterprise, Pro v21H2 - 22H2

Sistemas operacionais Encryption External Media

- A mídia externa precisa ter aproximadamente 55 MB disponíveis, além de espaço livre na mídia igual ao maior arquivo a ser criptografado para hospedar o Encryption External Media.
- Os detalhes a seguir oferecem suporte a sistemas operacionais ao acessar a mídia protegida da Dell.

Sistemas operacionais Windows suportados para acessar mídia criptografada (32 e 64 bits)
○ Windows 10: Education, Enterprise, Pro v1909-v22H2 (Atualização de novembro de 2019/19H2 - Atualização de novembro de 2022/22H2) **Nota:** OEMs e ODMs não são enviados com Windows 10 v2004 (Atualização de maio de 2020/20H1 e posterior) com arquitetura de 32 bits. Para obter mais informações, acesse https://docs.microsoft.com/windows-hardware/design/minimum/minimum-hardware-requirements-overview. ▪ Windows 10 2019 LTSC ▪ Windows 10 2021 LTSC ○ Windows 11: Enterprise, Pro v21H2 - 22H2

Sistemas operacionais Mac suportados para acessar mídias criptografadas (kernels de 64 bits)
○ macOS High Sierra 10.13.5 - 10.13.6 ○ macOS Mojave 10.14.0 - 10.14.4 ○ macOS Catalina 10.15.5 - 10.15.6

Localização

- O Encryption é compatível com interfaces do usuário de vários idiomas e foi traduzido nos idiomas a seguir.

Suporte de idioma	
○ EN - Inglês	○ JA - Japonês
○ ES - Espanhol	○ KO - Coreano
○ FR - Francês	○ PT-BR - Português, Brasil
○ IT - Italiano	○ PT-PT - Português, Portugal (ibérico)

Suporte de idioma	
○ DE - Alemão	

SED Manager

- 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 com 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 com criptografia automática que oferecem suporte ao módulo de HCA. Esta configuração não compatível seria uma configuração de reposição.
- Se o computador destinado para criptografia estiver equipado com uma unidade com 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.
- O SED Manager não é compatível com configurações de múltiplas unidades.
- **NOTA:**

  Em função da natureza do RAID e das SEDs, o Gerenciador 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 operacional travará quando alterado de *RAID=On* para *AHCI*.

- O instalador mestre instala os pré-requisitos a seguir, se eles ainda não estiverem instalados no computador. **Quando estiver usando o instalador filho**, você precisará instalar esse componente antes de instalar o SED Manager.

Pré-requisito
○ Visual C++ 2017 Update 3 ou Redistributable Package mais recente (x86 ou x64)
○ Os aplicativos e pacotes de instalação autenticados com certificados SHA1 funcionarão, mas um erro será exibido no endpoint durante a instalação ou execução do aplicativo sem essas atualizações instaladas

- A configuração de unidades de autocriptografia para o SED Manager difere entre unidades NVMe e não-NVMe (SATA), como se segue.
  - Qualquer unidade NVMe que estiver sendo aproveitada para PBA:
    - Se o dispositivo Dell foi produzido em 2018 ou posteriormente: RAID ON ou AHCI pode ser aproveitado com unidades NVMe.
    - O modo de inicialização do BIOS deve ser definido como UEFI (Unified Extensible Firmware Interface). As ROMs de operação preexistentes devem ser desativadas.
  - Qualquer unidade não NVMe que esteja sendo aproveitada para o PBA:
    - A operação SATA do BIOS pode ser definida como AHCI ou RAID ON.
    - O sistema operacional irá travar quando alternado de RAID ON > AHCI se os drivers do controlador AHCI não estiverem pré-instalados. Para obter instruções sobre como alternar de RAID > AHCI (ou vice-versa), consulte o artigo da base de conhecimento 124714.

  Os SEDs compatíveis com OPAL suportadas exigem drivers da tecnologia Intel Rapid Storage atualizados, localizados em www.dell.com/support. A Dell recomenda o driver mais recente da tecnologia de armazenamento Intel Rapid com unidades NVMe.

  NOTA: Os drivers da tecnologia Intel Rapid Storage são dependentes da plataforma. O driver do seu sistema pode ser encontrado no link acima com base no modelo do seu computador.

- As configurações de criptografia de vários discos com o SED Manager exigem o seguinte:
  - Todos os discos no sistema de destino devem ser SEDs.
  - Todos os discos no sistema de destino devem ser configurados no mesmo modo de inicialização.
  - No modo de inicialização UEFI, o sistema operacional pode ser instalado em qualquer disco de destino.

- No modo de inicialização Legacy, o sistema operacional deve ser instalado no primeiro disco (Disco 0). Se o sistema operacional não estiver instalado no primeiro disco, a criptografia de vários discos será desativada.

- Algumas versões do BIOS podem ativar o SID de bloco por padrão, o que pode inibir o SED Manager. Para obter mais informações, consulte o artigo da base de conhecimento 126083.
- O recurso de atualização direta do Windows 10 v1607 (Atualização de aniversário/Redstone 1), para o Windows 10 v1903 (May 2019 Update/19H1) não é compatível com o Dell Encryption. A Dell recomenda atualizar o sistema operacional para uma versão mais recente das atualizações do recurso se for atualizar para Windows 10 v1903. Qualquer tentativa de atualização do Windows 10 v1607 para v1903 resulta em uma mensagem de erro e a atualização é impedida.
- **NOTA:** É necessária uma senha para a Autenticação de pré-inicialização. A Dell recomenda configurar uma senha de mínimo 9 ou mais caracteres.

- **NOTA:** Uma senha é necessária para todos os usuários adicionados no painel *Adicionar usuário*. Usuários com senha de comprimento zero serão bloqueados da ativação seguinte do computador.
- **NOTA:** Computadores protegidos por SED Manager precisam ser atualizados para o Windows 10 v1703 (Creators Update/Redstone 2) ou mais recente antes de atualizar para Windows 10 v1903 (May 2019 Update/19H1) ou posterior. Se este caminho de upgrade for tentado, uma mensagem de erro será exibida.
- O SED Manager exige o uso do Dell Custom Credential Provider para sincronizar as alterações de senha do Windows e as chaves de criptografia de dados. Se você precisar usar aplicativos de terceiros que usam provedores de credenciais personalizados em execução em computadores protegidos pelo SED Manager, você deverá iniciar as alterações de senha do Windows por meio do Data Security Console. Para obter informações sobre como alterar sua senha no Data Security Console, consulte o capítulo *Senha* no Guia do usuário do Data Security Console.

Hardware

- Para obter a lista mais atualizada de SEDs compatíveis com Opal que são compatíveis com o SED Manager, consulte o artigo da base de conhecimento 126855.
- Para obter a lista mais atualizada de plataformas que são compatíveis com o SED Manager, consulte o artigo da base de conhecimento 126855.
- Para obter uma lista de dock stations e adaptadores que são compatíveis com o SED Manager, consulte o artigo da base de conhecimento 124241.

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-FR - (francês suíço)	EN-GB - Inglês (inglês britânico)
DE-CH - (alemão suíço)	EN-CA - Inglês (inglês canadense)
EN-US - Inglês (inglês americano)	

Suporte a teclado internacional - Non-UEFI	
AR - Árabe (usando letras latinas)	EN-US - Inglês (inglês americano)
DE-FR - (francês suíço)	EN-GB - Inglês (inglês britânico)
DE-CH - (alemão suíço)	EN-CA - Inglês (inglês canadense)

Sistemas operacionais

- A tabela a seguir detalha os sistemas operacionais compatíveis.

Sistemas operacionais Windows (32 e 64 bits)
○ Windows 10: Education, Enterprise, Pro v1909-v22H2 (Atualização de novembro de 2019/19H2 - Atualização de novembro de 2022/22H2) **Nota:** OEMs e ODMs não são enviados com Windows 10 v2004 (Atualização de maio de 2020/20H1 e posterior) com arquitetura de 32 bits. Para obter mais informações, acesse https://docs.microsoft.com/windows-hardware/design/minimum/minimum-hardware-requirements-overview. ▪ Windows 10 2019 LTSC ▪ Windows 10 2021 LTSC ○ Windows 11: Enterprise, Pro v21H2 - 22H2

Os recursos de autenticação estão disponíveis somente quando a autenticação pré-inicialização é ativada.

Localização

O SED Manager é compatível com interfaces do usuário multi-idiomas e foi traduzido nos idiomas a seguir. O modo UEFI e a autenticação de pré-inicialização são compatíveis nos idiomas a seguir:

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

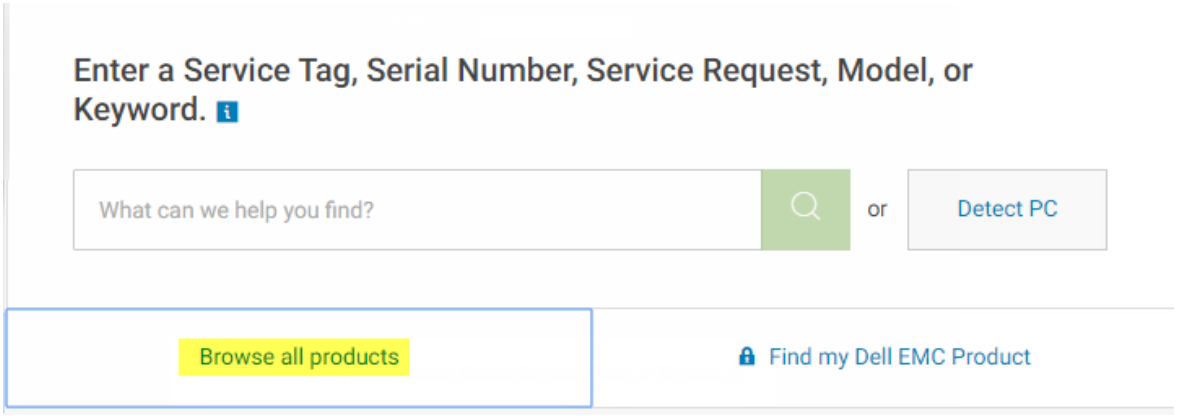
3

Fazer 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 **Procurar em todos os produtos**.



2. Selecione **Segurança** na lista de produtos.
3. Selecione **Dell Data Security**.

   Depois de fazer essa seleção uma vez, o site se lembra.

4. Selecione o produto Dell.

   Exemplos:

   Dell Encryption Enterprise

   Dell Endpoint Security Suite Enterprise

5. Selecione **Drivers e downloads**.
6. Selecione o tipo de sistema operacional do cliente desejado.
7. Selecione **Dell Encryption** na correspondência. A sequência descrita acima é apenas um exemplo, por isso, pode ser um pouco diferente. Por exemplo, pode ser que não haja quatro arquivos para você escolher.
8. Selecione **Download**.

   Vá para Instalar o Encryption Personal.

4

Instalação

Você pode instalar o Encryption Personal usando o instalador mestre (recomendado) ou extraindo os instaladores filhos do instalador mestre. De qualquer uma das formas, o Encryption Personal pode ser instalado pela interface do usuário, pela linha de comando ou por scripts e usando qualquer tecnologia push disponível para a sua organização.

Os usuários devem consultar os seguintes arquivos de ajuda para obter ajuda com o aplicativo:

NOTA: Se a criptografia baseada em política for instalada antes do Encryption Management Agent, poderá ocorrer falha no computador. Esse problema é causado por falha no carregamento do driver de suspensão de criptografia que gerencia o ambiente de PBA. Como solução temporária, use o instalador mestre ou certifique-se de que a criptografia baseada em política seja instalada depois do Encryption Management Agent.

- Consulte *Dell Encrypt Help* para aprender como usar os recursos do Encryption. Acesse a ajuda em `<Install dir>\Program Files\Dell\Dell Data Protection\Encryption\Help`.
- Consulte a Encryption External Media *Encryption External Media* para aprender sobre os recursos do Encryption External Media. Acesse a ajuda em `<Install dir>\Program Files\Dell\Dell Data Protection\Encryption`.
- Consulte a *Ajuda do Encryption Personal* para aprender como usar os recursos do Advanced Authentication. Acesse a ajuda em `<Install dir>\Program Files\Dell\Dell Data Protection\Security Tools\Help`.

Importar o direito

A instalação do Encryption Personal requer uma chave de registro no computador de destino. Essa chave de registro é adicionada por meio da interface de linha de comando, durante a instalação, ou por meio da GUI, antes da instalação.

Para adicionar a chave de registro por meio da interface de linha de comando, consulte Instalação por linha de comando.

Para adicionar a chave de registro por meio da GUI:

1. Abra um editor de texto.
2. Adicione o texto abaixo.

   ```
   [HKEY_LOCAL_MACHINE\Software\Dell\Dell Data Protection\Entitlement]

   "SaEntitlement"="1:PE:{XXXXX-XXX-XXXX-XXX-XXXX-
   XXXXXXXXXXXX}:xXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX="
   ```

3. Salve o arquivo de texto com a extensão `.reg`.
4. Clique duas vezes no arquivo de registro salvo para importar o direito do Encryption Personal.

Escolher um método de instalação

Há dois métodos para instalar o cliente. Selecione **um**:

- Instalação interativa – RECOMENDÁVEL
- Instalação por linha de comando

Instalação interativa

Para instalar o Encryption Personal, o instalador deve encontrar o direito apropriado no computador. Se o direito apropriado não for encontrado, o Encryption Personal não poderá ser instalado.

- O instalador mestre instala diversos clientes. No caso do Encryption Personal, ele instala o gerenciamento do Encryption e do SED.

- Os arquivos de log do instalador mestre estão localizados na pasta `C:\ProgramData\Dell\Dell Data Protection\Installer.`

1. Instale o direito no computador de destino, se necessário. Instruções para adicionar a qualificação ao computador estão incluídas com o e-mail, que discute informações de licença.
2. Copie o arquivo DDSSetup.exe para o computador local.
3. Clique duas vezes em DDSSetup.exe para iniciar o instalador.
4. Uma caixa de diálogo que alerta você sobre o status dos pré-requisitos de instalação. A instalação demora vários minutos.
5. Clique em **Avançar** na tela de boas-vindas.
6. Leia o acordo de licença, concorde com os termos e clique em **Avançar**.
7. Clique em **Avançar** para instalar o Encryption Personal no local padrão `C:\Program Files\Dell\Dell Data Protection\.`
8. O Authentication é instalado por padrão e não pode ser desmarcado. Isso está listado como Security Framework no instalador.

   Clique em **Avançar**.
9. Clique em **Instalar** para iniciar a instalação.

   Uma janela de status é exibida. A instalação demora vários minutos.
10. Selecione **Sim, quero reiniciar meu computador agora** e clique em **Concluir**.
11. Quando o computador tiver sido reiniciado, faça a autenticação no Windows.

A instalação do Encryption Personal e do Advanced Authentication está concluída.

O Assistente de instalação e configuração do Encryption Personal será coberto separadamente.

Depois de a execução do Assistente de instalação e configuração do Encryption Personal ter sido concluída, inicie o Console do administrador do Encryption Personal.

O restante desta seção fornece mais detalhes sobre as tarefas de instalação e pode ser pulado. Vá para Assistentes de configuração do Advanced Authentication e do Encryption Personal.

Instalação por linha de comando

Para instalar o Encryption Personal usando a linha de comando, primeiro, será necessário extrair os arquivos filhos executáveis do instalador mestre. Consulte Extrair os instaladores filhos do instalador mestre. Quando terminar, retorne para esta seção.

- Instale o direito no computador de destino, se necessário.
- **NOTA:** Os logs do Dell Encryption não especificam se um armazenamento em disco insuficiente causou a falha de instalação.
- Opções:

  Para uma instalação por linha de comando, os switches deverão ser especificados primeiro. A tabela a seguir detalha as opções disponíveis para a instalação.

Switch	Significado
/s	Modo silencioso
/z	Passar dados para a variável de sistema CMDLINE do InstallScript

- Parâmetros:

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

Parâmetros
InstallPath=caminho para local alternativo de instalação.
FEATURE=PE

Parâmetros
ENTITLEMENT=1:PE:{Chave de qualificação do Encryption Personal aqui} **NOTA:** Este parâmetro pode ser usado **apenas** com o Encryption Personal

- Exemplo de instalação por linha de comando

  A reinicialização foi suprimida nos exemplos de instalação por linha de comando. Entretanto, uma eventual reinicialização é necessária.

  Não será possível iniciar a criptografia com base na política até que o computador seja reinicializado.

  Lembre-se de cercar um valor que contenha um ou mais caracteres especiais, como um espaço em branco, com aspas com caractere de escape.

  As linhas de comando diferenciam letras maiúsculas de minúsculas.

- O exemplo a seguir instala o Encryption client (instalação silenciosa, sem reinicialização; instalação no local padrão `C:\Program Files\Dell\Dell Data Protection`), transmitindo a chave de qualificação diretamente para o instalador.

  DDPE_XXbit_setup.exe /s /v"ENTITLEMENT=1:PE:{XXXXX-XXX-XXXX-XXX-XXXX-XXXXX-XXXXXXX}:xXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX= /l*v c:\Shieldinstall.log /qn /norestart"

- O exemplo a seguir instala o Encryption Personal e a Advanced Authentication (instalação silenciosa, sem reinicialização; instalação no local padrão `C:\Program Files\Dell\Dell Data Protection`).

  ```
  DDSSetup.exe /s /z"\"FEATURE=PE\""
  ```

- O exemplo a seguir instala o Encryption Personal e a Advanced Authentication (instalação silenciosa, sem reinicialização; instalação no local padrão `C:\Program Files\Dell\My_New_Folder`).

  ```
  DDSSetup.exe /s /z"\"FEATURE=PE, InstallPath=C:\Program Files\Dell\My_New_Folder\""
  ```

  Quando o computador for reiniciado, faça a autenticação no Windows.

  A instalação do Encryption Personal e do Advanced Authentication está concluída.

  O Assistente de instalação e configuração do Encryption Personal será coberto separadamente.

  Depois de a execução do Assistente de instalação e configuração do Encryption Personal ter sido concluída, inicie o Console do administrador do Encryption Personal.

  O restante desta seção fornece mais detalhes sobre as tarefas de instalação e pode ser pulado. Vá para Assistentes de configuração do Advanced Authentication e do Personal Edition Wizards.

5

Assistentes de configuração do Advanced Authentication e do Encryption Personal

Faça login com seu nome de usuário e senha do Windows. Você acessa imediatamente o Windows. A interface pode parecer diferente do que você está acostumado a ver.

1. O UAC pode solicitar a você que execute o aplicativo. Em caso afirmativo, clique em Sim.
2. Depois da reinicialização da instalação inicial, o assistente de ativação do Advanced Authentication é mostrado. Clique em **Avançar**.
3. Digite uma nova Senha de administrador de criptografia (EAP - Encryption Administrator Password) e digite-a novamente. Clique em **Avançar**.

   Nota: a senha de administrador do Encryption deve ter no mínimo oito caracteres e não pode exceder 127 caracteres.
4. Informe um local de backup em uma unidade de rede ou em uma mídia removível para armazenar as informações de recuperação e clique em **Avançar**.
5. Clique em **Aplicar** para iniciar a ativação do ST.

   Depois que o assistente de ativação do Advanced Authentication tiver concluído, vá para a próxima etapa.
6. Inicie o Assistente de instalação do Encryption Personal com o ícone do Dell Encryption na área de notificação (ele pode abrir sozinho).

   Esse Assistente de configuração o ajuda a usar criptografia para proteger as informações deste computador. Enquanto o assistente não for concluído, não será possível iniciar a criptografia.

   Leia a tela de boas-vindas e clique em **Avançar**.
7. Selecione um modelo de política. O modelo de política estabelece as configurações padrão de políticas para criptografia.

   Você poderá facilmente aplicar um modelo de política diferente ou personalizar o modelo selecionado no Console de gerenciamento local quando a configuração inicial estiver concluída.

   Clique em **Avançar**.
8. Leia e confirme o aviso de senha do Windows. Se quiser criar uma senha do Windows agora, consulte Requisitos.
9. Crie uma Senha de administrador de criptografia (EAP — Encryption Administrator Password) com 8 a 127 caracteres e confirme. A senha deverá conter caracteres alfabéticos, numéricos e especiais. Essa senha pode ser a mesma que a EAP configurada para o Advanced Authentication, mas não há relação entre elas. **Anote e guarde essa senha em um local seguro**. Clique em **Avançar**.

   Nota: a senha de administrador do Encryption deve ter no mínimo oito caracteres e não pode exceder 127 caracteres.
10. Clique em **Procurar** para escolher uma unidade de rede ou um armazenamento removível e fazer o backup de suas chaves de criptografia (que são incorporadas a um aplicativo chamado LSARecovery_[nome_do_host].exe).

    No caso de determinadas falhas de computador, essas chaves serão usadas para recuperar seus dados.

    Além disso, alterações futuras nas políticas possivelmente exigirão que o backup das chaves de criptografia seja feito novamente. Se a unidade de rede ou o armazenamento removível estiver disponível, o backup de suas chaves de criptografia será feito em segundo plano. Entretanto, se o local não estiver disponível (por exemplo, se o dispositivo de armazenamento removível original não tiver sido inserido no computador), as alterações de política não entram em vigor até que o backup manual das chaves de criptografia seja feito.

    NOTA: Para obter informações sobre como fazer o backup manual das chaves de criptografia, clique em "**? > Ajuda**" no canto superior direito do Console de gerenciamento local ou clique em **Iniciar > Dell > Ajuda de criptografia**.

    Clique em **Avançar**.

11. Uma lista de configurações de criptografia é mostrada na tela Confirmar configurações de criptografia. Analise os itens e clique em **Confirmar** quando estiver satisfeito com as configurações.

    A configuração do computador é iniciada. Uma barra de status informa o andamento da configuração.

12. Clique em **Concluir** para concluir a configuração.

13. Uma reinicialização será necessária depois de configurar o computador para criptografia. Clique em **Reinicializar agora** ou você pode adiar a reinicialização 20 minutos por 5 vezes.

14. Depois de reinicializar o computador, abra o Console de gerenciamento local a partir do menu Iniciar para ver o status da criptografia.

    A criptografia ocorre em segundo plano. O Console de gerenciamento local pode ser deixado aberto ou fechado. A criptografia dos arquivos será feita em qualquer caso. O computador pode ser usado normalmente durante a criptografia.

15. O computador reinicializa mais uma vez quando a verificação terminar.

    Quando terminarem todas as varreduras de criptografia e reinicializações, você pode verificar o status de conformidade abrindo o Console de gerenciamento local. A unidade é identificada como "Em conformidade".

6

Definições do console de configuração

As configurações padrão permitem que os administradores e usuários usem a autenticação avançada imediatamente depois da ativação, sem necessidade de configuração adicional. Os usuários são adicionados automaticamente como usuários da autenticação avançada, ao iniciarem a sessão no computador com suas senhas do Windows, mas, por padrão, a autenticação por vários fatores no Windows não está ativada.

Para configurar os recursos de autenticação avançada, você precisa ser administrador no computador.

Alterar o local de backup e a senha do administrador

Depois da ativação da autenticação avançada, o local de backup e a senha do administrador podem ser alterados, caso seja necessário.

1. Como administrador, abra o Dell Data Security Console pelo atalho da área de trabalho.
2. Clique no bloco **Configurações de administrador**.
3. Na caixa de diálogo Autenticação, digite a senha do administrador que foi configurada durante a ativação e clique em **OK.**
4. Clique na guia **Configurações de administrador**.
5. Na página Alterar senha de administrador, para alterar a senha, digite uma nova senha com 8 a 32 caracteres e que contenha no mínimo uma letra, um número e um caractere especial.
6. Digite a senha uma segunda vez para confirmá-la e clique em **Aplicar**.
7. Para alterar o local no qual a chave de recuperação está armazenada, selecione **Alterar local de backup** no painel esquerdo.
8. Selecione um novo local para o backup e clique em **Aplicar**.

   O arquivo de backup precisa ser salvo em uma unidade de rede ou em mídia removível. O arquivo de backup contém as chaves que são necessárias para recuperar dados neste computador. O Dell ProSupport precisa ter acesso a esse arquivo para ajudar você a recuperar os dados.

   O backup dos dados de recuperação é feito automaticamente, no local especificado. Se o local não estiver disponível (por exemplo, se a unidade USB de backup não estiver inserida), o Advanced Authentication solicitará um local para fazer backup dos dados. O acesso aos dados de recuperação é necessário para iniciar a criptografia.

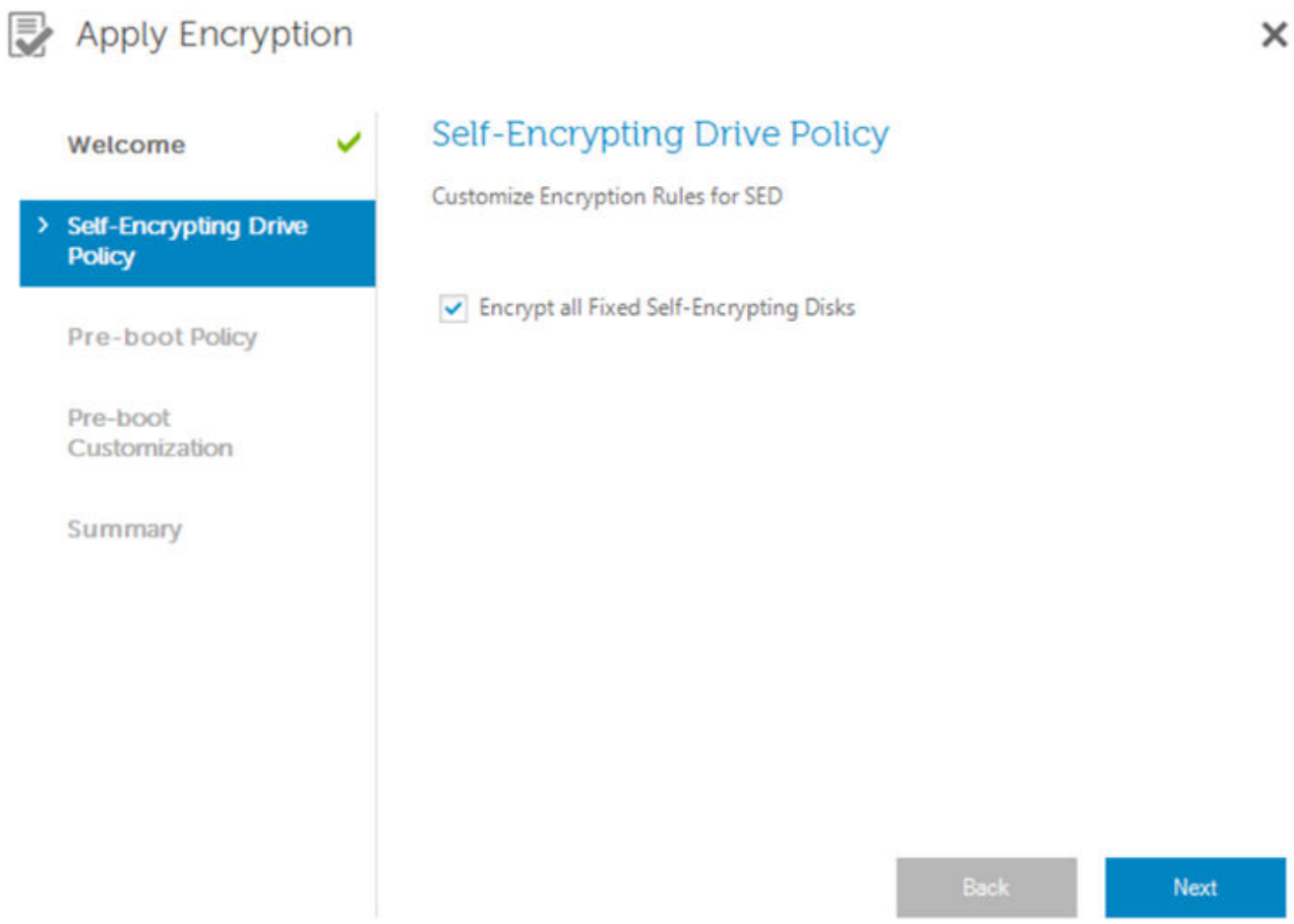
Configuração da autenticação pré-inicialização

A PBA está disponível se o seu computador estiver equipado com um SED. Ambos são configurados pela guia Criptografia. Quando o SED Manager assume a propriedade do SED, a PBA é ativada.

Para ativar o gerenciamento de SED:

1. No Data Security Console, clique no bloco **Configurações de administrador**.
2. Confirme que o local de backup possa ser acessado pelo computador.

   Se a mensagem *Local de backup não encontrado* for exibida e o local do backup estiver em uma unidade USB, sua unidade não está conectada ou está conectada em um slot diferente daquele usado durante o backup. Se a mensagem for mostrada e o local de backup estiver em uma unidade de rede, ela não pode ser acessada pelo computador. Se for necessária a alteração do local de backup, na guia **Configurações de administrador**, selecione **Alterar local do backup** para alterar o local para o slot atual ou para a unidade acessível. Alguns segundos após a alteração do local, o processo de ativação da criptografia poderá continuar.
3. Clique na guia **Criptografia** e, em seguida, clique em **Criptografar**.
4. Na página de Boas-vindas, clique em **Avançar**.
5. Selecione **Criptografar todos os discos de autocriptografia corrigidos** para ativar a criptografia de vários discos.



6. Na página Política de pré-inicialização, altere ou confirme os valores a seguir e clique em **Avançar**.

Tentativas de login de usuário não armazenado em cache	Quantas vezes um usuário desconhecido pode tentar fazer login. Um usuário que não tenha se conectado ao computador antes (nenhuma credencial armazenada em cache).
Tentativas de login de usuário armazenado em cache	O número de vezes que um usuário conhecido pode tentar fazer login.
Tentativas de responder às perguntas de recuperação	Número de vezes que o usuário pode tentar digitar a resposta correta.
Ativar senha para apagar criptografia	Selecione para ativar.
Digite a senha para apagar criptografia	Uma palavra ou código de até 100 caracteres usado como mecanismo de segurança à prova de falhas. Digitar essa palavra ou código no campo de nome de usuário ou senha durante a autenticação de pré-inicialização iniciará uma criptoeliminação, que remove as chaves do armazenamento seguro. Assim que esse processo for acionado, a unidade será irrecuperável. Deixe esse campo em branco se você não quiser uma senha para apagar criptografia disponível em caso de emergência. Deixe esse campo em branco se você não quiser ter uma senha para apagar criptografia disponível em caso de emergência.
Lembrar-me	Ativa ou desativa a capacidade dos usuários selecionarem Lembrar-me na tela de login do PBA.

7. Na página Personalização de pré-inicialização, digite uma mensagem personalizada para ser exibida na tela de Autenticação de pré-inicialização (PBA) e clique em **Avançar**.

Texto do título de pré-inicialização	Esse texto é mostrado na parte superior da tela de PBA. Se você deixar esse campo em branco, nenhum título será mostrado. O texto não passa para a linha seguinte e pode ser truncado após 17 caracteres.
Texto de informações de suporte	Texto a ser mostrado na tela de informações de suporte de PBA. Personalize a mensagem para incluir detalhes sobre como entrar em contato com o help desk ou com o administrador de segurança. Se não houver texto nesse campo, as informações de contato de suporte não estarão disponíveis para o usuário. A quebra do texto ocorre a nível de palavra, não a nível de caractere. Se uma palavra tiver mais de aproximadamente 50 caracteres, ela não será quebrada e nenhuma barra de rolamento estará presente; o texto ficará truncado.
Texto do aviso legal	Esse texto é mostrado antes que o usuário possa fazer login no dispositivo. Por exemplo: "Ao clicar em OK, você concorda em aceitar a política de utilização do computador". Se não for digitado texto nesse campo, o texto ou os botões OK/Cancelar não serão mostrados. A quebra do texto ocorre a nível de palavra, não a nível de caractere. Por exemplo, se você tiver uma única palavra com mais de aproximadamente 50 caracteres de comprimento, ela não é quebrada e nenhuma barra de rolagem está presente, por isso, o texto fica truncado.

8. Na página Resumo, clique em **Aplicar**.
9. Quando solicitado, clique em **Desligar**.

   Um desligamento completo é necessário para que a criptografia possa ser iniciada.

10. Depois do desligamento, reinicie o computador.

    A autenticação agora é gerenciada pelo Encryption Management Agent. Os usuários precisam fazer login na tela de PBA com suas senhas do Windows.

Alteração das configurações de gerenciamento de SED e PBA

Assim que você ativar a criptografia pela primeira vez e configurar a Política e a Personalização de pré-inicialização, as ações a seguir ficarão disponíveis na guia Criptografia:

- Alterar Política ou Personalização de pré-inicialização - Clique na guia **Encryption** e, em seguida, clique em **Alterar**.
- Desativar o gerenciamento de SED, por exemplo, para desinstalação - clique em **Descriptografar**.

Assim que você ativar o o gerenciamento de SED pela primeira vez e configurar a Política e a Personalização de pré-inicialização, as ações a seguir ficarão disponíveis na guia Configurações de pré-inicialização:

- Alterar Política ou Personalização de pré-inicialização - clique na guia **Configurações de pré-inicialização** e selecione **Política da unidade com criptografia automática**, **Política pré-inicialização** ou **Personalização de pré-inicialização**.

Gerenciar usuários e a autenticação dos usuários

Adicionar usuário

Os usuários do Windows tornam-se automaticamente usuários do Encryption Personal quando fazem login no Windows ou inscrevem uma credencial.

O computador deve estar conectado ao domínio para adicionar um usuário do domínio a partir da guia Adicionar usuário do Data Security Console.

1. No painel esquerdo da ferramenta Configurações de administrador, selecione **Usuários**.

2. Na parte superior direita da página Usuário, clique em **Adicionar usuário** para começar o processo de inscrição para um usuário existente do Windows.
3. Quando a caixa de diálogo Selecionar usuário for mostrada, selecione **Tipos de objeto**.
4. Digite o nome de objeto de um usuário na caixa de texto e clique em **Verificar nomes**.
5. Clique em **OK** quando tiver terminado.

Excluir usuário

1. No painel esquerdo da ferramenta Configurações de administrador, selecione **Usuários**.
2. Para excluir um usuário, localize a coluna do usuário e clique em **Remover**. (Role até a parte inferior da coluna do usuário para ver a opção Remover.)

Remover todas as credenciais inscritas de um usuário

1. Clique no bloco **Configurações do administrador** e faça a autenticação com a sua senha.
2. Clique na guia **Usuários** e localize o usuário que você deseja remover.
3. Clique em **Remover**. O comando Remover aparece em vermelho abaixo das configurações do usuário.

   Após a remoção, o usuário não conseguirá fazer login no computador, a menos que se inscreva novamente.

7

Desinstalar o instalador mestre

- Cada componente precisa ser desinstalado separadamente, seguidos pela desinstalação do instalador mestre. 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 para obter os instaladores filhos.
- Certifique-se de que a mesma versão do instalador mestre (e, com isso, os clientes) usada na instalação seja usada na desinstalação.
- Esse capítulo direciona você para outro capítulo que contém instruções *detalhadas* sobre como desinstalar os instaladores filho. Este capítulo explica **apenas** a última etapa, a desinstalação do instalador mestre.

Desinstale os clientes na seguinte ordem.

1. Desinstalar o Encryption Client.
2. Desinstalar o Encryption Management Agent.

O pacote de drivers não precisa ser desinstalado.

Vá para Escolher um método de desinstalação.

Escolher um método de desinstalação

Há dois métodos para desinstalar o instalador mestre. Selecione **um** deles:

- Desinstalar a partir de Adicionar ou Remover Programas
- Desinstalar a partir da linha de comando

Desinstalar de maneira interativa

1. Vá para *Desinstalar um programa* no Painel de controle do Windows (na caixa de pesquisa na barra de tarefas, digite Painel de controle; em seguida, selecione **Painel de controle** nos resultados).
2. Selecione o **Dell Installer** e clique com o botão esquerdo em **Alterar** para iniciar o Assistente de instalação.
3. Leia a tela de boas-vindas e clique em **Avançar**.
4. Siga os passos para desinstalar e clique em **Concluir**.
5. Reinicie o computador e faça login no Windows.

   O instalador mestre foi desinstalado.

Desinstalar a partir da linha de comando

- O exemplo a seguir desinstala silenciosamente o instalador mestre.

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

  Reinicie o computador ao terminar.

  O instalador mestre foi desinstalado.

  Vá para Desinstalar usando os instaladores filhos.

8

Desinstalar usando os instaladores filho

- A Dell recomenda usar o Desinstalador do Data Security para remover o Encryption Personal.
- O usuário que executa a descriptografia e a desinstalação precisa ser um administrador local ou de domínio. Se for desinstalar por linha de comando, as credenciais do administrador de domínio são necessárias.
- Se você instalou o Encryption Personal com o instalador mestre, os arquivos executáveis filhos precisam ser extraídos do instalador mestre antes da desinstalação, conforme mostrado em Extrair os instaladores filhos do instalador mestre.
- Certifique-se de que a mesma versão dos clientes usada na instalação seja usada na desinstalação.
- 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 devido a arquivos bloqueados.

Desinstalar o Encryption

- **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 a solução de problemas em 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.

  NOTA: Antes de desinstalar, certifique-se de que todos os modelos de política estão definidos como Desativado e insira qualquer mídia externa criptografada para a descriptografia correta.

  Este vídeo detalha a alteração nos modelos de política no Console de gerenciamento local.

- 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 dos dados ainda está em andamento se o serviço Encryption Removal Agent estiver presente no painel serviços.
-

Escolher um método de desinstalação

Há dois métodos para desinstalar o Encryption Client. Selecione **um** deles:

- Desinstalar de maneira interativa
- Desinstalar a partir da linha de comando

Desinstalar de maneira interativa

1. Vá para *Desinstalar um programa* no Painel de controle do Windows (na caixa de pesquisa na barra de tarefas, digite **Painel de controle** e, em seguida, selecione **Painel de controle** nos resultados).
2. Selecione **Dell Encryption XX-bit** e clique com o botão esquerdo em **Alterar** para iniciar o Assistente de configuração do Encryption Personal.
3. Leia a tela de boas-vindas e clique em **Avançar**.
4. Na tela Instalação do Agente de remoção de criptografia, selecione uma destas opções:

   NOTA: A segunda opção está ativada por padrão. **Se você quiser descriptografar arquivos, altere a seleção para a opção um**.

   - Agente de remoção de criptografia — Importar chaves de um arquivo

Para criptografia SDE, Usuário ou Comum, essa opção descriptografa os arquivos e desinstala o Encryption Client. ***Esta é a seleção recomendada.***

- Não instalar o Agente de remoção de criptografia

  Essa opção desinstala o Encryption Client, *mas não descriptografa os arquivos*. Esta opção deve ser usada **somente** para fins de solução de problemas, conforme instruções do Dell ProSupport.

  Clique em **Avançar**.

5. Em *Arquivo de backup*, digite o caminho para a unidade de rede ou para o local da mídia removível do arquivo de backup ou clique em **...** para procurar o local. O formato do arquivo é LSARecovery_[nome_do_host].exe.

   Insira a sua Senha de administrador da criptografia. Essa é a senha do Assistente de instalação quando o software foi instalado.

   Clique em **Avançar**.

6. Em *Fazer logon no serviço do Agente de descriptografia Dell como*, selecione **Conta do sistema local** e clique em **Concluir**.
7. Clique em **Remover** na tela Remover o programa.
8. Clique em **Concluir** na tela Configuração concluída.
9. Reinicie o computador e faça login no Windows.

A descriptografia está agora em andamento.

O processo de descriptografia pode levar várias horas, dependendo do número de unidades que estiverem sendo descriptografadas e da quantidade de dados dessas unidades. Para verificar o processo de descriptografia, consulte Verificar o status do Agente de remoção de criptografia.

Desinstalar a partir da linha de comando

- 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 um arquivo de log de desinstalação para cada instalador filho, para o usuário conectado em %temp%, os quais podem ser encontrados 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:\<any directory>\<any log file name>.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
`/s`	Modo silencioso
`/x`	Modo Desinstalar

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

- Depois de extraído do instalador mestre, o instalador do Encryption Client pode ser encontrado em `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: 2 - Obter as chaves usando um pacote de chaves forenses 0 - Não instalar o Agente de remoção de criptografia
CMGSILENTMODE	Propriedade de desinstalação silenciosa: 1 – Silenciosa – necessária ao executar com variáveis msiexec que contêm /q ou /qn 0 – Não silenciosa – só é possível quando variáveis msiexec contendo /q não estão presentes na sintaxe da linha de comando
DA_KM_PW	A senha da conta do administrador de domínio.
DA_KM_PATH	O caminho para o pacote de materiais de chaves.

- O exemplo a seguir desinstala o cliente Encryption sem instalar o Encryption Removal Agent.

```
DDPE_XXbit_setup.exe /s /x /v"CMG_DECRYPT=0 CMGSILENTMODE=1 DA_KM_PATH=C:
\FullPathToLSA.exe DA_KM_PW=password /qn /l C:\ddpe_uninstall.txt"
```

- O exemplo a seguir desinstala o cliente Encryption usando um pacote de chaves forenses. Copie o pacote de chaves forenses no disco local e, em seguida, execute este comando.

```
DDPE_XXbit_setup.exe /s /x /v"CMG_DECRYPT=2 CMGSILENTMODE=1 DA_KM_PATH=C:
\FullPathToForensicKeyBundle DA_KM_PW=password /qn /l C:\ddpe_uninstall.txt"
```

  Reinicie o computador ao terminar.

  O processo de descriptografia pode levar várias horas, dependendo do número de unidades que estiverem sendo descriptografadas e da quantidade de dados dessas unidades. Para verificar o processo de descriptografia, consulte Verificar o status do Agente de remoção de criptografia.

Desinstalar o Encryption Management Agent

Escolher um método de desinstalação

Há dois métodos para desinstalar o Encryption Management Agent, selecione **um** dos seguintes:

- Desinstalar de maneira interativa

- Desinstalar a partir da linha de comando

Desinstalar de maneira interativa

1. Vá para *Desinstalar um programa* no Painel de controle do Windows (na caixa de pesquisa na barra de tarefas, digite **Painel de controle** e, em seguida, selecione **Painel de controle** nos resultados).
2. Selecione **Dell Encryption Management Agent** e clique com o botão esquerdo em **Alterar** para iniciar o Assistente de configuração.
3. Leia a tela de boas-vindas e clique em **Avançar**.
4. Siga os passos para desinstalar e clique em **Concluir**.
5. Reinicie o computador e faça login no Windows.

Client Security Framework foi desinstalado.

Desinstalar a partir da linha de comando

- Depois de extraído do instalador mestre, o instalador do Encryption Management Agent pode ser encontrado em `C:\extracted\Encryption Management Agent\EMAgent_XXbit_setup.exe`.
- O exemplo a seguir desinstala silenciosamente o gerenciamento de SED.

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

  Desligue e reinicie o computador ao terminar.

9

Desinstalador do Data Security

Desinstalar Encryption Personal

A Dell fornece o Desinstalador do Data Security como um desinstalador principal. Esse utilitário reúne os produtos instalados atualmente e os remove na ordem correta.

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

Para obter mais informações ou para usar a CLI (Command Line Interface, Interface de linha de comando), consulte o artigo da base de conhecimento 125052.

O logs são gerados em `C:\ProgramData\Dell\Dell Data Protection\` para todos os componentes que foram removidos.

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

Clique em **Avançar**.

Opcionalmente, desmarque qualquer aplicativo da remoção e clique em **Avançar**.

Dependências obrigatórias são selecionadas ou apagadas automaticamente.

Para remover aplicativos sem instalar o Encryption Removal Agent, escolha **Não instalar o Encryption Removal Agent** e selecione **Avançar**.

Selecione **Encryption Removal Agent - Importar chaves de um arquivo**, e então selecione **Avançar**.

Navegue para o local das chaves de recuperação e, em seguida, digite a senha para o arquivo e clique em **Avançar**.

Selecione **Remover** para começar a desinstalação.

Clique em **Concluir** para concluir a remoção e reinicialize o computador. **Reiniciar o computador após clicar em concluído** é selecionado por padrão.

A desinstalação e a remoção estão concluídas.

10

Descrições de modelo e políticas

As dicas de contexto são mostradas quando você passa o mouse sobre uma política no Console de gerenciamento local.

Políticas

Política	Alta proteção para todas as unidades fixas e externas	Norma PCI	Norma sobre violação de dados	Norma HIPAA	Proteção básica para todas as unidades fixas e externas (padrão)	Proteção básica para todas as unidades fixas	Proteção básica apenas para a unidade do sistema	Proteção básica para unidades externas	Criptografia desativada	Descrição
Políticas de armazenamento fixo										
Criptografia SDE ativada	Verdadeiro								Falso	Esta política é a "política mestre" de todas as outras políticas de SDE. Se esta política estiver definida como Falsa, não haverá criptografia SDE, independentemente dos demais valores de política. O valor Verdadeiro significa que todos os dados não criptografados por outras políticas de criptografia com base em política são criptografados de acordo com a política de Regras de criptografia SDE. A alteração do valor dessa política exige uma reinicialização.
Algoritmo de criptografia de SDE	AES256									AES-256, AES-128
SDE - Regras de criptografia										Regras de criptografia usadas para criptografar/descriptografar determinadas unidades, diretórios e pastas. Se tiver dúvidas sobre a alteração dos valores

Política	Alta proteção para todas as unidades fixas e externas	Norma PCI	Norma sobre violação de dados	Norma HIPAA	Proteção básica para todas as unidades fixas e externas (padrão)	Proteção básica para todas as unidades fixas	Proteção básica apenas para a unidade do sistema	Proteção básica para unidades externas	Criptografia desativada	Descrição
										padrão, entre em contato com o Dell ProSupport.
Políticas de configuração geral										
Criptografia ativada	Verdadeiro							Falso		Esta política é a " política mestra" de todas as outras políticas de Configuração geral. Um valor Falso significa que nenhuma criptografia ocorre, independentemente de outros valores de política. O valor Verdadeiro significa que todas as políticas de criptografia estão ativadas. A alteração do valor dessa política aciona uma nova varredura para criptografar/ descriptografar arquivos.
Pastas comuns criptografadas										String - máximo de 100 entradas de 500 caracteres cada (até um máximo de 2.048 caracteres) Uma lista de pastas em unidades de ponto de extremidade que serão criptografadas ou excluídas da criptografia, que pode ser acessada por todos os usuários gerenciados que têm acesso ao ponto de extremidade. As letras de unidades disponíveis são: #: Refere-se a todas as unidades f#: Refere-se a todas as unidades fixas r#: Refere-se a todas as unidades removíveis Importante: a substituição da proteção do diretório

Política	Alta proteção para todas as unidades fixas e externas	Norma PCI	Norma sobre violação de dados	Norma HIPAA	Proteção básica para todas as unidades fixas e externas (padrão)	Proteção básica para todas as unidades fixas	Proteção básica apenas para a unidade do sistema	Proteção básica para unidades externas	Criptografia desativada	Descrição
										pode resultar em um computador que não inicializa e/ou necessitar de unidades de reformatação. Se a mesma pasta for especificada nesta política e na política Pastas de usuário criptografadas, esta política prevalecerá.
Algoritmo de criptografia comum	AES256									AES-256, Rijndael 256, AES 128, Rijndael 128 Arquivos de paginação do sistema são criptografados usando AES-128.
Lista de criptografia de dados de aplicativos	winword.exe excel.exe powerpnt.exe msaccess.exe winproj.exe outlook.exe acrobat.exe visio.exe mspub.exe notepad.exe wordpad.exe winzip.exe winrar.exe onenote.exe onenotem.exe									String - máximo de 100 entradas de 500 caracteres cada A Dell não recomenda adicionar explorer.exe ou iexplorer.exe à lista de criptografia de dados de aplicativos (ADE - Application Data Encryption), pois pode causar resultados inesperados ou não pretendidos. No entanto, explorer.exe é o processo usado para criar um novo arquivo Notepad na área de trabalho, usando o menu do botão direito do mouse. A configuração de criptografia pela extensão do arquivo, e não pela lista ADE, proporciona uma cobertura mais abrangente. Faça uma lista com os nomes de aplicativos (sem caminhos) cujos arquivos novos você deseja criptografar, separados por retornos de carro. Não use curingas. A Dell recomenda que a lista não inclua aplicativos/

Política	Alta proteção para todas as unidades fixas e externas	Norma PCI	Norma sobre violação de dados	Norma HIPAA	Proteção básica para todas as unidades fixas e externas (padrão)	Proteção básica para todas as unidades fixas	Proteção básica apenas para a unidade do sistema	Proteção básica para unidades externas	Criptografia desativada	Descrição
										instaladores que gravam arquivos essenciais do sistema. Isso pode resultar na criptografia de arquivos importantes do sistema, o que pode fazer com que o computador não consiga ser reinicializado. Nomes de processo comuns: outlook.exe, winword.exe, powerpnt.exe, msaccess.exe, wordpad.exe, mspaint.exe, excel.exe Os seguintes nomes de processos de sistema e instalador inseridos no código serão ignorados se especificados nesta política: hotfix.exe, update.exe, setup.exe, msiexec.exe, wuauclt.exe, wmiprvse.exe, migrate.exe, unregmp2.exe, ikernel.exe, wssetup.exe, svchost.exe
Chave de ADE	Comum									Comum ou usuário Escolha uma chave para indicar quem pode acessar arquivos criptografados pela lista de ADE e onde podem ser acessados. Comum, para que esses arquivos sejam acessíveis a todos os usuários gerenciados no ponto de extremidade onde foram criados (o mesmo nível de acesso de Pastas criptografadas comuns) e criptografados com o algoritmo de criptografia comum. Usuário, para que esses arquivos sejam acessíveis apenas ao usuário que os

Política	Alta proteção para todas as unidades fixas e externas	Norma PCI	Norma sobre violação de dados	Norma HIPAA	Proteção básica para todas as unidades fixas e externas (padrão)	Proteção básica para todas as unidades fixas	Proteção básica apenas para a unidade do sistema	Proteção básica para unidades externas	Criptografia desativada	Descrição
										criou, apenas no ponto de extremidade onde foram criados (o mesmo nível de acesso de Pastas criptografadas do usuário) e criptografados com o algoritmo de criptografia do usuário. Alterações a esta política não afetam os arquivos já criptografados devido a esta política.
Criptografar pastas pessoais do Outlook	Verdadeiro							Falso		Se Verdadeiro, criptografa pastas pessoais do Outlook.
Criptografar arquivos temporários	Verdadeiro							Falso		Se Verdadeiro, criptografa os caminhos listados nas variáveis de ambiente TEMP e TMP, com a chave de criptografia de dados do usuário.
Criptografar arquivos temporários da Internet	Verdadeiro	Falso								Se Verdadeiro, criptografa o caminho mostrado na lista da variável de ambiente CSIDL_INTERNET_CACHE com a chave de criptografia de dados do usuário. Para reduzir o tempo de varredura da criptografia, o cliente limpa o conteúdo de CSIDL_INTERNET_CACHE para criptografia inicial, bem como as atualizações a esta política. Esta política só é aplicável quando o Microsoft Internet Explorer é usado.
Criptografar documentos do	Verdadeiro								Falso	Se Verdadeiro, criptografa: · O perfil de usuários (`C:\Users\jsmith`) com a

Política	Alta proteção para todas as unidades fixas e externas	Norma PCI	Norma sobre violação de dados	Norma HIPAA	Proteção básica para todas as unidades fixas e externas (padrão)	Proteção básica para todas as unidades fixas	Proteção básica apenas para a unidade do sistema	Proteção básica para unidades externas	Criptografia desativada	Descrição
perfil do usuário										chave de criptografia de dados do usuário · \Users\Public com a chave de criptografia comum
Criptografar arquivo de paginação do Windows	Verdadeiro								Falso	Se Verdadeiro, criptografa o arquivo de paginação do Windows. A alteração nesta política exige uma reinicialização.
Serviços gerenciados										String - máximo de 100 entradas de 500 caracteres cada (até um máximo de 2.048 caracteres) Quando um serviço é gerenciado por esta política, é iniciado apenas após o usuário estar conectado e o cliente desbloqueado. Esta política também garante que o serviço gerenciado por ela seja interrompido antes que o cliente seja bloqueado durante o logout. Além disso, esta política pode evitar que um usuário se desconecte caso o serviço não esteja respondendo. A sintaxe é um nome de serviço por linha. Espaços no nome do serviço são suportados. Curingas não são suportados. Serviços gerenciados não são iniciados se um usuário não gerenciado fizer login.
Proteger limpeza pós-criptografia	Substituição do tipo three-pass	Substituição do tipo single-pass							Não substituir	Sem substituição, Substituição do tipo single-pass, Substituição do tipo three-pass, Substituição do tipo seven-pass

Política	Alta proteção para todas as unidades fixas e externas	Norma PCI	Norma sobre violação de dados	Norma HIPAA	Proteção básica para todas as unidades fixas e externas (padrão)	Proteção básica para todas as unidades fixas	Proteção básica apenas para a unidade do sistema	Proteção básica para unidades externas	Criptografia desativada	Descrição
										Quando as pastas especificadas por outras políticas nesta categoria forem criptografadas, esta política determinará o que acontece com o resíduo não criptografado dos arquivos originais: · A opção Sem substituição o apaga. Esse valor proporciona o processamento mais rápido da criptografia. · A opção Substituição do tipo single-pass o substitui com dados aleatórios. · A Substituição do tipo three-pass o substitui com um padrão normal de 1s e 0s, em seguida com seu complemento, e depois com dados aleatórios. · A Substituição do tipo seven-pass o substitui com um padrão normal de 1s e 0s, em seguida com seu complemento, e depois com dados aleatórios cinco vezes. Esse valor faz com que seja mais difícil recuperar arquivos originais da memória e produz o processamento de criptografia mais seguro.
Arquivo de hibernação do Windows protegido	Verdadeiro					Falso		Verdadeiro	Falso	Quando ativado, o arquivo de hibernação é criptografado apenas quando o computador entrar em hibernação. O cliente libera a proteção quando o computador sair da hibernação, oferecendo proteção sem afetar os usuários ou os aplicativos enquanto o computador estiver em uso.

Política	Alta proteção para todas as unidades fixas e externas	Norma PCI	Norma sobre violação de dados	Norma HIPAA	Proteção básica para todas as unidades fixas e externas (padrão)	Proteção básica para todas as unidades fixas	Proteção básica apenas para a unidade do sistema	Proteção básica para unidades externas	Criptografia desativada	Descrição
Evitar hibernação não protegida	Verdadeiro					Falso		Verdadeiro	Falso	Quando ativado, o cliente não permitirá a hibernação do computador se não conseguir criptografar os dados de hibernação.
Prioridade da verificação de estações de trabalho	Alta	Normal								Mais alta, Alta, Normal, Baixa, Mais baixa Especifica a prioridade relativa do Windows para varredura de pasta criptografada.
Pastas de usuário criptografadas										String - máximo de 100 entradas de 500 caracteres cada (até um máximo de 2.048 caracteres) Uma lista de pastas no disco rígido do ponto de extremidade a serem criptografadas com a Chave de criptografia de dados do usuário ou excluídas da criptografia. Esta política aplica-se a todas as unidades classificadas pelo Windows como discos rígidos. Você não pode usar essa política para criptografar unidades ou mídia removível cujo tipo é mostrado como disco removível. Em vez disso, use Criptografar mídia externa (EMS).
Algoritmo de criptografia do usuário	AES256									AES 256, Rijndael 256, AES 128, Rijndael 128 Algoritmo de criptografia usado para criptografar dados no nível do usuário individual. Você pode especificar valores diferentes para diferentes usuários do mesmo ponto de extremidade.

Política	Alta proteção para todas as unidades fixas e externas	Norma PCI	Norma sobre violação de dados	Norma HIPAA	Proteção básica para todas as unidades fixas e externas (padrão)	Proteção básica para todas as unidades fixas	Proteção básica apenas para a unidade do sistema	Proteção básica para unidades externas	Criptografia desativada	Descrição
Chave de criptografia de dados de usuário	Usuário	Comum		Usuário	Comum				Usuário	Comum ou usuário Escolha uma chave para indicar quem, e onde, pode acessar arquivos criptografados pelas seguintes políticas: · Pastas de usuário criptografadas · Criptografar pastas pessoais do Outlook · Criptografar arquivos temporários (\Documents and Settings\nomedeusuario\Local Settings\Temp somente) · Criptografar arquivos temporários da Internet · Criptografar documentos do perfil do usuário Selecione: · Comum, para que arquivos/pastas do usuário criptografados sejam acessíveis a todos os usuários gerenciados no ponto de extremidade onde foram criados (o mesmo nível de acesso de Pastas criptografadas do usuário) e que sejam criptografados com o algoritmo de criptografia comum. · Usuário, para que esses arquivos sejam acessíveis apenas ao usuário que os criou, apenas no ponto de extremidade onde foram criados (o mesmo nível de acesso de Pastas criptografadas do usuário) e criptografados com o algoritmo de criptografia do usuário. Se você optar por incorporar uma política

Política	Alta proteção para todas as unidades fixas e externas	Norma PCI	Norma sobre violação de dados	Norma HIPAA	Proteção básica para todas as unidades fixas e externas (padrão)	Proteção básica para todas as unidades fixas	Proteção básica apenas para a unidade do sistema	Proteção básica para unidades externas	Criptografia desativada	Descrição
										de criptografia para criptografar partições inteiras do disco, recomenda-se usar a política de criptografia SDE padrão, em vez da Comum ou do Usuário. Isso garante que todos os arquivos criptografados do sistema operacional sejam acessíveis quando o usuário gerenciado não estiver conectado.
Hardware Crypto Accelerator (suportado apenas com clientes Encryption da versão v8.3 à v8.9.1)										
A criptografia do Hardware Crypto Accelerator (HCA)	Falso									Esta é a "política mestre" de todas as outras políticas de aceleradores de criptografia por hardware (HCA - Hardware Crypto Accelerator). Se esta política estiver configurada como Falsa, não haverá criptografia HCA, independentemente dos demais valores de política. As políticas de HCA só podem ser usadas em computadores equipados com um acelerador de criptografia por hardware.
Volumes direcionados para criptografia	Todos os volumes fixos									Todos os volumes fixos ou apenas o volume do sistema Especifica quais volumes deverão ser criptografados.
Metadados forenses disponíveis na unidade criptografada HCA	Falso									Verdadeiro ou Falso Quando Verdadeiro, os metadados forenses são incluídos na unidade para facilitar o laboratório forense. Metadados incluídos:

Política	Alta proteção para todas as unidades fixas e externas	Norma PCI	Norma sobre violação de dados	Norma HIPAA	Proteção básica para todas as unidades fixas e externas (padrão)	Proteção básica para todas as unidades fixas	Proteção básica apenas para a unidade do sistema	Proteção básica para unidades externas	Criptografia desativada	Descrição
										• ID de máquina (MCID) da máquina atual • ID de dispositivo (DCID/SCID) da instalação de Encryption client atual Quando Falso, os metadados forenses não são incluídos na unidade. Alternar de Falso para Verdadeiro faz nova varredura com base nas políticas para adicionar dados forenses.
Permitir aprovação do usuário para criptografia da unidade secundária	Falso									A opção Verdadeiro permite que os usuários decidam se unidades adicionais devem ser criptografadas.
Algoritmo de criptografia	AES256									AES-256 ou AES-128
Políticas de controle de portas										
Sistema de controle de porta	Desativado									Habilitar ou desabilitar todas as políticas de sistema de controle de portas (PCS — Port Control System). Se esta política estiver definida como Desabilitar, nenhuma política de PCS será aplicada, independentemente de outros valores de políticas de sistema de controle de portas. as políticas de PCS exigem reinicialização para que a política tenha efeito.

Política	Alta proteção para todas as unidades fixas e externas	Norma PCI	Norma sobre violação de dados	Norma HIPAA	Proteção básica para todas as unidades fixas e externas (padrão)	Proteção básica para todas as unidades fixas	Proteção básica apenas para a unidade do sistema	Proteção básica para unidades externas	Criptografia desativada	Descrição
										NOTA: O bloqueio das operações do dispositivo resulta na exibição em branco dos nomes de dispositivos.
Porta: slot para Express Card	Ativado									Habilitar, desabilitar ou ignorar portas expostas por meio do slot para Express Card.
Porta: eSATA	Ativado									Habilitar, desabilitar ou ignorar o acesso da porta a portas SATA externas.
Porta: PCMCIA	Ativado									Habilitar, desabilitar ou ignorar o acesso da porta a portas PCMCIA.
Porta: Firewire (1394)	Ativado									Habilitar, desabilitar ou ignorar o acesso da porta a portas Firewire (1394) externas.
Porta: SD	Ativado									Habilitar, desabilitar ou ignorar o acesso da portas a portas do cartão SD.
Subclasse de armazenamento: controle da unidade externa	Bloqueado	Somente leitura			Acesso completo			Somente leitura	Acesso completo	FILHO da Classe: armazenamento. Classe: o armazenamento precisa estar Ativado para usar esta política. Essa política tem interações com PCS. Consulte Encryption External Media e interações de PCs. Acesso completo: a porta da unidade externa não tem restrições de dados de leitura/gravação aplicadas Somente leitura: permite o recurso de leitura. Gravação de dados está desativada Bloqueado: é porta é bloqueada para leitura/gravação

Política	Alta proteção para todas as unidades fixas e externas	Norma PCI	Norma sobre violação de dados	Norma HIPAA	Proteção básica para todas as unidades fixas e externas (padrão)	Proteção básica para todas as unidades fixas	Proteção básica apenas para a unidade do sistema	Proteção básica para unidades externas	Criptografia desativada	Descrição
										Essa política é baseada em ponto de extremidade e não pode ser substituída por uma política de usuário.
Porta: dispositivo de transferência de memória (MTD)	Ativado									Habilitar, desabilitar ou ignorar o acesso às portas do Dispositivo de transferência de memória (MTD — Memory Transfer Device).
Classe: armazenamento	Ativado									PAI para as próximas 3 políticas. Ative esta política para usar as três seguintes políticas de armazenamento de subclasse. A desativação desta política desativa as três políticas de armazenamento de subclasse, independentemente de seus valores.
Subclasse de armazenamento: controle da unidade ótica	Somente leitura	UDF somente				Acesso completo		UDF somente	Acesso completo	FILHO da Classe: armazenamento. Classe: o armazenamento precisa estar Ativado para usar esta política. Acesso completo: a porta da unidade óptica não tem restrições de dados de leitura/gravação aplicadas UDF somente: bloqueia todas as gravações de dados que não estejam no formato UDF (gravação de CD/DVD e ISO). Leitura de dados está ativada. Somente leitura: permite o recurso de leitura. Gravação de dados está desativada Bloqueado: é porta é bloqueada para leitura/gravação

Política	Alta proteção para todas as unidades fixas e externas	Norma PCI	Norma sobre violação de dados	Norma HIPAA	Proteção básica para todas as unidades fixas e externas (padrão)	Proteção básica para todas as unidades fixas	Proteção básica apenas para a unidade do sistema	Proteção básica para unidades externas	Criptografia desativada	Descrição
										Essa política é baseada em ponto de extremidade e não pode ser substituída por uma política de usuário. Universal Disk Format (UDF — Formato de disco universal) é uma implementação da especificação conhecida como ISO/IEC 13346 e ECMA-167. É um sistema de arquivos neutro, aberto a fornecedores, para armazenamento de dados de computador em uma ampla variedade de mídia. Essa política tem interações com PCS. Consulte Encryption External Media e interações de PCs.
Subclasse de armazenamento: controle da unidade de disquete	Bloqueado	Somente leitura				Acesso completo		Somente leitura	Acesso completo	FILHO da Classe: armazenamento. Classe: o armazenamento precisa estar Ativado para usar esta política. Acesso completo: a porta da unidade de disco não tem restrições de dados de leitura/gravação aplicadas Somente leitura: permite o recurso de leitura. Gravação de dados está desativada Bloqueado: é porta é bloqueada para leitura/gravação Essa política é baseada em ponto de extremidade e não pode ser substituída por uma política de usuário.
Classe: dispositivo portátil do Windows	Ativado									PAI para a próxima política. Ative esta política para ativar o dispositivo portátil de subclasse do Windows : política de armazenamento.

Política	Alta proteção para todas as unidades fixas e externas	Norma PCI	Norma sobre violação de dados	Norma HIPAA	Proteção básica para todas as unidades fixas e externas (padrão)	Proteção básica para todas as unidades fixas	Proteção básica apenas para a unidade do sistema	Proteção básica para unidades externas	Criptografia desativada	Descrição
										A desativação desta política desativa o dispositivo portátil de subclasse do Windows : política de armazenamento, independentemente de seu valor. Controla o acesso a todos os WPDs.
Dispositivo portátil de subclasse do Windows : armazenamento	Ativado									FILHO da Classe: dispositivo portátil do Windows Classe: o dispositivo portátil do Windows precisa estar Ativado para usar esta política. Acesso completo: a porta não tem restrições de dados de leitura/gravação aplicadas. Somente leitura: permite o recurso de leitura. Os dados de gravação são desativados. Bloqueado: a porta é bloqueada para leitura/gravação.
Classe: dispositivo de interface humana	Ativado									Controle o acesso a todos os HID (teclado e mouse). **Nota:** o bloqueio no nível da porta USB e o bloqueio no nível da classe de dispositivos de interface humana (HID - Human Interface Device) serão processados apenas se o tipo de chassi do computador puder ser identificado como um formato de laptop ou de notebook. O BIOS do computador é usado para a identificação do chassi.
Classe: outra	Ativado									Controla o acesso a todos os dispositivos

Política	Alta proteção para todas as unidades fixas e externas	Norma PCI	Norma sobre violação de dados	Norma HIPAA	Proteção básica para todas as unidades fixas e externas (padrão)	Proteção básica para todas as unidades fixas	Proteção básica apenas para a unidade do sistema	Proteção básica para unidades externas	Criptografia desativada	Descrição
										não cobertos por outras classes.
Políticas de armazenamento removível										
Criptografar mídia externa (EMS)	Verdadeiro					Falso		Verdadeiro	Falso	Esta política é a "política mestra" de todas as outras políticas de Armazenamento removível. O valor Falso significa que não há criptografia de armazenamento removível, independentemente de outros valores de política. O valor Verdadeiro significa que todas as políticas de criptografia de Armazenamento removível estão ativadas. Essa política tem interações com PCS. Consulte Encryption External Media e interações de PCs.
Excluir criptografia de CD/DVD (EMS)	Falso								Verdadeiro	Se Falso, criptografa dispositivos de CD/DVD. Essa política tem interações com PCS. Consulte Encryption External Media e interações de PCs.
EMS - Acesso a mídia não protegida	Bloquear		Somente leitura			Acesso completo		Somente leitura	Acesso completo	Bloqueado, Somente leitura, Acesso completo Essa política tem interações com PCS. Consulte Encryption External Media e interações de PCs. Quando esta política está definida para Bloquear o acesso, você não tem acesso ao armazenamento removível, a menos que ele seja criptografado. A escolha de Somente leitura ou Acesso completo

Política	Alta proteção para todas as unidades fixas e externas	Norma PCI	Norma sobre violação de dados	Norma HIPAA	Proteção básica para todas as unidades fixas e externas (padrão)	Proteção básica para todas as unidades fixas	Proteção básica apenas para a unidade do sistema	Proteção básica para unidades externas	Criptografia desativada	Descrição
										permite que você decida qual armazenamento removível criptografar. Se você optar por não criptografar o armazenamento removível e esta política estiver definida como acesso completo, você terá pleno acesso de leitura/gravação ao armazenamento removível. Se você optar por não criptografar o armazenamento removível e essa política for definida como Somente leitura, não será possível ler ou apagar os arquivos no armazenamento removível não criptografado, mas o cliente não permite que os arquivos sejam editados ou adicionados ao armazenamento removível a menos que seja criptografado.
EMS - Algoritmo de criptografia	AES256									AES-256, Rijndael 256, AES-128, Rijndael 128
EMS - Fazer varredura da mídia externa	Verdadeiro	Falso								Verdadeiro permite que a mídia removível seja verificada sempre que o dispositivo for inserido. Quando essa política está como Falso e a política do EMS Encrypt External Media está como Verdadeiro, somente arquivos novos e alterados são criptografados. Uma varredura ocorre em cada inserção, para que quaisquer arquivos adicionados à mídia removível sem

Política	Alta proteção para todas as unidades fixas e externas	Norma PCI	Norma sobre violação de dados	Norma HIPAA	Proteção básica para todas as unidades fixas e externas (padrão)	Proteção básica para todas as unidades fixas	Proteção básica apenas para a unidade do sistema	Proteção básica para unidades externas	Criptografia desativada	Descrição
										autenticação possam ser capturados. Os arquivos podem ser adicionados à mídia se a autenticação for recusada, mas os dados criptografados não podem ser acessados. Os arquivos adicionados não são criptografados neste caso. Assim, na próxima vez que a mídia for autenticada (para trabalhar com dados criptografados), os arquivos que possam ter sido adicionados serão examinados e criptografados.
EMS - Acessar dados criptografados em dispositivo não protegido	Verdadeiro									Se Verdadeiro, permite que o usuário acesse dados criptografados no armazenamento removível, independentemente de o ponto de extremidade estar criptografado ou não.
Lista de dispositivos do EMS permitidos										Esta política permite a especificação dos dispositivos de mídia removíveis que devem ser excluídos da criptografia do EMS. Todos os dispositivos de mídia removíveis que não estiverem nesta lista são protegidos. Máximo de 150 dispositivos com até 500 caracteres por PNPDeviceID. Máximo permitido de 2048 caracteres no total. Para localizar o PNPDeviceID do armazenamento removível: 1. Insira o dispositivo de armazenamento removível em um computador criptografado.

Política	Alta proteção para todas as unidades fixas e externas	Norma PCI	Norma sobre violação de dados	Norma HIPAA	Proteção básica para todas as unidades fixas e externas (padrão)	Proteção básica para todas as unidades fixas	Proteção básica apenas para a unidade do sistema	Proteção básica para unidades externas	Criptografia desativada	Descrição
										2. Abra o EMSService.log em C:\Programdata\Dell\Dell Data Protection\Encryption\EMS. 3. Localize "PNPDeviceID=" Por exemplo: 14.03.18 18:50:06.834 [I] [Volume "F:\"] PnPDeviceID = USBSTOR\DISK&VEN_SEAGATE&PROD_USB&REV_0409\2HC015KJ&0 Especifique o seguinte na política Lista de dispositivos do EMS permitidos: VEN=Fornecedor (exemplo: USBSTOR\DISK&VEN_SEAGATE) PROD=Nome do produto/do modelo (exemplo: &PROD_USB); também exclui da criptografia do EMS todas as unidades USB do Seagate; um valor VEN (exemplo: USBSTOR\DISK&VEN_SEAGATE) deve preceder esse valor REV=Revisão do firmware (exemplo: &REV_0409); também exclui o modelo específico que está sendo usado; os valores VEN e PROD devem preceder esse valor Número de série (exemplo: \2HC015KJ&0); exclui apenas este dispositivo; os valores VEN, PROD e REV devem preceder esse valor

Política	Alta proteção para todas as unidades fixas e externas	Norma PCI	Norma sobre violação de dados	Norma HIPAA	Proteção básica para todas as unidades fixas e externas (padrão)	Proteção básica para todas as unidades fixas	Proteção básica apenas para a unidade do sistema	Proteção básica para unidades externas	Criptografia desativada	Descrição
										Delimitadores permitidos: tabulações, vírgulas, ponto e vírgula, caractere hexadecimal 0x1E (caractere separador de registros)
EMS - Caracteres alfanuméricos obrigatórios na senha	Verdadeiro									Se Verdadeiro, exige uma ou mais letras na senha.
EMS - Caracteres maiúsculos e minúsculos obrigatórios na senha	Verdadeiro	Falso								Se Verdadeiro, exige pelo menos uma letra maiúscula e uma letra minúscula na senha.
EMS - Número de caracteres. obrigatórios na senha	8					6		8		1-40 caracteres Número mínimo de caracteres obrigatórios na senha.
EMS - Caracteres numéricos obrigatórios na senha	Verdadeiro	Falso								Se Verdadeiro, exige um ou mais caracteres numéricos na senha.
EMS - Tentativas permitidas de senha	2	3				4		3		1-10 Número de vezes que o usuário pode tentar digitar a senha correta.

Política	Alta proteção para todas as unidades fixas e externas	Norma PCI	Norma sobre violação de dados	Norma HIPAA	Proteção básica para todas as unidades fixas e externas (padrão)	Proteção básica para todas as unidades fixas	Proteção básica apenas para a unidade do sistema	Proteção básica para unidades externas	Criptografia desativada	Descrição
EMS - Caracteres especiais obrigatórios na senha	Verdadeiro	Falso							Verdadeiro	Se Verdadeiro, exige um ou mais caracteres especiais na senha.
EMS - Período de espera	30									0-5000 segundos Número de segundos que o usuário precisa esperar entre a primeira e a segunda rodada de tentativas de digitação do código de acesso.
EMS - Incremento no período de espera	30	20				10	30	10		0-5000 segundos Tempo incremental a adicionar ao período de espera anterior, após cada rodada malsucedida de tentativas de digitação do código de acesso.
EMS - Regras de criptografia										Regras de criptografia para criptografar/não criptografar determinadas unidades, diretórios e pastas. É permitido um total de 2.048 caracteres. Os caracteres "Espaço" e "Enter" usados para inclusão de linhas são contados como caracteres usados. Todas as regras que excederem o limite de 2.048 caracteres serão ignoradas. Os dispositivos de armazenamento que incorporam conexões de várias interfaces, como Firewire, USB, eSATA, etc. podem exigir o uso de Encryption External Media e de regras de criptografia para criptografar o dispositivo.

Política	Alta proteção para todas as unidades fixas e externas	Norma PCI	Norma sobre violação de dados	Norma HIPAA	Proteção básica para todas as unidades fixas e externas (padrão)	Proteção básica para todas as unidades fixas	Proteção básica apenas para a unidade do sistema	Proteção básica para unidades externas	Criptografia desativada	Descrição
										Isso é necessário em razão das diferenças na forma em que o sistema operacional Windows lida com dispositivos de armazenamento com base no tipo de interface. Consulte Como criptografar um iPod com o Encryption External Media.
EMS - Bloquear acesso a mídia que não pode ser protegida	Verdadeiro								Falso	Bloqueie o acesso a qualquer mídia removível menor que 55 MB e que, portanto, não tem capacidade de armazenamento suficiente para hospedar o Encryption External Media (como um disquete de 1,44 MB). Todo o acesso será bloqueado se EMS e esta política tiverem o valor Verdadeiro. Se EMS Encrypt External Media for Verdadeiro, mas essa política for Falsa, os dados podem ser lidos da mídia não criptografável, mas o acesso de gravação à mídia é bloqueado. Se o EMS Encrypt External Media estiver Falso, essa política não tem nenhum efeito e o acesso à mídia não criptografável não é afetado.
Políticas de controle de experiência do usuário										
Forçar reinicialização após atualização	Verdadeiro								Falso	Ao configurar o valor como Verdadeiro, o computador é reinicializado imediatamente para permitir o processamento da criptografia ou de atualizações relacionadas à política baseada em

Política	Alta proteção para todas as unidades fixas e externas	Norma PCI	Norma sobre violação de dados	Norma HIPAA	Proteção básica para todas as unidades fixas e externas (padrão)	Proteção básica para todas as unidades fixas	Proteção básica apenas para a unidade do sistema	Proteção básica para unidades externas	Criptografia desativada	Descrição
										dispositivo, como System Data Encryption (SDE).
Duração de cada atraso para reinicialização	5	10				20		15		O número de minutos de atraso quando o usuário escolhe adiar a reinicialização da política baseada em dispositivo.
Número de atrasos permitidos para reinicialização	+1					5		3		O número de vezes que o usuário pode adiar a reinicialização da política baseada em dispositivo.
Suprimir aviso de retenção de arquivo	Falso									Esta política controla se o usuário vê pop-ups de notificação se um aplicativo tentar acessar um arquivo enquanto o cliente o estiver processando.
Mostrar controle de processamento de criptografia local	Falso		Verdadeiro					Falso		Ao configurar o valor como Verdadeiro, o usuário verá uma opção de menu no ícone da área de notificação que permite que ele pause/reinicie a criptografia/descriptografia (dependendo do que o Encryption estiver fazendo no momento). Autorizar um usuário a pausar a criptografia pode permitir que ele impeça o Encryption client de criptografar ou descriptografar totalmente os dados de acordo com a política.
Permitir a criptografia apenas quando a tela	Falso		Opcional do usuário					Falso		Verdadeiro, Falso, Opcional do usuário Quando Verdadeiro, não há nenhuma criptografia ou descriptografia de dados

Política	Alta proteção para todas as unidades fixas e externas	Norma PCI	Norma sobre violação de dados	Norma HIPAA	Proteção básica para todas as unidades fixas e externas (padrão)	Proteção básica para todas as unidades fixas	Proteção básica apenas para a unidade do sistema	Proteção básica para unidades externas	Criptografia desativada	Descrição
estiver bloqueada										enquanto o usuário estiver trabalhando ativamente. O cliente só processa dados quando a tela estiver bloqueada. Opcional do usuário adiciona uma opção no ícone da área de notificação que permite ao usuário ativar ou desativar esse recurso. Quando Falso, o processamento da criptografia ocorre a qualquer momento, mesmo quando o usuário estiver trabalhando. A ativação dessa opção prolonga consideravelmente o tempo necessário para concluir a criptografia ou descriptografia.

Descrições de modelos

Alta proteção para todas as unidades fixas e externas

Esse modelo de política foi criado para as organizações que têm como objetivo principal reforçar a segurança e evitar riscos em toda a empresa. É melhor usada quando a segurança é muito mais importante do que a facilidade de uso, e a necessidade de exceções com políticas menos seguras para certos usuários, grupos ou dispositivos é mínima.

Este modelo de política:

- é uma configuração altamente restrita, que proporciona ainda mais proteção.
- oferece proteção à unidade do sistema e a todas as unidades fixas.
- criptografa todos os dados de dispositivos de mídia removíveis e evita o uso de dispositivos de mídia removíveis não criptografados.
- oferece controle de unidade óptica somente para leitura.

Norma PCI direcionada

O Padrão PCI de Segurança de Dados (PCI DSS - Payment Card Industry Data Security Standard) é um padrão multiuso que inclui requisitos de gerenciamento de segurança, políticas, procedimentos, arquitetura de rede, projeto de software e outras importantes medidas de proteção. Esse padrão abrangente tem como objetivo definir as diretrizes para que as organizações protejam de forma proativa os dados das contas dos clientes.

Este modelo de política:

- oferece proteção à unidade do sistema e a todas as unidades fixas.
- solicita aos usuários que criptografem os dispositivos de mídia removíveis.
- possibilita a gravação de CD/DVDs apenas UDF. A configuração do controle de porta permite acesso de leitura a todas as unidades ópticas.

Direcionada à Norma sobre violação de dados

A lei Sarbanes-Oxley exige controle adequado das informações financeiras. Como muitas dessas informações residem em formato eletrônico, a criptografia é o ponto de controle principal quando esses dados são armazenados ou transferidos. As diretrizes da lei Gramm-Leach-Bliley (GLB) (também conhecida como Lei de Modernização dos Serviços Financeiros) não exigem criptografia. Entretanto, o Conselho de Investigação Federal de Instituições Financeiras (FFIEC) faz a seguinte recomendação: "As instituições financeiras devem implantar a criptografia a fim de reduzir o risco de divulgação ou alteração de informações confidenciais armazenadas ou transmitidas". O projeto de lei 1386 do senado da Califórnia (California's Database Security Breach Notification Act) tem como objetivo proteger os cidadãos da Califórnia contra roubo de identidade exigindo que as organizações que tiveram sua segurança computacional violada notifiquem todos os indivíduos afetados. A única forma de uma organização evitar notificar os clientes é provar que todas as informações pessoais foram criptografadas antes da violação do sistema de segurança.

Este modelo de política:

- oferece proteção à unidade do sistema e a todas as unidades fixas.
- solicita aos usuários que criptografem os dispositivos de mídia removíveis.
- possibilita a gravação de CD/DVDs apenas UDF. A configuração do controle de porta permite acesso de leitura a todas as unidades ópticas.

Direcionada à Norma HIPAA

A Lei de Portabilidade e Responsabilidade de Seguros de Saúde (HIPAA) exige que as organizações de saúde implantem um número de proteções técnicas a fim de garantir a confidencialidade e a integridade de todas as informações individuais identificáveis relacionadas à saúde.

Este modelo de política:

- oferece proteção à unidade do sistema e a todas as unidades fixas.
- solicita aos usuários que criptografem os dispositivos de mídia removíveis.
- possibilita a gravação de CD/DVDs apenas UDF. A configuração do controle de porta permite acesso de leitura a todas as unidades ópticas.

Proteção básica para todas as unidades fixas e externas (padrão)

Esse modelo de política oferece a configuração recomendada, que proporciona alto nível de proteção sem causar impactos significativos na facilidade de uso do sistema.

Este modelo de política:

- oferece proteção à unidade do sistema e a todas as unidades fixas.
- solicita aos usuários que criptografem os dispositivos de mídia removíveis.
- possibilita a gravação de CD/DVDs apenas UDF. A configuração do controle de porta permite acesso de leitura a todas as unidades ópticas.

Proteção básica para todas as unidades fixas

Este modelo de política:

- oferece proteção à unidade do sistema e a todas as unidades fixas.
- possibilita a gravação de CD/DVDs em qualquer formato suportado. A configuração do controle de porta permite acesso de leitura a todas as unidades ópticas.

  Esse modelo de política não:

- fornece criptografia para dispositivos de mídia removíveis.

Proteção básica apenas para a unidade do sistema

Este modelo de política:

- fornece proteção para a unidade do sistema, geralmente a unidade C:, onde o sistema operacional é carregado.
- possibilita a gravação de CD/DVDs em qualquer formato suportado. A configuração do controle de porta permite acesso de leitura a todas as unidades ópticas.

  Esse modelo de política não:

- fornece criptografia para dispositivos de mídia removíveis.

Proteção básica para unidades externas

Este modelo de política:

- fornece proteção para os dispositivos de mídia removíveis.
- possibilita a gravação de CD/DVDs apenas UDF. A configuração do controle de porta permite acesso de leitura a todas as unidades ópticas.

  Esse modelo de política não:

- fornece proteção à unidade do sistema (geralmente a unidade C:, onde o sistema operacional é carregado) ou a outras unidades fixas.

Criptografia desativada

Esse modelo de política não oferece proteção por criptografia. Ao usar esse modelo, tome medidas adicionais para proteger seus dispositivos contra perda e roubo.

Esse modelo é útil para organizações que preferem iniciar sem nenhuma criptografia ativa durante a transição para segurança. Assim que a organização se adaptar à implantação, a criptografia pode ser moderadamente ativada por meio do ajuste de políticas individuais ou da aplicação de modelos mais sólidos para toda ou parte da organização.

11

Extrair instaladores filhos

- Para instalar cada cliente individualmente, extraia os arquivos executáveis filhos do instalador.
- Se o instalador mestre tiver sido usado na instalação, os clientes precisam ser desinstalados individualmente. Use esse processo para extrair os clientes do instalador mestre para que eles possam ser usados para desinstalação.

1. Na mídia de instalação Dell, copie o arquivo `DDSSetup.exe` para o computador local.
2. Abra um prompt de comando no mesmo local do arquivo `DDSSetup.exe` e digite:

   ```
   DDSSetup.exe /s /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\.`

Vá para Solução de problemas.

12

Solução de problemas

Fazendo upgrade usando atualizações de recursos do Windows 10 ou Windows 11

Para fazer upgrade do Windows 10 ou do Windows 11 usando atualizações de recursos, siga as instruções no artigo da base de conhecimento 125419.

Soluções de problemas do Dell Encryption

(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 é 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**.

Encryption External Media e interações de 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: Armazenamento > Armazenamento de subclasse: Controle de unidade externa. Se você pretende definir a política EMS - Acesso a mídia não protegida como *Acesso completo*, verifique se a política Armazenamento de subclasse: 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:

- Configure o Windows Media Encryption = Ativado.

- Configure Excluir criptografia de CD/DVD (EMS) = não selecionado.
- 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 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.

  NOTA: O WSScan deve ser executado no modo do sistema com a ferramenta PsExec, se um arquivo de destino for de propriedade da conta do sistema.

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: *Todas as unidades*, *Unidades fixas*, *Unidades removíveis* ou CDROM/DVDROM.
5. Selecione o tipo de relatório de criptografia: *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 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 no menu 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 **Apagar** para apagar as mensagens mostradas.

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.

Saída	Significado
Tipo de criptografia	O tipo de criptografia usada para criptografar o arquivo. **SysData:** chave 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

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 (selecione o serviço > clique com o botão direito > Atualizar) para atualizar seu status.

- **Aguardando a desativação de SDE** – O Encryption ainda está instalado, ainda está configurado ou ambos. A descriptografia não será iniciada até o 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.

- **Concluída** – A varredura de descriptografia está concluída. O serviço, o executável, o driver e o executável do driver estão agendados para serem apagados na próxima reinicialização.

Como criptografar um iPod com Encryption External Media

Essas regras desativam ou ativam a criptografia para essas pastas e tipos de arquivos em todos os dispositivos removíveis - não apenas no iPod. Tenha cuidado ao definir regras.

- A Dell não recomenda o uso do iPod Shuffle, pois podem ocorrer resultados inesperados.
- À medida que os iPods mudam, essas informações também podem mudar, por isso recomenda-se cautela ao permitir o uso de iPods em computadores habilitados com Encryption External Media.
- Como os nomes das pastas nos iPods dependem do modelo do iPod, a Dell recomenda criar uma política de exclusão que cubra todos os nomes de pastas, em todos os modelos de iPod.
- Para garantir que a criptografia de um iPod via Encryption External Media não torne o dispositivo inutilizável, digite as seguintes regras na política Regras de criptografia do Encryption External Media:

  -R#:\Calendars

  -R#:\Contacts

  -R#:\iPod_Control

  -R#:\Notes

  -R#:\Photos

- Você também pode forçar a criptografia de tipos específicos de arquivos nos diretórios acima. A adição das seguintes regras assegura que arquivos ppt, pptx, doc, docx, xls e xlsx sejam criptografados nos diretórios *excluídos* da criptografia pelas regras anteriores:

  ^R#:\Calendars;ppt.doc.xls.pptx.docx.xlsx

  ^R#:\Contacts;ppt.doc.xls.pptx.docx.xlsx

  ^R#:\iPod_Control;ppt.doc.xls.pptx.docx.xlsx

  ^R#:\Notes;ppt.doc.xls.pptx.docx.xlsx

  ^R#:\Photos;ppt.doc.xls.pptx.docx.xlsx

- A substituição dessas cinco regras pela seguinte regra forçará a criptografia de arquivos ppt, pptx, doc, docx, xls e xlsx em qualquer diretório do iPod, incluindo Calendários, Contatos iPod_Control, Notas e Fotos.

  ^R#:\;ppt.doc.xls.pptx.docx.xlsx

- As regras foram testadas nos seguintes iPods:

  - iPod Video 30 GB quinta geração

  - iPod Nano 2 GB segunda geração

  - iPod Nano 4 GB segunda geração

Drivers do 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. Acesse dell.com/support.
2. Selecione o modelo do seu computador.
3. Selecione **Drivers e Downloads**.
4. Selecione o **Sistema operacional** do computador de destino.
5. Selecione 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.

   NOTA:

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

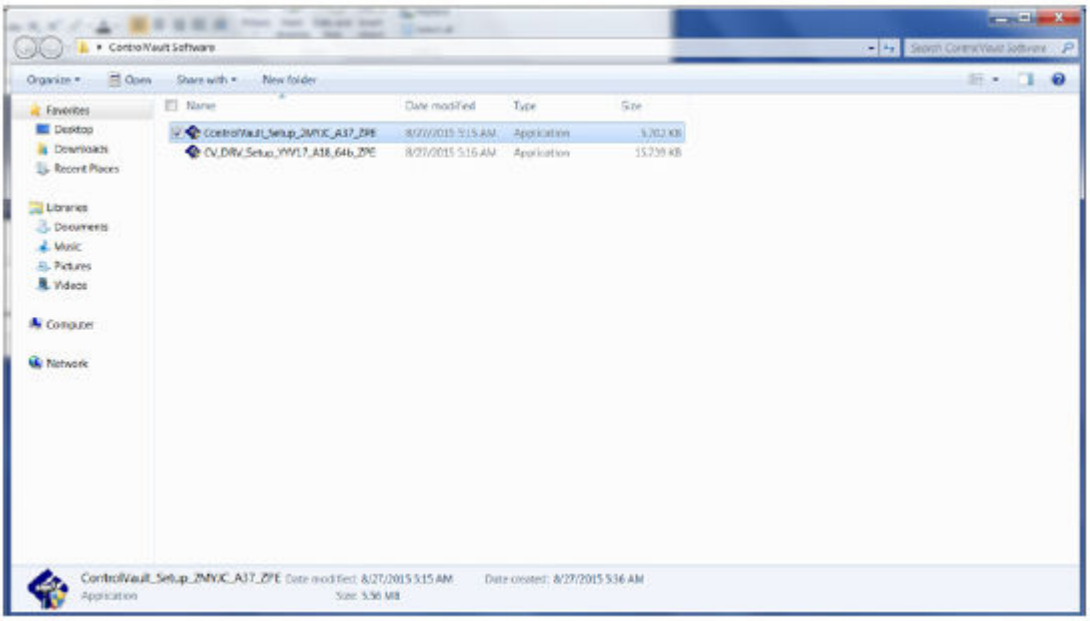
3. Clique em **Continuar** para começar.
4. Clique em **OK** para descompactar os arquivos do driver no local padrão `C:\Dell\Drivers\<New Folder>`.
5. Clique em **Sim** para criar uma nova pasta.
6. Clique em **Ok** quando for mostrada a mensagem de que a descompactação foi bem-sucedida.
7. A pasta 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

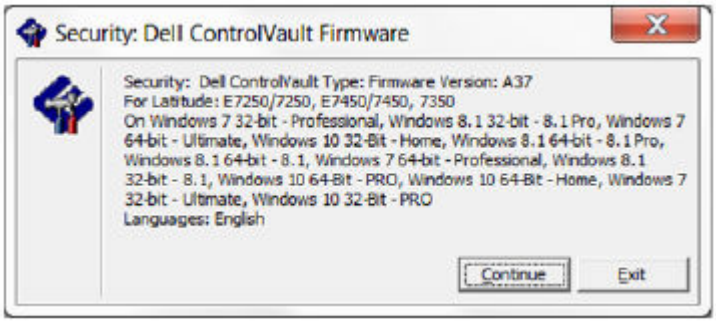
- O Gerenciador de dispositivos terá um dispositivo Dell ControlVault (e outros dispositivos) dependendo da configuração de hardware e do sistema operacional.

Instalação do firmware Dell ControlVault

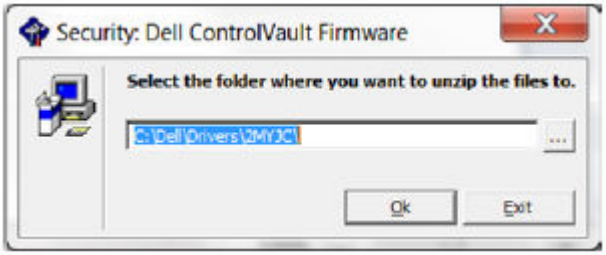
1. Navegue até a pasta na qual você fez o download do arquivo de instalação do firmware.



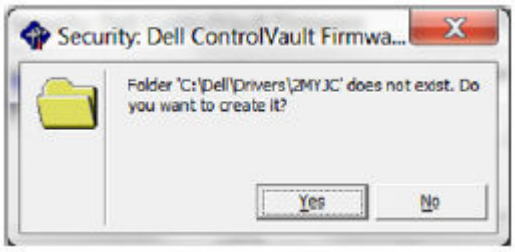
2. Clique duas vezes no firmware Dell ControlVault para abrir o arquivo executável autoextraível.
3. Clique em **Continuar** para começar.



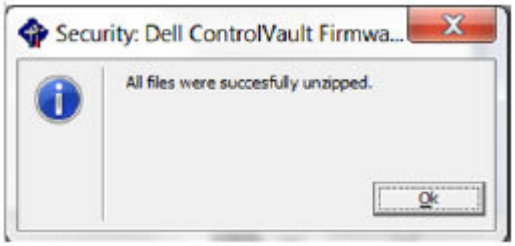
4. Clique em **OK** para descompactar os arquivos do driver no local padrão `C:\Dell\Drivers\<New Folder>`.



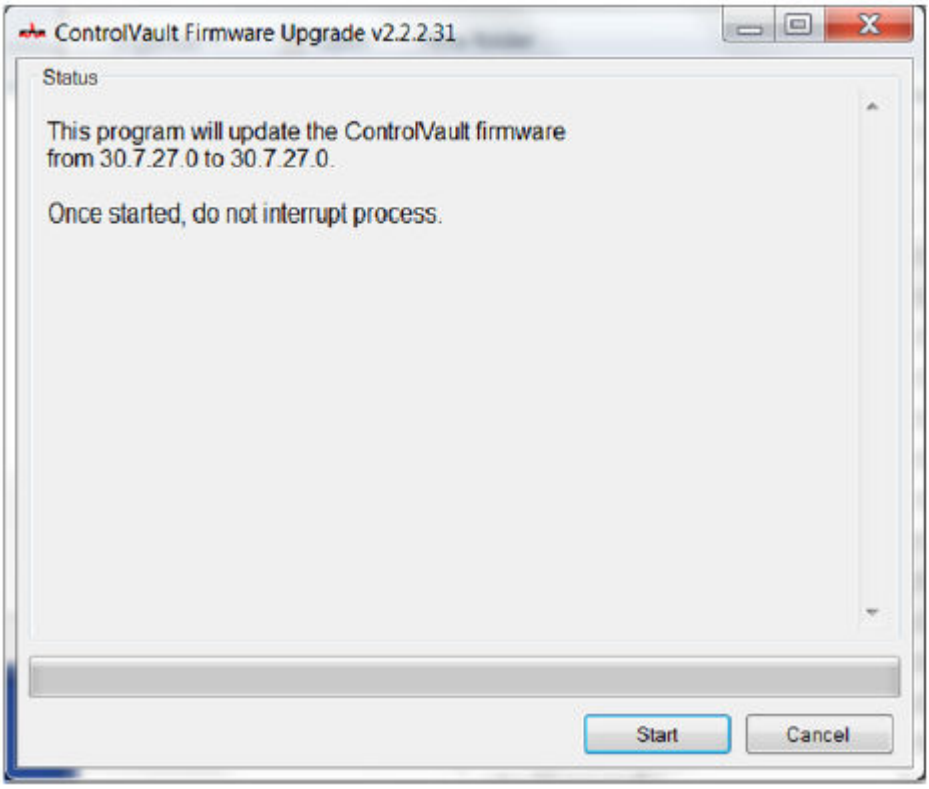
5. Clique em **Sim** para criar uma nova pasta.



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.



NOTA:

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.

Configurações de registro

Esta seção detalha todas as configurações de registro aprovadas pelo Dell ProSupport para computadores clientes locais.

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 a solução de problemas em 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 é 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 do 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

Usar Smart Cards com o login do Windows

- Para determinar se um smart card está presente e ativo, defina o seguinte valor:

  HKLM\SOFTWARE\Dell\Dell Data Protection\

  "SmartcardEnabled"=DWORD:1

  Se SmartcardEnabled estiver ausente ou tiver um valor de zero, o Credential Provider mostrará apenas a senha para autenticação.

  Se SmartcardEnabled tiver um valor diferente de zero, o Credential Provider mostrará opções para senha e autenticação de smart card.

- O seguinte valor de registro indica se Winlogon deve gerar uma notificação para eventos de logon de smart cards.

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

  "SmartCardLogonNotify"=DWORD:1

  0 = Desativado

  1 = Ativado

Preservar os arquivos temporários durante a instalação

- 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.

Alterar o comportamento padrão do prompt de usuário para iniciar ou atrasar a criptografia

- O client do Encryption exibe o prompt *`length of each policy update delay`* durante cinco minutos a 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 altera o comportamento para suspensão. Sem nenhuma interação do usuário, o processamento de criptografia é 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])

Alterar o uso padrão da chave SDUser

- 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 Encryption estiver processando uma atualização de política que inclui uma política do SDE ativa, o diretório de perfil de 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 essa 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.

Desativar/ativar criptografia para compartilhamento no menu de contexto de clique com o botão direito

- Para desativar ou ativar a opção *Criptografar para compartilhamento* no menu de clique com o botão direito, use a seguinte chave de registro.

  HKEY_LOCAL_MACHINE\SOFTWARE\Dell\Dell Data Protection\Encryption

  "DisplaySharing"=DWORD

  0 = desativar a opção Criptografar para compartilhamento no menu de contexto de clique com o botão direito

  1 = ativar a opção Criptografar para compartilhamento no menu de contexto de clique com o botão direito

Desativar/ativar a notificação para ativação do Encryption Personal

- HKCU\Software\Dell\Dell Data Protection\Encryption

  "HidePasswordPrompt"=DWORD

  1 = desativa o prompt de senha para ativação do Encryption Personal

  0 = ativa o prompt de senha para ativação do Encryption Personal

Desativar/ativar o prompt de reinicialização depois que o Agente de remoção de criptografia concluir a etapa final da descriptografia

- Para desativar o prompt que solicita que o usuário reinicialize o computador depois que o Agente de remoção de criptografia concluir a etapa final no processo de descriptografia, altere o seguinte valor de registro:

  HKLM\Software\Dell\Dell Data Protection

  "ShowDecryptAgentRebootPrompt"=DWORD

  Padrão = ativado

  1 = ativado (exibe o prompt)

  0 = desativado (oculta o prompt)

Advanced Authentication

Desativar Smart Card e serviços biométricos (opcional)

Se não quiser que o Advanced Authentication altere os serviços associados aos smart cards e dispositivos biométricos para um tipo de inicialização "automática", é possível desabilitar o recurso de inicialização do serviço.

Quando desabilitado, o Authentication não tenta iniciar estes três serviços:

- SCardSvr – Gerencia o acesso aos smart cards lidos pelo computador. Se esse serviço for interrompido, este computador não consegue ler os smart cards. 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 Smart Card.
- 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.

  Desativar esse recurso também cancela avisos associados aos serviços necessários que não estão em execução.

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

  [HKEY_LOCAL_MACHINE\SOFTWARE\DELL\Dell Data Protection]

  SmartCardServiceCheck=REG_DWORD:0

  Defina como 0 para ativar.

  Defina como 1 para desativar.

Usar smart cards com o login do Windows

- 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.

  NOTA: Excluir manualmente essa chave pode criar resultados involuntários para usuários sincronizando com a PBA, resultando na necessidade de uma recuperação manual.

- Para determinar se um smart card está presente e ativo, defina o seguinte valor:

  HKLM\SOFTWARE\Dell\Dell Data Protection\

  "SmartcardEnabled"=DWORD:1

  Se SmartcardEnabled estiver ausente ou tiver um valor de zero, o Credential Provider mostrará apenas a senha para autenticação.

  Se SmartcardEnabled tiver um valor diferente de zero, o Credential Provider mostrará opções para senha e autenticação de smart card.

- O seguinte valor de registro indica se Winlogon deve gerar uma notificação para eventos de logon de smart cards.

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

  "SmartCardLogonNotify"=DWORD:1

  0 = Desativado

  1 = Ativado

  Vá para Glossário.

- Para impedir que o gerenciamento de SED desative fornecedores de credenciais terceirizados, crie a seguinte chave de registro:

  HKLM\SOFTWARE\Dell\Dell Data Protection\

  "AllowOtherCredProviders" = DWORD:1

  0 = Desativado (padrão)

  1 = Ativado

- Por padrão, o Encryption Management Agent não gera mais políticas. Para gerar políticas para consumo futuro, crie a seguinte chave de registro:

  HKLM\Software\Dell\Dell Data Protection\

DWORD: DumpPolicies

Valor=1

Nota: é necessário reinicializar para que essa alteração entre em vigor.

- Para suprimir todas as “Notificações Torradeira” do Encryption Management Agent, o seguinte valor de registro deve ser definido no computador do cliente.

  [HKEY_LOCAL_MACHINE\SOFTWARE\Dell\Dell Data Protection]

  "PbaToastersAllowClose" =DWORD:1

  0=Ativado (padrão)

  1=Desativado

13

Glossário

Advanced Authentication - O produto Advanced Authentication fornece opções de leitor de cartão inteligente. O Advanced Authentication ajuda a gerenciar esses diversos métodos de autenticação, oferece suporte a login com unidades de criptografia automática, SSO e gerencia credenciais e senhas de usuário.

Senha de administrador de criptografia (EAP) - A EAP é uma senha administrativa exclusiva de cada computador. A maioria das configurações feitas no Console de gerenciamento local exige essa senha. Essa senha também é a mesma senha necessária para usar o seu arquivo LSARecovery_[hostname].exe para recuperar dados. Anote e guarde essa senha em um local seguro.

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.

Chaves de criptografia - Na maioria dos casos, o 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 de criptografia Comum torna os arquivos acessíveis a todos os usuários gerenciados no dispositivo em que foram criados. A chave de criptografia de Usuário torna os arquivos acessíveis apenas para o usuário que os criou, apenas no dispositivo em que foram criados. A chave de criptografia de Roaming de usuário torna os arquivos acessíveis apenas ao usuário que os criou, em qualquer dispositivo protegido do Windows ou Mac.

Varredura de criptografia - O processo de verificar as pastas a serem criptografadas 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 ocorre 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 log-on* estiver ativada, as pastas especificadas para criptografia são verificadas toda vez que o usuário fizer log-on. - 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) ativa uma varredura. Além disso, alternar entre a ativação e a desativação da criptografia aciona uma varredura de criptografia.

Autenticação de pré-inicialização (PBA) - A autenticação de pré-inicialização 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.

Logon único (SSO) - o SSO simplifica o processo de logon quando a autenticação multifatores está ativada, tanto na pré-inicialização como no logon do Windows. Se ativado, a autenticação será necessária na pré-inicialização apenas, e os usuários serão automaticamente conectados ao Windows. Se não estiver ativado, a autenticação talvez seja necessária mais de uma vez.

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 o 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.