Dell Encryption Personal

Installation Guide v11.9

January 2024
Rev. A01

DELL Technologies

Notas, avisos e advertências

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

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

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

Contents

1

Descrição geral

Este guia assume que o Advanced Authentication está instalado com o Encryption Personal.

Encryption Personal

O objetivo do Encryption Personal é proteger os dados no seu computador, mesmo que o computador seja perdido ou roubado.

Para garantir a segurança dos seus dados confidenciais, o Encryption Personal encripta os dados no seu computador Windows. Pode sempre aceder aos dados ao iniciar sessão no computador, mas utilizadores não autorizados não têm acesso a estes dados protegidos. Os dados permanecem sempre encriptados na unidade, mas porque a encriptação é transparente, não há necessidade de alterar a sua maneira de trabalhar com aplicações e dados.

Normalmente, a aplicação desencripta dados à medida que trabalha com eles. Ocasionalmente, uma aplicação pode tentar aceder a um ficheiro ao mesmo tempo que a aplicação o está a encriptar ou desencriptar. Se isto acontecer, um ou dois segundos depois, é exibida uma caixa de diálogo que lhe dá a opção de esperar ou cancelar a encriptação/desencriptação. Se escolher esperar, a aplicação liberta o ficheiro assim que está terminada (geralmente dentro alguns segundos).

Autenticação avançada

A Data Security Console é a interface que orienta os utilizadores durante a configuração das respetivas credenciais de PBA e perguntas de autorrecuperação, com base nas políticas definidas pelo administrador local.

Consulte Configurar as definições do administrador do Advanced Authentication e o *Dell Data Security Console User Guide* (Manual do utilizador da consola do Dell Data Security) para saber como utilizar a autenticação avançada.

Contacte o Dell ProSupport for Software

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

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

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

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

2

Requisitos

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

Encryption

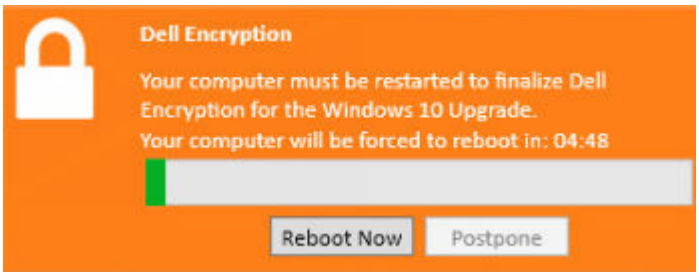
- O Encryption Personal requer elegibilidade para ser instalado com êxito. A elegibilidade é fornecida quando adquire o Encryption Personal. Consoante a forma como adquiriu o Encryption Personal, poderá instalar manualmente a elegibilidade, através das instruções que o acompanham. Também pode introduzir a elegibilidade na linha de comandos. Se o Encryption Personal for instalado com o Dell Digital Delivery, a instalação da elegibilidade é realizada pelo serviço Dell Digital Delivery. (Os mesmos binários são utilizados para Encryption Enterprise e Encryption Personal. A elegibilidade informa o instalador sobre a versão que deve instalar.)
- As contas Microsoft e Office 365 são suportadas ao executar o Encryption Personal v11.0 ou posterior no Windows 10.
- Para ativar uma conta Microsoft Live com Encryption Personal, consulte o artigo 124722 da BDC.
- É necessária uma palavra-passe do Windows (se ainda não existir nenhuma) para proteger o acesso aos dados encriptados. A criação de uma palavra-passe para o computador evita que outros iniciem sessão na sua conta de utilizador sem a sua palavra-passe. O Encryption Personal não será ativado se não for criada uma palavra-passe.
- O Dell Encryption não pode ser atualizado para a v10.7.0 a partir de versões anteriores à v8.16.0. Os pontos terminais com versões anteriores à v8.16.0 têm de ser atualizados para a v8.16.0 e, posteriormente, atualizados para a v10.7.0.
- O Dell Encryption utiliza o conjunto de instruções de encriptação da Intel, Integrated Performance Primitives (IPP). Para obter mais informações, consulte o artigo 126015 da BDC.

1. Aceda ao Painel de Controlo do Windows (**Iniciar** > **Painel de Controlo**).
2. Clique no ícone **Contas de utilizador**.
3. Clique em **Criar uma palavra-passe para a sua conta**.
4. Introduza uma nova palavra-passe e volte a introduzir a mesma.
5. Em alternativa, pode introduzir uma dica para palavra-passe.
6. Clique em **Criar palavra-passe**.
7. Reinicie o seu computador.

- Durante a implementação, devem ser seguidas as melhores práticas de TI. Estas incluem, entre outras, ambientes de teste controlados para os testes iniciais e a implementação progressiva para os utilizadores.
- A conta de utilizador que realiza a instalação/atualização/desinstalação deve ser um utilizador administrador local ou de domínio, que poderá ser atribuído temporariamente por uma ferramenta de implementação, como o Microsoft SMS. Não são suportados utilizadores não administradores com privilégios elevados.
- Realize uma cópia de segurança de todos os dados importantes antes de iniciar a instalação/desinstalação/atualização.
- Não realize alterações no computador, incluindo inserir ou remover unidades externas (USB) durante a instalação/desinstalação/atualização.
- Para reduzir o tempo de encriptação inicial (bem como o tempo de desencriptação em caso de desinstalação), execute o Assistente de limpeza de disco do Windows para remover ficheiros temporários e quaisquer outros dados desnecessários.
- Desative o modo de suspensão durante o varrimento de encriptação inicial para impedir a suspensão do computador caso este se encontre sem supervisão. A encriptação não é possível num computador em suspensão (tal como não é possível a desencriptação).
- O cliente Encryption não suporta configurações de duplo arranque, uma vez que é possível encriptar ficheiros de sistema do outro sistema operativo, o que poderia interferir com o respetivo funcionamento.
- O instalador principal não suporta atualizações a partir de componentes anteriores à v8.0. Extraia os instaladores subordinados do instalador principal e atualize o componente individualmente. Se tiver alguma dúvida ou questão, contacte a Dell ProSupport.
- O cliente Encryption agora suporta o modo Audit. O modo Audit permite que os administradores implementem o cliente Encryption como parte da imagem corporativa, em vez de usar um SCCM de outros fabricantes ou uma solução similar para implementar o cliente Encryption. Para obter instruções sobre como instalar o cliente Encryption numa imagem corporativa, consulte o artigo 129990 da BDC.
- O TPM é utilizado para selar a General Purpose Key. Assim, se o cliente Encryption for executado, limpe o TPM na BIOS antes de proceder à instalação de um novo sistema operativo no computador de destino.

- O cliente de encriptação foi sujeito a testes e é compatível com vários antivírus baseados em assinatura populares e soluções antivírus baseadas em inteligência artificial, incluindo McAfee Virus Scan Enterprise, McAfee Endpoint Security, Symantec Endpoint Protection, CylancePROTECT, CrowdStrike Falcon, Carbon Black Defense e vários outros. As exclusões impostas estão incluídas por predefinição em muitos fornecedores de antivírus para evitar incompatibilidades entre a análise de vírus e a encriptação.

  No caso de a sua organização utilizar um antivírus de um fornecedor que não esteja na lista, ou se estiver a experienciar quaisquer problemas de compatibilidade, consulte o artigo 126046 da BDC ou contacte o Dell ProSupport para obter assistência na validação da configuração de interoperabilidade entre as suas soluções de software e as soluções Dell Data Security.
- Não são suportadas reinstalações do sistema operativo. Para realizar a reinstalação do sistema operativo, faça uma cópia de segurança do computador em questão, realize a limpeza do computador, instale o sistema operativo e, em seguida, realize a recuperação dos dados encriptados seguindo os procedimentos de recuperação estabelecidos.
- Certifique-se de que verifica periodicamente a página dell.com/support para procurar a documentação e os avisos técnicos mais atuais.
- Após a atualização de funcionalidades do Windows 10, é **necessário** reiniciar para finalizar o Dell Encryption. A seguinte mensagem é exibida na área de notificação após as atualizações de funcionalidades do Windows 10:



Pré-requisitos

- É necessário o Microsoft .Net Framework 4.5.2 (ou posterior) para os instaladores principais e subordinados. O instalador não instala o componente Microsoft .Net Framework.

  NOTA: É necessário o .Net Framework 4.6 (ou posterior) quando em modo FIPS.

- O instalador principal instala os seguintes pré-requisitos se ainda não estiverem instalados no computador. **Quando utilizar o instalador subordinado**, é necessário instalar este componente antes de instalar o Encryption.

Pré-requisito
○ Visual C++ 2012 Update 4 ou Redistributable Package posterior (x86 ou x64) ○ Visual C++ 2017 Update 3 ou Redistributable Package posterior (x86 ou x64) ○ As aplicações e os pacotes de instalação com certificados de assinatura SHA1 irão funcionar, mas sem estas atualizações instaladas será apresentado um erro no ponto terminal durante a instalação ou a execução da aplicação

Hardware

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

Hardware
○ Processador Intel Pentium ou AMD ○ 110 MB de espaço livre em disco ○ 512 MB de RAM **NOTA:** É necessário espaço livre em disco adicional para encriptar os ficheiros no ponto terminal. Este tamanho varia de acordo com as políticas e com a capacidade da unidade.

- A tabela seguinte apresenta o hardware de computador opcional suportado.

Hardware opcional incorporado
○ TPM 1.2 ou 2.0

Sistemas operativos

- A tabela seguinte apresenta os sistemas operativos suportados.

Sistemas operativos 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:** os OEMs e ODMs não são fornecidos com o Windows 10 v2004 (Atualização de maio de 2020/20H1 e posterior) com a arquitetura de 32 bits. Para obter mais informações, consulte https://docs.microsoft.com/windows-hardware/design/minimum/minimum-hardware-requirements-overview. ■ Windows 10 2019 LTSC ■ Windows 10 2021 LTSC ○ Windows 11: Enterprise, Pro v21H2 —22H2

Sistemas operativos Encryption External Media

- O suporte de dados externo tem de ter aproximadamente 55 MB disponíveis, bem como espaço livre no suporte de dados igual ao maior ficheiro a encriptar para alojar o Encryption External Media.
- A seguir são apresentados os sistemas operativos suportados ao aceder a suportes de dados protegidos da Dell.

Sistemas operativos Windows compatíveis para aceder a suportes de dados encriptados (32 e 64 bits)
○ Windows 10: Education, Enterprise, Pro v1909-v22H2 (Atualização de novembro de 2019/19H2 — Atualização de novembro de 2022/22H2) **Nota:** os OEMs e ODMs não são fornecidos com o Windows 10 v2004 (Atualização de maio de 2020/20H1 e posterior) com a arquitetura de 32 bits. Para obter mais informações, consulte https://docs.microsoft.com/windows-hardware/design/minimum/minimum-hardware-requirements-overview. ■ Windows 10 2019 LTSC ■ Windows 10 2021 LTSC ○ Windows 11: Enterprise, Pro v21H2 —22H2

Sistemas operativos Mac compatíveis para aceder a suportes de dados encriptados (kernels de 64 bits)
○ macOS High Sierra 10.13.5–10.13.6 ○ macOS Mojave 10.14.0–10.14.4 ○ macOS Catalina 10.15.5–10.15.6

Localização

- O Encryption está em conformidade com a norma de interface de utilizador multilíngue e está localizado nos seguintes idiomas.

Suporte de idiomas	
○ EN — Inglês	○ JA — Japonês
○ ES — Espanhol	○ KO — Coreano
○ FR — Francês	○ PT-BR — Português, Brasil

Suporte de idiomas	
○ IT — Italiano	○ PT-PT — Português, Portugal (Ibérico)
○ DE — Alemão	

SED Manager

- O IPv6 não é suportado.
- Prepare-se para encerrar e reiniciar o computador após aplicar as políticas e quando estiver pronto para começar a implementá-las.
- Os computadores equipados com unidades de encriptação automática não podem ser utilizados com placas HCA. Existem incompatibilidades que impedem o aprovisionamento do HCA. A Dell não vende computadores com unidades de encriptação automática compatíveis com o módulo HCA. Esta configuração não suportada seria uma configuração pós-venda.
- Se o computador destinado à encriptação estiver equipado com uma unidade de encriptação automática, certifique-se de que a opção do Active Directory, *O utilizador deve alterar a palavra-passe no próximo início de sessão*, está desativada. A Autenticação de pré-arranque não suporta esta opção do Active Directory.
- O SED Manager não é suportado com configurações de várias unidades.
- **NOTA:**

  Devido à natureza do RAID e das SED, o SED Manager não suporta RAID. O problema de *RAID=On* nas SEDs é que o RAID necessita de acesso ao disco para ler e gravar dados relacionados com o RAID num setor elevado não disponível numa SED bloqueada desde o arranque, e não pode esperar até o utilizador iniciar sessão para ler estes dados. Para solucionar este problema, altere a operação SATA no BIOS de *RAID=On* para *AHCI*. Se o sistema operativo não incluir controladores AHCI pré-instalados, o sistema operativo irá falhar quando alterar de *RAID=On* para *AHCI*.

- O instalador principal instala os seguintes pré-requisitos se ainda não estiverem instalados no computador. **Quando utilizar o instalador subordinado**, tem de instalar estes componentes antes de instalar o SED Manager.

Pré-requisito
○ Visual C++ 2017 Update 3 ou Redistributable Package posterior (x86 ou x64)
○ As aplicações e os pacotes de instalação com certificados de assinatura SHA1 irão funcionar, mas sem estas atualizações instaladas será apresentado um erro no ponto terminal durante a instalação ou a execução da aplicação

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

  As SEDs compatíveis com OPAL suportadas requerem controladores Intel Rapid Storage Technology atualizados, localizados em www.dell.com/support. A Dell recomenda o controlador Intel Rapid Storage Technology mais recente com unidades NVMe.

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

- As configurações de encriptação em vários discos com o SED Manager exigem as seguintes condições:
  - Todos os discos no sistema de destino têm de ser SEDs.
  - Todos os discos no sistema de destino têm de ser configurados no mesmo modo de arranque.

- No modo de arranque UEFI, o sistema operativo pode ser instalado em qualquer disco de destino.
- No modo de arranque Legacy, o sistema operativo tem de ser instalado no primeiro disco (Disco n.º 0). Se o sistema operativo não estiver instalado no primeiro disco, a encriptação em vários discos é desativada.

- Algumas versões da BIOS podem ativar o Bloqueio SID por predefinição, o que pode inibir o SED Manager. Para obter mais informações, consulte o artigo 126083 da BDC.
- As Atualizações de Funcionalidades Diretas do Windows 10 v1607 (Atualização de Aniversário/Redstone 1) ao Windows 10 v1903 (Atualização de maio de 2019/19H1) não são suportadas com o Dell Encryption. A Dell recomenda a atualização do sistema operativo para uma Atualização de Funcionalidades mais recente se estiver a atualizar para o Windows 10 v1903. Qualquer tentativa de atualização direta do Windows 10 v1607 para o v1903 resulta numa mensagem de erro e a atualização é impedida.
- **NOTA:** É necessária uma palavra-passe com Autenticação de pré-arranque. A Dell recomenda definir uma palavra-passe com, pelo menos, 9 carateres.

- **NOTA:** É necessária uma palavra-passe para todos os utilizadores adicionados no painel *Adicionar utilizador*. Os utilizadores sem palavras-passe serão bloqueados e ficarão sem acesso ao computador após a ativação.
- **NOTA:** Os computadores protegidos pelo SED Manager têm de ser atualizados para o Windows 10 v1703 (Atualização para Criativos/Redstone 2) ou posterior antes de serem atualizados para o Windows 10 v1903 (Atualização de maio de 2019/19H1) ou posterior. Se tentar este procedimento de atualização, é apresentada uma mensagem de erro.
- O SED Manager requer a utilização do fornecedor de credenciais personalizado da Dell para sincronizar as alterações de palavra-passe do Windows e as chaves de encriptação de dados. Se precisar de utilizar aplicações de terceiros que utilizam fornecedores de credenciais personalizados executados em computadores protegidos por SED Manager, terá de iniciar alterações de palavra-passe do Windows através da Data Security Console. Para obter mais informações sobre como alterar a palavra-passe na Data Security Console, consulte o capítulo *Palavra-passe* no Guia do utilizador da Data Security Console.

Hardware

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

Teclados internacionais

A tabela que se segue indica teclados internacionais suportados com Autenticação de pré-arranque em computadores UEFI e não-UEFI.

Suporte de teclado internacional — UEFI	
DE-FR — Francês (Suíça)	EN-GB — Inglês (Reino Unido)
DE-CH — Alemão (Suíça)	EN-CA — Inglês (Canadá)
EN-US — Inglês (América)	

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

Sistemas operativos

- A tabela seguinte apresenta os sistemas operativos compatíveis.

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

As funcionalidades de autenticação só estão disponíveis quando a Autenticação de pré-arranque está ativada.

Localização

O SED Manager está em conformidade com a norma de interface de utilizador multilíngue e está localizado nos seguintes idiomas. O modo UEFI e a Autenticação de pré-arranque são suportados nos seguintes idiomas:

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

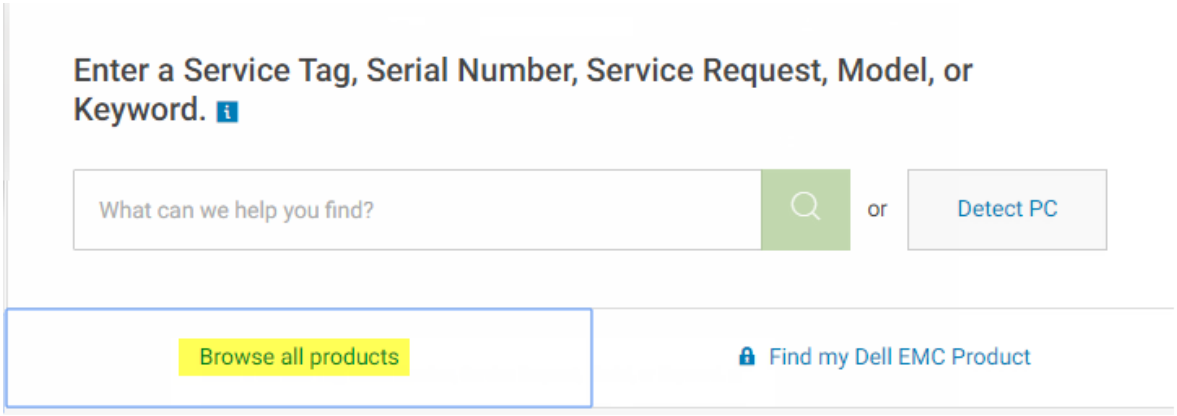
3

Transferir o software

Esta secção detalha a obtenção de software a partir de dell.com/support. Se já tiver o software, pode ignorar esta secção.

Aceda a dell.com/support para começar.

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



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

   Após efetuar esta seleção uma vez, o site memoriza as informações.
4. Selecione o produto Dell.

   Exemplos:

   Dell Encryption Enterprise

   Dell Endpoint Security Suite Enterprise
5. Selecione **Controladores e Transferências**.
6. Selecione o tipo de sistema operativo cliente desejado.
7. Selecione **Dell Encryption** nas correspondências. Isto é apenas um exemplo, pelo que, provavelmente, a realidade será ligeiramente diferente. Por exemplo, é possível que não existem quatro ficheiros para escolha.
8. Selecione **Transferir**.

   Avance para Instalar o Encryption Personal.

4

A instalação

Pode instalar o Encryption Personal utilizando o instalador principal (recomendado) ou extraindo os instaladores subordinados do instalador principal. De qualquer maneira, o Encryption Personal pode ser instalado pela interface do utilizador, linha de comandos ou scripts, e usando tecnologia push disponível para a sua organização.

Os utilizadores devem consultar os seguintes ficheiros de ajuda para assistência de aplicação:

NOTA: Se a Encriptação Baseada em Políticas for instalada antes do Encryption Management Agent, poderá ocorrer uma falha do computador. Este problema é causado devido à falha ao carregar o controlador de encriptação do modo Suspensão que gere o ambiente PBA. Como solução alternativa, utilize o instalador principal ou certifique-se de que a Encriptação Baseada em Políticas é instalada depois do Encryption Management Agent.

- Consulte a *Ajuda do Dell Encrypt* para saber como utilizar as funcionalidades do Encryption. Aceda à ajuda a partir de `<Install dir>\Program Files\Dell\Dell Data Protection\Encryption\Help`.
- Consulte a *Ajuda do* Encryption External Media para saber como utilizar as funcionalidades do Encryption External Media. Aceda à ajuda a partir de `<Install dir>\Program Files\Dell\Dell Data Protection\Encryption`.
- Consulte a *Ajuda do* Encryption Personal para saber como utilizar as funcionalidades do Advanced Authentication. Aceda à ajuda a partir de `<Install dir>\Program Files\Dell\Dell Data Protection\Security Tools\Help`.

Direito à Importação

A instalação do Encryption Personal requer uma chave de registo no computador de destino. Esta chave de registo é adicionada através da interface da Linha de Comandos durante a instalação ou através da GUI antes da instalação.

Para adicionar a chave de registo através da interface da Linha de Comandos, consulte Instalar a Linha de Comandos.

Para adicionar a chave de registo através da GUI:

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

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

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

3. Guarde o ficheiro de texto com a extensão `.reg`.
4. Clique duas vezes no ficheiro de registo guardado para importar o direito Encryption Personal.

Selecione um método de instalação

Existem dois métodos para instalar o cliente; selecione **um** dos seguintes:

- Instalar interativamente – RECOMENDADO
- Instalação através da Linha de Comandos

Instalação interativa

Para instalar o Encryption Personal, o instalador tem de encontrar a elegibilidade adequada no computador. Se não for encontrada a elegibilidade adequada, o Encryption Personal não pode ser instalado.

- O Instalador Principal instala vários clientes. No caso do Encryption Personal, este instala o Encryption e o SED Management.
- Os ficheiros de registo do instalador principal estão localizados em `C:\ProgramData\Dell\Dell Data Protection\Installer`.

1. Instale a elegibilidade no computador de destino se necessário. São incluídas instruções para adicionar elegibilidade ao computador no e-mail que aborda informações sobre a licença.
2. Copie DDSSetup.exe para o computador local.
3. Faça duplo clique em DDSSetup.exe para iniciar o instalador.
4. Surge uma caixa de diálogo que o alerta para o estado da instalação de pré-requisitos. Demora alguns minutos.
5. Clique em **Seguinte** no ecrã de boas-vindas.
6. Leia o contrato de licença, aceite os termos e clique em **Seguinte**.
7. Clique em **Seguinte** para instalar o Encryption Personal na localização predefinida em `C:\Program Files\Dell\Dell Data Protection\`.
8. A autenticação é instalada por predefinição e não é possível desselecionar. No instalador, está indicado como Security Framework.

   Clique em **Seguinte**.
9. Clique em **Instalar** para dar início à instalação.

   É apresentada uma janela de estado. Isto demora vários minutos.
10. Selecione **Sim, desejo reiniciar o computador agora** e clique em **Concluir**.
11. Uma vez que é reiniciado o computador, autentique para Windows.

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

A secção de configuração e assistente de configuração do Encryption Personal é abrangida em separado.

Assim que a configuração e o assistente de configuração do Encryption Personal estiverem concluídos, inicie a consola de administração do Encryption Personal.

O resto desta secção detalha mais tarefas de instalação e pode ser ignorada. Avance para Assistentes de configuração do Advanced Authentication e Encryption Personal.

Instalação através da Linha de Comandos

Para instalar o Encryption Personal utilizando a linha de comandos, os ficheiros subordinados executáveis devem primeiro ser extraídos do instalador principal. Consulte Extrair os Instaladores Subordinados do Instalador Principal. Assim que estiver concluído, volte a esta secção.

- Instale a elegibilidade no computador de destino se necessário.
- **NOTA:** Os registos Dell Encryption não especificam se a falha da instalação resultou de espaço insuficiente no disco.
- Opções:

  Para uma instalação com linha de comandos, primeiro deve especificar os switches. A tabela seguinte descreve as opções disponíveis para a instalação.

Opção	Significado
/s	Modo silencioso
/z	Passe os dados para o sistema InstallScript de CMDLINE variável.

- Parâmetros:

  A tabela seguinte descreve os parâmetros disponíveis para a instalação.

Parâmetros
InstallPath=caminho para local de instalação alternativo.
FEATURE=PE
ENTITLEMENT=1:PE:{Encryption Personal Entitlement key here}

Parâmetros
NOTA: Este parâmetro **só** pode ser utilizado com o Encryption Personal

- Exemplo de instalação através da Linha de Comandos

  Nestes exemplos de linha de comandos, o reinício foi suprimido. No entanto, é necessário um eventual reinício.

  A Encriptação Baseada em Políticas só pode ser iniciada após o reinício do computador.

  Certifique-se de que inclui um valor que contenha um ou mais caracteres especiais, como um espaço em branco, entre aspas duplas de escape.

  As linhas de comandos são sensíveis a maiúsculas e minúsculas.

- O exemplo seguinte instala o Encryption client (instalação silenciosa, sem reinício e instalado na localização predefinida `C:\Program Files\Dell\Dell Data Protection`), transmitindo a chave de elegibilidade 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 seguinte instala o Encryption Personal e a Advanced Authentication (instalação silenciosa, sem reinício, instalado na localização predefinida `C:\Program Files\Dell\Dell Data Protection`).

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

- O exemplo seguinte instala o Encryption Personal e a Advanced Authentication (instalação silenciosa, sem reinício, instalado na localização predefinida `C:\Program Files\Dell\My_New_Folder`).

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

  Uma vez que é reiniciado o computador, autentique para Windows.

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

  A secção de configuração e assistente de configuração do Encryption Personal é abrangida em separado.

  Assim que a configuração e o assistente de configuração do Encryption Personal estiverem concluídos, inicie a consola de administração do Encryption Personal.

  O resto desta secção detalha mais tarefas de instalação e pode ser ignorada. Avance para Assistentes de configuração de Advanced Authentication e Personal Edition.

5

Assistentes de configuração do Advanced Authentication e Encryption Personal

Inicie sessão com o seu nome de utilizador e palavra-passe do Windows. Acede ao Windows sem problemas. A interface poderá ser diferente daquilo a que está habituado.

1. O UAC poderá solicitar que execute a aplicação. Se for o caso, clique em Sim.
2. Após o reinício da instalação inicial, surge o assistente de ativação do Advanced Authentication. Clique em **Seguinte**.
3. Introduza e volte a introduzir uma nova palavra-passe de administração de encriptação (EAP). Clique em **Seguinte**.

   Nota: a Palavra-passe do Administrador do Encryption tem de ter, no mínimo, oito carateres e não pode exceder os 127 carateres.
4. Introduza uma localização de cópia de segurança numa unidade de rede ou no suporte de dados amovível para armazenar as informações de recuperação e clique em **Seguinte**.
5. Clique em **Aplicar** para iniciar a ativação do Advanced Authentication.

   Depois de o assistente ter concluído a ativação do Advanced Authentication, avance para o passo seguinte.
6. Inicie o assistente de configuração do Encryption Personal no ícone do Dell Encryption na área de notificação (pode iniciar autonomamente).

   Este Assistente de configuração ajuda-lhe a utilizar a encriptação para proteger as informações neste computador. Se este assistente não for concluído, a encriptação não pode começar.

   Leia o ecrã de Boas-vindas e clique em **Seguinte**.
7. Selecione um modelo de política. O modelo de política estabelece as predefinições da política para encriptação.

   É possível aplicar facilmente um modelo de política diferente ou personalizar o modelo selecionado na Consola de gestão local quando a configuração inicial estiver concluída.

   Clique em **Seguinte**.
8. Leia e confirme o aviso de palavra-passe do Windows. Se pretender criar agora uma palavra-passe do Windows, consulte os Requisitos.
9. Crie uma Palavra-passe do Administrador de Encriptação (EAP) de 8-127 carateres e confirme. A palavra-passe deve conter caracteres alfabéticos, numéricos e especiais. Esta palavra-passe pode ser a mesma que a EAP que definiu para o Advanced Authentication, mas não está relacionada com o mesmo. **Registe e guarde esta palavra-passe num local seguro**. Clique em **Seguinte**.

   Nota: a Palavra-passe do Administrador do Encryption tem de ter, no mínimo, oito carateres e não pode exceder os 127 carateres.
10. Clique **Procurar** para escolher a unidade de rede ou armazenamento removível para fazer uma cópia de segurança das suas chaves de encriptação (as quais estão numa aplicação chamada LSARecovery_[hostname].exe).

    Na eventualidade de ocorrerem determinadas falhas informáticas, estas chaves são utilizadas para recuperar os seus dados.

    Além disso, mudanças de políticas futuras requerem, por vezes, que sejam efetuadas novas cópias de segurança das chaves de encriptação. Se a unidade de rede ou a unidade de armazenamento amovível estiver disponível, as cópias de segurança das chaves de encriptação são realizadas em segundo plano. Contudo, se a localização não estiver disponível (por exemplo, quando o dispositivo de armazenamento amovível original não está inserido no computador), as mudanças de política não entram em vigor até que sejam efetuadas manualmente cópias de segurança das chaves de encriptação.

    NOTA: Para aprender a fazer manualmente cópias de segurança de chaves de encriptação, clique em "**? > Ajuda**" no canto superior direito da Consola de gestão local ou clique em **Iniciar > Dell > Ajuda do Encryption**.

    Clique em **Seguinte**.

11. No ecrã de Confirmar Definições de Encriptação, é exibida uma lista de Definições de Encriptação. Reveja os itens e, quando estiver satisfeito com as definições, clique em **Confirmar**.

    A configuração do computador inicia-se. Uma barra de estado informa sobre o progresso da configuração.

12. Clique em **Concluir** para finalizar a configuração.
13. É necessário reiniciar após o computador estar configurado para encriptação. Clique em **Reiniciar agora** ou adie o reinício 5 vezes por 20 minutos cada.
14. Assim que o computador for reiniciado, abra a consola de gestão local a partir do menu Iniciar para ver o estado da encriptação.

    A encriptação decorre em segundo plano. A consola de gestão local pode estar aberta ou fechada. De qualquer forma, a encriptação dos ficheiros avança. Pode continuar a utilizar o computador da forma habitual durante a encriptação.

15. Quando a análise estiver concluída, o computador é novamente reiniciado.

    Assim que todos os varrimentos de encriptação e reinícios estiverem concluídos, pode verificar o estado de conformidade iniciando a consola de gestão local. A unidade é denominada "Em conformidade".

6

Configurar as definições da Console

As predefinições permitem que os administradores e utilizadores utilizem a autenticação avançada imediatamente após a ativação, sem ser necessária uma configuração adicional. Os utilizadores são adicionados automaticamente como utilizadores de autenticação avançada quando iniciam sessão no computador com as respetivas palavras-passe do Windows, mas, por predefinição, a autenticação multifator do Windows não está ativada.

Para configurar as funcionalidades de autenticação avançada, tem de ser um administrador no computador.

Alterar a palavra-passe de administrador e a localização da cópia de segurança.

Após a ativação do Advanced Authentication, é possível alterar a palavra-passe do administrador e a localização da cópia de segurança, se necessário.

1. Como administrador, inicie a consola do Dell Data Security no atalho do ambiente de trabalho.
2. Clique no mosaico **Definições do Administrador**.
3. Na caixa de diálogo Autenticação, introduza a palavra-passe de administrador que foi configurada durante a ativação e clique em **OK.**
4. Clique no separador **Definições do administrador**.
5. Na página Alterar a palavra-passe de administrador, para alterar a palavra-passe, introduza uma nova palavra-passe que tenha entre 8 e 32 caracteres e que inclua pelo menos uma letra, um número e um carácter especial.
6. Introduza novamente a palavra-passe para confirmá-la, e clique em **Aplicar**.
7. Para alterar a localização de armazenamento da chave de recuperação, no painel esquerdo selecione **Alterar a localização da cópia de segurança**.
8. Selecione uma nova localização para a cópia de segurança, e clique em **Aplicar**.

   O ficheiro de cópia de segurança tem de ser guardado numa unidade de rede ou num suporte multimédia amovível. O ficheiro da cópia de segurança contém as chaves necessárias para a recuperação de dados neste computador. O Dell ProSupport terá de aceder a este ficheiro para ajudá-lo a recuperar dados.

   É efetuada automaticamente uma cópia de segurança dos dados de recuperação no local especificado. Se a localização não estiver disponível (por exemplo, se a sua unidade USB para cópia de segurança não estiver introduzida), o Advanced Authentication solicita-lhe uma localização para criar uma cópia de segurança dos seus dados. É necessário aceder aos dados de recuperação para iniciar a encriptação.

Configurar Autenticação de Pré-arranque

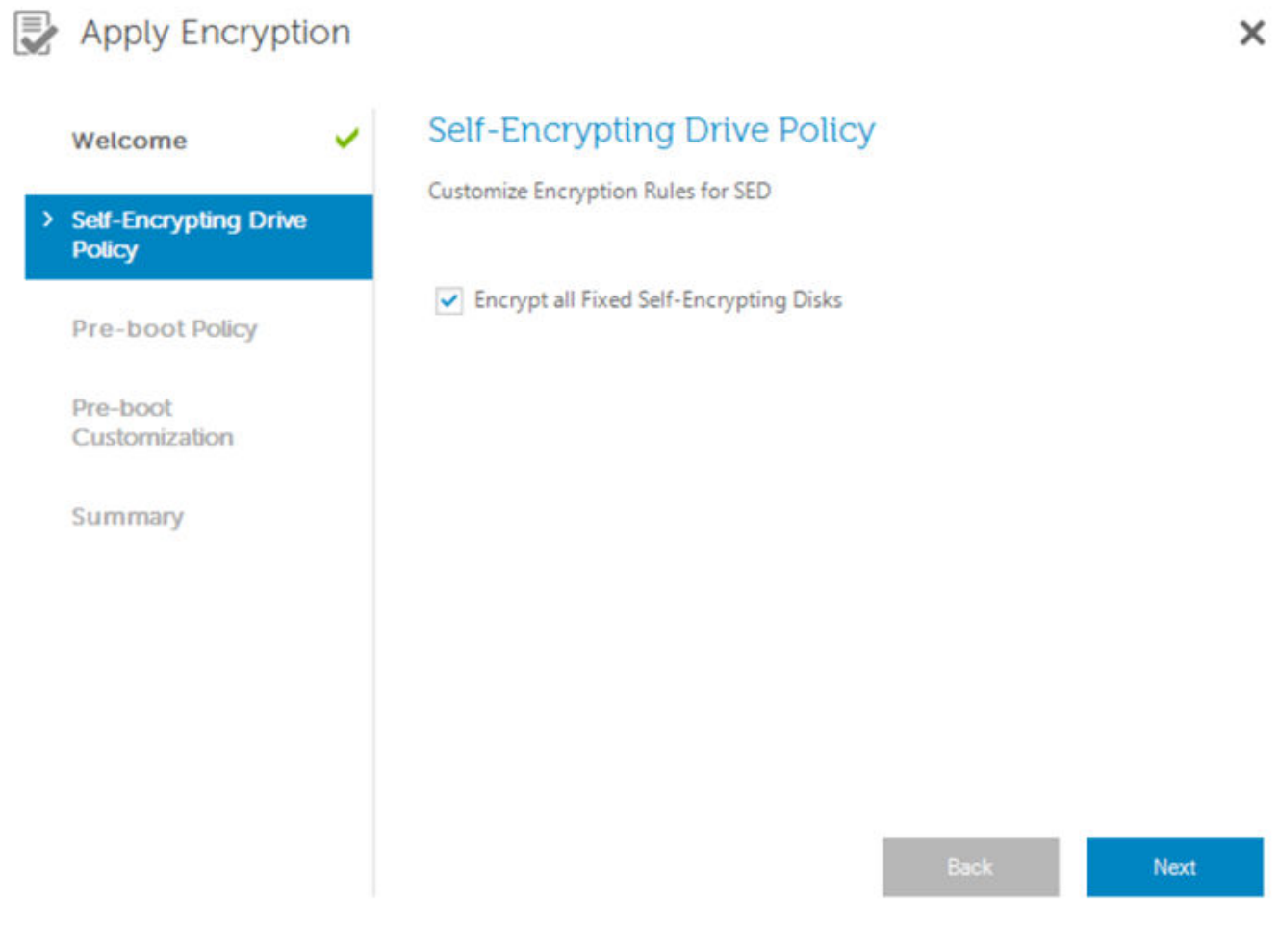
A PBA está disponível se o seu computador estiver equipado com uma SED. A PBA é configurada através do separador Encryption. Quando o SED Manager assume a propriedade da SED, a PBA é ativada.

Para ativar o SED Management:

1. No Data Security Console, clique no mosaico **Definições do administrador**.
2. Certifique-se de que a localização da cópia de segurança está acessível a partir do computador.

   Se for apresentada a mensagem *Localização da cópia de segurança não encontrada* e a localização da cópia de segurança estiver numa unidade USB, a sua unidade não está ligada ou está ligada a uma ranhura diferente da utilizada durante a cópia de segurança. Se a mensagem for exibida e a localização da cópia de segurança estiver numa unidade de rede, a unidade de rede está inacessível a partir do computador. Se for necessário alterar a localização da cópia de segurança, no separador **Definições do administrador**, selecione **Alterar a localização da cópia de segurança** para alterar o local da ranhura atual ou unidade acessível. Alguns segundos após a nova atribuição da localização, o processo de ativação da encriptação pode prosseguir.

3. Clique no separador **Encryption** e, em seguida, clique em **Encriptar**.
4. Na página de Boas-Vindas, clique em **Seguinte**.
5. Selecione **Encriptar todas as Unidades Encriptação Automática Fixas** para ativar a Encriptação em vários discos.



6. Na página de Política de pré-arranque, altere ou confirme os valores que se seguem e clique em **Seguinte**.

Tentativas de início de sessão do utilizador não armazenadas em cache	Número de vezes que um utilizador desconhecido pode tentar iniciar sessão (um utilizador que nunca tenha iniciado sessão no computador [sem credenciais armazenadas em cache]).
Tentativas de início de sessão do utilizador armazenadas em cache	Número de vezes que um utilizador conhecido pode tentar iniciar sessão.
Tentativas de resposta a perguntas de recuperação	Número de vezes que o utilizador pode tentar introduzir a resposta correta.
Ativar palavra-passe para apagar encriptação	Selecione para ativar.
Introduzir palavra-passe para apagar encriptação	Uma palavra ou código até 100 caracteres utilizados como mecanismo de segurança à prova de falhas. A introdução desta palavra ou código no campo de nome de utilizador ou palavra-passe durante a autenticação de pré-arranque inicia a eliminação de encriptação, que remove as chaves do armazenamento seguro. Depois de ativar este processo, é impossível recuperar a unidade. Deixe este campo em branco se não pretender uma palavra-passe para apagar encriptação disponível em caso de emergência.

	Deixe este campo em branco se não pretender ter uma palavra-passe para apagar encriptação disponível em caso de emergência.
Lembrar-me	Ativa ou desativa a capacidade de os utilizadores selecionarem a opção Lembrar-me no ecrã de início de sessão do PBA.

7. Na página de Personalização de pré-arranque, introduza o texto personalizado para exibir no ecrã de Autenticação de pré-arranque (PBA) e clique em **Seguinte.**

Texto do título de pré-arranque	Este texto é apresentado na parte superior do ecrã da PBA. Se deixar este campo em branco, não será apresentado qualquer título. O texto não é moldado (ou seja, o texto não passa para a linha seguinte), pelo que introduzir mais do que 17 caracteres poderá resultar no corte do texto.
Texto de informação de apoio	Texto a apresentar no ecrã de informação de apoio da PBA. Personalize a mensagem para incluir informações sobre como contactar o suporte técnico ou o administrador de segurança. Caso não seja introduzido qualquer texto neste campo, não estará disponível qualquer informação de contacto de suporte para o utilizador. A moldagem do texto ocorre ao nível da palavra, não ao nível dos caracteres. Se uma palavra tiver mais de 50 carateres, esta não passa para a linha seguinte nem é apresentada uma barra de deslocamento, fazendo com que o texto seja truncado.
Texto do aviso legal	Este texto é apresentado antes que o utilizador possa iniciar sessão no dispositivo. Por exemplo: "Se clicar em OK, concorda respeitar a política de utilização aceitável do computador." A não introdução de texto neste campo resulta na não apresentação de qualquer texto ou dos botões OK/Cancelar. A moldagem do texto ocorre ao nível da palavra, não ao nível dos caracteres. Por exemplo, se tiver uma única palavra que tenha mais de 50 caracteres de comprimento, esta não passa para a linha seguinte nem é apresentada uma barra de deslocamento; por conseguinte, o texto é cortado.

8. Na página de Resumo, clique em **Aplicar**.
9. Quando for solicitado, clique em **Encerrar**.

   É necessário um encerramento total antes de se poder iniciar a encriptação.

10. Após o encerramento, reinicie o computador.

    A autenticação agora é gerida pelo Encryption Management Agent. Os utilizadores necessitam de iniciar sessão no ecrã da PBA com as suas palavras-passe do Windows.

Alterar Definições da PBA e do SED Management

Depois de ativar a encriptação e configurar a Política e Personalização de pré-arranque pela primeira vez, as seguintes ações estão disponíveis no separador Encryption:

- Alterar a personalização ou a política de pré-arranque — Clique no separador **Encryption** e, em seguida, clique em **Alterar**.
- Desativar o SED Management, por exemplo, para a desinstalação — Clique em **Desencriptar**.

Depois de ativar o SED Management e configurar a Política e Personalização de Pré-arranque pela primeira vez, as seguintes ações estão disponíveis no separador Definições de Pré-arranque:

- Alterar a Política ou a Personalização de Pré-arranque — Clique no separador **Definições de pré-arranque** e selecione **Política da Unidade de Encriptação Automática**, **Política de Pré-arranque** ou **Personalização de Pré-arranque**.

Gestão e autenticação de utilizadores

Adicionar utilizador

Os utilizadores do Windows passam automaticamente a utilizadores do Encryption Personal quando iniciam sessão no Windows ou registam uma credencial.

O computador tem de estar ligado ao domínio para adicionar um utilizador de domínio no separador Adicionar utilizador da Data Security Console.

1. No painel esquerdo da ferramenta Definições do administrador, selecione **Utilizadores**.
2. Na parte superior direita da página Utilizador, clique em **Adicionar utilizador** para iniciar o processo de inscrição para um utilizador do Windows existente.
3. Quando for apresentada a caixa de diálogo Selecionar utilizadores, selecione **Tipos de objeto**.
4. Introduza um nome de objeto de utilizador na caixa de texto e clique em **Verificar nomes**.
5. Clique em **OK** quando tiver terminado.

Eliminar utilizador

1. No painel esquerdo da ferramenta Definições do administrador, selecione **Utilizadores**.
2. Para eliminar um utilizador, localize a coluna do utilizador e clique em **Remover**. (Desloque-se até ao fim da coluna do utilizador para ver a opção Remover.)

Remover todas as credenciais inscritas de um utilizador

1. Clique no mosaico **Definições do administrador** e autentifique-se com a sua palavra-passe.
2. Clique no separador **Utilizadores** e selecione o utilizador que pretende remover.
3. Clique em **Remover**. (O comando de Remoção aparece a vermelho na parte inferior das definições do utilizador).

   Uma vez removido, o utilizador não poderá iniciar sessão no computador, exceto de voltar a ser inscrito.

7

Desinstalar o instalador principal

- Cada componente tem de ser desinstalado separadamente, seguido pela desinstalação do instalador principal. Os clientes devem ser desinstalados numa **ordem específica para impedir falhas na desinstalação**.
- Sigas as instruções que constam em Extrair os Instaladores Subordinados do Instalador Principal para obter instaladores subordinados.
- Assegure-se que é utilizada a mesma versão do instalador principal (e assim como dos clientes) tanto para a desinstalação como para a instalação.
- Este capítulo direciona-o para outro capítulo que contém instruções *detalhadas* sobre como desinstalar os instaladores subordinados. Este capítulo explica **apenas** o último passo da desinstalação do instalador principal.

Desinstale os clientes pela seguinte ordem.

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

Não é necessário desinstalar o pacote de controladores.

Avance para Selecionar um método de desinstalação.

Selecione um método de desinstalação

Existem dois métodos para desinstalar o instalador principal, selecione **um** dos seguintes:

- Desinstalar a partir da opção Adicionar/remover programas
- Desinstalar a partir da Linha de Comandos

Desinstalar interativamente

1. Aceda a *Desinstalar um programa* no Painel de Controlo do Windows (na caixa de pesquisa da barra de tarefas, introduza **Painel de Controlo** e, em seguida, selecione Painel de controlo nos resultados).
2. Selecione o **Instalador Dell** e, com o botão esquerdo do rato, clique em **Alterar** para iniciar o assistente de configuração.
3. Leia o ecrã de Boas-vindas e clique em **Seguinte**.
4. Siga as indicações para desinstalar e clique em **Concluir**.
5. Reinicie o computador e inicie sessão no Windows.

   O instalador principal é desinstalado.

Desinstalar a partir da Linha de Comandos

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

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

  Reinicie o computador quando concluído.

  O instalador principal é desinstalado.

  Avance para Desinstalar utilizando os Instaladores Subordinados.

8

Desinstalar utilizando os instaladores subordinados

- A Dell recomenda a utilização do Desinstalador do Data Security para remover o Encryption Personal.
- O utilizador que efetua a desencriptação e a desinstalação necessita ter permissões de administrador a nível local ou do domínio. Ao desinstalar pela linha de comandos, são necessárias credenciais de administrador de domínio.
- Se instalou o Encryption Personal com o instalador principal, os ficheiros executáveis subordinados têm primeiro de ser extraídos do instalador principal antes da desinstalação, conforme ilustrado em Extrair os instaladores subordinados do instalador principal.
- Assegure-se que é utilizada a mesma versão dos clientes para a desinstalação e instalação.
- Se possível, programe a desencriptação para ser feita durante a noite.
- Desative o modo de suspensão para impedir a suspensão do computador caso este se encontre sem supervisão. A desencriptação não é possível num computador em suspensão.
- Encerre todos os processos e aplicações para minimizar as falhas devido a ficheiros bloqueados.

Desinstalar o Encryption

- **Antes de iniciar o processo de desinstalação**, consulte (Opcional) Criar um ficheiro de registo do Encryption Removal Agent. Este ficheiro de registo é útil para deteção e resolução de problemas numa operação de desinstalação/desencriptação. Se não pretender desencriptar ficheiros durante o processo de desinstalação, não é necessário criar um ficheiro de registo do Agente de remoção de encriptação.

  NOTA: Antes de efetuar a desinstalação, certifique-se de que todos os modelos de política estão definidos como Desativado e insira qualquer suporte de dados externo encriptado para uma desencriptação eficaz.

  Este vídeo descreve a alteração de modelos de política na Consola de gestão local.

- Após concluir a desinstalação, mas antes de reiniciar o computador, execute o WSScan para assegurar que todos os dados foram desencriptados. Consulte Utilizar o WSScan para obter instruções.
- Periodicamente, verifique o estado do Encryption Removal Agent. Se o serviço Encryption Removal Agent ainda se encontrar no painel de serviços, a desencriptação de dados ainda está a ser processada.
-

Selecione um método de desinstalação

Existem dois métodos para desinstalar o cliente Encryption, selecione **um** dos seguintes:

- Desinstalar interativamente
- Desinstalar através da Linha de Comandos

Desinstalar interativamente

1. Aceda a *Desinstalar um programa* no Painel de Controlo do Windows (na caixa de pesquisa da barra de tarefas, introduza **Painel de Controlo** e, em seguida, selecione **Painel de controlo** nos resultados).
2. Selecione **Dell Encryption XX-bit** e, com o botão esquerdo do rato, clique em **Alterar** para iniciar o assistente de configuração do Encryption Personal.
3. Leia o ecrã de Boas-vindas e clique em **Seguinte**.
4. No ecrã de Instalação do Encryption Removal Agent, selecione uma das seguintes opções:

NOTA: A segunda opção está ativada por predefinição. **Se pretender desencriptar ficheiros, certifique-se de que altera a seleção para a primeira opção**.

- Encryption Removal Agent - importar chaves de ficheiro

  Para encriptação SDE, de Utilizador ou Comum, esta opção desencripta ficheiros e desinstala o cliente Encryption. ***Esta é a seleção recomendada.***

- Não instalar o Encryption Removal Agent

  Esta opção desinstala o cliente Encryption, *mas não desencripta ficheiros*. Esta opção pode ser utilizada **apenas** para resolução de problemas, conforme indicado pelo Dell ProSupport.

  Clique em **Seguinte**.

5. Em *Ficheiro de cópia de segurança*, introduza o caminho para a unidade de rede ou a localização do suporte de dados amovível do ficheiro de cópia de segurança ou clique em **...** para procurar a localização. O formato do ficheiro é LSARecovery_[hostname].exe.

   Introduza a palavra-passe do administrador de encriptação. Esta é a palavra-passe do Assistente de configuração quando o software está instalado.

   Clique em **Seguinte**.

6. Em *Início de sessão do Dell Decryption Agent Service como*, selecione **Conta do sistema local** e clique em **Concluir**.
7. Clique em **Remover** no ecrã Remover o programa.
8. Clique em **Concluir** no ecrã Configuração concluída.
9. Reinicie o computador e inicie sessão no Windows.

A desencriptação está agora em curso.

O processo de desencriptação pode demorar várias horas, dependendo do número de unidades a ser desencriptadas e da quantidade de dados nessas unidades. Para verificar o processo de desencriptação, consulte Verificar o estado do Encryption Removal Agent.

Desinstalar através da Linha de Comandos

- As opções e parâmetros da linha de comandos são sensíveis a maiúsculas e minúsculas.
- Certifique-se de que inclui um valor que contenha um ou mais caracteres especiais, como um espaço em branco na linha de comandos, entre aspas duplas de escape. Os parâmetros da linha de comandos são sensíveis a maiúsculas e minúsculas.
- Utilize estes instaladores para desinstalar os clientes utilizando uma instalação com script, com ficheiros batch ou qualquer outra tecnologia push disponível na sua organização.
- Ficheiros de registo

  O Windows cria ficheiros de registo de desinstalação de instalador subordinado únicos para o utilizador com início de sessão em %temp%, localizado em `C:\Users\<UserName>\AppData\Local\Temp.`

  Se decidir adicionar um ficheiro de registo separado quando executar o instalador, certifique-se de que ficheiro de registo tem um nome único uma vez que os ficheiros de registo de instalador subordinado não são acrescentados. O comando .msi padrão pode ser utilizado para criar um ficheiro de registo utilizando /l `C:\<any directory>\<any log file name>.log`. A Dell não recomenda a utilização de "/l*v" (registo verboso) na desinstalação através da linha de comandos, uma vez que o nome de utilizador/palavra-passe são guardados no ficheiro de registo.

- Todos os instaladores subordinados utilizam as mesmas opções de apresentação e parâmetros .msi básicos, exceto quando indicado, para as desinstalações através da linha de comandos. As opções devem ser especificadas em primeiro lugar. A opção /v é obrigatória e necessita de um argumento. Outros parâmetros vão dentro de um argumento que é passado para a opção /v.

  As opções de apresentação podem ser especificadas no final do argumento passado para a opção /v para alcançar o comportamento esperado. Não utilize /q e /qn na mesma linha de comandos. Utilize apenas ! e - após /qb.

Opção	Significado
/v	Passa variáveis para o .msi dentro do setup.exe
/s	Modo silencioso

Opção	Significado
/x	Modo de desinstalação

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

- Uma vez extraído a partir do instalador principal, o instalador do cliente Encryption pode estar localizado em `C:\extracted\Encryption\DDPE_XXbit_setup.exe`.
- A tabela seguinte descreve os parâmetros disponíveis para a desinstalação.

Parâmetro	Seleção
CMG_DECRYPT	Propriedade para selecionar o tipo de instalação do Encryption Removal Agent 2 - Obter chaves utilizando um pacote de chaves forenses 0 – Não instalar o Encryption Removal Agent
CMGSILENTMODE	Propriedade para a desinstalação silenciosa: 1 - Silencioso - necessário ao executar com variáveis msiexec. contendo /q ou /qn 0 - Não Silencioso - apenas possível quando não existem variáveis msiexec contendo /q na sintaxe de linhas de comandos
DA_KM_PW	A palavra-passe da conta de administrador do domínio.
DA_KM_PATH	Caminho para o pacote de material da chave.

- O exemplo seguinte desinstala o cliente de 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 seguinte desinstala o cliente Encryption utilizando um pacote de chaves forenses. Copie o pacote de chaves forenses para o disco local e 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 quando concluído.

  O processo de desencriptação pode demorar várias horas, dependendo do número de unidades a ser desencriptadas e da quantidade de dados nessas unidades. Para verificar o processo de desencriptação, consulte Verificar o estado do Encryption Removal Agent.

Desinstalar o Encryption Management Agent

Selecione um método de desinstalação

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

- Desinstalar interativamente
- Desinstalar através da Linha de Comandos

Desinstalar interativamente

1. Aceda a *Desinstalar um programa* no Painel de Controlo do Windows (na caixa de pesquisa da barra de tarefas, introduza **Painel de Controlo** e, em seguida, selecione **Painel de controlo** nos resultados).
2. Selecione **Dell Encryption Management Agent** e, com o botão esquerdo do rato, clique em **Alterar** para iniciar o assistente de configuração.
3. Leia o ecrã de Boas-vindas e clique em **Seguinte**.
4. Siga as indicações para desinstalar e clique em **Concluir**.
5. Reinicie o computador e inicie sessão no Windows.

O Cliente Security Framework está desinstalado.

Desinstalar através da Linha de Comandos

- Uma vez extraído a partir do instalador principal, o instalador do Encryption Management Agent pode estar localizado em `C:\extracted\Encryption Management Agent\EMAgent_XXbit_setup.exe`.
- O seguinte exemplo desinstala o SED Management de forma silenciosa.

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

  Encerre e reinicie o computador quando concluído.

9

Desinstalador do Data Security

Desinstalar Encryption Personal

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

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

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

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

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

Clique em **Seguinte**.

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

As dependências necessárias são automaticamente selecionadas ou desmarcadas.

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

Selecione **Encryption Removal Agent – Importar chaves a partir de um ficheiro** e, em seguida, selecione **Seguinte**.

Aceda à localização das chaves de recuperação e, em seguida, introduza a frase de acesso para o ficheiro e clique em **Seguinte**.

Selecione **Remover** para iniciar a desinstalação.

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

A desinstalação e remoção estão concluídas.

10

Descrições de políticas e modelos

Dicas são exibidas quando você passa o rato sobre uma política na consola de gestão local.

Políticas

Política	Proteção agressiva para todas as unidades fixas e externas	Norma PCI	Norma contra a violação de dados	Norma HIPAA	Proteção básica para todas as unidades fixas e externas (predefinição)	Proteção básica para todas as unidades fixas	Proteção básica apenas para a unidade do sistema	Proteção básica para unidades externas	Encriptação desativada	Descrição
Políticas de armazenamento fixo										
Encriptação SDE ativada	Verdadeiro								Falso	Esta política é a "política principal" para todas as outras políticas System Data Encryption (SDE). Se o valor desta política for Falso, não ocorre qualquer encriptação SDE, independentemente de outros valores de políticas. Um valor Verdadeiro significa que todos os dados não encriptados por outras políticas de encriptação baseadas em políticas são encriptados de acordo com a política de Regras de encriptação SDE. Alterar o valor desta política requer um reinício.
Algoritmo de encriptação SDE	AES256									AES-256, AES-128
Regras de encriptação SDE										As regras de encriptação a utilizar para encriptar/não encriptar determinadas unidades, diretórios e pastas.

Política	Proteção agressiva para todas as unidades fixas e externas	Norma PCI	Norma contra a violação de dados	Norma HIPAA	Proteção básica para todas as unidades fixas e externas (predefinição)	Proteção básica para todas as unidades fixas	Proteção básica apenas para a unidade do sistema	Proteção básica para unidades externas	Encriptação desativada	Descrição
										Contacte o Dell ProSupport para obter ajuda em caso de dúvidas acerca da alteração dos valores predefinidos.
Políticas de definições gerais										
Encriptação ativada	Verdadeiro							Falso		Esta política é a "política principal" para todas as políticas das Definições Gerais. Um valor Falso, implica que não ocorre qualquer encriptação, independentemente de outros valores de políticas. Um valor Verdadeiro implica que todas as políticas de encriptação são ativadas. Alterar o valor desta política ativa um novo varrimento para encriptar/desencriptar ficheiros.
Pastas encriptadas comuns										Cadeia - máximo de 100 entradas de 500 caracteres cada (até um máximo de 2048 caracteres) Uma lista de pastas em unidades de pontos finais a encriptar ou excluir da encriptação, que pode depois ser acedida por todos os utilizadores geridos que tenham acesso ao endpoint. As letras disponíveis para as unidades são: #: Refere-se a todas as unidades #: Refere-se a todas as unidades fixas #: Refere-se a todas as unidades amovíveis

Política	Proteção agressiva para todas as unidades fixas e externas	Norma PCI	Norma contra a violação de dados	Norma HIPAA	Proteção básica para todas as unidades fixas e externas (predefinição)	Proteção básica para todas as unidades fixas	Proteção básica apenas para a unidade do sistema	Proteção básica para unidades externas	Encriptação desativada	Descrição
										Importante: ignorar a proteção do diretório pode resultar num computador impossível de iniciar e/ou exigir a reformatação das unidades. Se a mesma pasta for especificada nesta política e na política de Pastas Encriptadas do Utilizador, prevalece esta política.
Algoritmo de encriptação comum	AES256									AES-256, Rijndael 256, AES 128, Rijndael 128 Os ficheiros de paginação do sistema são encriptados utilizando AES-128.
Lista de encriptação de dados da aplicação	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									Cadeia - máximo de 100 entradas de 500 caracteres cada A Dell não recomendada a adição do ficheiro explorer.exe ou iexplorer.exe à lista ADE, pois podem ocorrer resultados imprevistos ou indesejados. No entanto, o explorer.exe é o processo utilizado para criar um novo ficheiro do Bloco de notas no ambiente de trabalho utilizando o menu de contexto. Definir a encriptação por extensão do ficheiro, em vez da utilização da lista ADE, proporciona uma cobertura mais completa. Elabore uma lista dos nomes dos processos das aplicações (sem caminhos) cujos novos ficheiros pretende encriptar, separados por quebras de linha. Não utilize caracteres universais.

Política	Proteção agressiva para todas as unidades fixas e externas	Norma PCI	Norma contra a violação de dados	Norma HIPAA	Proteção básica para todas as unidades fixas e externas (predefinição)	Proteção básica para todas as unidades fixas	Proteção básica apenas para a unidade do sistema	Proteção básica para unidades externas	Encriptação desativada	Descrição
										A Dell recomenda não listar aplicações/ferramentas de instalação que escrevam em ficheiros críticos do sistema. Se o fizer, este procedimento poderá resultar na encriptação de ficheiros do sistema importantes, que poderão impossibilitar o arranque do computador. Nomes de processo comuns: outlook.exe, winword.exe, powerpnt.exe, msaccess.exe, wordpad.exe, mspaint.exe, excel.exe Os nomes de processos do sistema e instalador codificados pelo hardware que se seguem são ignorados se forem 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 encriptação de dados da aplicação	Comum									Comum ou utilizador Escolha uma chave para indicar quem pode aceder aos ficheiros encriptados pela Lista de encriptação de dados da aplicação e onde. Comum, para que estes ficheiros estejam acessíveis a todos os utilizadores geridos no endpoint em que foram criados (o mesmo nível de acesso das Pastas encriptadas comuns) e

Política	Proteção agressiva para todas as unidades fixas e externas	Norma PCI	Norma contra a violação de dados	Norma HIPAA	Proteção básica para todas as unidades fixas e externas (predefinição)	Proteção básica para todas as unidades fixas	Proteção básica apenas para a unidade do sistema	Proteção básica para unidades externas	Encriptação desativada	Descrição
										sejam encriptados com o algoritmo de encriptação Comum. Utilizador, para que estes ficheiros estejam acessíveis apenas para o utilizador que os criou e apenas no endpoint em que foram criados (o mesmo nível de acesso das Pastas encriptadas do utilizador) e sejam encriptados com o algoritmo de encriptação do Utilizador. Alterações a esta política não afetam os ficheiros já encriptados devido a esta política.
Encriptar pastas pessoais do Outlook	Verdadeiro							Falso		Verdadeiro encripta pastas pessoais do Outlook.
Encriptar ficheiros temporários	Verdadeiro							Falso		O valor Verdadeiro encripta os caminhos listados nas variáveis do ambiente TEMP e TMP com a Chave de encriptação de dados do utilizador.
Encriptar ficheiros temporários da Internet	Verdadeiro	Falso								O valor Verdadeiro encripta o caminho listado na variável do ambiente CSIDL_INTERNET_CACHE com a Chave de encriptação de dados do utilizador. Para reduzir o tempo de varrimento da encriptação, o cliente limpa o conteúdo de CSIDL_INTERNET_CACHE para a encriptação inicial, bem como as atualizações a esta política.

Política	Proteção agressiva para todas as unidades fixas e externas	Norma PCI	Norma contra a violação de dados	Norma HIPAA	Proteção básica para todas as unidades fixas e externas (predefinição)	Proteção básica para todas as unidades fixas	Proteção básica apenas para a unidade do sistema	Proteção básica para unidades externas	Encriptação desativada	Descrição
										Esta política é aplicável ao utilizar apenas o Microsoft Internet Explorer.
Encriptar documentos do perfil de utilizador	Verdadeiro								Falso	Verdadeiro encripta: · O perfil de utilizadores (`C:\Users\jsmith`) com a Chave de encriptação de dados do utilizador · \Users\Public com a Chave de encriptação comum
Encriptar o ficheiro de paginação do Windows	Verdadeiro								Falso	Verdadeiro encripta o ficheiro de paginação do Windows. Uma alteração a esta política exige um reinício.
Serviços geridos										Cadeia - máximo de 100 entradas de 500 caracteres cada (até um máximo de 2048 caracteres) Quando um serviço é gerido por esta política, o serviço apenas é iniciado depois de o utilizador ter iniciado sessão e o cliente ter sido desbloqueado. Esta política também garante que o serviço gerido por esta política é interrompido antes de o cliente ser bloqueado durante o encerramento. Esta política também pode evitar um encerramento do utilizador se um serviço não estiver a responder. A sintaxe consiste num nome de serviço por linha. São suportados espaços no nome do serviço. Não são suportados caracteres universais.

Política	Proteção agressiva para todas as unidades fixas e externas	Norma PCI	Norma contra a violação de dados	Norma HIPAA	Proteção básica para todas as unidades fixas e externas (predefinição)	Proteção básica para todas as unidades fixas	Proteção básica apenas para a unidade do sistema	Proteção básica para unidades externas	Encriptação desativada	Descrição
										Os serviços geridos não são iniciados se um utilizador não gerido iniciar sessão.
Limpeza de pós-encriptação segura	Substituição de três passos	Substituição de passo único							Sem substituição	Sem substituição, substituição de passo único, substituição de três passos, substituição de sete passos Após a encriptação das pastas especificadas por outras políticas nesta categoria, esta política determina o que acontece aos resíduos não encriptados dos ficheiros originais: · Sem substituição elimina-os. Esta valor resulta no processamento de encriptação mais rápido. · Substituição de passo único substitui-os por dados aleatórios. · Substituição de três passos substitui por um padrão normalizado de 1s e 0s, em seguida, pelo seu complemento e, depois, por dados aleatórios. · Substituição de sete passos substitui por um padrão normalizado de 1s e 0s, em seguida, pelo seu complemento e, depois, por dados aleatórios cinco vezes. Este valor torna mais difícil a recuperação dos ficheiros originais a partir da memória, e resulta no processamento de encriptação mais seguro.
Proteger o ficheiro de	Verdadeiro					Falso		Verdadeiro	Falso	Quando ativado, o ficheiro de hibernação é encriptado apenas quando

Política	Proteção agressiva para todas as unidades fixas e externas	Norma PCI	Norma contra a violação de dados	Norma HIPAA	Proteção básica para todas as unidades fixas e externas (predefinição)	Proteção básica para todas as unidades fixas	Proteção básica apenas para a unidade do sistema	Proteção básica para unidades externas	Encriptação desativada	Descrição
hibernação do Windows										o computador entra no estado de hibernação. O cliente desativa a proteção quando o computador sai da hibernação, fornecendo proteção sem afetar os utilizadores ou as aplicações durante a utilização do computador.
Impedir hibernação não segura	Verdadeiro					Falso		Verdadeiro	Falso	Quando ativado, o cliente não permite a hibernação do computador se o cliente não conseguir encriptar os dados de hibernação.
Prioridade da análise da estação de trabalho	Elevada	Normal								A mais alta, Alta, Normal, Baixa, A mais baixa Especifica a prioridade relativa do Windows da análise da pasta encriptada.
Pastas encriptadas do utilizador										Cadeia - máximo de 100 entradas de 500 caracteres cada (até um máximo de 2048 caracteres) Uma lista de pastas na unidade de disco rígido do endpoint a ser encriptada com a chave de encriptação de dados do Utilizador ou a ser excluída da encriptação. Esta política aplica-se a todas as unidades classificadas pelo Windows como unidades de disco rígido. Não pode utilizar esta política para encriptar unidades ou suportes de dados amovíveis cujos tipos sejam apresentados como Disco amovível; em alternativa, utilize Suporte de dados externo de encriptação EMS.

Política	Proteção agressiva para todas as unidades fixas e externas	Norma PCI	Norma contra a violação de dados	Norma HIPAA	Proteção básica para todas as unidades fixas e externas (predefinição)	Proteção básica para todas as unidades fixas	Proteção básica apenas para a unidade do sistema	Proteção básica para unidades externas	Encriptação desativada	Descrição
Algoritmo de encriptação do utilizador	AES256									AES 256, Rijndael 256, AES 128, Rijndael 128 Algoritmo de encriptação utilizado para encriptar os dados ao nível do utilizador individual. Pode especificar valores diferentes para utilizadores diferentes do mesmo endpoint.
Chave de User Data Encryption	Utilizador	Comum		Utilizador	Comum				Utilizador	Comum ou utilizador Escolha uma chave para indicar quem pode aceder aos ficheiros encriptados pelas seguintes políticas e onde: · Pastas encriptadas do utilizador · Encriptar pastas pessoais do Outlook · Encriptar ficheiros temporários (\Documents and Settings\username\Local Settings\Temp only) · Encriptar ficheiros temporários da Internet · Encriptar documentos do perfil de utilizador Selecione: · Comum para que Ficheiros/Pastas encriptados pelo utilizador estejam acessíveis a todos os utilizadores geridos no endpoint em que foram criados (o mesmo nível de acesso que as Pastas encriptadas comuns) e encriptados com o algoritmo de encriptação Comum. · Utilizador, para que estes ficheiros estejam acessíveis apenas para o

Política	Proteção agressiva para todas as unidades fixas e externas	Norma PCI	Norma contra a violação de dados	Norma HIPAA	Proteção básica para todas as unidades fixas e externas (predefinição)	Proteção básica para todas as unidades fixas	Proteção básica apenas para a unidade do sistema	Proteção básica para unidades externas	Encriptação desativada	Descrição
										utilizador que os criou e apenas no endpoint em que foram criados (o mesmo nível de acesso das Pastas encriptadas do utilizador) e sejam encriptados com o algoritmo de encriptação do Utilizador. Se optar por incorporar uma política de encriptação para encriptar partições inteiras do disco, recomendamos que utilize a política de encriptação SDE predefinida em vez de Comum ou Utilizador. Desta forma, garante que quaisquer ficheiros do sistema operativo que sejam encriptados permanecem acessíveis durante estados em que o utilizador gerido não tem a sessão iniciada.
Hardware Crypto Accelerator (suportado apenas por clientes Encryption v8.3 a v8.9.1)										
Hardware Crypto Accelerator (HCA)	Falso									Esta política é a "política principal" para todas as outras políticas de Hardware Crypto Accelerator (HCA). Se o valor desta política for Falso, não ocorre qualquer encriptação do HCA, independentemente de outros valores de políticas. As políticas HCA apenas podem ser utilizadas em computadores equipados com Hardware Crypto Accelerator.
Volumes visados para encriptação	Todos os volumes fixos									Todos os volumes fixos ou Apenas o volume do sistema.

Política	Proteção agressiva para todas as unidades fixas e externas	Norma PCI	Norma contra a violação de dados	Norma HIPAA	Proteção básica para todas as unidades fixas e externas (predefinição)	Proteção básica para todas as unidades fixas	Proteção básica apenas para a unidade do sistema	Proteção básica para unidades externas	Encriptação desativada	Descrição
										Especifique que volume(s) se destina(m) a encriptação.
Metadados forenses disponíveis na unidade encriptada do HCA	Falso									Verdadeiro ou Falso Quando o valor é Verdadeiro, os metadados forenses são incluídos na unidade para facilitar as tarefas forenses. Metadados incluídos: ● ID da Máquina (MCID) da máquina atual ● ID do dispositivo (DCID/SCID) de instalação do Encryption client atual. Quando o valor é Falso, os metadados forenses não são incluídos na unidade. Mudar de Falso para Verdadeiro aciona um novo varrimento com base nas políticas para adicionar dados forenses.
Permitir a aprovação do utilizador da encriptação da unidade secundária	Falso									Verdadeiro permite aos utilizadores decidir se são encriptadas unidades adicionais.
Algoritmo de encriptação	AES256									AES-256 ou AES-128
Políticas de controlo das portas										
Sistema de controlo das portas	Desativado									Ativar ou desativar todas as políticas do sistema de controlo de portas. Se esta política for definida

Política	Proteção agressiva para todas as unidades fixas e externas	Norma PCI	Norma contra a violação de dados	Norma HIPAA	Proteção básica para todas as unidades fixas e externas (predefinição)	Proteção básica para todas as unidades fixas	Proteção básica apenas para a unidade do sistema	Proteção básica para unidades externas	Encriptação desativada	Descrição
										como Desativar, não são aplicadas quaisquer políticas do Sistema de controlo de portas, independentemente dos valores de outras políticas do Sistema de controlo de portas. As políticas de PCS requerem um reinício para que a política tenha efeito. **NOTA:** Se bloquear as operações do dispositivo os nomes do dispositivo serão apresentados em branco.
Porta: ranhura para Express Card	Ativada									Ativar, Desativar ou Ignorar as portas expostas através da ranhura Express Card.
Porta: eSATA	Ativada									Ativar, Desativar ou Ignorar o acesso da porta para portas SATA externas.
Porta: PCMCIA	Ativada									Ativar, Desativar ou Ignorar o acesso da porta para portas PCMCIA.
Porta: Firewire (1394)	Ativada									Ativar, Desativar ou Ignorar o acesso da porta a portas Firewire externas (1394).
Porta: SD	Ativada									Ativar, Desativar ou Ignorar o acesso a portas de cartões SD.
Subclasse de armazenamento: Controlo da unidade externa	Bloqueado	Só de leitura			Acesso ilimitado			Só de leitura	Acesso ilimitado	Classe de SUBORDINADOS: armazenamento. Classe: o armazenamento tem de estar Ativado para usar esta política. Esta política tem interações com PCS.

Política	Proteção agressiva para todas as unidades fixas e externas	Norma PCI	Norma contra a violação de dados	Norma HIPAA	Proteção básica para todas as unidades fixas e externas (predefinição)	Proteção básica para todas as unidades fixas	Proteção básica apenas para a unidade do sistema	Proteção básica para unidades externas	Encriptação desativada	Descrição
										Consulte Interações de PCS e Encryption External Media Acesso total: a Porta da Unidade Externa não tem restrições de dados de leitura/gravação aplicadas Só de leitura: permite a capacidade de leitura. A escrita de dados está desativada. Bloqueada: a porta é bloqueada para capacidade de leitura/gravação Esta política baseia-se no endpoint e não pode ser substituída pela política do utilizador.
Porta: Dispositivo de Transferência de Memória (MTD)	Ativada									Ativar, Desativar ou Ignorar o acesso a portas do Dispositivo de transferência de memória (MTD).
Classe: armazenamento	Ativada									PRINCIPAL para as 3 políticas seguintes. Defina esta política como Ativa para utilizar as 3 políticas de Armazenamento de subclasse seguintes. A desativação desta política para Desativada desativa as 3 políticas de Armazenamento de subclasse - independentemente do seu valor.
Subclasse de armazenamento: Controlo da	Só de leitura	Apenas UDF				Acesso ilimitado		Apenas UDF	Acesso ilimitado	Classe de SUBORDINADOS: armazenamento. Classe: o armazenamento tem de estar Ativado para usar esta política.

Política	Proteção agressiva para todas as unidades fixas e externas	Norma PCI	Norma contra a violação de dados	Norma HIPAA	Proteção básica para todas as unidades fixas e externas (predefinição)	Proteção básica para todas as unidades fixas	Proteção básica apenas para a unidade do sistema	Proteção básica para unidades externas	Encriptação desativada	Descrição
unidade ótica										Acesso total: a Porta da Unidade Ótica não tem restrições de dados de leitura/gravação aplicadas Apenas UDF: bloqueia todas as gravações de dados que não estejam no formato UDF (gravação de CD/DVD e ISO). A leitura de dados está ativada. Só de leitura: permite a capacidade de leitura. A escrita de dados está desativada. Bloqueada: a porta é bloqueada para capacidade de leitura/gravação Esta política baseia-se no endpoint e não pode ser substituída pela política do utilizador. Universal Disk Format (UDF) é uma implementação da especificação conhecida como ISO/IEC 13346 e ECMA-167 e consiste num sistema de ficheiros independente do fornecedor aberto para o armazenamento de dados informáticos numa vasta gama de suportes de dados. Esta política tem interações com PCS. Consulte Interações de PCS e Encryption External Media
Subclasse de armazenamento: Controlo da Unidade	Bloqueado	Só de leitura				Acesso ilimitado		Só de leitura	Acesso ilimitado	Classe de SUBORDINADOS: armazenamento. Classe: o armazenamento tem de estar Ativado para usar esta política.

Política	Proteção agressiva para todas as unidades fixas e externas	Norma PCI	Norma contra a violação de dados	Norma HIPAA	Proteção básica para todas as unidades fixas e externas (predefinição)	Proteção básica para todas as unidades fixas	Proteção básica apenas para a unidade do sistema	Proteção básica para unidades externas	Encriptação desativada	Descrição
de Disquete										Acesso total: a Porta da Unidade de Disquete não tem restrições de dados de leitura/gravação aplicadas Só de leitura: permite a capacidade de leitura. A escrita de dados está desativada. Bloqueada: a porta é bloqueada para capacidade de leitura/gravação Esta política baseia-se no endpoint e não pode ser substituída pela política do utilizador.
Classe: Dispositivos Portáteis do Windows (WPD)	Ativada									PRINCIPAL para a política seguinte. Ative esta política para ativar o dispositivo portátil de subclasse do Windows (WPD): política de armazenamento. Desative esta política para desativar o dispositivo portátil de subclasse do Windows (WPD): política de armazenamento - independentemente do seu valor. Controlar o acesso a todos os Dispositivos portáteis Windows.
Dispositivos Portáteis de Subclasse do Windows (WPD): armazenamento	Ativada									Classe de SUBORDINADOS: Dispositivos Portáteis do Windows (WPD) Classe: os Dispositivos Portáteis do Windows (WPD) têm de estar Ativados para usar esta política. Acesso total: a porta não tem restrições de dados de leitura/gravação aplicadas.

Política	Proteção agressiva para todas as unidades fixas e externas	Norma PCI	Norma contra a violação de dados	Norma HIPAA	Proteção básica para todas as unidades fixas e externas (predefinição)	Proteção básica para todas as unidades fixas	Proteção básica apenas para a unidade do sistema	Proteção básica para unidades externas	Encriptação desativada	Descrição
										Só de leitura: permite a capacidade de leitura. A escrita de dados está desativada. Bloqueada: a porta é bloqueada para capacidade de leitura/gravação.
Classe: Dispositivo de Interface Humana (HID)	Ativada									Controlar o acesso a todos os Dispositivos de interface humana (teclados, ratos). **Nota:** o bloqueio no nível da porta USB e o bloqueio no nível da classe HID apenas serão processados se for possível identificar o tipo de estrutura do computador como um fator de forma portátil/ notebook. A identificação da estrutura depende do BIOS do computador.
Classe: outra	Ativada									Controlar o acesso a todos os dispositivos não abrangidos por outras Classes.
Políticas de dispositivos amovíveis										
EMS: Encriptar suporte multimédia externo	Verdadeiro					Falso	Verdadeiro	Falso		Esta política é a "política principal" para todas as políticas de Armazenamento amovível. Um valor Falso implica que não ocorre qualquer encriptação das unidades de armazenamento amovíveis, independentemente de outros valores de políticas. Um valor Verdadeiro implica que todas as políticas de armazenamento amovível estão ativadas.

Política	Proteção agressiva para todas as unidades fixas e externas	Norma PCI	Norma contra a violação de dados	Norma HIPAA	Proteção básica para todas as unidades fixas e externas (predefinição)	Proteção básica para todas as unidades fixas	Proteção básica apenas para a unidade do sistema	Proteção básica para unidades externas	Encriptação desativada	Descrição
										Esta política tem interações com PCS. Consulte Interações de PCS e Encryption External Media
EMS: Excluir encriptação de CD/DVD	Falso								Verdadeiro	Falso encripta dispositivos de CD/DVD. Esta política tem interações com PCS. Consulte Interações de PCS e Encryption External Media
EMS: Acesso a suportes multimédia desprotegidos	Bloquear		Só de leitura			Acesso ilimitado		Só de leitura	Acesso ilimitado	Bloquear, Só de leitura, Acesso ilimitado Esta política tem interações com PCS. Consulte Interações de PCS e Encryption External Media Quando esta política é definida como Bloquear acesso, não tem acesso ao armazenamento amovível, a menos que esteja encriptado. Escolher Só de leitura ou Acesso ilimitado permite decidir o armazenamento amovível a encriptar. Se optar por não encriptar o armazenamento amovível e esta política estiver definida como Acesso ilimitado, tem acesso de leitura/escrita ilimitado ao armazenamento amovível. Se optar por não encriptar o armazenamento amovível e esta política for configurada para Só de leitura, não é possível ler nem eliminar os ficheiros existentes no armazenamento amovível não encriptado, mas o

Política	Proteção agressiva para todas as unidades fixas e externas	Norma PCI	Norma contra a violação de dados	Norma HIPAA	Proteção básica para todas as unidades fixas e externas (predefinição)	Proteção básica para todas as unidades fixas	Proteção básica apenas para a unidade do sistema	Proteção básica para unidades externas	Encriptação desativada	Descrição
										cliente não irá permitir que nenhum ficheiro seja editado ou adicionado ao armazenamento amovível, a não ser que esteja encriptado.
EMS: Algoritmo de encriptação	AES256									AES-256, Rijndael 256, AES-128, Rijndael 128
EMS: Analisar suporte multimédia externo	Verdadeiro	Falso								O valor Verdadeiro permite que o suporte de dados amovível seja analisado sempre que é inserido. Quando esta política é definida como Falsa e a política Suporte de dados externo de encriptação EMS é definida como Verdadeira, apenas os ficheiros novos e alterados são encriptados. Ocorre uma análise a cada inserção de modo a que possam ser detetados quaisquer ficheiros adicionados ao suporte de dados amovível sem autenticação. É possível adicionar ficheiros ao suporte de dados se a autenticação for recusada, mas não é possível aceder aos dados encriptados. Neste caso, os ficheiros adicionados não são encriptados, pelo que da próxima vez que o suporte de dados for autenticado (para trabalhar com dados encriptados), quaisquer ficheiros que tenham sido adicionados são verificados e encriptados.
EMS: Aceder	Verdadeiro									Verdadeiro permite ao utilizador aceder a

Política	Proteção agressiva para todas as unidades fixas e externas	Norma PCI	Norma contra a violação de dados	Norma HIPAA	Proteção básica para todas as unidades fixas e externas (predefinição)	Proteção básica para todas as unidades fixas	Proteção básica apenas para a unidade do sistema	Proteção básica para unidades externas	Encriptação desativada	Descrição
dados encriptados num dispositivo desprotegido										dados encriptados no armazenamento amovível quer o endpoint esteja encriptado ou não.
Lista branca de dispositivo EMS										Esta política permite a especificação de dispositivos de suportes de dados amovíveis a excluir da encriptação. Quaisquer dispositivos de suporte de dados amovíveis que não estejam nesta lista são protegidos. Máximo de 150 dispositivos com um máximo de 500 caracteres permitidos por PNPDeviceID. Máximo de 2048 caracteres no total permitido. Para encontrar a PNPDeviceID para armazenamento amovível: 1. Insira o dispositivo de armazenamento amovível num computador encriptado. 2. Abra o EMSService.log em C:\Programdata\Dell\Dell Data Protection\Encryption\EMS. 3. Procure a "PNPDeviceID=" Por exemplo: 14.03.18 18:50:06.834 [I] [Volume "F:\"] PnPDeviceID = USBSTOR\DISK&VEN_SEAGATE&PROD_USB&REV_0409\2HC015KJ&0

Política	Proteção agressiva para todas as unidades fixas e externas	Norma PCI	Norma contra a violação de dados	Norma HIPAA	Proteção básica para todas as unidades fixas e externas (predefinição)	Proteção básica para todas as unidades fixas	Proteção básica apenas para a unidade do sistema	Proteção básica para unidades externas	Encriptação desativada	Descrição
										Especifique o seguinte na política de lista branca de dispositivo EMS: VEN=Vendor (Por exemplo: USBSTOR\DISK&VEN_SEAGATE) PROD=Product/Model Name (Por exemplo: &PROD_USB); também exclui da proteção do EMS todos os controladores USB da Seagate; um valor VEN (Por exemplo: USBSTOR\DISK&VEN_SEAGATE) tem de preceder este valor REV=Firmware Revision (Por exemplo: &REV_0409); também exclui o modelo específico em uso; os valores VEN e PROD têm de preceder este valor O Número de série (Por exemplo: \2HC015KJ&0); apenas exclui este dispositivo; valores VEN, PROD, e REV têm de preceder este valor Delimitadores permitidos: separadores, vírgulas, ponto e vírgula, caráter hexadecimal 0x1E (Caráter de separação de registo)
EMS: caracteres alfa necessários na palavra-passe	Verdadeiro									Verdadeiro requer uma ou mais letras na palavra-passe.
EMS: maiúsculas e minúscula	Verdadeiro	Falso								Verdadeiro requer, pelo menos, uma letra maiúscula e uma letra

Política	Proteção agressiva para todas as unidades fixas e externas	Norma PCI	Norma contra a violação de dados	Norma HIPAA	Proteção básica para todas as unidades fixas e externas (predefinição)	Proteção básica para todas as unidades fixas	Proteção básica apenas para a unidade do sistema	Proteção básica para unidades externas	Encriptação desativada	Descrição
s necessárias na palavra-passe										minúscula na palavra-passe.
Número de caracteres EMS necessário na palavra-passe	8					6		8		1-40 caracteres Número de caracteres mínimo obrigatório na palavra-passe.
EMS: caracteres numéricos necessários na palavra-passe	Verdadeiro	Falso								Verdadeiro requer um ou mais caracteres numéricos na palavra-passe.
EMS: tentativas de palavra-passe permitidas	2	3				4		3		1-10 O número de vezes que o utilizador pode tentar introduzir a palavra-passe correta.
EMS: caracteres especiais necessários na palavra-passe	Verdadeiro	Falso							Verdadeiro	Verdadeiro requer um ou mais caracteres especiais na palavra-passe.
EMS: tempo de espera	30									0-5000 segundos Número de segundos que um utilizador deve aguardar entre a primeira e a segunda ronda de tentativas de introdução do código de acesso.

Política	Proteção agressiva para todas as unidades fixas e externas	Norma PCI	Norma contra a violação de dados	Norma HIPAA	Proteção básica para todas as unidades fixas e externas (predefinição)	Proteção básica para todas as unidades fixas	Proteção básica apenas para a unidade do sistema	Proteção básica para unidades externas	Encriptação desativada	Descrição
EMS : Incremento do tempo de espera	30	20				10	30	10		0-5000 segundos Tempo incremental a adicionar ao tempo de espera anterior após cada ronda sem êxito de tentativas de introdução do código de acesso.
EMS: regras de encriptação										As regras de encriptação para encriptar/não encriptar determinadas unidades, diretórios e pastas. É permitido um total de 2048 caracteres. Os carateres de Espaço e Enter utilizados para adicionar linhas entre as filas contam como carateres utilizados. Quaisquer regras que excedam o limite de 2048 são ignoradas. Os dispositivos de armazenamento que incorporem ligações multi-interface, tais como Firewire, USB, eSATA, etc., poderão exigir a utilização do Encryption External Media e das regras de encriptação para a encriptação do dispositivo. Isto é necessário devido às diferenças na forma como o sistema operativo Windows trata os dispositivos de armazenamento com base no tipo de interface. Consulte Como encriptar um iPod com o Encryption External Media.
EMS: Bloquear o acesso a suporte	Verdadeiro								Falso	Bloqueia o acesso a qualquer suporte de dados amovível com menos de 55 MB e, por conseguinte,

Política	Proteção agressiva para todas as unidades fixas e externas	Norma PCI	Norma contra a violação de dados	Norma HIPAA	Proteção básica para todas as unidades fixas e externas (predefinição)	Proteção básica para todas as unidades fixas	Proteção básica apenas para a unidade do sistema	Proteção básica para unidades externas	Encriptação desativada	Descrição
multimédia não protegível										tem uma capacidade de armazenamento insuficiente para receber Encryption External Media (tal como uma disquete de 1,44 MB). O acesso ilimitado é bloqueado se a opção EMS e esta política tiverem ambas o valor Verdadeiro. Se o suporte de dados externo de encriptação EMS tiver o valor Verdadeiro, mas esta política tiver o valor Falso, é possível ler os dados a partir do suporte de dados não encriptável, mas o acesso de escrita ao suporte dados é bloqueado. Se o suporte de dados externo de encriptação EMS tiver o valor falso, esta política não tem qualquer efeito e o acesso ao suporte de dados não encriptável não sofre qualquer impacto.
Políticas de controlo de experiência do utilizador										
Forçar reinício nas atualizações	Verdadeiro								Falso	Definir o valor para Verdadeiro faz com que o computador reinicie imediatamente para permitir o processamento de encriptação ou atualizações relativamente à política baseada no dispositivo, como a System Data Encryption (SDE).
Duração do atraso de cada reinício	+5	10				20		15		O número de minutos de atraso quando o utilizador opta por atrasar o reinício para a política baseada no dispositivo.

Política	Proteção agressiva para todas as unidades fixas e externas	Norma PCI	Norma contra a violação de dados	Norma HIPAA	Proteção básica para todas as unidades fixas e externas (predefinição)	Proteção básica para todas as unidades fixas	Proteção básica apenas para a unidade do sistema	Proteção básica para unidades externas	Encriptação desativada	Descrição
Número de atrasos de reinício permitido	1					+5		3		O número de vezes que o utilizador pode atrasar o reinício para a política baseada no dispositivo.
Suprimir notificação de contenção de ficheiro	Falso									Esta política controla se os utilizadores veem janelas de pop-up de notificação se uma aplicação tentar aceder a um ficheiro enquanto o cliente estiver a processá-lo.
Apresentar controlo local de processamento de encriptação	Falso		Verdadeiro					Falso		Definir o valor para Verdadeiro permite que o utilizador veja uma opção do menu no ícone da área de notificação que lhe permite interromper/retomar a encriptação/desencriptação (dependendo do que é que o Encryption está a fazer no momento). Permitir que um utilizador interrompa a encriptação poderá permitir ao utilizador impedir que o Encryption client encripte ou desencripte totalmente os dados conforme estipulado pela política.
Permitir o processamento da encriptação apenas quando o ecrã estiver bloqueado	Falso		Opcional do utilizador					Falso		Verdadeiro, Falso, Opcional do utilizador Quando o valor for Verdadeiro, não ocorre a encriptação ou desencriptação de dados enquanto o utilizador estiver a trabalhar ativamente. O cliente apenas processa os dados quando o ecrã está bloqueado. A função Opcional do utilizador adiciona uma opção ao ícone da área de notificação permitindo

Política	Proteção agressiva para todas as unidades fixas e externas	Norma PCI	Norma contra a violação de dados	Norma HIPAA	Proteção básica para todas as unidades fixas e externas (predefinição)	Proteção básica para todas as unidades fixas	Proteção básica apenas para a unidade do sistema	Proteção básica para unidades externas	Encriptação desativada	Descrição
										ao utilizador ativar ou desativar esta função. Quando o valor é Falso, o processamento da encriptação ocorre a qualquer momento, mesmo enquanto o utilizador estiver a trabalhar. Ativar esta opção aumenta significativamente o tempo necessário para concluir a encriptação ou desencriptação.

Descrições de modelos

Proteção agressiva para todas as unidades fixas e externas

O modelo da política destina-se a organizações cujo objetivo principal é implementar um forte sistema de segurança e evitar riscos em toda a empresa. É mais aconselhável quando a segurança é significativamente mais importante do que a usabilidade e a necessidade de excepções de política menos seguras para utilizadores, grupos ou dispositivos específicos é mínima.

O modelo de política:

- é uma configuração altamente restrita, fornecendo maior proteção.
- fornece proteção para a unidade do sistema e todas as unidades fixas.
- encripta todos os dados em dispositivos de suporte de dados amovível e impede a utilização de dispositivos de suporte de dados amovível não encriptados.
- fornece controlo de unidades ópticas apenas de leitura.

Cumprimos as normas PCI

O padrão PCI de segurança de dados (PCI DSS - Payment Card Industry Data Security Standard) é uma norma de segurança multifacetada que inclui requisitos para diretrizes, procedimentos e gestão da segurança, arquitetura de redes, design de software e outras medidas de proteção vitais. A norma abrangente destina-se a definir diretrizes para as organizações protegerem proativamente os dados das contas dos clientes.

O modelo de política:

- fornece proteção para a unidade do sistema e todas as unidades fixas.
- pede aos utilizadores para encriptarem dispositivos de suporte de dados amovível.
- permite gravar apenas CD/DVD UDF. A configuração do controlo das portas permite o acesso para leitura a todas as unidades ópticas.

Cumprimos as normas contra a violação de dados

O decreto-lei americano Sarbanes-Oxley Act exige controlos adequados para informação financeira. Uma vez que muita desta informação reside em formato eletrónico, a encriptação é um ponto de controlo essencial quando estes dados são guardados ou transferidos. As diretrizes do decreto-lei Gramm-Leach-Bliley Act (GLB - também conhecido como Financial Services Modernization Act) não exigem encriptação. Contudo, o Conselho Federal de Análise de Instituições Financeiras (Federal Financial Institutions Examination Council - FFIEC) recomenda que "as instituições financeiras utilizem encriptação para reduzir o risco de divulgação ou alteração de informações confidenciais em armazenamento e em trânsito". O Projeto de Lei do Senado da Califórnia 1386 (Lei de Notificação de Violação de Segurança de Base de Dados do Estado da Califórnia) tem como objetivo proteger os moradores do estado da Califórnia contra roubo de identidade exigindo que as organizações que sofreram violações de segurança computacional notifiquem todos os indivíduos afetados. A única forma que uma organização tem de evitar as notificações aos seus clientes é provando que toda a informação pessoal estava encriptada antes da violação da segurança.

O modelo de política:

- fornece proteção para a unidade do sistema e todas as unidades fixas.
- pede aos utilizadores para encriptarem dispositivos de suporte de dados amovível.
- permite gravar apenas CD/DVD UDF. A configuração do controlo das portas permite o acesso para leitura a todas as unidades ópticas.

Cumprimos as normas do HIPAA

O decreto-lei americano Health Insurance Portability and Accountability Act (HIPAA) exige que as organizações de cuidados de saúde implementem várias salvaguardas técnicas para protegerem a confidencialidade e integridade de toda a informação de saúde individualmente identificável.

O modelo de política:

- fornece proteção para a unidade do sistema e todas as unidades fixas.
- pede aos utilizadores para encriptarem dispositivos de suporte de dados amovível.
- permite gravar apenas CD/DVD UDF. A configuração do controlo das portas permite o acesso para leitura a todas as unidades ópticas.

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

Este modelo de política fornece a configuração recomendada, que proporciona um elevado nível de proteção sem afetar significativamente a usabilidade do sistema.

O modelo de política:

- fornece proteção para a unidade do sistema e todas as unidades fixas.
- pede aos utilizadores para encriptarem dispositivos de suporte de dados amovível.
- permite gravar apenas CD/DVD UDF. A configuração do controlo das portas permite o acesso para leitura a todas as unidades ópticas.

Proteção básica para todas as unidades fixas

O modelo de política:

- fornece proteção para a unidade do sistema e todas as unidades fixas.
- permite gravar CD/DVD em qualquer formato compatível. A configuração do controlo das portas permite o acesso para leitura a todas as unidades ópticas.

  Este modelo de política não:

- fornece encriptação para dispositivos de suporte de dados amovível.

Proteção básica apenas para a unidade do sistema

O modelo de política:

- fornece proteção para a unidade do sistema, normalmente a unidade C:, onde o sistema operativo é carregado.
- permite gravar CD/DVD em qualquer formato compatível. A configuração do controlo das portas permite o acesso para leitura a todas as unidades ópticas.

  Este modelo de política não:

- fornece encriptação para dispositivos de suporte de dados amovível.

Proteção básica para unidades externas

O modelo de política:

- fornece proteção para dispositivos de suporte de dados amovível.
- permite gravar apenas CD/DVD UDF. A configuração do controlo das portas permite o acesso para leitura a todas as unidades ópticas.

  Este modelo de política não:

- fornece proteção para a unidade do sistema (normalmente a unidade C:, onde o sistema operativo é carregado) ou outras unidades fixas.

Encriptação desativada

Este modelo de política não fornece proteção de encriptação. Quando usar este modelo, implemente medidas adicionais para salvaguardar dispositivos contra a perda e roubo de dados.

Este modelo é útil para organizações que preferem começar sem qualquer encriptação ativa para transitar para a segurança. À medida que a organização se sente mais confortável com a sua implementação, a encriptação pode ser lentamente ativada, ajustando políticas individuais ou aplicando modelos mais fortes em toda a organização (ou partes da mesma).

11

Extrair os instaladores subordinados

- Para instalar cada cliente individualmente, extraia os ficheiros executáveis subordinados do instalador.
- Se o instalador principal foi utilizado para instalar, os clientes devem ser desinstalados individualmente. Utilize este processo para extrair os clientes do instalador principal para que possam ser utilizados para a desinstalação.

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

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

   O caminho de extração não pode exceder os 63 caracteres.

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

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

Avance para a Resolução de problemas.

12

Deteção e Resolução de Problemas

Atualização utilizando as Atualizações de Funcionalidades do Windows 10 ou Windows 11

Para atualizar o Windows 10 ou Windows 11 utilizando as Atualizações de Funcionalidades, siga as instruções apresentadas no artigo 125419 da BDC.

Resolução de problemas do Dell Encryption

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

- Antes de iniciar o processo de desinstalação, é possível criar, de forma opcional, um ficheiro de registo do Agente de remoção de encriptação. Este ficheiro de registo é útil para resolução de problemas numa operação de desinstalação/desencriptação. Se não pretender desencriptar ficheiros durante o processo de desinstalação, não é necessário criar este ficheiro de registo.
- O ficheiro de registo do Encryption Removal Agent apenas é criado após a execução do serviço Encryption Removal Agent, que ocorre somente quando o computador é reiniciado. Quando o cliente for desinstalado com êxito e o computador for totalmente desencriptado, o ficheiro de registo é eliminado definitivamente.
- O caminho do ficheiro de registo é `C:\ProgramData\Dell\Dell Data Protection\Encryption`.
- Crie a seguinte entrada de registo no computador destinado à desencriptação.

  [HKLM\Software\Credant\DecryptionAgent]

  "LogVerbosity"=DWORD:2

  0: sem registos

  1: regista os erros que impedem a execução do serviço

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

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

  5: regista as informações de depuração

Encontrar versão do TSS

- O TSS é um componente que interage com o TPM. Para encontrar a versão do TSS, aceda a (localização predefinida) `C:\Program Files\Dell\Dell Data Protection\Drivers\TSS\bin > tcsd_win32.exe`. Clique com o botão direito do rato no ficheiro e selecione **Propriedades**. Verifique a versão do ficheiro no separador **Detalhes**.

Interações de PCS e Encryption External Media

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

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

Para encriptar os dados gravados em CD/DVD

- Defina a encriptação de suportes de dados do Windows = Ligado.
- Defina EMS: Excluir encriptação de CD/DVD = não selecionado.
- Defina a Subclasse de armazenamento: Controlo da unidade ótica = Apenas UDF.

Utilizar o WSScan

- O WSScan permite-lhe assegurar que todos os dados são desencriptados quando desinstalar o Encryption, para além de visualizar o estado de encriptação e identificar ficheiros desencriptados que devem ser encriptados.
- São necessários privilégios de administrador para executar este utilitário.

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

Execute a

1. Copie WSScan.exe do suporte de instalação Dell para o computador Windows a verificar.
2. Inicie uma linha de comandos na localização acima e introduza **wsscan.exe** na mesma. O WSScan é iniciado.
3. Clique em **Avançadas**.
4. Selecione o tipo de unidade a analisar: *Todas as unidades, Unidades fixas*, *Unidades amovíveis* ou *CDROM/DVDROM*.
5. Selecione o tipo de relatório de encriptação: *Ficheiros encriptados*, *Ficheiros não encriptados*, *Todos os ficheiros* ou *Ficheiros não encriptados em violação*:
   - *Ficheiros encriptados* - Para assegurar que todos os dados são desencriptados quando desinstalar o Encryption. Siga o processo de desencriptação de dados existente, por exemplo, a emissão de uma atualização de política de desencriptação. Após desencriptar os dados, mas antes de reiniciar para preparar a desinstalação, execute o WSScan para garantir que todos os dados estão desencriptados.
   - *Ficheiros desencriptados* - Para identificar ficheiros que não estão encriptados, com indicação se os ficheiros devem ser encriptados (S/N).
   - *Todos os ficheiros* - Para indicar todos os ficheiros encriptados e desencriptados, com indicação se os ficheiros devem ser encriptados (S/N).
   - *Ficheiros desencriptados em violação* - Para identificar ficheiros que não estão encriptados e deviam estar.
6. Clique em **Procurar**.

OU

1. Clique em **Avançadas** para alternar a visualização para **Simples** para analisar uma pasta particular.
2. Aceda a Definições de análise e introduza o caminho da pasta no campo *Caminho da pesquisa*. Se este campo for utilizado, a seleção no menu é ignorada.
3. Caso não pretenda gravar os resultados de saída do WSScan num ficheiro, desmarque a caixa de verificação **Saída para ficheiro**.
4. Se pretender, altere o caminho e o nome de ficheiro predefinidos em *Caminho*.
5. Selecione **Adicionar a ficheiro existente** se não pretende substituir quaisquer ficheiros de saída WSScan existentes.
6. Escolha o formato de saída:
   - Selecione Formato de relatório para obter uma lista de estilos de relatório de saída de análise. Este é o formato predefinido.
   - Selecione Ficheiro de valor delimitado para uma saída que possa ser importada para uma aplicação de folha de cálculo. O delimitador predefinido é "|", embora possa ser alterado para, no máximo, 9 carateres alfanuméricos, um espaço ou sinais de pontuação do teclado.
   - Selecione a opção Valores cotados para colocar cada valor entre aspas duplas.
   - Selecione Ficheiro de largura fixa para uma saída não delimitada, com uma linha contínua de informações de comprimento fixo acerca de cada ficheiro encriptado.
7. Clique em **Procurar**.

   Clique em **Parar a pesquisa** para parar a sua pesquisa. Clique em **Limpar** para eliminar as mensagens apresentadas.

Resultado do WSScan

As informações do WSScan acerca dos ficheiros encriptados contêm os seguintes dados.

Exemplo de saída:

[2015-07-28 07:52:33] SysData.7vdlxrsb._SDENCR_: "c:\temp\Dell - test.log" continua encriptado por AES256

Saída	Significado
Carimbo de data/hora	A data e a hora em que o ficheiro foi analisado.
Tipo de encriptação	O tipo de encriptação utilizado para encriptar o ficheiro. **SysData:** chave SDE. **Utilizador:** chave de encriptação do utilizador. **Comum:** chave de encriptação Comum. O WSScan não indica ficheiros encriptados utilizando o Encrypt for Sharing.
KCID	A ID do computador principal. Tal como apresentado no exemplo acima, "**7vdlxrsb**" Se estiver a analisar uma unidade de rede mapeada, o relatório da análise não apresenta uma KCID.
UCID	A ID do utilizador. Tal como apresentado no exemplo acima, "**_SDENCR_**" A UCID é partilhada por todos os utilizadores desse computador.
Ficheiro	O caminho do ficheiro encriptado. Tal como apresentado no exemplo acima, "**c:\temp\Dell - test.log**"
Algoritmo	O algoritmo de encriptação utilizado para encriptar o ficheiro. Tal como apresentado no exemplo acima, "**continua encriptado por AES256**" RIJNDAEL 128 RIJNDAEL 256 AES-128 AES-256 3DES

Verificar o estado do Encryption Removal Agent

O Encryption Removal Agent apresenta o respetivo estado na área de descrição do painel de serviços (Iniciar > Executar > services.msc > OK) da seguinte forma. Atualize periodicamente o serviço (selecione o serviço > clique com o botão direito do rato > Atualizar) para atualizar o respetivo estado.

- **A aguardar a desativação do SED** - o Encryption continua instalado, continua configurado, ou ambos. A desencriptação apenas tem início quando o Encryption for desinstalado.
- **Varrimento inicial** – O serviço está a realizar um varrimento inicial, calculando o número de ficheiros encriptados e de bytes. O varrimento inicial ocorre uma vez.
- **Varrimento de desencriptação** – O serviço está a desencriptar ficheiros e, possivelmente, a solicitar a desencriptação de ficheiros bloqueados.
- **Desencriptar no reinício (parcial)** – O varrimento de desencriptação está concluído e alguns ficheiros bloqueados (mas não todos) serão desencriptados no próximo reinício.
- **Desencriptar no reinício** – O varrimento de desencriptação está concluído e todos os ficheiros bloqueados serão desencriptados no próximo reinício.
- **Não foi possível desencriptar todos os ficheiros** – O varrimento de desencriptação foi concluído, mas não foi possível desencriptar todos os ficheiros. Este estado significa que ocorreu uma das seguintes situações:
  - Não foi possível agendar a desencriptação dos ficheiros bloqueados, uma vez que eram demasiado grandes ou ocorreu um erro ao realizar o pedido de desbloqueio dos mesmos.
  - Ocorreu um erro de entrada/saída ao desencriptar os ficheiros.
  - Não foi possível desencriptar os ficheiros através da política.
  - Os ficheiros estão marcados como devendo estar encriptados.

- Ocorreu um erro durante o varrimento de desencriptação.
- Em todos os casos, é criado um ficheiro de registo (se estiver configurada a criação de registos) quando estiver definido LogVerbosity=2 (ou superior). Para a resolução de problemas, defina a verbosidade do registo para 2 e reinicie o serviço do Agente de Remoção de Encriptação para forçar outro varrimento de desencriptação.

- **Concluído** - O varrimento da desencriptação está concluído. É agendada a eliminação do serviço, do executável, do controlador e do executável do controlador para a reinicialização de sistema seguinte.

Como encriptar um iPod com o Encryption External Media

Estas regras desativam ou ativam a encriptação para estas pastas e tipos de ficheiros para todos os dispositivos amovíveis - não apenas um iPod. Tenha cuidado ao definir regras.

- A Dell não recomenda a utilização do iPod Shuffle, uma vez que podem ocorrer resultados inesperados.
- À medida que os iPods mudam, esta informação também poderá mudar, pelo que se aconselha cautela ao permitir a utilização de iPods em computadores ativados com Encryption External Media.
- Uma vez que os nomes das pastas nos iPods dependem do modelo de iPod, a Dell recomenda a criação de uma política de exclusão que abranja todos os nomes de pastas, em todos os modelos de iPod.
- Para garantir que a encriptação de um iPod através do Encryption External Media não torna o dispositivo inutilizável, introduza as seguintes regras na política de Regras de encriptação para Encryption External Media:

  -R#:\Calendars

  -R#:\Contactos

  -R#:\iPod_Control

  -R#:\Notas

  -R#:\Fotos

- Também pode forçar a encriptação de tipos de ficheiros específicos nos diretórios acima. Adicionar as seguintes regras garante que os ficheiros ppt, pptx, doc, docx, xls e xlsx são encriptados nos diretórios *excluídos* da encriptação através das seguintes regras:

  ^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

- Substituir estas cinco regras pela regra que se segue força a encriptação dos ficheiros ppt, pptx, doc, docx, xls e xlsx em qualquer diretório no iPod, incluindo os Calendários, Contactos, iPod_Control, Notas e Fotos:

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

- As regras foram testadas face aos seguintes iPods:

  iPod Video de 30 GB, quinta geração

  iPod Nano de 2 GB, segunda geração

  iPod Mini de 4 GB, segunda geração

Controladores do Dell ControlVault

Atualização de controladores e firmware do Dell ControlVault

- Os controladores e firmware do Dell ControlVault instalados de fábrica nos computadores Dell estão desatualizados e devem ser atualizados mediante o procedimento abaixo descrito e na ordem em que se encontra.
- Se uma mensagem de erro for apresentada durante a instalação do cliente e lhe pedir para sair do programa de instalação para atualizar os controladores do Dell ControlVault, pode seguramente dispensar a mensagem para continuar a instalação do cliente. Os controladores (e firmware) do Dell ControlVault podem ser atualizados após a conclusão da instalação do cliente.

Transferência dos controladores mais recentes

1. Aceda a dell.com/support.
2. Selecione o modelo do seu computador.
3. Selecione **Controladores e transferências**.
4. Selecione o **Sistema operativo** do computador de destino.
5. Selecione a categoria **Segurança**.
6. Transfira e guarde os controladores do Dell ControlVault.
7. Transfira e guarde o firmware do Dell ControlVault.
8. Copie os controladores e o firmware nos computadores de destino, se necessário.

Instale o controlador do Dell ControlVault

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

   NOTA:

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

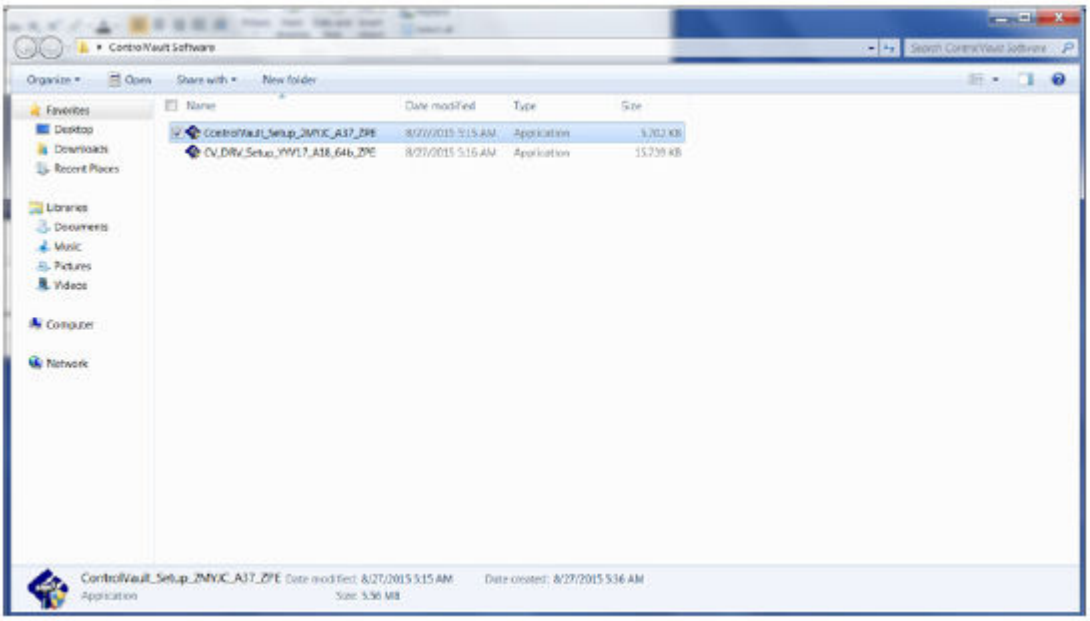
3. Clique em **Continuar** para iniciar.
4. Clique em **Ok** para descomprimir os ficheiros de controladores na localização predefinida em `C:\Dell\Drivers\<New Folder>`.
5. Clique em **Sim** para permitir a criação de uma nova pasta.
6. Clique em **Ok** quando for apresentada a mensagem de que a descompressão dos ficheiros foi bem-sucedida.
7. A pasta que contém os ficheiros deve ser apresentada após a extração. Caso não seja apresentada, navegue até à pasta na qual extraiu os ficheiros. Neste caso, a pasta é **JW22F**.
8. Clique duas vezes em **CVHCI64.MSI** para iniciar o programa de instalação dos controladores. [este exemplo é **CVHCI64.MSI** neste modelo (CVHCI para um computador de 32 bits)].
9. Clique em **Seguinte** no ecrã de boas-vindas.
10. Clique em **Seguinte** para instalar os controladores na localização predefinida em `C:\Program Files\Broadcom Corporation\Broadcom USH Host Components\.`
11. Selecione a opçã **Completo** e clique em **Seguinte**.
12. Clique em **Instalar** para iniciar a instalação dos controladores.
13. Opcionalmente, marque a caixa para apresentar o ficheiro de registo do programa de instalação. Clique em **Concluir** para sair do assistente.

Verificação da instalação dos controladores

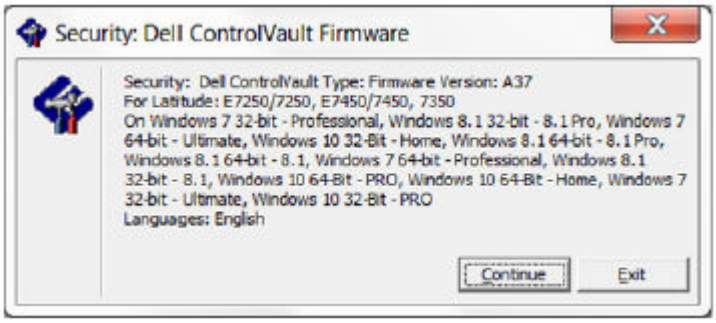
- O Gestor de dispositivos terá um dispositivo Dell ControlVault (e outros dispositivos) dependendo da configuração de hardware e do sistema operativo.

Instalação do firmware do Dell ControlVault

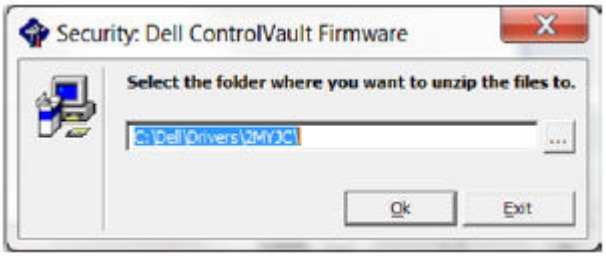
1. Navegue até à pasta para onde transferiu o ficheiro de instalação do firmware.



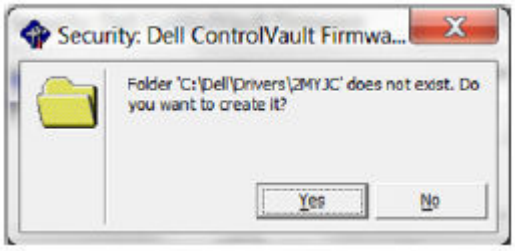
2. Clique duas vezes no firmware do Dell ControlVault para iniciar o ficheiro executável de extração automática.
3. Clique em **Continuar** para iniciar.



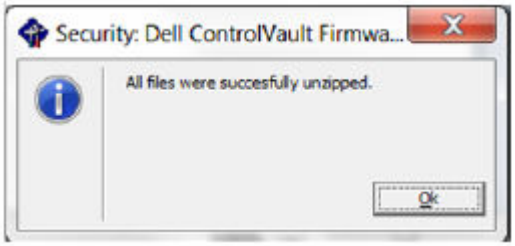
4. Clique em **Ok** para descomprimir os ficheiros de controladores na localização predefinida em `C:\Dell\Drivers\<New Folder>`.



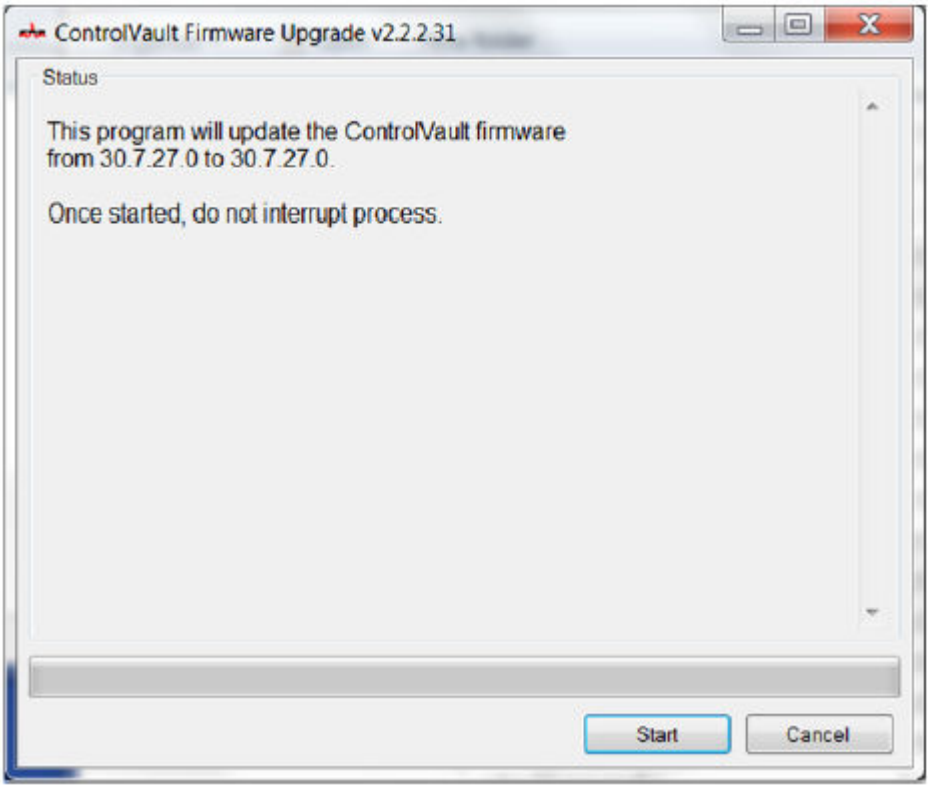
5. Clique em **Sim** para permitir a criação de uma nova pasta.



6. Clique em **Ok** quando for apresentada a mensagem de que a descompressão dos ficheiros foi bem-sucedida.



7. A pasta que contém os ficheiros deve ser apresentada após a extração. Caso não seja apresentada, navegue até à pasta na qual extraiu os ficheiros. Selecione a pasta de **firmware**.
8. Clique duas vezes em **ushupgrade.exe** para iniciar o programa de instalação do firmware.
9. Clique em **Iniciar** para iniciar a atualização do firmware.



NOTA:

No caso de atualização a partir de uma versão mais antiga de firmware, pode ser-lhe solicitada a palavra-passe de administrador. Introduza `Broadcom` como palavra-passe e clique em **Enter** se esta caixa de diálogo for apresentada.

Várias mensagens de estado serão apresentadas.

10. Clique em **Reiniciar** para concluir a atualização do firmware.

    A atualização dos controladores e do firmware do Dell ControlVault foi concluída.

Definições de registo

Esta secção detalha todas as definições de registo aprovadas pelo Dell ProSupport para computadores cliente locais.

Encryption

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

- Antes de iniciar o processo de desinstalação, é possível criar, de forma opcional, um ficheiro de registo do Agente de remoção de encriptação. Este ficheiro de registo é útil para deteção e resolução de problemas numa operação de desinstalação/desencriptação. Se não pretender desencriptar ficheiros durante o processo de desinstalação, não é necessário criar este ficheiro de registo.
- O ficheiro de registo do Encryption Removal Agent apenas é criado após a execução do serviço Encryption Removal Agent, que ocorre somente quando o computador é reiniciado. Quando o cliente for desinstalado com êxito e o computador for totalmente desencriptado, o ficheiro de registo é eliminado definitivamente.
- O caminho do ficheiro de registo é `C:\ProgramData\Dell\Dell Data Protection\Encryption.`
- Crie a seguinte entrada de registo no computador destinado à desencriptação.

  [HKLM\Software\Credant\DecryptionAgent]

  "LogVerbosity"=DWORD:2

  0: sem registos

  1: regista os erros que impedem a execução do serviço

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

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

  5: regista as informações de depuração

Utilizar Smart Cards com início de sessão no Windows

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

  HKLM\SOFTWARE\Dell\Dell Data Protection\

  "SmartcardEnabled"=DWORD:1

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

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

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

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

  "SmartCardLogonNotify"=DWORD:1

  0 = Desativado

  1 = Ativado

Preservar ficheiros temporários durante a instalação

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

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

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

  [HKLM\SOFTWARE\CREDANT\CMGShield]

  "DeleteTempFiles"=REG_DWORD:0

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

Alterar a ação predefinida do utilizar para iniciar ou atrasar a encriptação

- O cliente de Encriptação apresenta o aviso *`length of each policy update delay`* durante cinco minutos de cada vez. Se o utilizador não responder ao comando, o atraso seguinte é automaticamente iniciado. O comando de atraso final inclui uma contagem decrescente e uma barra de progresso e é apresentado até que o utilizador responda ou até que o atraso final expire e o encerramento/reinício solicitado ocorra.

  Pode alterar a ação do utilizador para iniciar ou atrasar a encriptação, para evitar o processamento da encriptação sem que o utilizador responda ao comando. Para isso, configure o registo com o seguinte valor de registo:

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

"SnoozeBeforeSweep"=DWORD:1

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

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

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

Alterar a utilização predefinida da chave SDUser

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

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

  [HKEY_LOCAL_MACHINE\SOFTWARE\Credant\CMGShield]

  "EnableSDUserKeyUsage"=DWORD:00000000

  Se esta chave de registo não existir ou estiver definida para qualquer outro valor que não 0, a chave SDUser é utilizada para encriptar estes diretórios de utilizador.

Desativar/ativar o Encrypt for Sharing no menu de contexto do botão direito do rato

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

  HKEY_LOCAL_MACHINE\SOFTWARE\Dell\Dell Data Protection\Encryption

  "DisplaySharing"=DWORD

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

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

Desativar/Ativar a notificação para a ativação do Encryption Personal

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

  "HidePasswordPrompt"=DWORD

  1 = desativa o pedido de palavra-passe para a ativação do Encryption Personal

  0 = ativa o pedido de palavra-passe para a ativação do Encryption Personal

Desativar/Ativar o aviso de reinício depois de o Encryption Removal Agent concluir o estado final da desencriptação

- Para desativar a solicitação ao utilizador para reiniciar o computador depois de o Encryption Removal Agent concluir o seu estado final no processo de desencriptação, modifique o seguinte valor de registo.

  HKLM\Software\Dell\Dell Data Protection

  "ShowDecryptAgentRebootPrompt"=DWORD

  Predefinição = ativado

  1 = ativado (apresenta aviso)

  0 = desativado (oculta aviso)

Autenticação avançada

Desativar Smart Card e serviços biométricos (opcional)

Se não pretender que o Advanced Authentication altere os serviços associados aos smart cards e aos dispositivos biométricos para um modo de arranque "automático", pode desativar a funcionalidade de arranque de serviços.

Quando desativada, a autenticação não tenta iniciar estes três serviços:

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

  A desativação desta funcionalidade também suprime alertas associados aos serviços necessários que não estão a ser executados.

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

  [HKEY_LOCAL_MACHINE\SOFTWARE\DELL\Dell Data Protection]

  SmartCardServiceCheck=REG_DWORD:0

  Defina como 0 para Ativar.

  Defina como 1 para Desativar

Utilizar Smart Cards com início de sessão no Windows

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

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

  "PBAIsActivated"=DWORD (32 bits):1

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

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

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

  HKLM\SOFTWARE\Dell\Dell Data Protection\

  "SmartcardEnabled"=DWORD:1

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

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

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

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

  "SmartCardLogonNotify"=DWORD:1

  0 = Desativado

  1 = Ativado

  Avance para o Glossário.

- Para evitar que o SED Management desative fornecedores de credenciais de outros fabricantes, crie a seguinte chave de registo:

  HKLM\SOFTWARE\Dell\Dell Data Protection\

  "AllowOtherCredProviders" = DWORD:1

  0=Desativado (predefinição)

  1=Ativado

- Por predefinição, o Encryption Management Agent já não envia políticas. Para emitir políticas futuras utilizadas, crie a seguinte chave de registo:

  HKLM\Software\Dell\Dell Data Protection\

  DWORD: DumpPolicies

Value=1

Nota: é necessário reiniciar para que esta alteração tenha efeito.

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

  [HKEY_LOCAL_MACHINE\SOFTWARE\Dell\Dell Data Protection]

  "PbaToastersAllowClose" =DWORD:1

  0=Ativado (predefinição)

  1=Desativado

13

Glossário

Advanced Authentication - O produto Advanced Authentication fornece opções de leitor de Smart Card. O Advanced Authentication ajuda a gerir estes vários métodos de autenticação, suporta o início de sessão com unidades de encriptação automática, SSO e gere as credenciais e palavras-passe do utilizador.

Palavra-passe de administrador para encriptação (EAP) - A EAP é uma palavra-passe administrativa exclusiva de cada computador. A maioria das alterações à configuração efetuadas na Consola de gestão local requerem esta palavra-passe. Esta é também a mesma palavra-passe que é necessária para usar o ficheiro LSARecovery_[hostname].exe para recuperar dados. Registe e guarde esta palavra-passe num local seguro.

Encryption Client - O Encryption Client é o componente no dispositivo que aplica as políticas de segurança, quer o endpoint esteja ligado à rede, desligado da rede, ou seja perdido ou roubado. Ao criar um ambiente de computação fidedigno para endpoints, o cliente Encryption funciona como uma camada no topo do sistema operativo do dispositivo e proporciona autenticação, encriptação e autorização aplicadas de forma consistente para maximizar a proteção de informações sensíveis.

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

Varrimento de encriptação - processo de análise das pastas a serem encriptadas para assegurar que os ficheiros contidos estão no estado de encriptação adequado. As operações comuns de criação e mudança de nome de ficheiros não acionam um varrimento de encriptação. É importante entender quando pode ocorrer um varrimento de encriptação e o que pode afetar os tempos de varrimento resultantes, da seguinte forma: - Um varrimento de encriptação ocorre após a receção inicial de uma política com a encriptação ativada. Isto pode ocorrer imediatamente depois da ativação se a sua política tem a encriptação ativada. - Se a *política Analisar ambiente de trabalho ao iniciar sessão* estiver ativada, as pastas especificadas para a encriptação são submetidas a varrimento em cada início de sessão do utilizador. - Um varrimento pode ser acionado novamente sob determinadas alterações de política subsequentes. Qualquer alteração de política relacionada com a definição das pastas de encriptação, algoritmos de encriptação, utilização da chave de encriptação (utilizador de versos comuns), aciona um varrimento. Adicionalmente, a alternância entre a encriptação ativada e desativada aciona um varrimento de encriptação.

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

Início de sessão único (SSO) - O SSO simplifica o processo de início de sessão quando uma autenticação multi-factores é activada no pré-arranque e no início de sessão do Windows. Se estiver ativado, a autenticação só é necessária no pré-arranque e os utilizadores iniciam a sessão automaticamente no Windows. Se estiver desativado, a autenticação poderá ser necessária várias vezes.

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

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