Dell Data Protection | Personal Edition

Guia de instalação v8.13

Notas, avisos e advertências

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

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

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

Guia de Instalação do Personal Edition

2017 - 04

Rev. A01

Índice

1

Descrição geral do Personal Edition

Este guia assume que a aplicação Security Tools serão instaladas com o Personal Edition.

Personal Edition

O objetivo do Personal Edition é proteger os dados no seu computador, mesmo se o computador for perdido ou roubado.

Para garantir a segurança dos seus dados confidenciais, o Personal Edition encripta os dados no seu computador Windows. Pode sempre aceder aos dados quando inicie a sessão no computador, mas utilizadores não autorizados não terão 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, o cliente Encryption desencripta dados à medida que trabalha com eles. Ocasionalmente, uma aplicação pode tentar aceder a um ficheiro ao mesmo tempo que o cliente Encryption está a encriptar ou desencriptar. Se isto acontecer, um ou dois segundos depois, o cliente Encryption exibe uma caixa de diálogo que lhe dá a opção de esperar ou cancelar a encriptação/desencriptação. Se escolher esperar, o cliente Encryption liberta o ficheiro assim que está terminado (geralmente dentro alguns segundos).

Security Tools

A finalidade de Security Tools é fornecer uma solução de segurança ponto a ponto para suporte a Advanced Authentication.

Security Tools oferece uma assistência de multifatores para a autenticação do Windows com palavras-passe, leitores de impressões digitais e smart cards, "sem contacto" e "com contacto", bem como autoinscrição, Palavras-passe monouso (OTP) e Início de sessão de um só passo (Início de sessão de passo único [SSO]).

A Consola de segurança é a interface de Security Tools que orienta o utilizador durante a configuração das suas credenciais e perguntas de autorrecuperação, com base nas políticas definidas pelo administrador.

A ferramenta Definições de administrador é disponibilizada aos utilizadores com privilégios de administrador e é utilizada para configurar políticas de autenticação e opções de recuperação, gerir utilizadores e configurar definições avançadas, bem como definições específicas das credenciais suportadas para o início de sessão do Windows.

Consulte Configurar as definições do administrador do Security Tools e o *Manual do utilizador* do *Dell Console* para saber como utilizar as aplicações do Security Tools.

Contacte o Dell ProSupport

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

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

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

Para número de telefone fora dos Estados Unidos, consulte Dell ProSupport International Phone Numbers (Números de telefone internacionais do Dell ProSupport).

2

Requisitos do Personal Edition

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

Cliente de encriptação

- O Personal Edition requer elegibilidade para ser instalado com êxito. A elegibilidade é fornecida quando adquire o Personal Edition. Dependendo de como compra o Personal Edition, pode necessitar instalar manualmente a elegibilidade. Se assim for, siga as instruções simples que acompanham a elegibilidade. Se o Personal Edition for instalado com o Dell Digital Delivery, a instalação da elegibilidade é realizada pelo serviço Dell Digital Delivery. (São utilizados os mesmos binários para Enterprise Edition e Personal Edition. A elegibilidade informa o instalador sobre a versão que deve instalar).
- A Dell recomenda vivamente que seja utilizada 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.
  a Aceda ao Painel de Controlo do Windows (**Iniciar** > **Painel de Controlo**).
  b Clique no ícone **Contas de utilizador**.
  c Clique em **Criar uma palavra-passe para a sua conta**.
  d Introduza uma nova palavra-passe e volte a introduzir a mesma.
  e Em alternativa, pode introduzir uma dica para palavra-passe.
  f Clique em **Criar palavra-passe**.
  g 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 ou Dell KACE. Não são suportados utilizadores não administradores com privilégios elevados.
- Realize uma cópia de segurança de todos os dados importantes antes de iniciar a instalação/desinstalação/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 terceiros ou uma solução similar para implementar o cliente Encryption. Para instruções sobre como instalar o cliente Encryption numa imagem corporativa, consulte http://www.dell.com/support/article/us/en/19/SLN304039.
- O TPM é utilizado para selar o GPK. Por conseguinte, se o cliente de Encriptação estiver a ser executado, limpe o TPM na BIOS antes de proceder à instalação de um novo sistema operativo no computador cliente.
- O cliente Encryption foi sujeito a testes e é compatível com McAfee, com o cliente Symantec, Kaspersky e MalwareBytes. Existem exclusões implementadas para estes fornecedores de produtos anti-vírus, para evitar incompatibilidades entre a monitorização anti-vírus e a encriptação. O cliente Encryption foi também testado com o Microsoft Enhanced Mitigation Experience Toolkit.

No caso de a sua organização fazer uso de um antivírus de um fornecedor que não esteja na lista, consulte o artigo KB SLN298707 ou contacte o Dell ProSupport para obter assistência.

- Não é suportada a atualização de versão do sistema operativo com o cliente Encryption instalado. Desinstale e desencripte o cliente Encryption, atualize para o novo sistema operativo e, em seguida, reinstale o cliente Encryption.

  Para além disso, não são suportadas reinstalações de sistema operativo. Para realizar a reinstalação do sistema operativo, faça uma cópia de segurança do computador em questão, realize a limpeza do computador, instale o sistema operativo e, em seguida, realize a recuperação dos dados encriptados seguindo os procedimentos de recuperação estabelecidos.
- Assegure-se de verificar periodicamente a página www.dell.com/support para procurar a documentação mais atual e Conselhos técnicos.

Pré-requisitos do Encryption Client

- É necessário o Microsoft .Net Framework 4.5.2 (ou posterior)

  Todos os computadores enviados da fábrica da Dell são previamente equipados com o Microsoft .Net Framework 4.5.2 (ou posterior). No entanto, se não instalar em hardware Dell ou se atualizar o cliente num hardware Dell mais antigo, deve verificar qual a versão do Microsoft .Net instalada e atualizar a versão, **antes de instalar o cliente** para impedir falhas na instalação/atualização. Para verificar a versão instalada do Microsoft .Net, siga estas instruções no computador onde pretende efetuar a instalação: http://msdn.microsoft.com/en-us/library/hh925568(v=vs.110).aspx. Para instalar o Microsoft .Net Framework 4.5.2, navegue para https://www.microsoft.com/en-us/download/details.aspx?id=42643.
- O instalador principal instala o Microsoft Visual C++ 2012 Update 4, se este ainda não estiver instalado no computador. **Quando utilizar o instalador subordinado**, é necessário instalar este componente antes de instalar o cliente Encryption.

Pré-requisito
• Visual C++ 2012 Update 4 ou Redistributable Package posterior (x86 e x64)
• Microsoft SQL Server Compact 3.5 SP2 (x86 e x64)

Hardware do Encryption Client

- A tabela seguinte apresenta o hardware de computador suportado.

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

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

Hardware opcional incorporado
• TPM 1.2 ou 2.0

Sistemas operativos do Encryption Client

- A tabela seguinte apresenta os sistemas operativos suportados.

Sistemas operativos Windows (32 e 64 bits)
• Windows 7 SP0-SP1: Enterprise, Professional, Ultimate
• Windows Embedded Standard 7 com modelo de Compatibilidade entre Aplicações (a encriptação do hardware não é suportada)
• Windows 8: Enterprise, Pro

Sistemas operativos Windows (32 e 64 bits)

- Windows 8.1 Atualização 0-1: Enterprise Edition, Pro Edition
- Windows Embedded 8.1 Industry Enterprise (a encriptação do hardware não é suportada)
- Windows 10: Education, Enterprise, Pro
- VMware Workstation 5.5 e posterior

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

Sistemas operativos para External Media Shield (EMS)

- A tabela seguinte apresenta os sistemas operativos suportados ao aceder a suportes com proteção EMS.

> **NOTA: O External Media deve ter, aproximadamente, 55 MB disponíveis, bem como espaço livre no suporte multimédia igual ao maior ficheiro a encriptar para alojar o EMS.**

> **NOTA:**
> O Windows XP é suportado apenas quando se utiliza o EMS Explorer.

Sistemas operativos Windows compatíveis para aceder a suportes multimédia protegidos pelo EMS (32 e 64 bits)

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

Sistemas operativos Mac compatíveis para aceder a suportes multimédia protegidos pelo EMS (kernels de 64 bits)

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

Suporte de idiomas do Encryption Client

- O cliente Encryption está em conformidade com a norma MUI (Multilingual User Interface - Interface de utilizador multilíngue) e suporta os seguintes idiomas.

Suporte de idiomas

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

Cliente Advanced Authentication

- Quando utilizar Advanced Authentication, os utilizadores terão acesso seguro ao computador através de credenciais da Advanced Authentication geridas e registadas utilizando o Security Tools. O Security Tools será o gestor principal das credenciais de autenticação

para o Início de sessão do Windows, incluindo a palavra-passe do Windows, impressões digitais e smart cards. As credenciais de palavra-passe por imagem, PIN e impressão digital registadas através do sistema operativo da Microsoft não serão reconhecidas pelo Início de sessão do Windows.

Para continuar a utilizar o sistema operativo da Microsoft para gerir as credenciais de utilizador, não instale ou desinstale o Security Tools.

- A funcionalidade Palavra-passe monouso (OTP) do Security Tools requer que um TPM esteja presente, ativado e que tenha proprietário. A funcionalidade OTP não é suportada com TPM 2.0. Para eliminar e definir a propriedade do TPM, consulte https://technet.microsoft.com/en-us/library/cc749022%28v=ws.10%29.aspx#BKMK_S2.

Hardware do Cliente Advanced Authentication

- A tabela seguinte lista a autenticação de hardware suportada.

Leitores de impressão digital e de smart cards

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

Cartões sem contacto

- Cartões sem contacto com leitores de cartões sem contacto incorporados nos portáteis Dell especificados

Smart Cards

- Smart Cards PKCS #11 que utilizam o cliente ActivIdentity

  NOTA: O cliente ActivIdentity não se encontra pré-carregado e tem de ser instalado separadamente.
- Cartões CSP
- Cartão de acesso comum (CAC)
- Cartões SIPRNet/Classe B

- Os controladores e firmware do Dell ControlVault, leitores de impressão digital e de smart cards (conforme ilustrado abaixo) não estão incluídos nos ficheiros executáveis do instalador principal ou do instalador subordinado. Os controladores e firmware têm de ser mantidos atualizados e podem ser transferidos a partir de http://www.dell.com/support e selecionando o seu modelo de computador. Transfira os controladores e firmware adequados com base no seu hardware de autenticação.

  - Dell ControlVault
  - NEXT Biometrics Fingerprint Driver
  - Validity FingerPrint Reader 495 Driver
  - O2Micro Smart Card Driver

  Se estiver a realizar a instalação em hardware não Dell, transfira os controladores e firmware atualizados a partir do Web site do vendedor correspondente. As instruções de instalação dos controladores do Dell ControlVault estão disponíveis em Controladores do Dell ControlVault.
- A tabela seguinte apresenta os modelos de computador Dell compatíveis com cartões SIPR Net.

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

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

Sistemas operativos do Cliente Advanced Authentication

Sistemas operativos Windows

- A tabela seguinte apresenta os sistemas operativos suportados.

Sistemas operativos Windows (32 e 64 bits)
• Windows 7 SP0-SP1: Enterprise, Professional, Ultimate • Windows 8: Enterprise, Pro • Windows 8.1 Atualização 0-1: Enterprise Edition, Pro Edition • Windows 10: Education, Enterprise, Pro

NOTA: O modo UEFI não é suportado pelo Windows 7.

Sistemas operativos de dispositivos móveis

- Os sistemas operativos móveis seguintes são suportados com a funcionalidade Palavra-passe monouso do Security Tools.

Sistemas operativos para Android
• 4.0 - 4.0.4 Ice Cream Sandwich • 4.1 - 4.3.1 Jelly Bean • 4.4 - 4.4.4 KitKat • 5.0 - 5.1.1 Lollipop

Sistemas operativos iOS
• iOS 7.x • iOS 8.x

Sistemas operativos Windows Phone
• Windows Phone 8.1 • Windows 10 Mobile

Suporte de idiomas do Cliente Advanced Authentication

- O cliente Advanced Authentication está em conformidade com a norma MUI (Interface de utilizador multilíngue) e suporta os seguintes idiomas. O modo UEFI e a Autenticação de pré-arranque não são suportados em russo, chinês tradicional ou chinês simplificado.

Suporte de idiomas

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

Avance para Obter software.

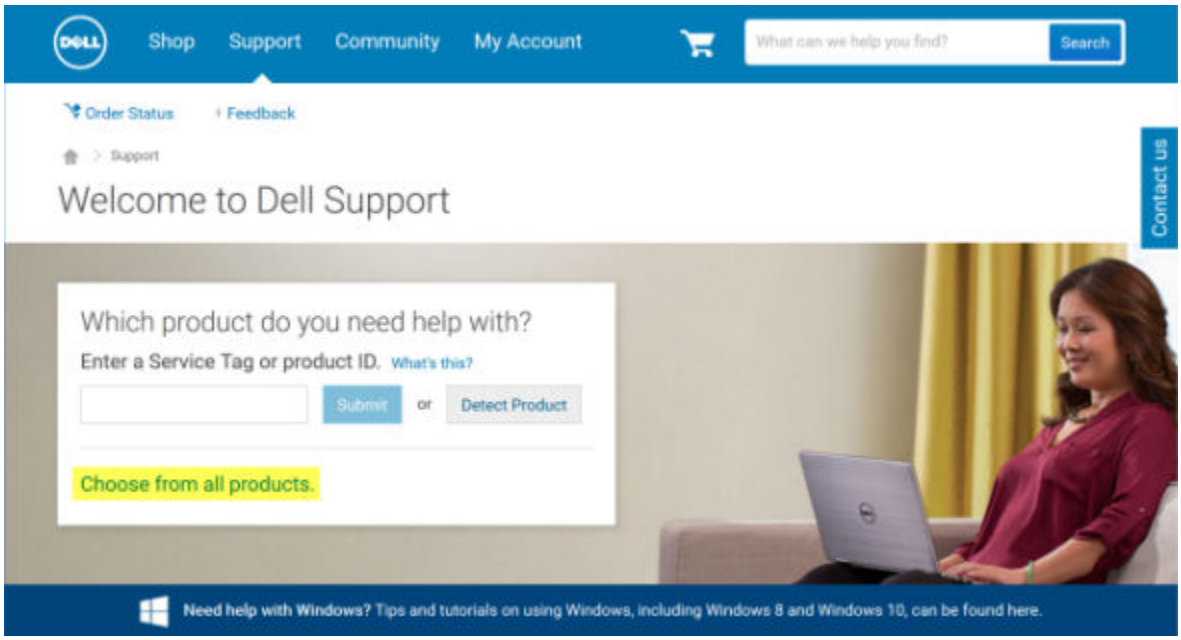
3

Download the 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 **Selecionar de entre todos os produtos**.



2 Select **Software & Security** from the list of products.

3 Select **Endpoint Security Solutions** in the *Software and Security* section.
Após efetuar esta seleção uma vez, o site irá memorizar as informações.

4 Selecione o produto Dell Data Protection.
Exemplos:

Dell Encryption

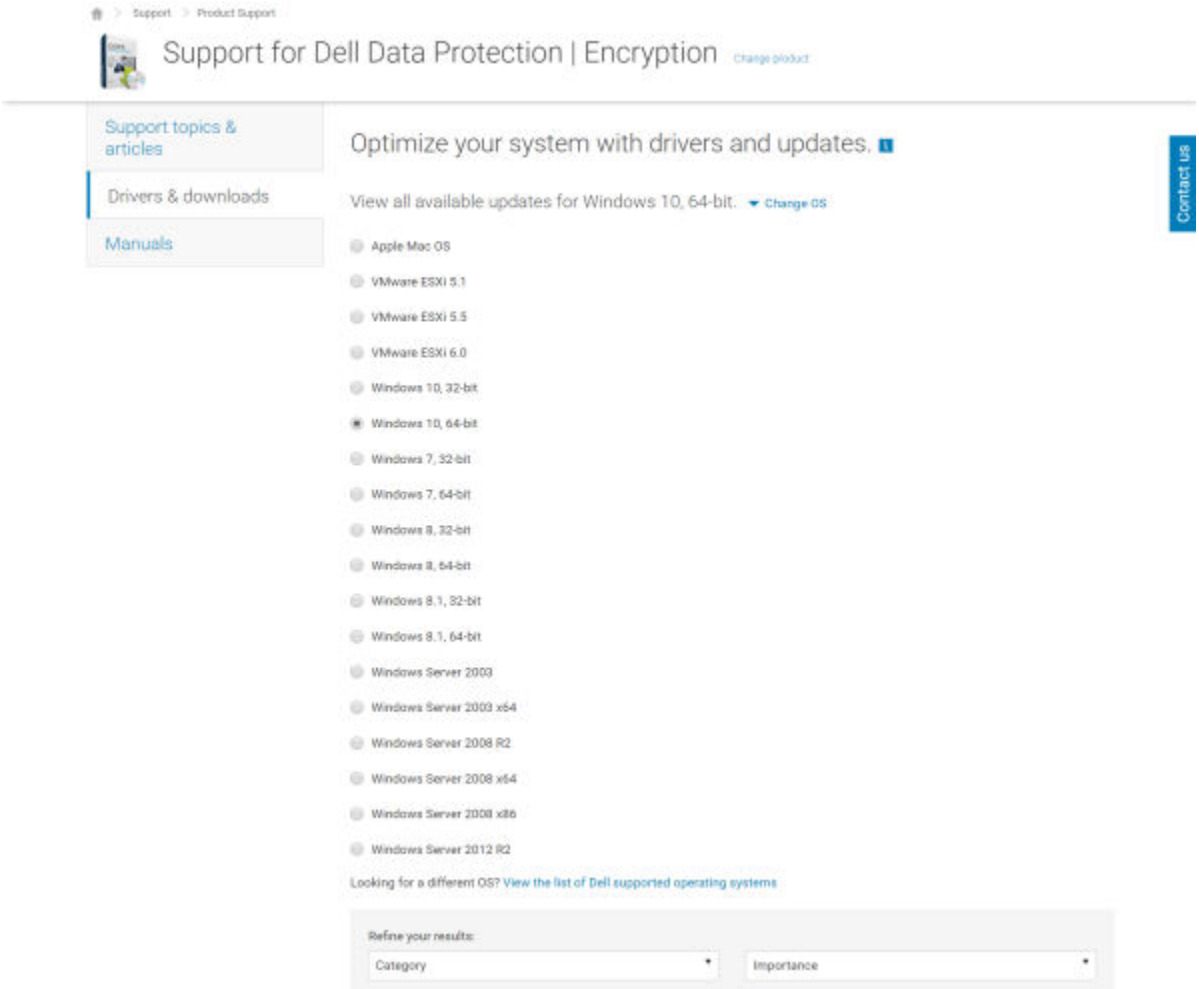
Dell Endpoint Security Suite

Dell Endpoint Security Suite Enterprise

5 Select **Drivers & downloads**.

6 Selecione o tipo de sistema operativo cliente desejado.

7 Select **Dell Data Protection (4 files)** in the matches. Isto é apenas um exemplo, pelo que, provavelmente, a realidade será ligeiramente diferente. Por exemplo, poderá não haver 4 ficheiros para escolha.



8 Select **Download File** or A**dd to My Download List #XX**.
Proceed to Install Personal Edition.

4

Instalação do Personal Edition

Pode instalar o Personal Edition usando o instalador principal (recomendado) ou extraindo os instaladores subordinados do instalador principal. De qualquer maneira, o Personal Edition 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:

- Consulte a *Ajuda do Dell Encrypt* para saber como utilizar a funcionalidade do cliente Encryption. Aceda à ajuda a partir de **<Install dir>:\Program Files\Dell\Dell Data Protection\Encryption\Help**
- Consulte a *Ajuda do EMS* para saber como utilizar as funcionalidades do External Media Shield. Aceda à ajuda a partir de **<Install dir>:\Program Files\Dell\Dell Data Protection\Encryption\EMS**.
- Consulte a *Ajuda de Ferramentas de Segurança* 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**.

Selecione um método de instalação

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

- Instalar o Personal Edition usando o Instalador Principal - RECOMENDADO
- Instalar o Personal Edition utilizando os Instaladores Subordinados

Instalar o Personal Edition usando o Instalador Principal - RECOMENDADO

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

O Instalador do Dell Data Protection é normalmente designado por Instalador principal, uma vez que instala múltiplos clientes. No caso do Personal Edition, este instala o cliente Encryption e o cliente Advanced Authentication.

Se a instalação utiliza a interface do utilizador do instalador principal, o Personal Edition pode ser instalado num computador de cada vez.

Os ficheiros de registo do instalador principal estão localizados em **C:\ProgramData\Dell\Dell Data Protection\Installer.**

Selecione um método:

Instalação utilizando a Interface de Utilizador

Instalação utilizando a Linha de Comandos

Instalação utilizando a Interface de Utilizador

Instale a elegibilidade no computador de destino se necessário.

Copie DDPSetup.exe para o computador local.

Faça duplo clique em DDPSetup.exe para iniciar o instalador.

Surge uma caixa de diálogo que o alertam para o estado da instalação dos pré-requisitos. Demora alguns minutos.

Clique em **Seguinte** no ecrã de boas-vindas.

Leia o acordo de licença, aceite os termos e clique em **Seguinte**.

Clique em **Seguinte** para instalar o Personal Edition na localização predefinida: **C:\Program Files\Dell\Dell Data Protection\.**

Security Tools é instalado por predefinição e não é possível anular a sua seleção. No instalador, está indicado como Security Framework.

Advanced Authentication é instalado por predefinição e não é possível anular a sua seleção.

Clique em **Seguinte**.

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

É apresentada uma janela de estado. Isto demora vários minutos.

Selecione **Sim, desejo reiniciar o computador agora** e clique em **Concluir**.

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

A instalação do Personal Edition + Security Tools está concluída.

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

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

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

Instalação utilizando a Linha de Comandos

Instale a elegibilidade no computador de destino se necessário.

Opções:

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

Opção	Significado
-y -gm2	Passe os dados para o extrator autónomo
/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

Exemplo de instalação com Linha de Comandos

Embora o reinício seja suprimido nestes exemplos, é necessário um eventual reinício. A encriptação 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 Personal Edition e Security Tools (instalação silenciosa, sem reinício e instalado na localização predefinida **C:\Program Files\Dell\Dell Data Protection**).

```
DDPSetup.exe -y -gm2 /S /z"\"FEATURE=PE\""
```

O exemplo seguinte instala o Personal Edition e Security Tools (instalação silenciosa, sem reinício e instalado numa localização alternativa C:\Program Files\Dell\My_New_Folder).

```
DDPSetup.exe -y -gm2 /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 Personal Edition + Security Tools está concluída.

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

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

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

Instalar o Personal Edition utilizando os Instaladores Subordinados

Para instalar o Personal Edition usando os instaladores subordinados, 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.

Instalação com 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.

Utilize estes instaladores para instalar os clientes utilizando uma instalação com script, ficheiros batch ou qualquer outra tecnologia push disponível na sua organização.

Nestes exemplos de linha de comandos, o reinício foi suprimido. No entanto, é necessário um eventual reinício. A encriptação só pode ser iniciada após o reinício do computador.

Ficheiros de registo: o Windows cria ficheiros de registo de instalação únicos através do instalador subordinado para o utilizador com sessão iniciada em %temp% localizados 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*v C:\<any directory>\<any log file name>.log.

Todos os instaladores subordinados utilizam as mesmas opções .msi básicas e as mesmas opções de visualização em instalações por linha de comandos, exceto onde referido. 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 *.exe
/s	Modo silencioso
/i	Modo de instalação

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

Instalar controladores

Os controladores e firmware do Dell ControlVault, leitores de impressão digital e smart cards **não** estão incluídos nos ficheiros executáveis do instalador principal ou do instalador subordinado. Os controladores e firmware têm de ser mantidos atualizados e podem ser transferidos a partir de http://www.dell.com/support e selecionando o seu modelo de computador. Transfira os controladores e firmware adequados com base no seu hardware de autenticação.

Dell ControlVault

NEXT Biometrics Fingerprint Driver

Validity FingerPrint Reader 495 Driver

O2Micro Smart Card Driver

Se estiver a realizar a instalação em hardware não Dell, transfira os controladores e firmware atualizados a partir do Web site do vendedor correspondente.

Em seguida:

Instalar clientes Advanced Authentication

Os utilizadores iniciam sessão na PBA utilizando as respetivas credenciais do Windows.

Locate the file at **C:\extracted\Security Tools** and **C:\extracted\Security Tools\Authentication.**

Exemplo de instalação com Linha de Comandos

\Security Tools

O exemplo seguinte instala o Security Framework (instalação silenciosa, sem reinício e instalado na localização predefinida C:\Program Files\Dell\Dell Data Protection).

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

:

Na v8.x, é necessário este cliente para Advanced Authentication.

De seguida:

\Security Tools\Authentication

O exemplo seguinte instala o Security Tools (instalação silenciosa, sem reinício e instalado na localização predefinida C:\Program Files\Dell\Dell Data Protection).

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

De seguida:

Instalar o Encryption Client

Reveja os requisitos do Encryption Client se a sua organização utilizar um certificado assinado por uma autoridade raiz, como EnTrust ou Verisign. É necessária uma alteração na configuração de registo no computador cliente para ativar a validação do certificado.

O ficheiro está localizado em **C:\extracted\Encryption.**

Exemplo de instalação com Linha de Comandos

O exemplo seguinte instala o Personal Edition, encripta para partilha, oculta ícones de sobreposição, sem caixa de diálogo, sem barra de progresso e suprime o reinício.

```
DDPE_XXbit_setup.exe /s /v"HIDEOVERLAYICONS=1 REBOOT=ReallySuppress /qn"
```

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

A instalação do Personal Edition + Security Tools está concluída. A secção de configuração e assistente de configuração do Personal Edition é abrangida em separado.

Avance para os Assistentes de configuração de Security Tools e Personal Edition.

Assistentes de configuração de Security Tools e Personal Edition

Inicie sessão com o seu nome de utilizador e palavra-passe do Windows. Será passado através do 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 de Security Tools. Clique em **Seguinte**.

3 Introduza e volte a introduzir uma nova palavra-passe de administração de encriptação (EAP). Clique em **Seguinte**.

4 Introduza uma localização de cópia de segurança numa unidade de rede ou no suporte multimédia amovível para armazenar as informações de recuperação e clique em **Seguinte**.

5 Clique em **Aplicar** para iniciar a ativação de Security Tools.

6 Após a conclusão do assistente de ativação de Security Tools, inicie o assistente de configuração do Personal Edition a partir do ícone do DDP no tabuleiro do sistema (pode ser iniciado sozinho).

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 9-32 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 Security Tools, mas não está relacionada com a mesma. **Registe e guarde esta palavra-passe num local seguro**. Clique em **Seguinte**.

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 > Todos os Programas > Dell > Dell Data Protection > Encryption > Encryption Help.**

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 será 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 será denominada "Em conformidade".

Avance para Configurar as definições de administração de Security Tools.

Configurar as Definições do Administrador do Security Tools

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

Para configurar as funcionalidades do Security Tools, tem de ser um administrador no computador.

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

Após a ativação do Security Tools, a palavra-passe de administrador e a localização da cópia de segurança podem ser alteradas, se necessário.

1. Como administrador, inicie o Security Tools 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, se pretender 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.

   Os dados de recuperação serão automaticamente copiados para o local especificado. Se a localização não estiver disponível (por exemplo, se a sua unidade USB para cópia de segurança não estiver introduzida), Security Tools solicita-lhe uma localização para criar uma cópia de segurança dos seus dados. Será necessário aceder aos dados de recuperação para iniciar a encriptação.

Configurar opções de autenticação

Os controlos no separador Autenticação permitem-lhe definir opções de início de sessão e personalizar as definições de cada opção.

NOTA: A opção de Palavra-passe Monouso não é apresentada em Opções de Recuperação se o TPM não estiver presente, ativado e tiver proprietário.

Configurar opções de início de sessão

Na página de Opções de Início de Sessão, pode configurar as políticas de início de sessão. Por predefinição, todas as credenciais suportadas estão listadas em Opções Disponíveis.

Para configurar as opções de início de sessão:

No painel esquerdo, em Autenticação, selecione **Opções de Início de Sessão**.

Para escolher a função que pretende configurar, selecione a função na lista **Aplicar opções de início de sessão**: **Utilizadores** ou **Administradores**. Todas as alterações que efetuar nesta página serão aplicadas apenas ao papel que selecionar.

Defina Opções disponíveis para autenticação.

Por predefinição, cada método de autenticação é configurado para ser utilizado individualmente, não em combinação com outros métodos de autenticação. Pode alterar as predefinições das seguintes formas:

Para definir um conjunto de opções de autenticação, em Opções disponíveis, clique em para selecionar o primeiro método de autenticação. Na caixa de diálogo Opções disponíveis, selecione o segundo método de autenticação e, em seguida, clique em **OK**.

Por exemplo, pode exigir impressão digital e uma palavra-passe como credenciais de início de sessão. Na caixa de diálogo, selecione o segundo método de autenticação que precisa ser utilizado com a autenticação com impressão digital.

Para permitir que cada método de autenticação seja utilizado individualmente, na caixa de diálogo de opções disponíveis deixe o segundo método de autenticação definido como **Nenhum**, e clique em **OK**.

Para remover uma opção de início de sessão, em Opções disponíveis na página Opções de início de sessão, clique em **X** para remover o método.

Para adicionar uma nova combinação de métodos de autenticação, clique em **Adicionar uma opção**.

Defina Opções de Recuperação para os utilizadores recuperarem o acesso ao computador, se ficarem bloqueados.

Para permitir aos utilizadores definirem um conjunto de perguntas e respostas que podem utilizar para recuperar o acesso ao computador, selecione **Perguntas de recuperação**.

Para impedir a utilização de Perguntas de recuperação, desmarque esta opção.

Para permitir que os utilizadores recuperem o acesso através da utilização de um dispositivo móvel, selecione **Palavra-passe monouso**. Quando a Palavra-passe monouso (OTP) é selecionada como método de recuperação, não está disponível como opção de início de sessão no ecrã de início de sessão do Windows.

Para utilizar a funcionalidade OTP para início de sessão, desmarque a opção em Opções de Recuperação. Quando desmarcada como método de recuperação, a opção OTP aparece numa página de início de sessão do Windows, desde que pelo menos um utilizador esteja inscrito na OTP.

: Como administrador, controla a forma como a Palavra-passe Monouso pode ser utilizada - para autenticação ou para recuperação. A funcionalidade OTP pode ser utilizada para autenticação ou para recuperação, mas não para ambas. A configuração afeta todos os utilizadores do computador ou todos os administradores, com base na seleção no campo Opções de Início de Sessão, Aplicar Opções de Início de Sessão.

Se a opção de Palavra-passe monouso não for apresentada em Opções de recuperação, a configuração do seu computador não suporta a mesma. Para obter mais informações, consulte Requisitos.

Para obrigar o utilizador a contactar o suporte técnico se perder ou se esquecer das credenciais de início de sessão, desmarque ambas as caixas de verificação de Opções de recuperação: Perguntas de recuperação e Palavra-passe monouso.

Para definir um período de tempo no qual os utilizadores podem inscrever as suas credenciais de autenticação, selecione **Período de tolerância**.

A funcionalidade Período de tolerância permite-lhe definir a data em que a Opção de início de sessão começará a ser aplicada. Pode configurar uma Opção de início de sessão antes da data em que começará a ser aplicada e definir um período de tempo em que os utilizadores a poderão inscrever. Por predefinição, a política é aplicada de imediato.

Para alterar a data da aplicação da Opção de início de sessão de *Imediatamente*, a caixa de diálogo Período de tolerância, clique no menu de lista pendente e selecione **Data especificada**. Clique na seta para baixo que se encontra à direita do campo da data para apresentar um calendário e, em seguida, selecione uma data no calendário. A aplicação da política é iniciada, aproximadamente, às 00:01 da data selecionada.

Os utilizadores podem receber um alerta para inscreverem as suas credenciais necessárias no próximo início de sessão do Windows (por predefinição). Além disso, é possível definir lembretes regulares. Selecione o intervalo dos lembretes no menu de lista pendente *Lembrar utilizador*.

:

O lembrete apresentado ao utilizador é ligeiramente diferente, consoante o fato de o utilizador estar no ecrã de Início de sessão do Windows ou numa sessão do Windows na altura em que o lembrete é acionado. Os lembretes não aparecem nos ecrãs de início de sessão ou de Autenticação de pré-arranque.

Funcionalidade durante o período de tolerância

Durante um determinado período de tolerância, após cada início de sessão, é apresentada a notificação de Credenciais adicionais quando o utilizador ainda não tiver inscrito as credenciais mínimas necessárias para satisfazer uma opção de início de sessão alterada. O conteúdo da mensagem é: *Encontram-se disponíveis credenciais adicionais para inscrição.*

Se estiverem disponíveis outras credenciais mas as mesmas não forem necessárias, a mensagem só é apresentada uma vez após a política ter sido alterada.

Clicar na notificação tem os seguintes resultados, consoante o contexto:

Se nenhuma credencial tiver sido inscrita, é apresentado o assistente de Configuração, permitindo que os Utilizadores administrativos realizem configurações relacionadas com o computador e dando aos utilizadores a oportunidade de inscreverem as credenciais mais comuns.

Após a inscrição inicial de credenciais, se clicar na notificação será apresentado o assistente de Configuração na Consola de segurança do DDP.

Funcionalidade após a expiração do Período de tolerância

Em qualquer caso, após expirado o Período de tolerância, os utilizadores não podem iniciar sessão sem terem inscrito as credenciais exigidas pela Opção de início de sessão. Se um utilizador tentar iniciar sessão com uma credencial ou combinação de credenciais que não satisfaça a Opção de início de sessão, o assistente de Configuração é apresentado na parte superior do ecrã de início de sessão do Windows.

Se o utilizador inscrever com êxito as credenciais necessárias, terá a sessão iniciada no Windows.

Se um utilizador não registar com êxito as credenciais necessárias, ou cancelar o assistente, é direccionado para o ecrã de início de sessão do Windows.

Para guardar as definições da função selecionada, clique em **Aplicar**.

Configurar a Autenticação do Password Manager

Na página Password Manager, pode configurar de que forma os utilizadores autenticam para Password Manager.

Para configurar a autenticação através do Password Manager:

No painel esquerdo, em Autenticação, selecione **Password Manager**.

Para escolher a função que pretende configurar, selecione a função na lista **Aplicar opções de início de sessão**: **Utilizadores** ou **Administradores**. Todas as alterações que efetuar nesta página serão aplicadas apenas ao papel que selecionar.

Opcionalmente, selecione a caixa de verificação **Não exigir palavra-passe** para permitir o início de sessão automático da função de utilizador selecionada em todas as aplicações de software e Web sites da Internet com credenciais armazenadas no Password Manager.

Defina Opções disponíveis para autenticação.

Por predefinição, cada método de autenticação é configurado para ser utilizado individualmente, não em combinação com outros métodos de autenticação. Pode alterar as predefinições das seguintes formas:

Para definir um conjunto de opções de autenticação, em Opções disponíveis, clique em para selecionar o primeiro método de autenticação. Na caixa de diálogo Opções disponíveis, selecione o segundo método de autenticação e, em seguida, clique em **OK**.

Por exemplo, pode exigir impressão digital e uma palavra-passe como credenciais de início de sessão. Na caixa de diálogo, selecione o segundo método de autenticação que precisa ser utilizado com a autenticação com impressão digital.

Para permitir que cada método de autenticação seja utilizado individualmente, na caixa de diálogo de opções disponíveis deixe o segundo método de autenticação definido como **Nenhum**, e clique em **OK**.

Para remover uma opção de início de sessão, em Opções disponíveis na página Opções de início de sessão, clique em **X**para remover o método.

Para adicionar uma nova combinação de métodos de autenticação, clique em **Adicionar uma opção**.

Para guardar as definições da função selecionada, clique em **Aplicar**.

 **: Selecione o botão Predefinições para restaurar as definições para os valores originais.**

Configurar Perguntas de recuperação

Na página Perguntas de Recuperação, pode selecionar as questões que serão apresentadas aos utilizadores quando definirem Perguntas de Recuperação pessoais e respostas. As Perguntas de Recuperação permitem que os utilizadores recuperem o acesso aos respetivos computadores no caso de expiração ou esquecimento da palavra-passe.

Para configurar Perguntas de Recuperação:

No painel esquerdo, em Autenticação, selecione **Perguntas de Recuperação**.

Na página Perguntas de Recuperação, selecione pelo menos três Perguntas de Recuperação predefinidas.

Alternativamente, é possível adicionar um máximo de três perguntas personalizadas à lista a partir da qual o utilizador escolhe.

Para guardar as Perguntas de recuperação, clique em **Aplicar**.

Configurar a autenticação através da digitalização de impressão digital

Para configurar a autenticação através da Digitalização de impressão digital:

No painel do lado esquerdo, em Autenticação, selecione **Impressões digitais**.

Em Inscrições, defina o número mínimo e máximo de dedos que um utilizador pode inscrever.

Defina a sensibilidade do digitalizador de impressões digitais.

Quanto menor a sensibilidade, maior a variância de aceitação e a probabilidade de aceitação de uma digitalização falsa. Contudo, com uma definição elevada, o sistema poderá rejeitar impressões digitais legítimas. A definição de maior sensibilidade reduz a taxa de falsa aceitação em 1 para 10 mil digitalizações.

Para remover todas as digitalizações de impressão digital e inscrições de credenciais do leitor de impressão digital, clique em **Limpar leitor**. Isto remove apenas os dados que está a adicionar no momento. Não elimina digitalizações e inscrições armazenados em sessões anteriores.

Para guardar as definições, clique em **Aplicar**.

Configurar a autenticação de palavra-passe monouso

: A funcionalidade de Palavra-passe monouso (OTP) requer que um TPM esteja presente, ativado e tenha proprietário. Para obter instruções sobre a configuração do TPM, consulte Configuração de pré-instalação para palavra-passe monouso.

Para utilizar a funcionalidade Palavra-passe monouso, o utilizador gera uma Palavra-passe monouso com a aplicação Security Tools Mobile no dispositivo móvel e, em seguida, introduz a palavra-passe no computador. A palavra-passe só pode ser utilizada uma vez e é válida durante um período de tempo limitado.

Para reforçar a segurança, o administrador pode certificar-se de que a aplicação móvel é segura solicitando uma palavra-passe.

Na página Dispositivo móvel, pode configurar definições que aumentam ainda mais a segurança do dispositivo móvel e da Palavra-passe monouso.

Para configurar a autenticação de Palavra-passe Monouso:

No painel esquerdo, em Autenticação, selecione **Dispositivo Móvel**.

Para que seja solicitada ao utilizador a introdução de uma palavra-passe para aceder à aplicação Security Tools Mobile no dispositivo móvel, selecione **Exigir palavra-passe**.

: A ativação da política *Exigir palavra-passe* após a inscrição dos dispositivos móveis num computador resulta na anulação da inscrição de todos os dispositivos móveis. Será solicitado aos utilizadores que voltem a inscrever os seus dispositivos móveis depois da ativação da política.

Quando a caixa de verificação **Exigir palavra-passe** é selecionada, os utilizadores devem desbloquear o respetivo dispositivo móvel para aceder à aplicação Security Tools Mobile. Se não existir um bloqueio de dispositivo no dispositivo móvel, será solicitada a palavra-passe.

Para especificar o comprimento da Palavra-passe monouso (OTP), em **Comprimento da palavra-passe monouso**, selecione o número de caracteres da palavra-passe a exigir.

Para especificar o número de hipóteses que o utilizador tem para introduzir a Palavra-passe monouso corretamente, em **Tentativas de início de sessão do utilizador permitidas**, selecione um número entre **5** e **30**.

Quando o número máximo de tentativas for atingido, a funcionalidade OTP será desativada até que o utilizador inscreva novamente o dispositivo móvel.

: A Dell recomenda a definição de pelo menos um outro método de autenticação, além da Palavra-passe Monouso.

Configurar a inscrição de smart card

O DDP|Security Tools suporta dois tipos de smart cards: de contacto e sem contacto.

Os cartões de contacto necessitam de um leitor de smart cards para inserir o cartão. Os cartões de contacto são apenas compatíveis com computadores do domínio. Os cartões CAC e SIPRNet são cartões de contacto. Devido à natureza avançada destes cartões, o utilizador será obrigado a escolher um certificado depois de inserir o seu cartão para iniciar a sessão.

Os cartões sem contacto são suportados por computadores sem domínio e por computadores configurados com especificações de domínio.

Os utilizadores podem inscrever um smart card de contato por conta de utilizador, ou vários cartões sem contacto por conta.

Os smart cards não são suportados com Autenticação de pré-arranque.

: Ao remover a inscrição de um smart card de uma conta com vários cartões inscritos, todos os cartões terão a sua inscrição cancelada ao mesmo tempo.

Para configurar a inscrição de smart card:

No separador Autenticação da ferramenta Definições do administrador, selecione **Smartcard**.

Configurar permissões avançadas

Clique em **Avançado** para modificar as opções avançadas do utilizador final. Em *Avançadas*, pode, opcionalmente, permitir que os utilizadores efetuem a autoinscrição das respetivas credenciais ou modifiquem as credenciais inscritas e ativar o início de sessão de passo único.

Selecione ou limpe as caixas de verificação:

Permitir que os utilizadores inscrevam credenciais - Por predefinição, a caixa de verificação está selecionada. Os utilizadores podem inscrever credenciais sem a intervenção de um administrador. Se limpar esta caixa de verificação, as credenciais necessitam ser inscritas pelo administrador.

Permitir que o utilizador altere as credenciais inscritas - Por predefinição, a caixa de verificação está selecionada. Quando selecionada, os utilizadores podem modificar ou eliminar as suas credenciais inscritas sem a intervenção de um administrador. Se limpar esta caixa de verificação, as credencias deixam de poder ser alteradas ou eliminadas por um simples utilizador, mas precisam ser alteradas ou eliminadas pelo administrador.

: Para inscrever as credenciais de um utilizador, aceda à página *Utilizadores* da ferramenta Definições de administrador, selecione um utilizador e clique em Inscrever.

Permitir início de sessão de passo único - O início de sessão de passo único é o Início de sessão único (SSO). Por predefinição, a caixa de verificação está selecionada. Quando esta funcionalidade é ativada, os utilizadores precisam introduzir as respetivas credencias apenas no ecrã de Autenticação de pré-arranque. Os utilizadores iniciam a sessão automaticamente no Windows. Se desmarcar a caixa de verificação, o utilizador poderá ter de iniciar sessão várias vezes.

: Esta opção não pode ser selecionada, exceto se a definição Permitir que os utilizadores inscrevam credenciais também seja selecionada.

Clique em **Aplicar** quando tiver terminado.

Gerir autenticação do utilizador

Os controlos no separador Autenticação de Definições do Administrador permitem definir opções de início de sessão do utilizador e personalizar as configurações para cada um.

Para gerir a autenticação do utilizador:

1 Enquanto administrador, clique no mosaico **Definições de administrador**.
2 Clique no separador **Utilizadores** para gerir e ver o estado de inscrição dos utilizadores. A partir deste separador, pode:
   - Inscrever novos utilizadores
   - Adicionar ou alterar credenciais
   - Remover credenciais de um utilizador

NOTA:

O campo **Iniciar sessão**e **Sessão**indicam o estado de inscrição de um utilizador.

Quando o estado **Iniciar sessão**está definido para **OK**, todas as inscrições de que o utilizador precisa para iniciar sessão foram concluídas. Quando o estado de **Sessão**está definido **OK**, todas as inscrições de que o utilizador precisa para utilizar o Password Manager foram concluídas.

Se um dos estados está definido para **Não**, significa que o utilizador precisa de concluir inscrições adicionais. Para ver as inscrições em falta, selecione a ferramenta **Definições de administrador** e abra o separador **Utilizadores**. As caixas com marcas de verificação cinzentas indicam inscrições incompletas. Em alternativa, clique no mosaico **Inscrições** e analise a coluna **Política** do separador **Estado**, onde são indicadas as inscrições obrigatórias.

Adicionar novos utilizadores

: Quaisquer novos utilizadores do Windows serão adicionados automaticamente quando iniciarem uma sessão no Windows ou inscreverem credenciais.

Clique em **Adicionar utilizador**para iniciar o processo de inscrição de um utilizador do Windows existente.

Quando for apresentada a caixa de diálogo *Selecionar utilizadores*, selecione o **Tipos de objeto**.

Introduza um nome de objeto de utilizador na caixa de texto e clique em **Verificar nomes**.

Clique em **OK** quando tiver terminado.

É aberto o assistente de Inscrição.

Continue para Inscrever ou alterar credenciais do utilizador para obter instruções.

Inscrever ou alterar credenciais do utilizador

O administrador pode inscrever ou alterar as credenciais de um utilizador, se solicitado pelo mesmo. No entanto, algumas atividades de inscrição necessitam da presença do utilizador como, por exemplo, responder a questões de recuperação e digitalizar as suas impressões digitais.

Para inscrever ou alterar credenciais de utilizador:

Em Definições de administrador, clique no separador **Utilizadores**.

Na página Utilizadores, clique em **Inscrever**.

Na página de Boas-vindas, clique em **Seguinte**.

Na caixa de diálogo Autenticação necessária, inicie sessão com a palavra-passe do Windows do utilizador e clique em **OK**.

Na página Palavra-passe, para alterar a palavra-passe do Windows do utilizador, introduza e confirme uma nova palavra-passe e clique em **Seguinte**.

Para ignorar a alteração da palavra-passe, clique em **Ignorar**. O assistente permite-lhe ignorar credenciais que não pretende inscrever. Para regressar a uma página, clique em **Anterior**.

Siga as instruções apresentadas em cada página e clique no botão adequado: **Seguinte**, **Ignorar** ou **Retroceder**.

Na página Sumário, confirme as credenciais inscritas e, uma vez terminado a inscrição, clique em **Aplicar**.

Para regressar a uma página de inscrição de credenciais de modo a fazer alterações, clique em **Anterior** até chegar à página em que deseja alterar os dados.

Para mais informação detalhada sobre a inscrição de uma credencial ou para alterar uma credencial, consulte o *Manual do utilizador da Consola*.

Remover uma credencial inscrita

Clique no mosaico **Definições do Administrador**.

Clique no separador **Utilizadores** e selecione o utilizador que deseja mudar.

Coloque o rato por cima da marca de verificação da credencial que pretende remover. Transforma-se em ⊗.

Clique no símbolo ⊗ e, em seguida, clique em **Sim** para confirmar a eliminação.

: Não é possível remover uma credencial desta forma quando esta é a única credencial inscrita do utilizador. Além disso, a Palavra-passe não pode ser removida com este método. Utilize o comando Remover para remover completamente o acesso de um utilizador ao computador.

Remover todas as credenciais inscritas de um utilizador

Clique no mosaico **Definições do Administrador**.

Clique no separador **Utilizadores** e selecione o utilizador que pretende remover.

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 sem ser novamente inscrito.

Desinstalar utilizando 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 Client Security Framework.
3 Desinstalar Advanced Authentication.

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 a partir da opção Adicionar/remover programas

Aceda a "Desinstalar um programa" no Painel de Controlo do Windows (**Iniciar** > **Painel de Controlo** > **Programas e Funcionalidades** > **Desinstalar um Programa.**).

Selecione o **Instalador do Dell Data Protection** e, com o botão esquerdo do rato, clique em **Alterar** para iniciar o Assistente de configuração.

Leia o ecrã de Boas-vindas e clique em **Seguinte**.

Siga as indicações para desinstalar e clique em **Concluir**.

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.

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

- 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 Personal Edition 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 cliente 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 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.
- 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 utilizando a Interface de Utilizador

Desinstalar a partir da Linha de Comandos

Desinstalar utilizando a Interface de Utilizador

Aceda a "Desinstalar um programa" no Painel de Controlo do Windows (**Iniciar** > **Painel de Controlo** > **Programas e Funcionalidades** > **Desinstalar um Programa.**).

Selecione **Encriptação** e, com o botão esquerdo do rato, clique em **Alterar** para iniciar o Assistente de configuração do Personal Edition.

Leia o ecrã de Boas-vindas e clique em **Seguinte**.

No ecrã de Instalação do Encryption Removal Agent, selecione uma das seguintes opções:

: 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**.

Na caixa de texto *Ficheiro de Cópia de Segurança*, introduza o caminho para a unidade de rede ou a localização do suporte multimédia amovível do ficheiro de cópia de segurança ou clique em **...** para procurar a localização. O formato do ficheiro é LSARecovery_[hostname].exe.

Introduza a sua palavra-passe de administrador de encriptação na caixa de texto Palavra-passe. Esta é a palavra-passe que foi configurada no Assistente de configuração quando instalou ou software.

Clique em **Seguinte**.

No ecrã *Início de sessão do Dell Decryption Agent Service como*, existem duas opções. Selecione **Conta do sistema local**. Clique em **Concluir**.

Clique em **Remover** no ecrã Remover o programa.

Clique em **Concluir** no ecrã Configuração concluída.

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 a partir 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 padrão .msi 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 – Silenciosa 0 – Não silenciosa
DA_KM_PW	A palavra-passe da conta de Administrador de 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 cliente Advanced Authentication

Selecione um método de desinstalação

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

Desinstalar utilizando a Interface de Utilizador
Desinstalar a partir da Linha de Comandos

Desinstalar utilizando a Interface de Utilizador

Aceda a "Desinstalar um programa" no Painel de Controlo do Windows (**Iniciar** > **Painel de Controlo** > **Programas e Funcionalidades** > **Desinstalar um Programa.**).

Selecione **Autenticação de Security Tools** e, com o botão esquerdo do rato, clique em **Alterar** para iniciar o Assistente de configuração.

Leia o ecrã de Boas-vindas e clique em **Seguinte**.

Introduza a Palavra-passe do Administrador.

Siga as indicações para desinstalar e clique em **Concluir**.

Reinicie o computador e inicie sessão no Windows.

A Autenticação de Security Tools está desinstalada.

Desinstalar a partir da Linha de Comandos

Uma vez extraído a partir do instalador principal, o instalador do cliente Advanced Authentication pode estar localizado em **C:\extracted \Security Tools\Authentication\<x64/x86>\setup.exe**.

O seguinte exemplo desinstala o cliente Advanced Authentication de forma silenciosa.

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

Encerre e reinicie o computador quando concluído.

Avance para Descrições de políticas e modelos.

Desinstalar o Client Security Framework

Selecione um método de desinstalação

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

Desinstalar utilizando a Interface de Utilizador
Desinstalar a partir da Linha de Comandos

Desinstalar utilizando a Interface de Utilizador

Aceda a "Desinstalar um programa" no Painel de Controlo do Windows (**Iniciar** > **Painel de Controlo** > **Programas e Funcionalidades** > **Desinstalar um Programa.**).

Selecione **Client Security Framework** e, com o botão esquerdo do rato, clique em **Alterar** para iniciar o Assistente de configuração.

Leia o ecrã de Boas-vindas e clique em **Seguinte**.

Siga as indicações para desinstalar e clique em **Concluir**.

Reinicie o computador e inicie sessão no Windows.

O Cliente Security Framework está desinstalado.

Desinstalar a partir da Linha de Comandos

Uma vez extraído a partir do instalador principal, o instalador do cliente Client Security Framework pode estar localizado em **C:\extracted\Security Tools\EMAgent_**.

O seguinte exemplo desinstala o cliente SED de forma silenciosa.

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

Encerre e reinicie o computador quando concluído.

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 implica que todos os dados não encriptados por outras políticas de encriptação inteligentes serão 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, 3DES
Regras de encriptação SDE										As regras de encriptação a utilizar para encriptar/não encriptar determinadas unidades, diretórios e pastas. Contacte o Dell ProSupport para obter ajuda em caso de dúvidas acerca da alteração dos valores predefinidos.
Políticas de definições gerais										

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
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 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.

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 comum	AES256									AES 256, Rijndael 256, AES 128, Rijndael 128, 3DES 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. 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, frontpg.exe, powerpnt.exe, msaccess.exe, wordpad.exe, mspaint.exe, excel.exe Os nomes de processos do sistema e instalador codificados pelo hardware que

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
										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 deve poder aceder aos ficheiros encriptados pela Lista de encriptação de dados da aplicação e onde. Comum, se pretender 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 sejam encriptados com o Algoritmo de encriptação comum. Utilizador, se pretender 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

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
										com a Chave de encriptação de dados do utilizador
Encriptar ficheiros temporários da Internet	Verdadeiro	Falso								Verdadeiro encripta o caminho listado na variável do ambiente CSIDL_INTERNET_CACHE com a Chave de User Data Encryption. 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. 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 só é iniciado depois de o utilizador ter iniciado a 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

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
										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. Não serão iniciados os Serviços geridos se for iniciada a sessão por um utilizador não gerido.
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.

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
Ficheiro de hibernação do Windows seguro	Verdadeiro					Falso		Verdadeiro	Falso	Quando ativado, o ficheiro de hibernação é encriptado apenas quando 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 encriptar com a Chave de encriptação de dados do utilizador ou a excluir 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 multimédia externos cujos tipos sejam apresentados como Disco amovível; em alternativa, utilize Encriptar suporte multimédia externo do EMS.
Algoritmo de encriptação do utilizador	AES256									AES 256, Rijndael 256, AES 128, Rijndael 128, 3DES Algoritmo de encriptação utilizado para encriptar os

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 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 deve poder 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 Selecionar: · Comum se pretender 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 se pretender que estes ficheiros estejam acessíveis apenas ao utilizador que os criou no endpoint em que foram criados (o mesmo nível de acesso que as Pastas encriptadas do utilizador) e encriptados com o Algoritmo de encriptação do utilizador.

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
										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)										
Acelerador criptográfico de hardware (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 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. Especifique que volume(s) se destina(m) a encriptação.
Metadados forenses disponíveis na unidade encriptada 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) da instalação do Shield atual. Quando o valor for Falso, os metadados forenses não são incluídos na unidade. Mudar de Falso para Verdadeiro aciona um novo

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
										varrimento, com base nas políticas HCA, 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 como Desativar, não são aplicadas quaisquer políticas do Sistema de controlo de portas, independentemente de outras políticas do Sistema de controlo de portas. **Nota**: as políticas de PCS requerem um reinício para que a política tenha efeito.
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.

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
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. Consulte Interações com EMS e PCS. 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 unidade ótica	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. Acesso total: a Porta da Unidade Ótica não tem

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
										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 com EMS e PCS.
Subclasse de armazenamento: Controlo da Unidade de Disquete	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. 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.

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
										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. 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

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
										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. Esta política tem interações com PCS. Consulte Interações com EMS e PCS.
EMS: Excluir encriptação de CD/DVD	Falso								Verdadeiro	Falso encripta dispositivos de CD/DVD. Esta política tem interações com PCS. Consulte Interações com EMS e PCS.
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 com EMS e PCS. 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

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
										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 poderá ler nem eliminar os ficheiros existentes no armazenamento amovível não encriptado, mas o cliente não irá permitir que nenhum ficheiro seja editado ou adicionado ao armazenamento amovível, a não ser que seja encriptado.
EMS: Algoritmo de encriptação	AES256									AES 256, Rijndael 256, AES 128, Rijndael 128, 3DES
EMS: Analisar suporte multimédia externo	Verdadeiro	Falso								Verdadeiro permite que o EMS analise o armazenamento amovível de cada vez que é introduzida uma unidade de armazenamento amovível. Quando esta política é definida como Falso e a política EMS de Encriptar suporte multimédia externo é definida como Verdadeira, o EMS encripta apenas os ficheiros novos e alterados. Ocorre uma análise a cada inserção de modo a que o EMS possa detetar quaisquer ficheiros adicionados ao armazenamento amovível sem autenticação. É possível adicionar ficheiros ao armazenamento amovível se recusar a autenticação, mas não é possível o acesso a dados encriptados. Os ficheiros adicionados não serão encriptados neste caso,

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
										pelo que da próxima vez que autenticar o armazenamento amovível para trabalhar com dados encriptados, o EMS analisa-o e encripta quaisquer ficheiros que possam ter sido adicionados sem encriptação.
EMS: Aceder dados encriptados num dispositivo desprotegido	Verdadeiro									Verdadeiro permite ao utilizador aceder a 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 externos a excluir da proteção do EMS Quaisquer dispositivos de suporte multimédia externos que não estejam nesta lista serão 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 protegido. 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 minúsculas necessárias na palavra-passe	Verdadeiro	Falso								Verdadeiro requer, pelo menos, uma letra maiúscula e uma letra minúscula na palavra-passe.
Número de caracteres EMS necessário	8					6		8		1-40 caracteres Número de caracteres mínimo obrigatório na palavra-passe.

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
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.
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.

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 dispositivos de armazenamento que incorporem ligações multi-interface, tais como Firewire, USB, eSATA, etc., poderão exigir a utilização do EMS 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 EMS.
EMS: Bloquear o acesso a suporte multimédia não protegível	Verdadeiro								Falso	Bloqueia o acesso a qualquer unidade de armazenamento amovível com menos de 17 MB e, por conseguinte, com capacidade de armazenamento insuficiente para acolher um Removable Media Shield (proteção de suporte multimédia amovível) (tal como uma disquete de 1,44 MB). O acesso ilimitado é bloqueado se a opção Encriptar suporte multimédia externo e esta política tiverem ambas o valor Verdadeiro. Se Encriptar suporte multimédia externo tiver o valor Verdadeiro, mas esta política tiver o valor Falso, é possível ler os dados a partir da unidade de armazenamento amovível não encriptável, mas o acesso de escrita ao suporte multimédia é bloqueado. Se Encriptar suporte multimédia externo tiver o valor Falso, esta política não surte qualquer efeito e o acesso ao armazenamento amovível não encriptável não sofre qualquer impacto.
Políticas de controlo de experiência do utilizador										
Forçar reinício nas	Verdadeiro								Falso	Definir o valor para Verdadeiro faz com que o computador reinicie imediatamente para

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
atualizações										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.
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 no ícone do tabuleiro do sistema que lhe permite interromper/retomar a encriptação/desencriptação (dependendo do que o Shield está a fazer no momento). **NOTA: Permitir que um utilizador interrompa a encriptação poderá permitir ao utilizador impedir que o Shield 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 só processa os dados quando o ecrã está bloqueado.

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
										Opcional do utilizador adiciona uma opção ao ícone do tabuleiro do sistema permitindo ao utilizador ativar ou desativar esta função. Quando o valor for 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 armazenamento amovíveis e impede a utilização de dispositivos de armazenamento amovíveis 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 armazenamento amovíveis.
- 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 armazenamento amovíveis.
- 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 armazenamento amovíveis.
- 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 armazenamento amovíveis.
- 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 armazenamento amovíveis.

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 armazenamento amovíveis.

Proteção básica para unidades externas

O modelo de política:

fornece proteção para dispositivos de armazenamento amovíveis.

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).

Avance para Configuração de pré-instalação para palavra-passe monouso.

10

Configuração de pré-instalação para palavra-passe monouso

Estas funcionalidades do Personal Edition precisam de ser configuradas **antes** de dar início à instalação.

Inicializar o TPM

- Tem de ser membro do grupo local de Administradores ou equivalente.
- O computador tem de estar equipado com um BIOS e um TPM compatíveis.

Esta tarefa é necessária se utilizar a Palavra-passe monouso (OTP).

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

Extrair os Instaladores Subordinados do Instalador Principal

- 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 multimédia de instalação Dell, copie o ficheiro`DDPSetup.exe` para o computador local.

2 Abra uma linha de comandos na mesma localização do ficheiro`DDPSetup.exe` e introduza:

```
DDPSetup.exe /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

Resolução de problemas

Atualização para o Windows 10 Anniversary Update

Os computadores instalados com Encryption devem utilizar um pacote Windows 10 Upgrade especificamente configurado para atualizarem para o Windows 10 Anniversary Update. A versão configurada do pacote atualizado garante que a Dell Data Protection consegue gerir o acesso aos seus ficheiros encriptados para protegê-los contra danos durante o processo de atualização.

Para atualizar para a versão Windows 10 Anniversary, siga as instruções indicadas no seguinte artigo:

http://www.dell.com/support/article/us/en/19/SLN298382

Resolução de problemas do Encryption Client

Atualização para o Windows 10 Anniversary

Para atualizar para a versão de atualização do Windows 10 Anniversary, siga as instruções apresentadas no artigo seguinte: http://www.dell.com/support/article/us/en/19/SLN298382.

(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 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 com EMS e PCS

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

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

Para encriptar os dados gravados em CD/DVD

- Defina EMS: Encriptar suporte multimédia externo = Verdadeiro.
- Definir EMS: excluir encriptação de CD/DVD = Falso.
- 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 Client, 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.

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 no menu pendente: *Todas as unidades, Unidades fixas*, *Unidades amovíveis* ou *CDROM/ DVDROM*.

5 Selecione o Tipo de relatório de encriptação pretendido no menu pendente: *Ficheiros encriptados*, *Ficheiros desencriptados*, *Todos os ficheiros* ou *Ficheiros desencriptados em violação*:

   - *Ficheiros encriptados* - Para assegurar que todos os dados são desencriptados quando desinstalar o Encryption Client. 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 na caixa pendente será 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 de encriptação 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

Saída	Significado
	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 cliente Encryption continua instalado, continua configurado, ou ambos. A desencriptação não será iniciada antes de o cliente Encryption ser 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 resolução de problemas, defina a verbosidade do registo para 2 e reinicie o serviço de 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 no próximo reinício.

Como encriptar um iPod com o EMS

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.

- Não é recomendada a utilização do iPod Shuffle, uma vez que podem ocorrer resultados inesperados.
- À medida que os iPods mudam, esta informação também poderá mudar, por isso, é aconselhada cautela ao permitir a utilização de iPods em computadores ativados com EMS.
- Uma vez que os nomes das pastas nos iPods dependem do modelo de iPod, recomendamos 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 EMS não torna o dispositivo inutilizável, introduza as seguintes regras na política de Regras de encriptação para EMS:

  -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 support.dell.com.
2. Selecione o modelo do seu computador.
3. Selecione **Controladores e transferências**.
4. Selecione o **Sistema operativo** do computador de destino.
5. Expanda 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

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

Clique duas vezes no controlador do Dell ControlVault para iniciar o ficheiro executável de extração automática.

:

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

Clique em **Continuar** para iniciar.

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

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

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

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**.

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)].

Clique em **Seguinte** no ecrã de boas-vindas.

Clique em **Seguinte** para instalar os controladores na localização predefinida de C:\Program Files\Broadcom Corporation\Broadcom USH Host Components\.

Selecione a opção **Completo** e clique em **Seguinte**.

Clique em **Instalar** para iniciar a instalação dos controladores.

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.

:

No caso de atualização a partir de uma versão mais antiga de firmware, ser-lhe-á pedida 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.

Cliente de encriptação

(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 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 utilizar smart cards com Autenticação do Windows, o valor de registo seguinte deve ser configurado no computador cliente.

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

"MSSmartcardSupport"=dword:1

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 Encryption apresenta o aviso de *duração de cada atraso da atualização de política* a cada cinco minutos. 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 irá alterar a ação predefinida para suspensão. Quando não houver interação do utilizador, o processamento da encriptação será 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 POLÍTICA PERMITIDOS × DURAÇÃO DE CADA ATRASO DE ATUALIZAÇÃO DE POLÍTICA) + (5 MINUTOS × [NÚMERO DE ATRASOS DE ATUALIZAÇÃO DE POLÍTICA PERMITIDOS - 1])

Alterar a utilização predefinida da chave SDUser

A Encriptação de Dados do Sistema (SDE) é aplicada com base no valor de política para Regras de Encriptação SDE. Por predefinição, os diretórios adicionais estão protegidos quando a política de Ativação de Encriptação SDE está Selecionada. Para mais informações, procure "Regras de Encriptação SDE" em Ajuda de Administração. Quando o cliente de Encriptação está a processar uma atualização de política que inclui uma política SDE ativa, o diretório de perfil de utilizador atual está encriptado por predefinição com a chave SDUser (uma chave de utilizador) em vez de com a chave SDE (uma chave de dispositivo). A chave SDUser é também utilizada para encriptar ficheiros ou pastas que são copiados (não movidos) para um diretório de utilizador que não é 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 será utilizada para encriptar estes diretórios de utilizador.

Cliente Advanced Authentication

Desativar Smart Card e serviços biométricos (opcional)

Se não pretender que Security Tools 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.

Com a funcionalidade desativada, o Security Tools não tentará iniciar os três serviços seguintes:

SCardSvr - Gere o acesso a smart cards lidos pelo computador. Se este serviço for interrompido, o computador deixará de poder ler smart cards. Se este serviço for desativado, não será 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 utilizar smart cards com Autenticação do Windows, o valor de registo seguinte deve ser configurado no computador cliente.

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

"MSSmartcardSupport"=dword:1

Avance para o Glossário.

13

Glossário

Advanced Authentication - O produto Advanced Authentication fornece opções de impressão digital, smart card e leitor de smart card sem contacto totalmente integradas. O Advanced Authentication ajuda a gerir estes múltiplos métodos de autenticação de hardware, suporta o início de sessão com unidades de encriptação automática, SSO e gere as credenciais e palavras-passe do utilizador. Adicionalmente, o Advanced Authentication pode ser utilizado para aceder não apenas a PCs, mas também a qualquer Web site, SaaS ou aplicação. Uma vez que os utilizadores inscrevem as suas credenciais, o Advanced Authentication permite a utilização dessas credenciais para iniciar sessão no dispositivo e realizar a substituição da palavra-passe.

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 caso seja preciso 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 Client utiliza a chave 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 Comum torna os ficheiros acessíveis a todos os utilizadores geridos no dispositivo em que foram criados. A chave de Utilizador torna os ficheiros acessíveis apenas ao utilizador que os criou, e apenas no dispositivo em que foram criados. A chave de Roaming de utilizador torna os ficheiros acessíveis apenas ao utilizador que os criou, em qualquer dispositivo Windows (ou Mac) protegido.

Varrimento de encriptação - Um varrimento de encriptação é o processo de análise das pastas a serem encriptadas num endpoint protegido 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, como se segue: - Um varrimento de encriptação irá ocorrer 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 Estação de trabalho de análise na Política de início de sessão está ativada, as pastas especificadas para a encriptação serão 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), acionará um varrimento. Adicionalmente, a alternância entre a encriptação ativada e desativada irá acionar um varrimento de encriptação.

Palavra-Passe monouso (OTP) - Uma palavra-passe monouso é uma palavra-passe que apenas pode ser utilizada uma vez e que é válida por um período de tempo limitado. A OTP requer que o TPM esteja presente, ativado e tenha proprietário. Para ativar a palavra-passe monouso (OTP), um dispositivo móvel é emparelhado com o computador que está a utilizar a Consola de segurança e a aplicação Security Tools Mobile. A aplicação Security Tools Mobile gera a palavra-passe no dispositivo móvel que é utilizado para iniciar sessão no computador no ecrã de início de sessão do Windows. Com base na politica, a funcionalidade OTP pode ser utilizada para recuperar o acesso ao computador se uma palavra-passe expirou ou foi esquecida, se a OTP não foi utilizada para iniciar sessão no computador. A funcionalidade OTP pode ser utilizada para autenticação ou recuperação, mas não para ambas. A segurança da OTP excede a de outros métodos de autenticação, uma vez que a palavra-passe gerada apenas pode ser utilizada uma vez e expira num curto período de tempo.

Autenticação de pré-arranque (PBA) - A Autenticação de pré-arranque funciona como uma extensão do BIOS ou do firmware de arranque e garante um ambiente seguro, à prova de adulteração e exterior 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 de 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 encriptação SDE, é iniciada a desencriptação automática de todos os diretórios e ficheiros encriptados pela SDE para os utilizadores aplicáveis, independentemente de outras políticas 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. O TPM é também necessário para utilização com a funcionalidade de Palavra-passe monouso.