

Dell Data Protection

Guia de Recuperação para Encriptação de
Ficheiros/Pastas, Hardware Crypto Accelerator,
Unidades de Encriptação Automática (SEDs),
e Chave de Diretrizes Gerais

v8.10



© 2016 Dell Inc.

Marcas comerciais registradas e marcas comerciais utilizadas nos conjuntos de documentos Dell Data Protection | Encryption, Dell Data Protection | Endpoint Security Suite, Dell Data Protection | Endpoint Security Suite Enterprise, Dell Data Protection | Security Tools, e Dell Data Protection | Cloud Edition: Dell™ e o logótipo da Dell, Dell Precision™, OptiPlex™, ControlVault™, Latitude™, XPS® e KACE™ são marcas comerciais da Dell Inc. Cylance® e o logótipo Cylance são marcas comerciais registradas da Cylance, Inc. nos Estados Unidos e noutros países. McAfee® e o logótipo da McAfee são marcas comerciais ou marcas comerciais registradas da McAfee, Inc. nos Estados Unidos e noutros países. Intel®, Pentium®, Intel Core Inside Duo®, Itanium® e Xeon® são marcas comerciais registradas da Intel Corporation nos Estados Unidos e noutros países. Adobe®, Acrobat®, e Flash® são marcas comerciais registradas da Adobe Systems Incorporated. Authen Tec® e Eikon® são marcas comerciais registradas da Authen Tec. AMD® é uma marca comercial registada da Advanced Micro Devices, Inc. Microsoft®, Windows® e Windows Server®, Internet Explorer®, MS-DOS®, Windows Vista®, MSN®, ActiveX®, Active Directory®, Access®, ActiveSync®, BitLocker®, BitLocker To Go®, Excel®, Hyper-V®, Silverlight®, Outlook®, PowerPoint®, OneDrive®, SQL Server® e Visual C++® são marcas comerciais ou marcas comerciais registradas da Microsoft Corporation nos Estados Unidos e/ou noutros países. VMware® é uma marca comercial registada ou marca comercial da VMware, Inc. nos Estados Unidos ou noutros países. Box® é uma marca comercial registada da Box. DropboxSM é uma marca de serviço da Dropbox, Inc. Google™, Android™, Google™ Chrome™, Gmail™, YouTube™ e Google™ Play são marcas comerciais ou marcas comerciais registradas da Google Inc. nos Estados Unidos e noutros países. Apple®, Aperture®, App StoreSM, Apple Remote Desktop™, Apple TV®, Boot Camp™, FileVault™, iCloud®SM, iPad®, iPhone®, iPhoto®, iTunes Music Store®, Macintosh®, Safari® e Siri® são marcas de serviço, marcas comerciais ou marcas comerciais registradas da Apple, Inc. nos Estados Unidos e/ou outros países. GO ID®, RSA®, e SecurID® são marcas comerciais registradas da EMC Corporation. EnCase™ e Guidance Software® são marcas comerciais ou marcas comerciais registradas da Guidance Software. Entrust® é uma marca comercial registada da Entrust®, Inc. nos Estados Unidos e noutros países. InstallShield® é uma marca comercial registada da Flexera Software nos Estados Unidos, China, União Europeia, Hong Kong, Japão, Taiwan e Reino Unido. Micron® e RealSSD® são marcas comerciais registradas da Micron Technology, Inc. nos Estados Unidos e noutros países. Mozilla® Firefox® é uma marca comercial registada da Mozilla Foundation nos Estados Unidos e/ou outros países. iOS® é uma marca comercial ou uma marca comercial registada da Cisco Systems, Inc. nos Estados Unidos e alguns outros países e é utilizada sob licença. Oracle® e Java® são marcas comerciais registradas da Oracle e/ou das respetivas filiais. Os outros nomes podem ser marcas comerciais dos respetivos proprietários. SAMSUNG™ é uma marca comercial da SAMSUNG nos Estados Unidos ou noutros países. Seagate® é uma marca comercial registada da Seagate Technology LLC nos Estados Unidos e/ou noutros países. Travelstar® é uma marca comercial registada da HGST, Inc. nos Estados Unidos e noutros países. UNIX® é uma marca comercial registada da The Open Group. VALIDITY™ é uma marca comercial da Validity Sensors, Inc. nos Estados Unidos e noutros países. VeriSign® e outras marcas relacionadas são marcas comerciais ou marcas comerciais registradas da VeriSign, Inc. ou das respetivas filiais ou subsidiárias nos Estados Unidos e noutros países e licenciadas à Symantec Corporation. KVM on IP® é uma marca comercial registada da Video Products. Yahoo!® é uma marca comercial registada da Yahoo! Inc.

Este produto utiliza partes do programa 7-Zip. O código-fonte encontra-se disponível em www.7-zip.org. O licenciamento é efetuado ao abrigo da licença GNU LGPL + restrições unRAR (www.7-zip.org/license.txt).

2016-07

Protegido por uma ou mais patentes dos Estados Unidos, incluindo: Número 7665125; Número 7437752; e Número 7665118.

As informações contidas neste documento estão sujeitas a alterações sem aviso prévio.

Índice

1	Introdução	5
2	Recuperação de Encriptação de Ficheiro/Pasta	7
	Requisitos de Recuperação	7
	Visão Geral do Processo de Recuperação	7
	Realizar Recuperação FFE	8
	Obter o Ficheiro de Recuperação - Computador Gerenciado Remotamente	8
	Obter o Ficheiro de Recuperação - Computador Gerenciado Localmente	9
	Realizar uma Recuperação	9
3	Recuperação do Hardware Crypto Accelerator	11
	Requisitos de Recuperação	11
	Visão Geral do Processo de Recuperação	11
	Realizar a Recuperação do HCA	12
	Obter o Ficheiro de Recuperação - Computador Gerenciado Remotamente	12
	Obter o Ficheiro de Recuperação - Computador Gerenciado Localmente	13
	Realizar uma Recuperação	13
4	Recuperação de Unidade de encriptação automática (SED)	15
	Requisitos de Recuperação	15
	Visão Geral do Processo de Recuperação	15
	Realizar a Recuperação da SED	16
	Obter o Ficheiro de Recuperação - Cliente SED Gerenciado Remotamente	16
	Obter o Ficheiro de Recuperação - Cliente SED Gerenciado Remotamente	16
	Realizar uma Recuperação	16
5	Recuperação da Chave de Diretrizes Gerais	17
	Recuperar a GPK	17
	Obter o Ficheiro de Recuperação	17
	Realizar uma Recuperação	18

6	Recuperação de Dados de Unidade Encriptada	19
	Recuperar Dados de Unidades Encriptadas	19
7	Recuperação do BitLocker Manager	21
	Recuperar dados	21
	Apêndice A - Gravação do ambiente de recuperação	23
	Gravação do ambiente de recuperação ISO para CD/DVD	23
	Gravação do ambiente de recuperação no suporte de dados amovível	23

Introdução

Esta secção descreve o que é necessário para criar o ambiente de recuperação.

- Cópia do software do ambiente de recuperação transferida - localizada na pasta Kit de Recuperação do Windows no suporte de dados de instalação do Dell Data Protection
- CD-R, DVD-R ou suporte de dados USB formatado
 - Se gravar um CD ou DVD, reveja [Apêndice A - Gravação do ambiente de recuperação](#) para obter mais informações.
 - Se utilizar um suporte de dados USB, reveja [Apêndice A - Gravação do ambiente de recuperação](#) para obter mais informações.
- Pacote de recuperação para dispositivo falhado
 - Para clientes geridos remotamente, as instruções seguintes explicam como obter um pacote de recuperação a partir do seu Dell Data Protection Server.
 - Para clientes geridos localmente, o conjunto do pacote de recuperação foi criado durante a configuração numa unidade de rede partilhada ou num suporte de dados externo. Localize este conjunto antes de prosseguir.

Recuperação de Encriptação de Ficheiro/Pasta

Com a recuperação de Encriptação de Ficheiro/Pasta (FFE), poderá recuperar o acesso ao que se segue:

- Um computador que não inicie e que disponibilize a linha de comandos para realizar recuperação SDE.
- Um computador no qual não possa aceder a dados encriptados ou políticas de edição.
- Um servidor executando Dell Data Protection | Server Encryption que cumpra quaisquer das condições precedentes.
- Um computador no qual a placa]Hardware Crypto Accelerator ou a placa-mãe/TPM deva ser substituída.

Requisitos de Recuperação

Para recuperação FFE, necessita do seguinte:

- Kit de Recuperação do Windows para criar um disco de arranque especial - O kit contém ficheiros que serão utilizados para criar uma imagem do Windows PE (WinPE) e personalizá-la com software e controladores do Dell Data Protection. O kit está localizado na pasta Kit de Recuperação do Windows, no suporte multimédia de instalação do Dell Data Protection.

Visão Geral do Processo de Recuperação

Para recuperar um sistema que tenha falhado:

- 1 Crie a ISO de Recuperação e grave-a num CD/DVD ou crie um USB de arranque. Consulte [Apêndice A - Gravação do ambiente de recuperação](#).
- 2 Obtenha o ficheiro de Recuperação.
- 3 Realize a recuperação.

Realizar Recuperação FFE

Siga estes passos para realizar uma recuperação FFE.

Obter o Ficheiro de Recuperação - Computador Gerenciado Remotamente

Para fazer download do ficheiro `LSARecovery_<machinename_domain>.exe`:

- 1 Abra a Remote Management Console e, no painel esquerdo, selecione **Gestão > Recuperar Endpoint**.
- 2 No campo Nome de Anfitrião, introduza o nome de domínio completamente qualificado do endpoint e clique em **Procurar**.
- 3 Na janela Recuperação melhorada, introduza uma Palavra-passe de recuperação e clique em **Transferir**.

NOTA: Terá de recordar esta palavra-passe para aceder às chaves de recuperação.

- 4 Copie o ficheiro `LSARecovery_<machinename_domain>.exe` para um local onde possa ser acedido quando inicializado em WinPE.

Obter o Ficheiro de Recuperação - Computador Gerenciado Localmente

Para obter o ficheiro de recuperação da Personal Edition:

- 1 Localize o ficheiro de recuperação com o nome **LSAReccovery_<systemname>.exe**. Este ficheiro foi guardado numa unidade de rede ou armazenamento amovível quando executou o Assistente de configuração ao instalar o Personal Edition.
- 2 Copie o ficheiro **LSAReccovery_<systemname>.exe** para o computador de destino (o computador para recuperar dados).

Realizar uma Recuperação

- 1 Utilizando o suporte de dados de arranque criado anteriormente, arranque num sistema de recuperação ou no dispositivo onde se encontra a unidade que está a tentar recuperar. Será aberto um Ambiente WinPE.
- 2 Introduza **x** e pressione **Enter** para obter uma linha de comandos.
- 3 Navegue até ao ficheiro de recuperação e inicie-o.
- 4 Selecione uma opção:
 - O meu sistema não inicia e apresenta uma mensagem a solicitar a execução de uma recuperação de SDE. Isto irá permitir reconstruir as verificações de hardware que o Encryption Client realiza ao iniciar o SO.
 - O meu sistema não permite que aceda a dados encriptados ou edite políticas, ou está a ser reinstalado. Utilize se for necessário substituir a placa Hardware Crypto Accelerator ou a placa principal/TPM deve ser substituída.
- 5 Na caixa de diálogo Cópia de Segurança e Informação de Recuperação, confirme que a informação sobre o computador cliente a ser recuperado é correta e clique em **Seguinte**.
Ao recuperar computadores de outra marca que não a Dell, os campos Número de série e Etiqueta de serviço estarão em branco.
- 6 Na caixa de diálogo que lista os volumes do computador, selecione todas as unidades aplicáveis e clique em **Seguinte**.
Pressione Shift e clique ou pressione Control e clique para destacar várias unidades.
Se a unidade selecionada não estiver encriptada por FFE, não será possível efetuar a recuperação da mesma.
- 7 Introduza a sua palavra-passe de recuperação e clique em **Continuar**.
Com um cliente gerido remotamente, esta é a palavra-passe fornecida no [Etapa 3 em Obter o Ficheiro de Recuperação - Computador Gerenciado Remotamente](#).
No Personal Edition, a palavra-passe é a Palavra-passe de administrador de encriptação configurada para o sistema no momento em que as palavras-passe foram colocadas sob garantia.
- 8 Na caixa de diálogo Recuperar, clique em **Recuperar**. O processo de recuperação é iniciado.
- 9 Quando a recuperação estiver concluída, clique em **Concluir**.

NOTA: Certifique-se de que remove qualquer suporte de dados USB ou CD/DVD utilizado para arranque da máquina. O não cumprimento desta indicação poderá resultar no arranque para o ambiente de recuperação.

- 10 O computador deverá estar totalmente operacional após ser reinicializado. No caso do problema persistir, contacte o Dell ProSupport.

Recuperação do Hardware Crypto Accelerator

Com a Recuperação do Hardware Crypto Accelerator (HCA) do Dell Data Protection, pode recuperar o acesso a:

- Ficheiros numa unidade encriptada por HCA - Este método descripta a unidade utilizando as chaves fornecidas. Pode seleccionar a unidade específica que deseja descriptar durante o processo de recuperação.
- Uma unidade encriptada por HCA após uma substituição de hardware - Este método é utilizado após ter de substituir a placa do HCA (Hardware Crypto Accelerator) ou uma placa-mãe/TPM. Pode executar uma recuperação para adquirir novamente acesso aos dados encriptados sem descriptar a unidade.

Requisitos de Recuperação

Para a recuperação do HCA, necessita do seguinte:

- Acesso a um ambiente de recuperação ISO
- CD/DVD ou suporte de dados USB de arranque

Visão Geral do Processo de Recuperação

Para recuperar um sistema que tenha falhado:

- 1 Crie a ISO de Recuperação e grave-a num CD/DVD ou crie um USB de arranque. Consulte [Apêndice A - Gravação do ambiente de recuperação](#).
- 2 Obtenha o ficheiro de Recuperação.
- 3 Realize a recuperação.

Realizar a Recuperação do HCA

Siga estes passos para realizar uma recuperação do HCA.

Obter o Ficheiro de Recuperação - Computador Gerenciado Remotamente

Para transferir o ficheiro `LSARecovery_<machinename_domain.com>.exe` que foi gerado quando instalou o Dell Data Protection:

- 1 Abra a Remote Management Console e, no painel esquerdo, seleccione **Gestão > Recuperar Endpoint**.
- 2 No campo Nome de Anfitrião, introduza o nome de domínio completamente qualificado do endpoint e clique em **Procurar**.
- 3 Na janela Recuperação melhorada, introduza uma Palavra-passe de recuperação e clique em **Transferir**.

NOTA: Terá de recordar esta palavra-passe para aceder às chaves de recuperação.

O ficheiro `LSARecovery_<machinename_domain.com>.exe` é transferido.

Obter o Ficheiro de Recuperação - Computador Gerenciado Localmente

Para obter o ficheiro de recuperação da Personal Edition:

- 1 Localize o ficheiro de recuperação com o nome **LSAReccovery_<systemname>.exe**. Este ficheiro foi guardado numa unidade de rede ou armazenamento amovível quando executou o Assistente de configuração ao instalar o Personal Edition.
- 2 Copie o ficheiro **LSAReccovery_<systemname>.exe** para o computador de destino (o computador para recuperar dados).

Realizar uma Recuperação

- 1 Utilizando o suporte de dados de arranque criado anteriormente, arranque num sistema de recuperação ou no dispositivo onde se encontra a unidade que está a tentar recuperar.
Será aberto um Ambiente WinPE.
- 2 Digite **x** e pressione **Enter** para obter uma linha de comandos.
- 3 Navegue até ao ficheiro de recuperação guardado e inicie-o.
- 4 Selecione uma opção:
 - Quero descriptar a minha unidade encriptada HCA.
 - Quero restaurar o acesso à minha unidade encriptada HCA.
- 5 Na caixa de diálogo Cópia de segurança e Informações de recuperação, certifique-se de que a Etiqueta de serviço ou o Número do recurso estão corretos e clique em **Seguinte**.
- 6 Na caixa de diálogo que lista os volumes do computador, selecione todas as unidades aplicáveis e clique em **Seguinte**.
Pressione Shift e clique ou pressione Control e clique para destacar várias unidades.
Se a unidade selecionada não estiver encriptada por HCA, não será possível efetuar a recuperação da mesma.
- 7 Introduza a sua palavra-passe de recuperação e clique em **Continuar**.
Num computador gerenciado remotamente, esta é a palavra-passe fornecida no [Etapa 3](#) em [Obter o Ficheiro de Recuperação - Computador Gerenciado Remotamente](#).
Num computador gerido localmente, esta palavra-passe é a Palavra-passe de administrador de encriptação configurada para o sistema no Personal Edition no momento em que as palavras-passe foram colocadas sob garantia.
- 8 Na caixa de diálogo Recuperar, clique em **Recuperar**. O processo de recuperação é iniciado.
- 9 Quando solicitado, navegue até ao ficheiro de recuperação guardado e clique em **OK**.
Se está a realizar uma descriptação completa, a seguinte caixa de diálogo mostra o estado. Este processo poderá demorar algum tempo.
- 10 Quando a mensagem mostra a indicação de que a recuperação finalizou com êxito, clique em **Concluir**. O computador reinicializar-se-á.

O computador deverá estar totalmente operacional após ser reinicializado. No caso do problema persistir, contacte o Dell ProSupport.

Recuperação de Unidade de encriptação automática (SED)

Com a Recuperação da SED, pode recuperar o acesso a ficheiros numa SED através dos seguintes métodos:

- Realize o desbloqueamento da unidade uma única vez para ignorar e remover a Autenticação de Pré-Inicialização (PBA).
 - Com um cliente SED gerenciado remotamente, a PBA pode ser reativada mais tarde através da Remote Management Console.
 - Com um cliente SED gerenciado localmente, a PBA pode ser ativada através da Consola de Administração da Security Tools.
- Desbloqueie, e de seguida remova permanentemente a PBA da unidade. O Single Sign-On não funcionará com a PBA removida.
 - Com um cliente SED gerenciado remotamente, a remoção da PBA requerer-lhe-á a desativação do produto a partir da Remote Management Console se for necessário reativar a PBA no futuro.
 - Com um cliente SED gerenciado localmente, a remoção da PBA requerer-lhe-á a desativação do produto no interior do SO se for necessário reativar a PBA no futuro.

Requisitos de Recuperação

Para a recuperação da SED, necessita do seguinte:

- Acesso ao ambiente de recuperação ISO
- CD/DVD ou suporte de dados USB de arranque

Visão Geral do Processo de Recuperação

Para recuperar um sistema que tenha falhado:

- 1 Crie a ISO de Recuperação e grave-a num CD/DVD ou crie um USB de arranque. Consulte [Apêndice A - Gravação do ambiente de recuperação](#).
- 2 Obtenha o ficheiro de Recuperação.
- 3 Realize a recuperação.

Realizar a Recuperação da SED

Siga estes passos para realizar uma recuperação da SED.

Obter o Ficheiro de Recuperação - Cliente SED Gerenciado Remotamente

- 1 Obtenha o ficheiro de recuperação.

O ficheiro de recuperação pode ser transferido a partir da Remote Management Console. Para transferir o ficheiro `<hostname>-sed-recovery.dat` que foi gerado quando instalou o Dell Data Protection:

- a Abra a Remote Management Console e, no painel esquerdo, selecione **Gestão > Recuperar dados** e, em seguida, selecione o separador **SED**.
- b No ecrã Recuperação de dados, no campo Nome de anfitrião, introduza o nome de domínio completamente qualificado do endpoint e, em seguida, clique em **Procurar**.
- c No campo SED, selecione uma opção.
- d Clique em **Criar ficheiro de recuperação**.
O ficheiro `<hostname>-sed-recovery.dat` é transferido.

Obter o Ficheiro de Recuperação - Cliente SED Gerenciado Remotamente

- 1 Obtenha o ficheiro de recuperação.

O ficheiro foi gerado e está acessível a partir do local de cópia de segurança que selecionou ao instalar o Dell Data Protection | Security Tools no computador. O nome do ficheiro é `OpalSPkey<systemname>.dat`.

Realizar uma Recuperação

- 1 Utilizando o suporte de dados de arranque criado, arranque num sistema de recuperação ou no dispositivo onde se encontra a unidade que está a tentar recuperar. Abre-se um ambiente WinPE com a aplicação de recuperação.
- 2 Escolha uma opção e pressione **Enter**.
- 3 Selecione **Procurar**, localize o ficheiro de recuperação e, em seguida, clique em **Abrir**.
- 4 Selecione uma opção e clique em **OK**.
 - **Desbloqueio da unidade uma única vez** - Este método ignora e remove a PBA. Mais tarde, pode ser novamente ativado através da Remote Management Console (para um cliente SED gerenciado remotamente) ou através da Consola de Administrador da Security Tools (para um cliente SED gerenciado localmente).
 - **Desbloquear a unidade e remover a PBA** - Este método desbloqueia e, de seguida, remove permanentemente a PBA da unidade. A remoção da PBA requerer-lhe-á a desativação do produto a partir da Remote Management Console (para um cliente SED gerenciado remotamente) ou no interior do SO (para um cliente SED gerenciado localmente) se for necessário reativar a PBA no futuro. O Single Sign-On não funcionará com a PBA removida.
- 5 A recuperação está agora concluída. Pressione qualquer tecla para voltar ao menu.
- 6 Pressione **r** para reiniciar o computador.

NOTA: Certifique-se de que remove qualquer suporte USB ou CD/DVD utilizado para arranque do computador. O não cumprimento desta indicação poderá resultar no arranque para o ambiente de recuperação.

- 7 O computador deverá estar totalmente operacional após ser reinicializado. No caso do problema persistir, contacte o Dell ProSupport.

Recuperação da Chave de Diretrizes Gerais

A Chave de Diretrizes Gerais (GPK) é utilizada para criptografar parte do registo para utilizadores do domínio. No entanto, durante o processo de arranque, em casos raros, pode corromper-se e não abrir. Se é o caso, mostrar-se-ão os seguintes erros no ficheiro CMGShield.log

```
[12.06.13 07:56:09:622 GeneralPurposeK: 268] GPK - Failure while unsealing data [error = 0xd]
[12.06.13 07:56:09:622 GeneralPurposeK: 631] GPK - Unseal failure
[12.06.13 07:56:09:622 GeneralPurposeK: 970] GPK - Failure to get keys for the registry driver
```

Se a GPK não abrir, a GPK tem de ser recuperada extraíndo-a do pacote de recuperação que é obtido por download a partir do Servidor.

Recuperar a GPK

Obter o Ficheiro de Recuperação

Para transferir o ficheiro `LSARecovery_<machinename_domain.com>.exe` que foi gerado quando instalou o Dell Data Protection:

- 1 Abra a Remote Management Console e, no painel esquerdo, seleccione **Gestão > Recuperar Endpoint**.
- 2 No campo Nome de Anfitrião, introduza o nome de domínio completamente qualificado do endpoint e clique em **Procurar**.

- 3 Na janela Recuperação melhorada, introduza uma Palavra-passe de recuperação e clique em **Transferir**

NOTA: Terá de recordar esta palavra-passe para aceder às chaves de recuperação.

O ficheiro `LSARecovery_<machinename_domain.com>.exe` é transferido.

Realizar uma Recuperação

- 1 Utilizando o suporte de dados de arranque criado no [Apêndice A - Gravação do ambiente de recuperação](#), arranque num sistema de recuperação ou no dispositivo onde se encontra a unidade que está a tentar recuperar.
Será aberto um Ambiente WinPE.
- 2 Introduza `x` e pressione **Enter** para obter uma linha de comandos.
- 3 Navegue até ao ficheiro de recuperação e inicie-o.
Abre-se uma caixa de diálogo de diagnóstico do Encryption Client e o ficheiro de recuperação está a ser gerado em segundo plano.
- 4 Numa solicitação de comando administrativo, execute `LSARecovery_<machinename_domain.com>.exe -p <password> -gpk`
Devolve o `GPKRCVR.txt` para o seu computador.
- 5 Copie o ficheiro `GPKRCVR.txt` para a raiz da unidade do SO do computador.
- 6 Reinicie o computador.
O ficheiro `GPKRCVR.txt` será consumido pelo sistema operativo e regenerará a `GPK` nesse computador.
- 7 Se solicitado, reinicialize novamente.

Recuperação de Dados de Unidade Encriptada

Se não for possível efetuar o arranque do computador de destino e não existir qualquer falha de hardware, a recuperação de dados pode ser realizada no computador iniciado num ambiente de recuperação. Se o computador de destino não estiver inicializável e existir falha de hardware ou for um dispositivo USB, a recuperação de dados pode ser realizada por arranque numa unidade escrava. Ao tornar uma unidade em escrava, pode ver-se o sistema de ficheiros e pesquisar os diretórios. No entanto, se tentar abrir ou copiar um ficheiro, ocorre um erro *Acesso negado*.

Recuperar Dados de Unidades Encriptadas

Para recuperar dados de unidades encriptadas:

- 1** Para obter o ID de DCID/Recuperação a partir do computador, escolha uma opção:
 - a** Execute o WSScan em qualquer ficheiro onde estejam armazenados Dados encriptados comuns. A ID de recuperação/DCID de oito caracteres é apresentada depois de “Comum”.
 - b** Abra a Remote Management Console e seleccione o separador **Detalhes e ações** do endpoint.
 - c** Na secção Shield Detail do ecrã Endpoint Detail, localize a ID de recuperação/DCID.

- 2 Para fazer download da chave a partir do Servidor, navegue até e execute o utilitário Dell Administrative Unlock (CMGAu).
O utilitário Dell Administrative Unlock pode ser obtido a partir de Dell ProSupport.
- 3 Na caixa de diálogo do Dell Administrative Utility (CMGAu), insira a seguinte informação (alguns campos podem estar previamente preenchidos) e clique em **Seguinte**.

Servidor:	Nome de Anfitrião Completamente Qualificado do Servidor, por exemplo: Servidor do Dispositivo: https://<server.organization.com>:8081/xapi Security Server: https://<server.organization.com>:8443/xapi/
Dell Admin:	O nome da conta para o Administrador Forense (ativado no Servidor)
Palavra-passe do Admin Dell:	A palavra-passe da conta para o Administrador Forense (ativado no Servidor)
MCID:	Limpe o campo MCID
DCID:	A ID de recuperação/DCID que obteve anteriormente.
- 4 Na caixa de diálogo do Dell Administrative Utility, selecione **Não, transferir a partir de um servidor agora** e clique em **Seguinte**.

NOTA: Se o Encryption Client não estiver instalado, é apresentada uma mensagem com indicação de *Falha no desbloqueio*. Mude para um computador com o Encryption Client instalado.
- 5 Após completar o download e o desbloqueio, copie os ficheiros que deseja recuperar a partir desta unidade. Todos os ficheiros são legíveis. ***Não clique em Concluir até ter recuperado os ficheiros.***
- 6 Após ter recuperado os ficheiros e estar pronto para os bloquear novamente, clique em **Concluir**.
Após clicar em Concluir, os ficheiros encriptados já não estarão disponíveis.

Recuperação do BitLocker Manager

Para recuperar dados, deve obter uma palavra-passe de recuperação ou um pacote de chaves da Remote Management Console, o que lhe permite então desbloquear os dados do computador.

Recuperar dados

- 1 Como Administrador Dell, inicie sessão na Remote Management Console.
- 2 No painel do lado esquerdo, clique em **Gestão > Recuperar dados**.
- 3 Clique no separador *Gestor*.
- 4 Para o *BitLocker*:

Introduza a **ID de recuperação** que recebeu do BitLocker. Opcionalmente, se introduzir o Nome de anfitrião e o Volume, a ID de recuperação é preenchida.

Clique em **Obter palavra-passe de recuperação** ou **Criar pacote de chaves**.

Dependendo do modo de recuperação, irá utilizar esta palavra-passe de recuperação ou pacote de chaves para recuperar os dados.

No *TPM*:

Introduza o **Nome de anfitrião**.

Clique em **Obter palavra-passe de recuperação** ou **Criar pacote de chaves**.

Dependendo do modo de recuperação, irá utilizar esta palavra-passe de recuperação ou pacote de chaves para recuperar os dados.

- 5 Para concluir a recuperação, consulte [Instruções da Microsoft para a Recuperação](#).

NOTA: Se o BitLocker Manager não for “proprietário” do TPM, o pacote de chaves e a palavra-passe do TPM não estarão disponíveis na base de dados da Dell. Será apresentada uma mensagem de erro, indicando que a Dell não consegue encontrar a chave, o que corresponde ao comportamento esperado.

Para recuperar um TPM cujo “proprietário” é uma entidade diferente do BitLocker Manager, deve seguir o processo para recuperar o TPM desse proprietário específico ou seguir o seu processo existente para recuperação do TPM.

A

Apêndice A - Gravação do ambiente de recuperação

Gravação do ambiente de recuperação ISO para CD/DVD

A ligação seguinte contém o processo necessário para utilizar o Microsoft Windows 7/8/10 para criar um CD ou DVD de arranque para o ambiente de recuperação.

<http://windows.microsoft.com/en-us/windows7/burn-a-cd-or-dvd-from-an-iso-file>

Gravação do ambiente de recuperação no suporte de dados amovível

Para criar uma USB de arranque, siga as instruções contidas neste artigo da Microsoft:

[https://technet.microsoft.com/en-us/library/jj200124\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/jj200124(v=ws.11).aspx)



0XXXXXA0X