Encryption Recovery v11.9

January 2024
Rev. A01

DELL Technologies

Notas, avisos e advertências

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

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

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

Contents

1

Como começar a recuperação

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

- CD-R, DVD-R ou suporte de dados amovível formatado
  - Se gravar um CD ou DVD, consulte Gravar o ISO Ambiente de Recuperação em CD/DVD para obter detalhes.
  - Se utilizar um suporte de dado amovível, consulte Gravar o Ambiente de Recuperação em Suportes de Dados Amovíveis para obter detalhes.
- Grupo de recuperação para dispositivo com falhas
  - Para clientes geridos remotamente, as instruções que se seguem explicam como obter um grupo de recuperação do seu servidor Dell Security Management Server.
  - Para clientes geridos localmente, o grupo de recuperação foi criado durante a configuração numa unidade de rede partilhada ou num suporte de dados externo. Localize este pacote antes de prosseguir.

Contacte o Dell ProSupport for Software

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

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

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

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

2

Recuperação de encriptação Policy-based ou de ficheiro/pasta

A recuperação é necessária quando o computador encriptado não inicializa no sistema operativo. Isto ocorre quando o registo é incorretamente modificado ou quando ocorreram alterações de hardware num computador encriptado.

Com a recuperação de Encriptação Policy-based ou 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 que apresenta um BSOD com o Código STOP 0x6gf ou 0x74.
- Um computador no qual não possa aceder a dados encriptados ou políticas de edição.
- Um servidor executando o Dell Encryption que cumpra quaisquer das condições precedentes.
- Um computador no qual a placa]Hardware Crypto Accelerator ou a placa-mãe/TPM deva ser substituída.

  NOTA: O Hardware Crypto Accelerator não é suportado, a começar pela versão v8.9.3.

Realizar a Recuperação System Data Encryption ou FFE

Siga estes passos para realizar uma recuperação System Data Encryption.

Visão Geral do Processo de Recuperação

NOTA: Para Dell Servers a executar a v10.2.8 e versões anteriores, a recuperação requer um ambiente de 32 bits. Os Dell Servers a executar a v10.2.9 e versões posteriores oferecem conjuntos de recuperação de 32 bits e 64 bits.

Para recuperar um sistema que tenha falhado:

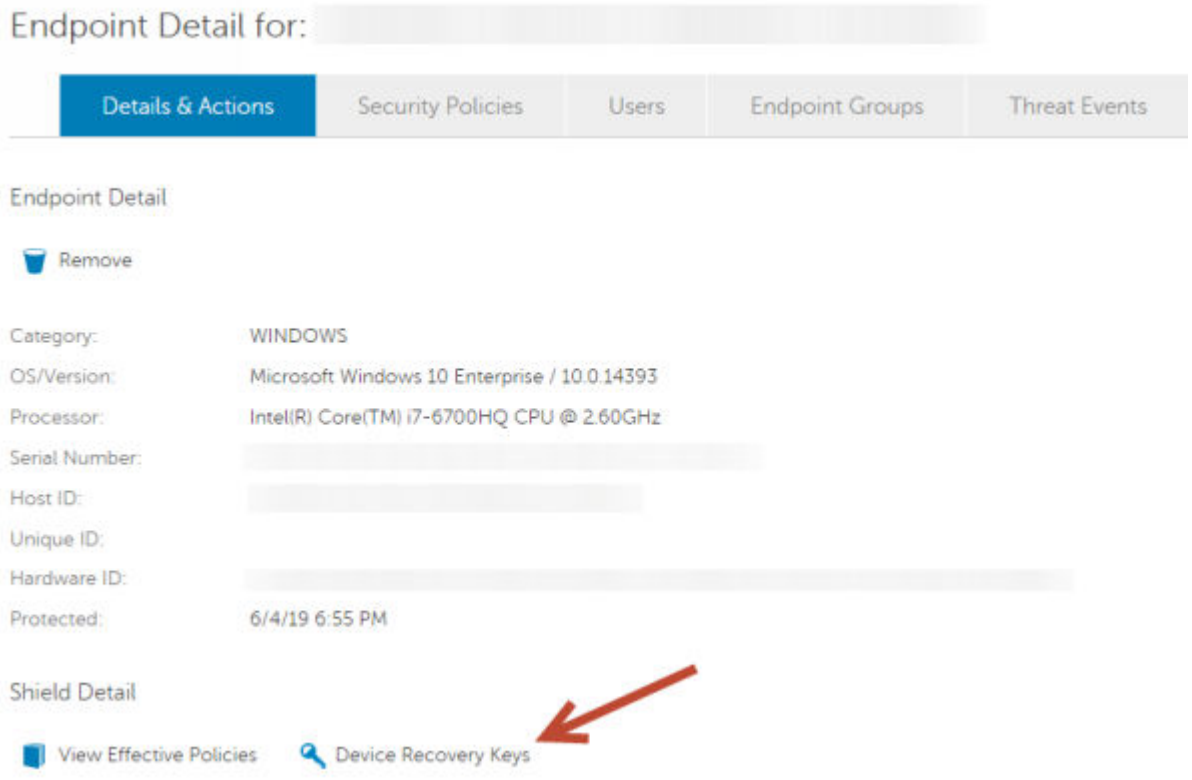
1. Grave o ambiente de recuperação num CD/DVD ou crie um USB de arranque. Consulte o Anexo A - Gravação do ambiente de recuperação.
2. Obtenha o ficheiro de Recuperação.
3. Realize a recuperação.

Obter o ficheiro de recuperação - Encriptação baseada em políticas ou Cliente de encriptação FFE

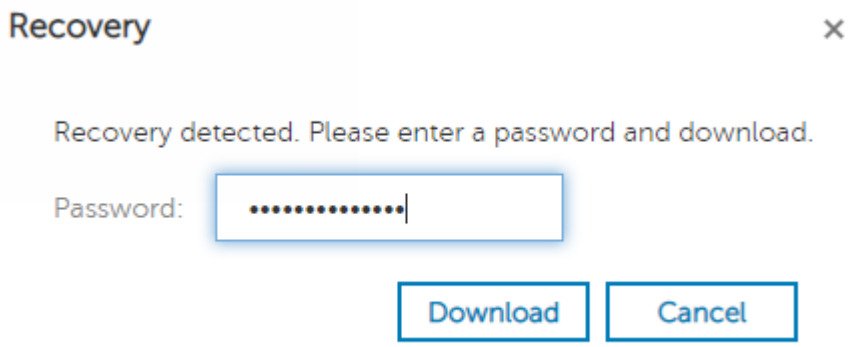
Obtenha o ficheiro de recuperação.

O ficheiro de recuperação pode ser transferido a partir da Management Console. Para transferir as Chaves de Recuperação do Disco geradas quando instalou o Dell Encryption:

a. Abra a Management Console e, no painel esquerdo, selecione **Populações > Pontos Terminais**.
b. Introduza o nome do anfitrião do ponto terminal e, em seguida, clique em **Procurar**.
c. Selecione o nome do ponto terminal.
d. Clique em **Chaves de recuperação do dispositivo**.



e. Introduza uma palavra-passe para transferir as Chaves de Recuperação do Dispositivo.



f. Copie as Chaves de Recuperação do Dispositivo para uma localização onde possam ser acedidas ao reinicializar em WinPE.

Obter o Ficheiro de Recuperação - Computador Gerenciado Localmente

Para obter o ficheiro de recuperação da Encryption Personal:

1. Localize o ficheiro de recuperação com o nome **LSARecovery_<systemname** > **.exe**. Este ficheiro foi guardado numa unidade de rede ou unidade de armazenamento amovível quando executou o assistente de configuração ao instalar a Encryption Personal.

2. Copie **LSARecovery_<systemname** > **.exe** para o computador de destino (o computador para recuperar dados).

Realizar uma Recuperação

1. Usando o suporte multimédia de arranque criado anteriormente, arranque num sistema de recuperação ou no dispositivo onde se encontra a unidade que deseja recuperar. Será aberto um Ambiente WinPE.

NOTA: Desative o SecureBoot antes de executar o processo de recuperação. Quando terminar, volte a ativar o SecureBoot.

2. Introduza **x** e prima **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 permitir-lhe-á recompilar as comprovações de hardware que o cliente de Encriptação realiza ao inicializar o SO.
   - O meu sistema não permite que aceda a dados encriptados ou edite políticas, ou está a ser reinstalado.

     Utilize isto se a placa HCA (Hardware Crypto Accelerator) ou a placa-mãe/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 está correta e clique em **Seguinte**.

   Ao recuperar computadores de outra marca que não a Dell, os campos Número de Série e Etiqueta de Património 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 Policy-Based ou FFE, não será recuperada.
7. Introduza a sua palavra-passe de recuperação e clique em **Seguinte**.

   Com um cliente gerido remotamente, trata-se da palavra-passe fornecida no passo e de Obter o Ficheiro de Recuperação - Computador Gerido Remotamente.

   No Encryption Personal, a palavra-passe é a Palavra-passe do administrador de encriptação configurada para o sistema no momento em que as palavras-passe foram postas sob caução.
8. Na caixa de diálogo Recuperar, clique em **Recuperar**. O processo de recuperação inicia.
9. Quando a recuperação estiver concluída, clique em **Concluir**.

   NOTA:

   Certifique-se de que retira qualquer suporte USB ou CD/DVD usado para inicializar a máquina. O incumprimento deste princípio poderá resultar na inicialização novamente no ambiente de recuperação.
10. O computador deverá estar totalmente operacional após ser reinicializado. No caso do problema persistir, contacte o Dell ProSupport.

Recuperação de Dados de Unidade Encriptada

Se não for possível efetuar o arranque do computador de destino e não existir falha de hardware, pode ser realizada uma recuperação de dados no computador iniciado num ambiente de recuperação. Se não for possível efetuar o arranque do computador de destino e existir falha de hardware, ou se este for um dispositivo USB, a recuperação de dados pode ser realizada através da utilização de um suporte de dados de arranque alternativo. Ao ligar uma unidade protegida pelo Dell Encryption a outro sistema que também tenha o Dell Encryption instalado, os ficheiros ficarão visíveis ao explorar os diretórios. No entanto, se tentar abrir ou copiar um ficheiro, é apresentado um erro de *Acesso negado*. Ao ligar uma unidade com o Dell Encrypted a um sistema que não tenha o Dell Encryption instalado, a tentativa de abrir os dados resulta na apresentação de texto criptográfico.

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 DCID/ID de recuperação de oito caracteres é apresentada após "Comuns".

   b. Abra a Consola de Gestão Remota e, em seguida, selecione o separador **Detalhes e ações** correspondente ao ponto final.
   c. Na secção Detalhes da proteção do ecrã Detalhes do ponto final, localize a DCID/ID de recuperação.

2. Para transferir a chave 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 utilitário Dell Administrative (CMGAu), insira a seguinte informação (alguns campos podem estar previamente preenchidos) e clique em **Seguinte**.

   Servidor: Nome de anfitrião totalmente qualificado do Servidor, por exemplo:

   Servidor do dispositivo (clientes de versão anterior a 8.x): **https://<server.organization.com>:8081/xapi**

   Servidor de segurança: **https://<server.organization.com>:8443/xapi/**

   Admin Dell: o nome da conta do Administrador Forense (ativado no Security Management Server/Security Management Server Virtual)

   Palavra-passe do admin Dell: a palavra-passe da conta do Administrador Forense (ativada no Security Management Server/Security Management Server Virtual)

   MCID: limpe o campo MCID

   DCID: a DCID/ID de recuperação que obteve anteriormente.

4. Na caixa de diálogo do utilitário Dell Administrative, selecione **Não, realizar a transferência a partir de um servidor agora** e clique em **Seguinte**.

   NOTA:

   Se o cliente de Encriptação não estiver instalado, é apresentada uma mensagem que indica *Desbloqueio falhou*. Mude-se para um computador com o cliente de Encriptação 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. Depois de recuperar os ficheiros e estar pronto para voltar a bloquear os ficheiros, clique em **Concluir**.

   Depois de clicar em Concluir, os ficheiros encriptados deixam de estar disponíveis.

3

Recuperação do Hardware Crypto Accelerator

NOTA: O Hardware Crypto Accelerator não é suportado, a começar pela versão v8.9.3.

Com a Recuperação do Hardware Crypto Accelerator (HCA) poderá recuperar o acesso ao que se segue:

- Ficheiros numa unidade encriptada por HCA - Este método desencripta a unidade utilizando as chaves fornecidas. Pode selecionar a unidade específica que deseja desencriptar durante o processo de recuperação.
- Uma unidade encriptada por HCA após uma substituição de hardware - Este método é utilizando 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 desencriptar a unidade.

Requisitos de Recuperação

Para a recuperação do HCA, necessita do seguinte:

- Acesso ao ISO do ambiente de recuperação (A recuperação requer um ambiente de 32 bits)
- Suporte de dados USB ou CD/DVD de arranque

Visão Geral do Processo de Recuperação

NOTA: A recuperação requer um ambiente de 32 bits.

Para recuperar um sistema que tenha falhado:

1. Grave o ambiente de recuperação num CD/DVD ou crie um USB de arranque. Consulte o Anexo 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.

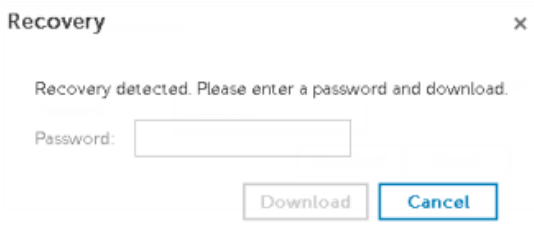
Obter o ficheiro de recuperação - Computador gerido remotamente

Para transferir o ficheiro **<machinename_domain.com>.exe** gerado durante a instalação do Dell Encryption:

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

   NOTA:

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



Obter o Ficheiro de Recuperação - Computador Gerenciado Localmente

Para obter o ficheiro de recuperação da Encryption Personal:

1. Localize o ficheiro de recuperação com o nome **LSARecovery_<systemname** > **.exe**. Este ficheiro foi guardado numa unidade de rede ou unidade de armazenamento amovível quando executou o assistente de configuração ao instalar a Encryption Personal.

2. Copie **LSARecovery_<systemname** > **.exe** para o computador de destino (o computador para recuperar dados).

Realizar uma Recuperação

1. Usando o suporte multimédia de arranque criado anteriormente, arranque num sistema de recuperação ou no dispositivo onde se encontra a unidade que deseja recuperar.

   Será aberto um Ambiente WinPE.

   NOTA: Desative o SecureBoot antes de executar o processo de recuperação. Quando terminar, ative o SecureBoot.

2. Introduza **x** e prima **Enter** para obter uma linha de comandos.

3. Navegue até ao ficheiro de recuperação guardado e inicie-o.

4. Selecione uma opção:
   - Quero desencriptar a minha unidade encriptada HCA.
   - Quero restaurar o acesso à minha unidade encriptada HCA.

5. Na caixa de diálogo Cópia de Segurança e Informação de Recuperação, confirme que a etiqueta de serviço ou número de série são 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 está encriptada por HCA, não se recuperará.

7. Introduza a sua palavra-passe de recuperação e clique em **Seguinte**.

   Num computador gerido remotamente, trata-se da palavra-passe fornecida no passo 3 de Obter o ficheiro de recuperação - Computador gerido remotamente.

   Num computador gerenciado localmente, esta palavra-passe é a Palavra-Passe de Administrador de Encriptação configurada para o sistema na Personal Edition no momento em que as palavras-passe foram postas sob garantia.

8. Na caixa de diálogo Recuperar, clique em **Recuperar**. O processo de recuperação inicia.

9. Quando solicitado, navegue até ao ficheiro de recuperação guardado e clique em **OK**.

   Se está a realizar uma desencriptação completa, a seguinte caixa de diálogo mostra o estado. Esta operação pode 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.

4

Recuperação de Unidade de encriptação automática (SED)

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

- Efetue o desbloqueamento único da unidade para ignorar a Autenticação de pré-arranque (PBA).
- 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:

- Aceda ao ISO de ambiente de recuperação
- Suporte de dados USB ou CD/DVD de arranque

Visão Geral do Processo de Recuperação

NOTA: Para Dell Servers a executar a v10.2.8 e versões anteriores, a recuperação requer um ambiente de 32 bits. Os Dell Servers a executar a v10.2.9 e versões posteriores oferecem conjuntos de recuperação de 32 bits e 64 bits.

Para recuperar um sistema que tenha falhado:

1. Grave o ambiente de recuperação num CD/DVD ou crie um USB de arranque. Consulte o Anexo 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

Obtenha o ficheiro de recuperação.

O ficheiro de recuperação pode ser transferido a partir da Remote Management Console. Para transferir o ficheiro *<nome do anfitrião>-sed-recovery.dat* gerado durante a instalação do Dell Data Security:

a. Abra a Consola de Gestão Remota e, no painel esquerdo, selecione **Gestão > Recuperar dados** e, em seguida, selecione o separador **SED**.
b. No ecrã de Recuperação de Dados, no campo Nome do Anfitrião, introduza o nome de domínio totalmente qualificado do ponto final e, em seguida, clique em **Pesquisar**.
c. No campo SED, selecione uma opção.

d. Clique em **Criar ficheiro de recuperação**.

É transferido o ficheiro **<nome do anfitrião>-sed-recovery.dat**.

Obter o Ficheiro de Recuperação - Cliente SED Gerenciado Remotamente

Obtenha o ficheiro de recuperação.
O ficheiro foi gerado e é acessível a partir do local de cópia de segurança que selecionou ao instalar o software Advanced Authentication no computador. O nome do ficheiro é *OpalSPkey<systemname>.dat*.

Realizar uma Recuperação

1. Usando o suporte multimédia de arranque criado anteriormente, arranque num sistema de recuperação ou no dispositivo onde se encontra a unidade que deseja recuperar. Abre-se um ambiente WinPE com a aplicação de recuperação.

   NOTA: Desative o SecureBoot antes de executar o processo de recuperação. Quando terminar, ative o SecureBoot.

2. Escolha a primeira opção e prima **Enter**.
3. Selecione **Procurar**, localize o ficheiro de recuperação e, em seguida, clique em **Abrir**.
4. Selecione uma opção e clique em **OK**.
   - **Desbloqueio único da unidade -** Este método ignora a PBA.
   - **Desbloquear unidade e remover PBA -** Este método desbloqueia e, em 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. Prima qualquer tecla para voltar ao menu.
6. Prima **r** para reiniciar o computador.

   NOTA:

   Certifique-se de que retira qualquer suporte USB ou CD/DVD usado para inicializar o computador. O incumprimento deste princípio poderá resultar na inicialização novamente no ambiente de recuperação.

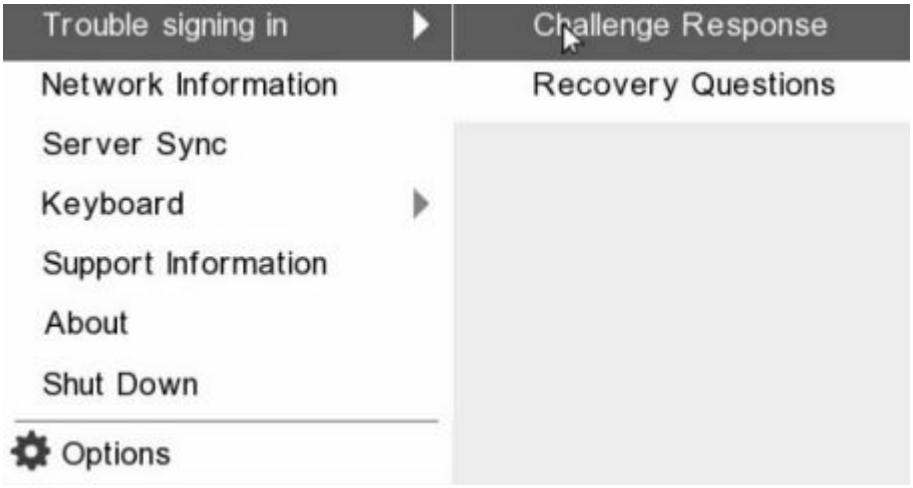
7. O computador deverá estar totalmente operacional após ser reinicializado. No caso do problema persistir, contacte o Dell ProSupport.

Recuperação de Desafio com SED

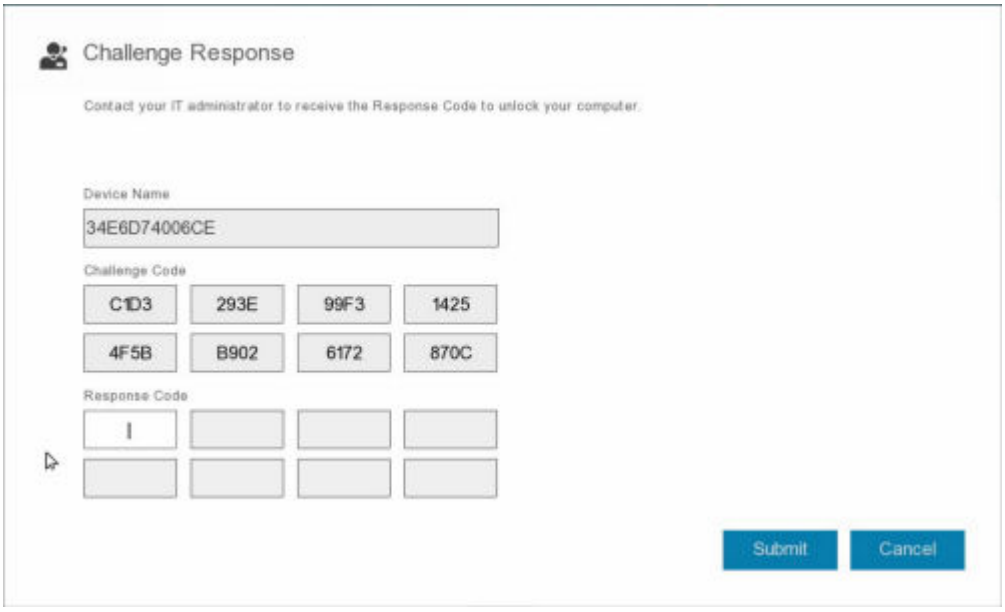
Ignorar o Ambiente de Autenticação de pré-arranque

NOTA: O método de recuperação Desafio/Resposta só está disponível para contas de utilizador de domínio.

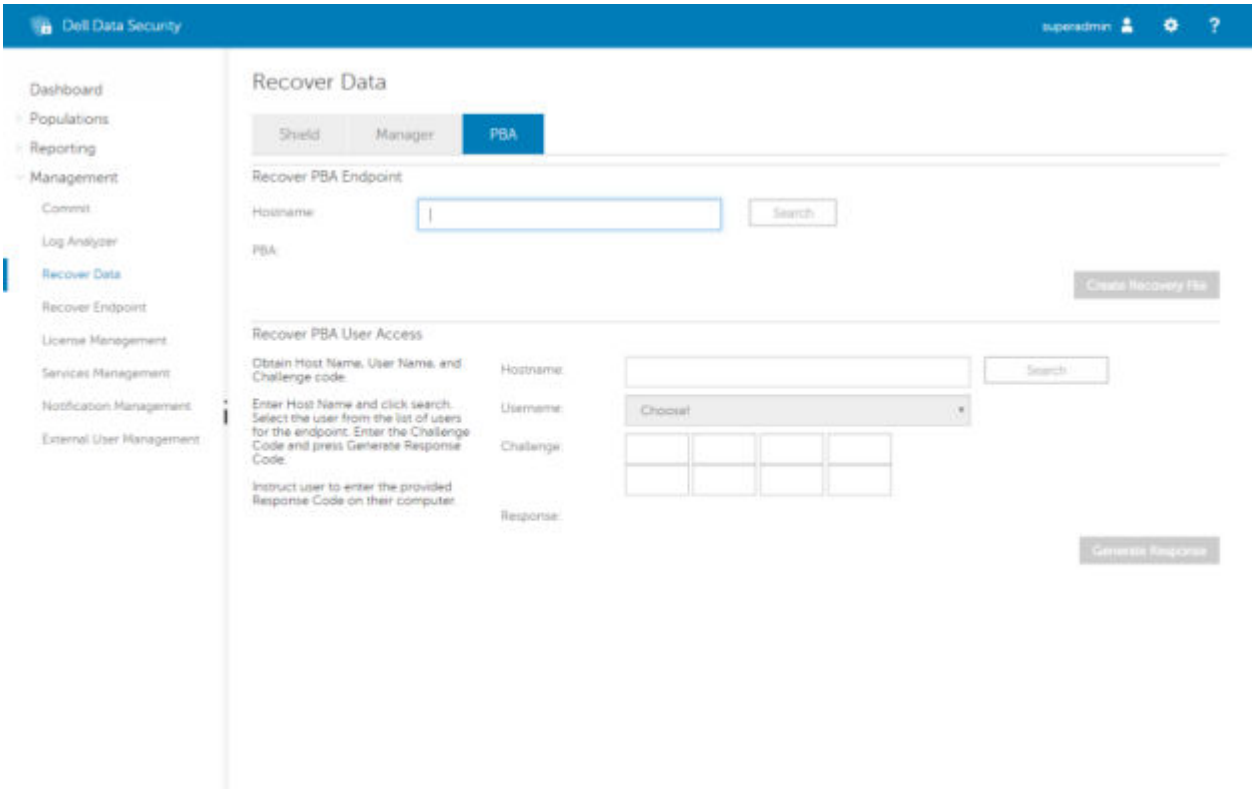
Os utilizadores esquecem-se das palavras-passe e telefonam para o Suporte Técnico para obter assistência para ultrapassar o ambiente PBA. Utilize o mecanismo de Desafio/Resposta que está incorporado no dispositivo. Este mecanismo é configurado por utilizador e tem por base um conjunto rotativo de caracteres alfanuméricos. O utilizador deve introduzir o seu nome no campo **Nome de utilizador** e, em seguida, selecionar **Opções > Desafio Resposta**.



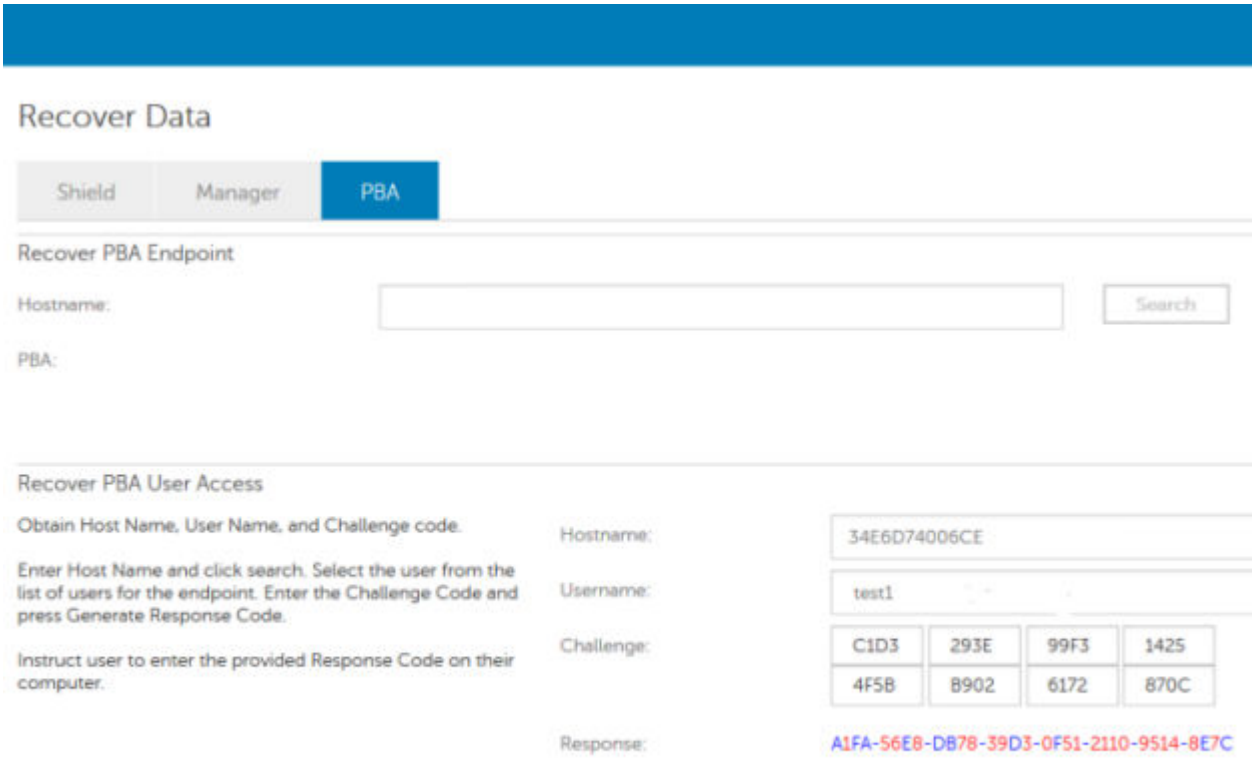
A seguinte informação é apresentada após selecionar **Desafio Resposta**.



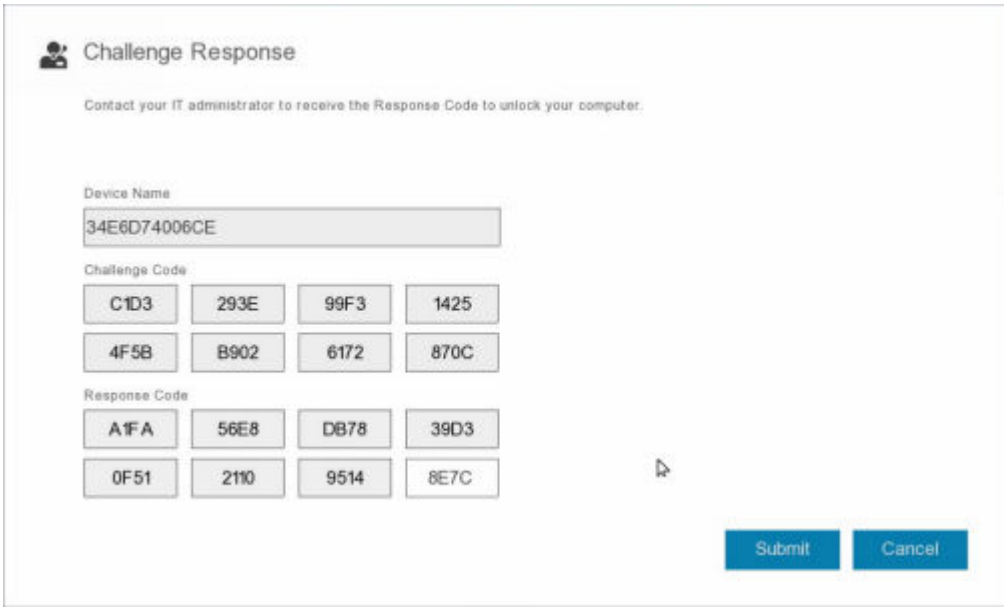
O campo **Nome do dispositivo** é utilizado pelo técnico de Suporte Técnico na Remote Management Console para encontrar o dispositivo correto e, em seguida, é selecionado um nome de utilizador. Isto pode ser encontrado em **Gestão > Recuperar dados** no separador **PBA**.



O código de desafio é fornecido ao técnico de Suporte Técnico, que introduz os dados e, em seguida, clica no botão **Gerar resposta**.



Os dados resultantes estão codificados por cor para ajudar a discernir entre números (vermelho) ou caracteres alfabéticos (azul). Estes dados são lidos ao utilizador final, que os introduz no ambiente PBA e, em seguida, clica no botão **Enviar**, abrindo o ambiente de trabalho do Windows.



Após a autenticação bem-sucedida, é apresentada a seguinte mensagem:

Recuperação do desafio concluída.

5

Recuperação da Full Disk Encryption

A recuperação permite-lhe recuperar o acesso a ficheiros numa unidade encriptada com a Full Disk Encryption.

NOTA: A desencriptação não deve ser interrompida. Se a desencriptação for interrompida, pode ocorrer perda de dados.

Requisitos de Recuperação

Para executar a recuperação da Full Disk Encryption, necessita do seguinte:

- Aceda ao ISO de ambiente de recuperação
- Suporte de dados USB ou CD/DVD de arranque

Visão Geral do Processo de Recuperação

NOTA: A recuperação requer um ambiente de 64 bits.

Para recuperar um sistema que tenha falhado:

1. Grave o ambiente de recuperação num CD/DVD ou crie um USB de arranque. Consulte o Anexo A - Gravação do ambiente de recuperação.
2. Obtenha o ficheiro de Recuperação.
3. Realize a recuperação.

Realizar recuperação da Full Disk Encryption

Siga estes passos para realizar uma recuperação da Full Disk Encryption.

Obter o Ficheiro de Recuperação - Cliente da Full Disk Encryption

Obtenha o ficheiro de recuperação.

Transfira o ficheiro de recuperação da Remote Management Console. Para transferir o ficheiro *<nome do anfitrião>-sed-recovery.dat* gerado durante a instalação do Dell Data Security:

a. Abra a Consola de Gestão Remota e, no painel esquerdo, selecione **Gestão > Recuperar dados** e, em seguida, selecione o separador **PBA**.
b. No ecrã de Recuperação de Dados, no campo Nome do Anfitrião, introduza o nome de domínio totalmente qualificado do ponto final e, em seguida, clique em **Pesquisar**.
c. No campo SED, selecione uma opção.
d. Clique em **Criar ficheiro de recuperação**.

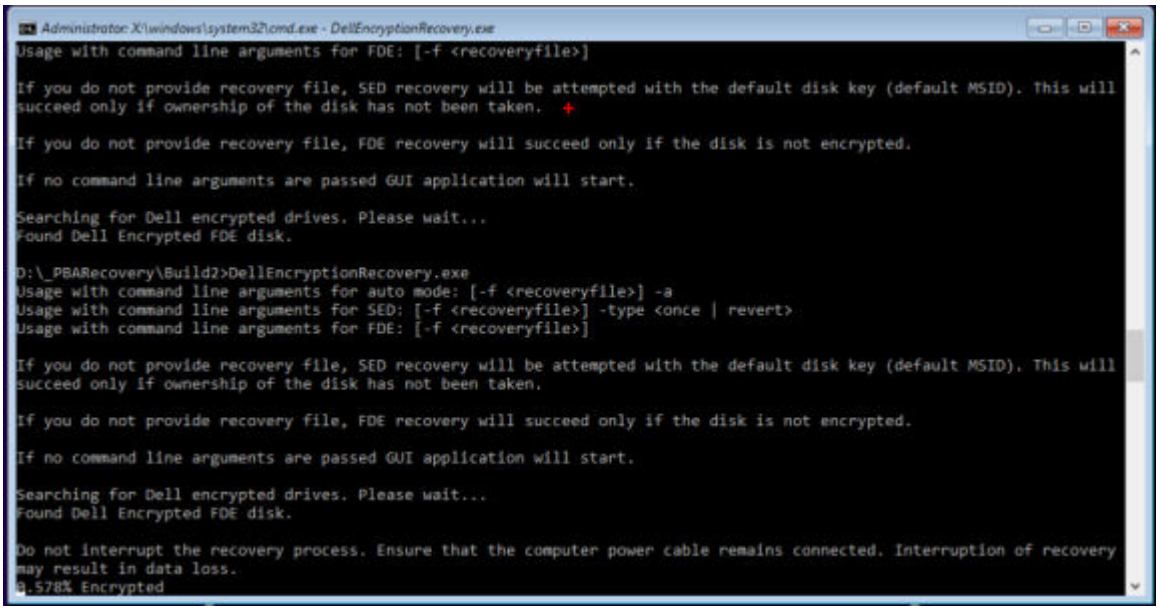
   É transferido o ficheiro **<nome do anfitrião>-sed-recovery.dat**.

Realizar uma Recuperação

1. Usando o suporte multimédia de arranque criado anteriormente, arranque num sistema de recuperação ou no dispositivo onde se encontra a unidade que deseja recuperar. Abre-se um ambiente WinPE com a aplicação de recuperação.

   NOTA: Desative o SecureBoot antes de executar o processo de recuperação. Quando terminar, volte a ativar o SecureBoot.

2. Escolha a primeira opção e prima **Enter**.
3. Selecione **Procurar**, localize o ficheiro de recuperação e, em seguida, clique em **Abrir**.
4. Clique em **OK**.



5. A recuperação está agora concluída. Prima qualquer tecla para voltar ao menu.
6. Prima **r** para reiniciar o computador.

   NOTA:

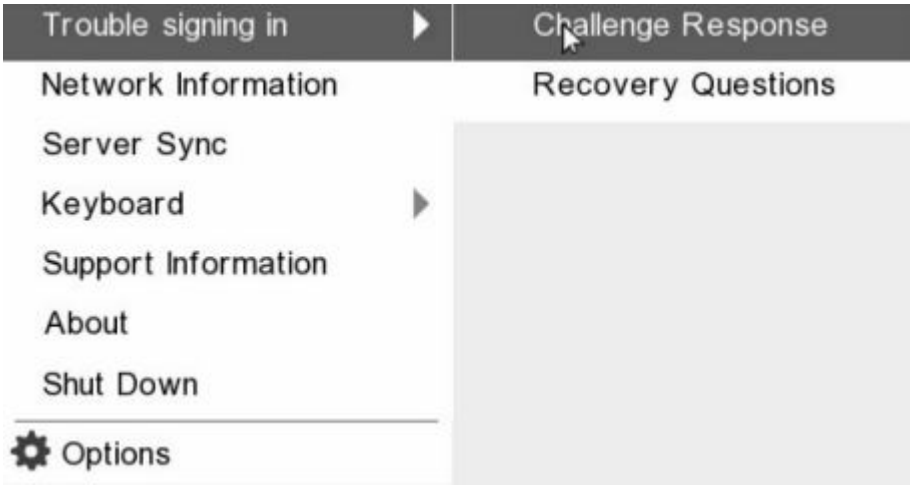
   Certifique-se de que retira qualquer suporte USB ou CD/DVD usado para inicializar o computador. O incumprimento deste princípio poderá resultar na inicialização novamente no ambiente de recuperação.

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

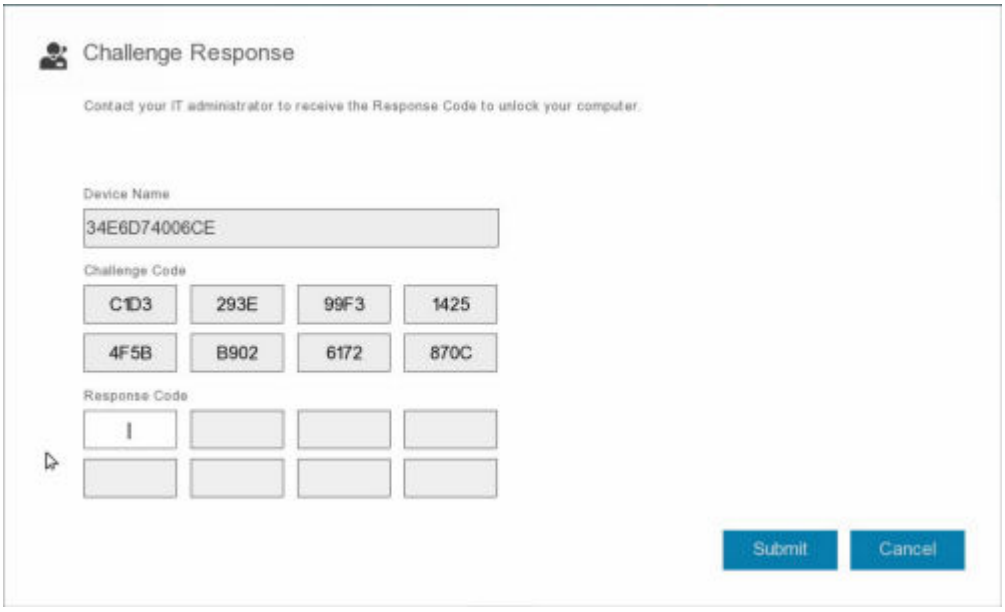
Recuperação de Desafio com Full Disk Encryption

Ignorar o ambiente de Autenticação de pré-arranque

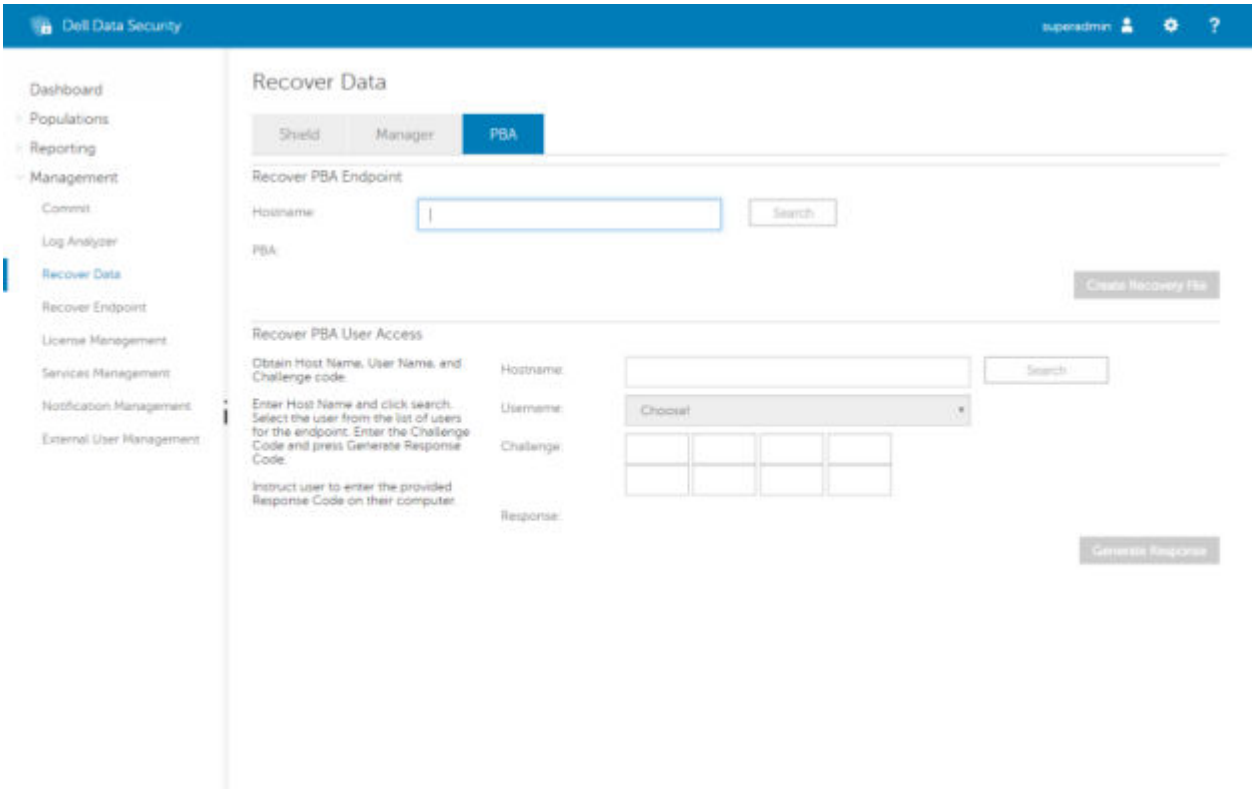
Os utilizadores esquecem-se das palavras-passe e telefonam para o Suporte Técnico para obter assistência para ultrapassar o ambiente PBA. Utilize o mecanismo de Desafio/Resposta que está incorporado no dispositivo. Este mecanismo é configurado por utilizador e tem por base um conjunto rotativo de caracteres alfanuméricos. O utilizador deve introduzir o seu nome no campo **Nome de utilizador** e, em seguida, selecionar **Opções > Desafio Resposta**.



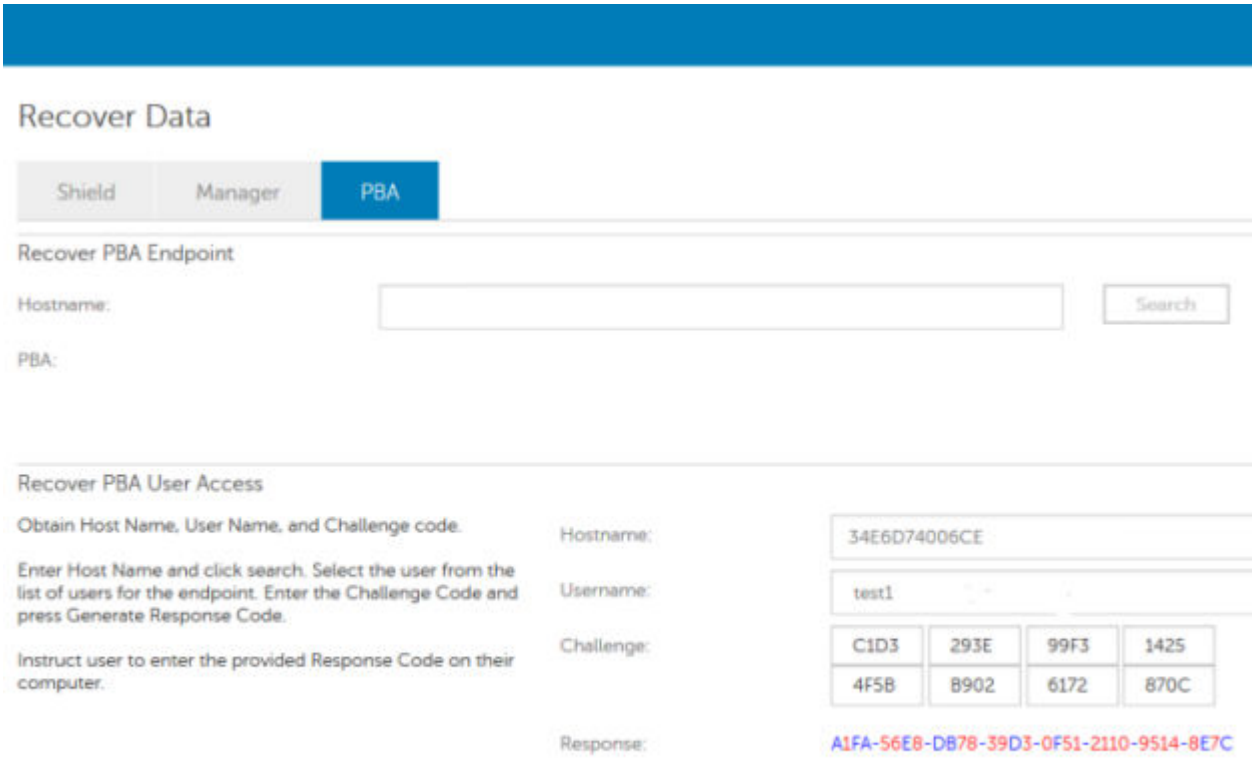
A seguinte informação é apresentada após selecionar **Desafio Resposta**.



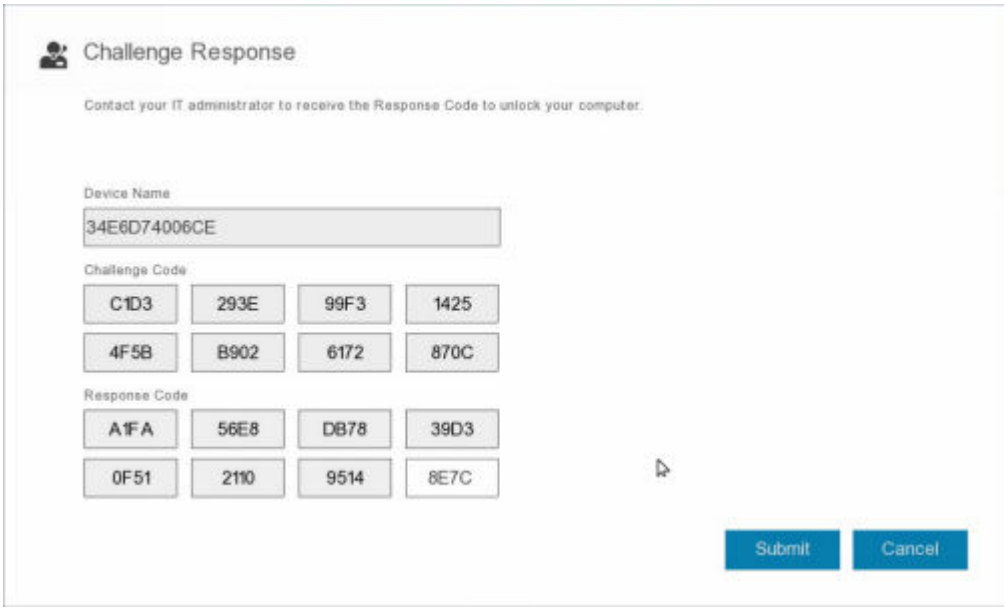
O campo **Nome do dispositivo** é utilizado pelo técnico de Suporte Técnico na Remote Management Console para encontrar o dispositivo correto e, em seguida, é selecionado um nome de utilizador. Isto pode ser encontrado em **Gestão > Recuperar dados** no separador **PBA**.



O código de desafio é fornecido ao técnico de Suporte Técnico, que introduz os dados e, em seguida, clica no botão **Gerar resposta**.



Os dados resultantes estão codificados por cor para ajudar a discernir entre números (vermelho) ou caracteres alfabéticos (azul). Estes dados são lidos ao utilizador final, que os introduz no ambiente PBA e, em seguida, clica no botão **Enviar**, abrindo o ambiente de trabalho do Windows.



Após a autenticação bem-sucedida, é apresentada a seguinte mensagem:

Recuperação do desafio concluída.

6

Recuperação da Full Disk Encryption e Dell Encryption

Este capítulo descreve os passos de recuperação necessários para recuperar o acesso a ficheiros protegidos da Dell Encryption num disco protegido pela Full Disk Encryption.

NOTA: A desencriptação não deve ser interrompida. Se a desencriptação for interrompida, pode ocorrer perda de dados.

Requisitos de Recuperação

Para executar a recuperação da Full Disk Encryption e Dell Encryption, necessita do seguinte:

- Aceda ao ISO de ambiente de recuperação
- Suporte de dados USB ou CD/DVD de arranque

Visão Geral do Processo de Recuperação

NOTA: A recuperação da Full Disk Encryption requer um ambiente de 64 bits. Para Dell Servers a executar a v10.2.8 e versões anteriores, a recuperação Policy-Based Encryption e FFE requer um ambiente de 32 bits. Os Dell Servers a executar a v10.2.9 e versões posteriores oferecem conjuntos de recuperação de 32 bits e 64 bits.

Para recuperar um sistema que tenha falhado:

1. Grave o ambiente de recuperação num CD/DVD ou crie um USB de arranque. Consulte o Anexo A - Gravação do ambiente de recuperação.
2. Obter os ficheiros de recuperação da Dell Encryption e Full Disk Encryption.
3. Realize a recuperação.

Realizar recuperação de um disco encriptado pela Full Disk Encryption e Dell Encryption

Siga estes passos para realizar a recuperação de um disco encriptado pela Full Disk Encryption e Dell Encryption.

Obter o Ficheiro de Recuperação - Cliente da Full Disk Encryption

Obtenha o ficheiro de recuperação.

Transfira o ficheiro de recuperação da Remote Management Console. Para transferir o ficheiro *<nome do anfitrião>-sed-recovery.dat* gerado durante a instalação do Dell Data Security:

a. Abra a Consola de Gestão Remota e, no painel esquerdo, selecione **Gestão > Recuperar dados** e, em seguida, selecione o separador **PBA**.
b. No ecrã de Recuperação de Dados, no campo Nome do Anfitrião, introduza o nome de domínio totalmente qualificado do ponto final e, em seguida, clique em **Pesquisar**.
c. No campo SED, selecione uma opção.
d. Clique em **Criar ficheiro de recuperação**.

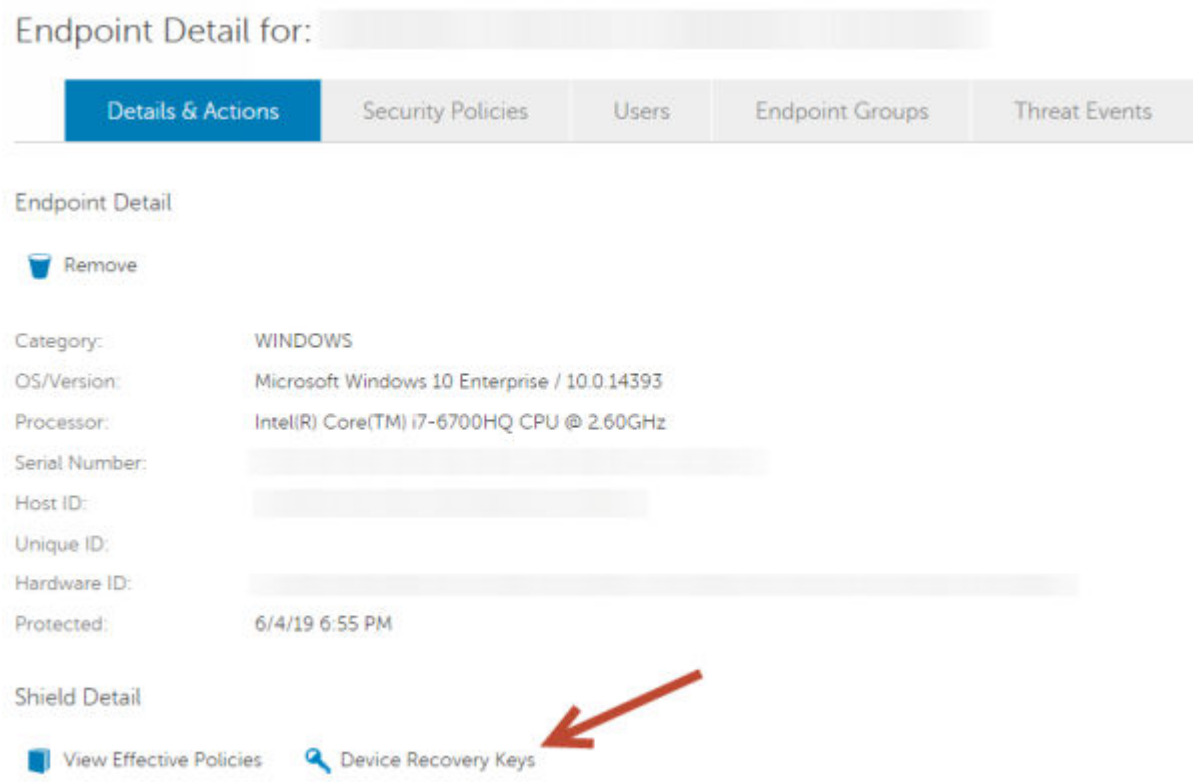
   É transferido o ficheiro **<nome do anfitrião>-sed-recovery.dat**.

Obter o ficheiro de recuperação - Encriptação baseada em políticas ou Cliente de encriptação FFE

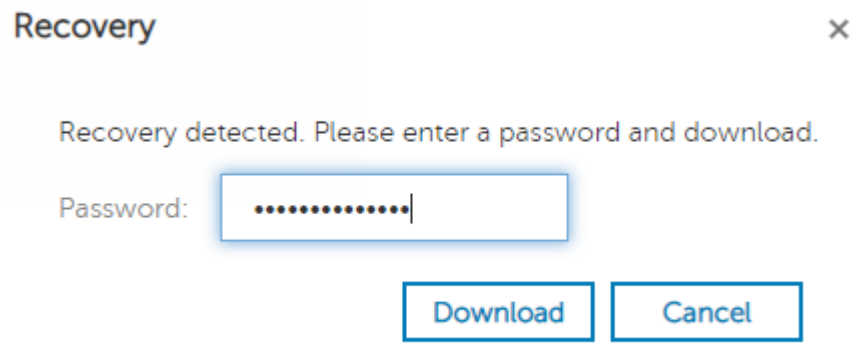
Obtenha o ficheiro de recuperação.

O ficheiro de recuperação pode ser transferido a partir da Management Console. Para transferir as Chaves de Recuperação do Disco geradas quando instalou o Dell Encryption:

a. Abra a Management Console e, no painel esquerdo, selecione **Populações > Pontos Terminais**.
b. Introduza o nome do anfitrião do ponto terminal e, em seguida, clique em **Procurar**.
c. Selecione o nome do ponto terminal.
d. Clique em **Chaves de recuperação do dispositivo**.



e. Introduza uma palavra-passe para transferir as Chaves de Recuperação do Dispositivo.

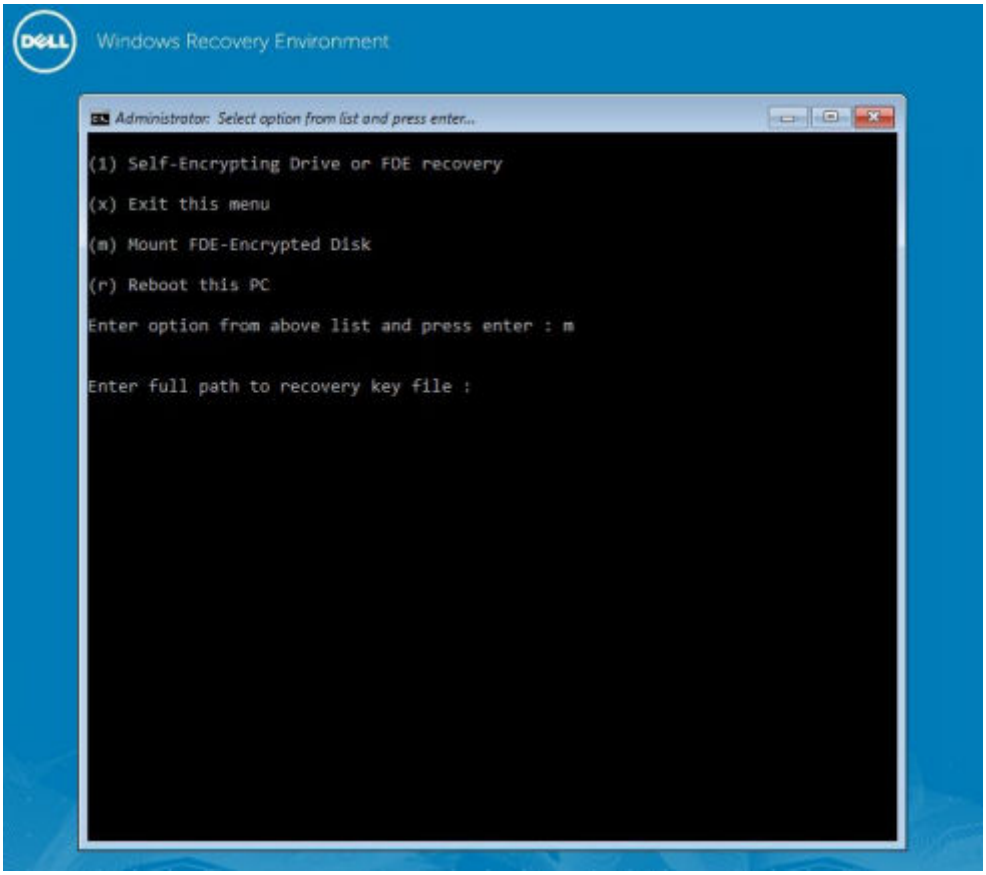


f. Copie as Chaves de Recuperação do Dispositivo para uma localização onde possam ser acedidas ao reinicializar em WinPE.

Realizar uma Recuperação

1. Usando o suporte multimédia de arranque criado anteriormente, arranque num sistema de recuperação ou no dispositivo onde se encontra a unidade que deseja recuperar. Abre-se um ambiente WinPE com a aplicação de recuperação.

NOTA: Desative o SecureBoot antes de executar o processo de recuperação. Quando terminar, volte a ativar o SecureBoot.

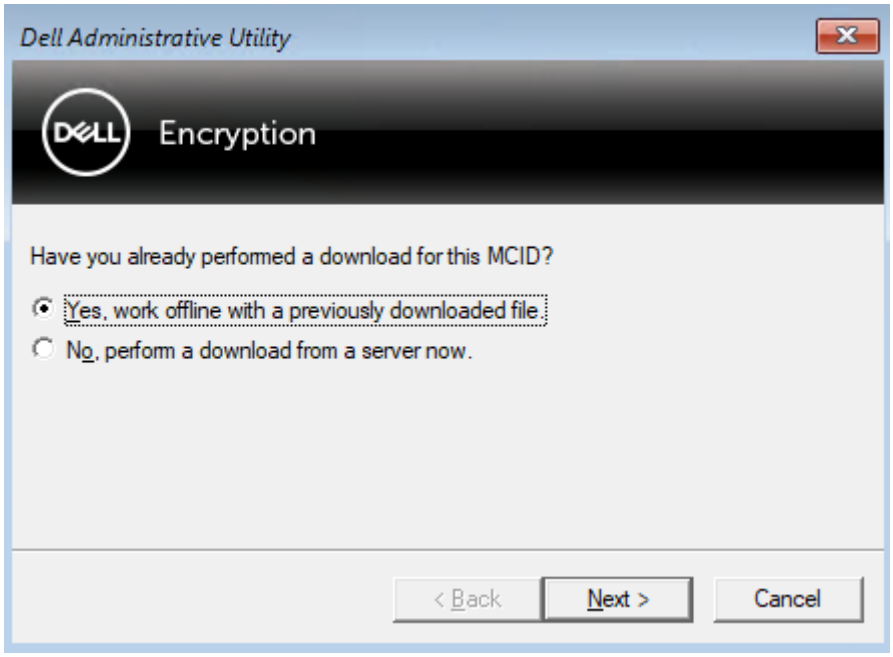


2. Escolha a terceira opção e prima **Enter**.
3. Quando solicitado, introduza o nome e a localização do ficheiro de recuperação.
4. Ao utilizar a chave de recuperação, o disco encriptado pela Full Disk Encryption é instalado.

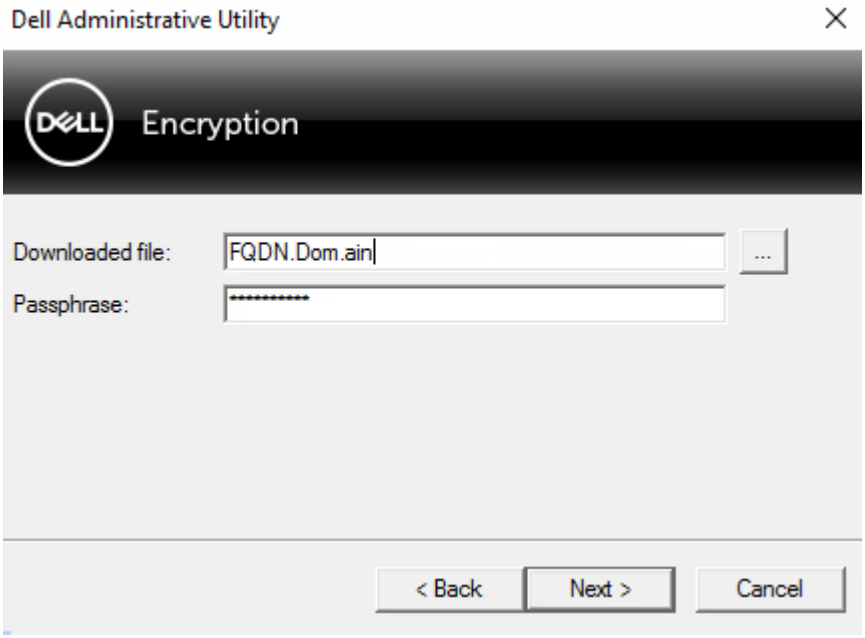
```
Enter option from above list and press enter : m

Enter the full path to the recovery key file: c:\recovery\opalSPKey.DESKTOP-XXYYZZ.recovery.dat

Recoveryfile loaded
--------------------   Disk 0   --------------------
     Cylinders       = 15566
     Tracks/cylinder = 255
     Sectors/track   = 63
     Bytes/sector    = 512
     Disk size       = 128035676160 (Bytes)
                     = 119.24 GB
---> Disk 0, returned status...........: EDriverStatus_Success
--------------------   Disk 1   --------------------
     Cylinders       = 973
     Tracks/cylinder = 255
     Sectors/track   = 63
     Bytes/sector    = 512
     Disk size       = 8004304896 (Bytes)
                     = 7.45 GB
---> Disk 0, returned status...........: EDriverStatus_DriveNotEncrypted
```

5. Aceda ao utilitário CMGAu.exe utilizando o seguinte comando: `cd DDPEAdminUtilities\`
6. Inicie o CMGAu.exe utilizando o seguinte comando: `\DDPEAdminUtilities>CmgAu.exe`

   Selecione **Sim, trabalhar offline com um ficheiro previamente transferido**.



7. No campo **Ficheiro transferido:**, introduza a localização do **Pacote de recuperação**, introduza a **Frase de acesso** do administrador forense e selecione **Seguinte**.



Quando a recuperação estiver concluída, clique em **Concluir**.

NOTA:

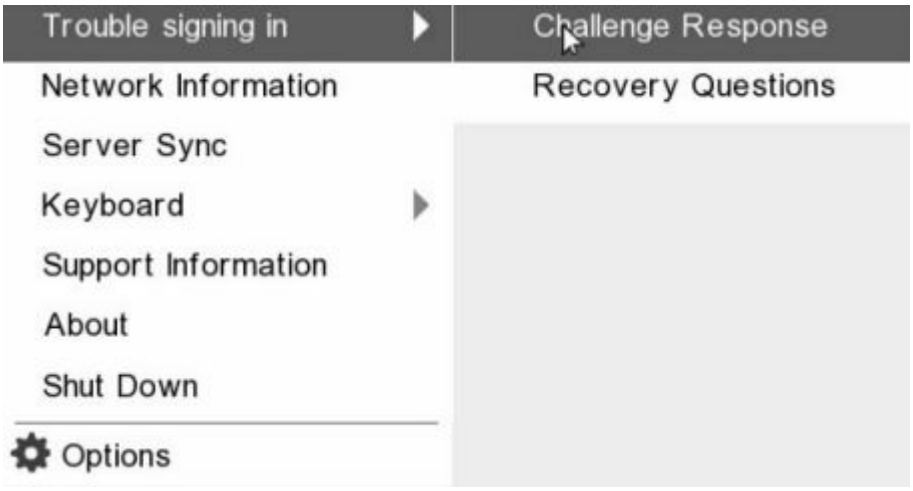
Certifique-se de que retira qualquer suporte USB ou CD/DVD usado para inicializar o computador. O incumprimento deste princípio poderá resultar na inicialização novamente no ambiente de recuperação.

8. Depois de o computador ser reiniciado, deverá ter acesso aos ficheiros encriptados. No caso do problema persistir, contacte o Dell ProSupport.

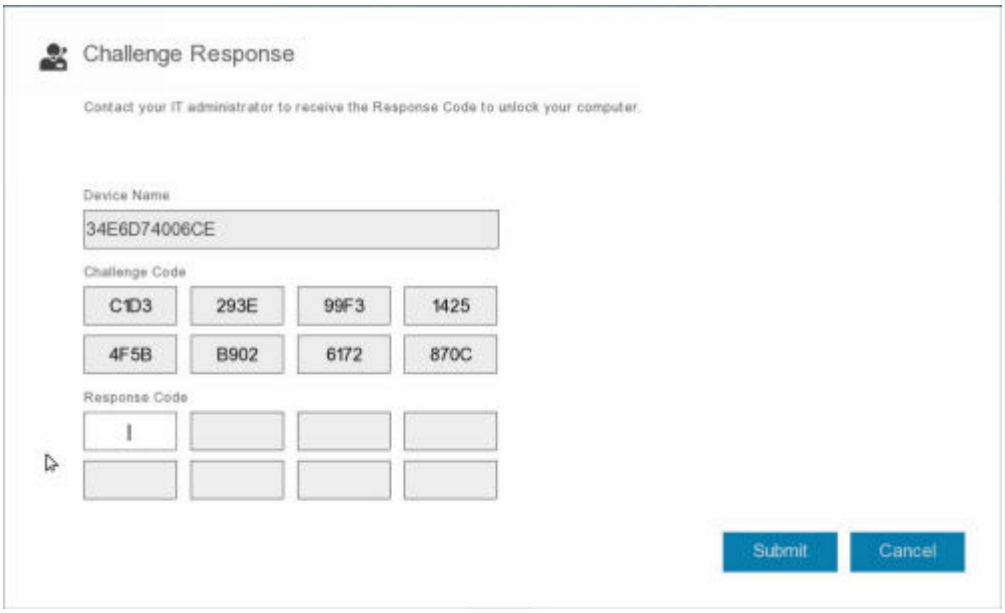
Recuperação de Desafio com Full Disk Encryption

Ignorar o ambiente de Autenticação de pré-arranque

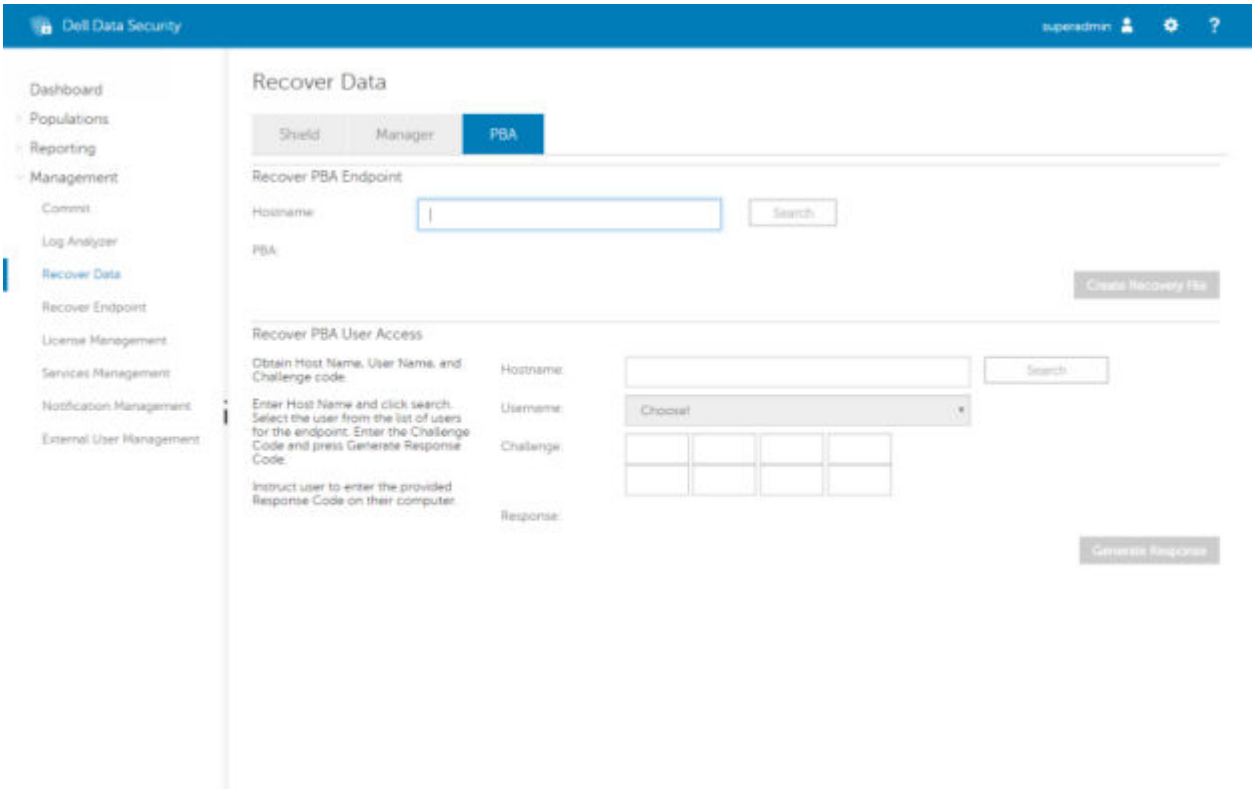
Os utilizadores esquecem-se das palavras-passe e telefonam para o Suporte Técnico para obter assistência para ultrapassar o ambiente PBA. Utilize o mecanismo de Desafio/Resposta que está incorporado no dispositivo. Este mecanismo é configurado por utilizador e tem por base um conjunto rotativo de caracteres alfanuméricos. O utilizador deve introduzir o seu nome no campo **Nome de utilizador** e, em seguida, selecionar **Opções > Desafio Resposta**.



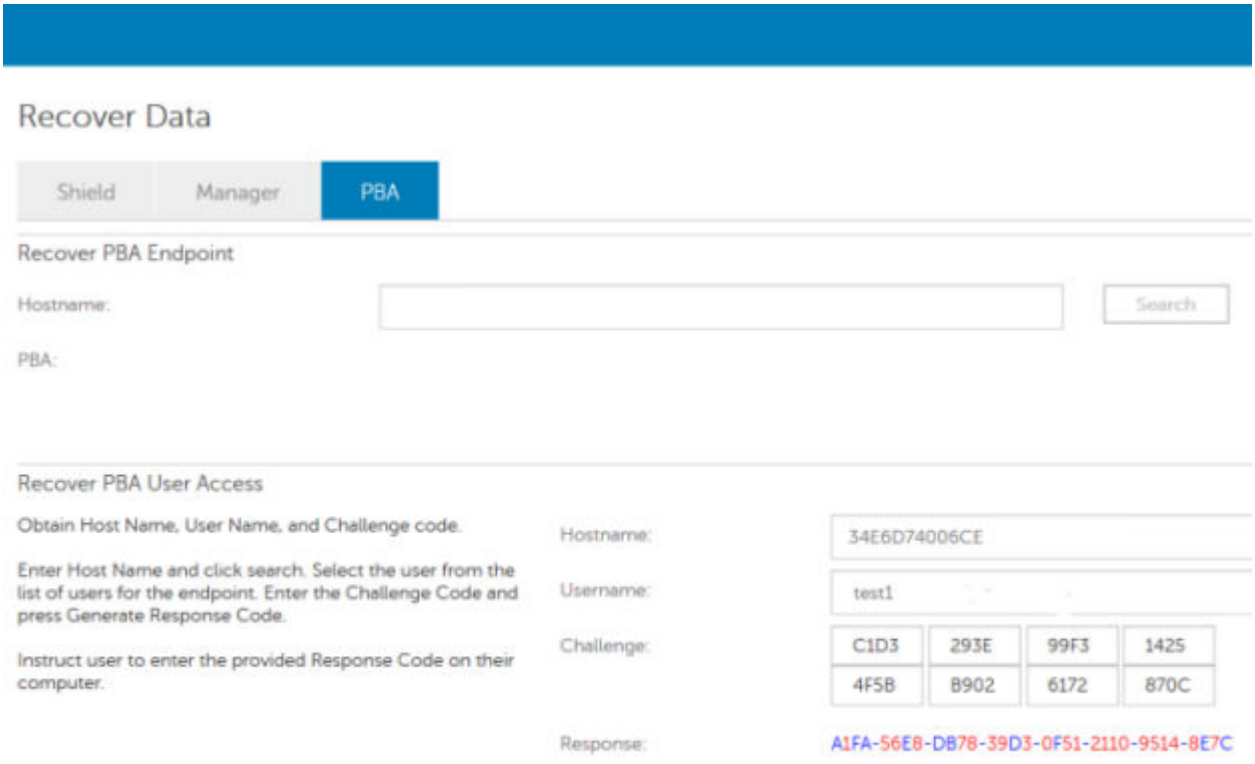
A seguinte informação é apresentada após selecionar **Desafio Resposta**.



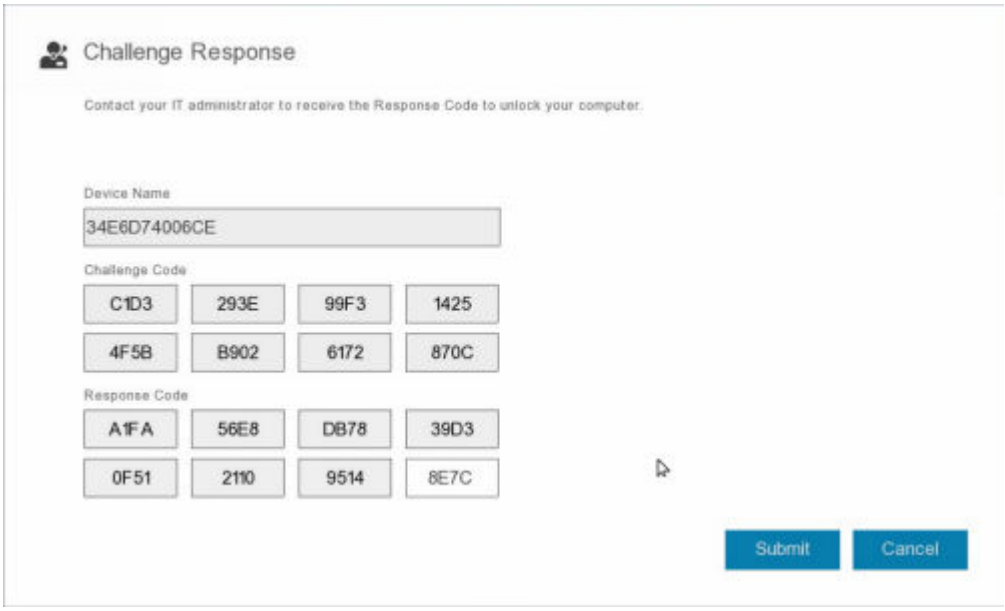
O campo **Nome do dispositivo** é utilizado pelo técnico de Suporte Técnico na Remote Management Console para encontrar o dispositivo correto e, em seguida, é selecionado um nome de utilizador. Isto pode ser encontrado em **Gestão > Recuperar dados** no separador **PBA**.



O código de desafio é fornecido ao técnico de Suporte Técnico, que introduz os dados e, em seguida, clica no botão **Gerar resposta**.



Os dados resultantes estão codificados por cor para ajudar a discernir entre números (vermelho) ou caracteres alfabéticos (azul). Estes dados são lidos ao utilizador final, que os introduz no ambiente PBA e, em seguida, clica no botão **Enviar**, abrindo o ambiente de trabalho do Windows.



Após a autenticação bem-sucedida, é apresentada a seguinte mensagem:

Recuperação do desafio concluída.

7

Controlo de dispositivos PBA

O controlo de dispositivos PBA aplica-se a endpoints encriptados através de SED ou Full Disk Encryption.

Utilização do controlo de dispositivos PBA

Os comandos PBA para um endpoint específico são realizados na área de Controlo de dispositivos PBA. Cada comando tem uma classificação de prioridade. Um comando com uma classificação de prioridade superior cancela comandos com prioridades inferiores na fila de implementação. Para obter uma lista de classificações de prioridade dos comandos, consulte *AdminHelp*, disponível ao clicar em ? na Remote Management Console. Os Controlos de dispositivos PBA estão disponíveis na página Detalhes de endpoint da Remote Management Console.

Estão disponíveis os seguintes comandos no Controlo de dispositivos PBA:

- **Bloquear** - Bloqueia o ecrã PBA e impede o início de sessão no computador por parte de qualquer utilizador.
- **Desbloquear** - Desbloqueia o ecrã PBA depois de ter sido bloqueado neste endpoint, quer através do envio de um comando de bloqueio ou por exceder o número máximo de tentativas de autenticação permitidas pela política.
- **Remover utilizadores** - Remove todos os utilizadores do PBA.
- **Ignorar início de sessão** - Ignora o ecrã PBA uma vez para que um utilizador possa aceder ao computador sem se autenticar. O utilizador precisará no entanto de iniciar sessão no Windows depois de ter ignorado o ecrã PBA.
- **Limpar** - O comando Limpar efetua o "restauro para o estado de fábrica" da unidade encriptada. O comando Limpar pode ser utilizado para reconfigurar um computador ou, numa situação de emergência, limpar o computador tornando os dados irrecuperáveis de forma permanente. Certifique-se de que é o comportamento pretendido antes de invocar este comando. Na Full Disk Encryption, o comando Limpar apaga a unidade de forma criptográfica e a PBA é removida. Para SED, o comando Wipe apaga a unidade de forma criptográfica e a PBA apresenta a mensagem "Dispositivo bloqueado". Para reconfigurar o SED, remova a PBA com a aplicação de Recuperação SED.

8

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 extraindo-a do pacote de recuperação que é transferido a partir do Dell Server.

Recuperar a GPK

Obter o Ficheiro de Recuperação

Para transferir o ficheiro **<machinename_domain.com>.exe** gerado durante a instalação do Dell Data Security:

1. Abra a Remote Management Console e, no painel esquerdo, selecione **Gestão** > **Recuperar endpoint**.
2. No campo Nome do anfitrião, introduza o nome de domínio totalmente qualificado do endpoint e clique em **Procurar**.
3. Na janela Recuperação, 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 **<machinename_domain.com>.exe** é transferido.

Realizar uma Recuperação

1. Criar suporte de dados de inicialização do ambiente de recuperação. Para obter instruções, consulte o Anexo A - Gravação do ambiente de recuperação.

   NOTA: Desative o SecureBoot antes de executar o processo de recuperação. Quando terminar, ative o SecureBoot.

2. Arranque com esse suporte de dados num sistema de recuperação ou no dispositivo onde se encontra a unidade que pretende recuperar.

   Será aberto um Ambiente WinPE.

3. Introduza **x** e prima **Enter** para obter uma linha de comandos.
4. Navegue até ao ficheiro de recuperação e inicie-o.

   Abre-se uma caixa de diálogo de diagnóstico do cliente e o ficheiro de recuperação é gerado em segundo plano.

5. Numa linha de comandos administrativa, execute **<machinename_domain.com** > **.exe** > **-p <password** > **-gpk**

   Devolve o GPKRCVR.txt para o seu computador.

6. Copie o ficheiro **GPKRCVR.txt** a partir da raiz da unidade do SO do computador.

7. Reinicie o computador.

   O ficheiro GPKRCVR.txt será consumido pelo sistema operativo e regenerará a GPK nesse computador.

8. Se solicitado, reinicialize novamente.

9

Recuperação do BitLocker Manager

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

Recuperar dados

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

   Introduza o **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 chave**.

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

   Para o *TPM*:

   Introduza o **Nome de anfitrião**.

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

   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 uma das seguintes opções:
   - Windows 7
   - Windows 8
   - Windows 10

   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.

10

Recuperação da palavra-passe

É comum os utilizadores esquecerem a respetiva palavra-passe. Felizmente, há várias formas para os utilizadores recuperarem o acesso a um computador com autenticação pré-reinicialização quando isso acontece.

- A funcionalidade de Perguntas de recuperação oferece autenticação baseada em perguntas e respostas.
- Os códigos de Desafio/Resposta permitem aos utilizadores trabalhar com o seu Administrador para recuperarem o acesso ao computador. Esta funcionalidade está disponível apenas para utilizadores com computadores geridos pela sua organização.

Perguntas de recuperação

A primeira vez que um utilizador inicia sessão no computador, é-lhe solicitado que responda a um conjunto padrão de perguntas configuradas pelo administrador. Depois de introduzir as respostas a estas perguntas, da próxima vez que se esquecer da sua palavra-passe, são solicitadas as respostas ao utilizador. Partindo do princípio que respondeu corretamente às perguntas, consegue iniciar sessão e recuperar o acesso ao Windows.

Pré-requisitos

- As perguntas de recuperação têm de ser configuradas pelo Administrador.
- É preciso que o utilizador tenha inserido as respostas às perguntas.
- Antes de clicar na opção do menu **Problemas ao iniciar sessão**, o utilizador deve introduzir um nome de utilizador e domínio válidos.

Para aceder às Perguntas de recuperação a partir do ecrã de início de sessão da PBA:

1. Introduza um nome de domínio e um nome de utilizador válidos.
2. No canto inferior esquerdo do ecrã, clique em **Opções** > **Problemas ao iniciar sessão**.
3. Quando for apresentada a caixa de diálogo de perguntas e respostas, introduza as respostas que inseriu quando respondeu às Perguntas de recuperação da primeira vez que iniciou a sessão.

11

Recuperação de palavra-passe do Encryption External Media

O Encryption External Media permite-lhe proteger suportes de armazenamento amovíveis tanto dentro como fora da sua organização, permitindo aos utilizadores encriptar unidades USB e outros suportes de armazenamento amovíveis. O utilizador atribui uma palavra-passe a cada suporte de dados amovível que pretenda proteger. Esta secção descreve o processo de recuperação do acesso a um dispositivo USB encriptado quando o utilizador se esquece da palavra-passe do dispositivo.

Recuperar o acesso aos dados

Quando um utilizador introduz incorretamente a sua palavra-passe tantas vezes que excede o número de tentativas de introdução da palavra-passe, o dispositivo USB é colocado no modo de Autenticação manual.

A autenticação manual é o processo de fornecimento de códigos do cliente a um administrador com sessão iniciada no Dell Server.

No modo de Autenticação manual, o utilizador tem duas opções para repor a sua palavra-passe e recuperar o acesso aos seus dados.

O administrador fornece um Código de acesso ao cliente, permitindo ao utilizador repor a sua palavra-passe e recuperar o acesso aos seus dados encriptados.

1. Quando a sua palavra-passe lhe for solicitada, clique no botão **Esqueci-me**.

   É apresentada a caixa de diálogo de confirmação.

2. Clique em **Sim** para confirmar. Depois da confirmação, o dispositivo entra em modo de Autenticação manual.
3. Contacte o Administrador da Assistência técnica e forneça-lhe os códigos que aparecem na caixa de diálogo.
4. Enquanto Administrador da Assistência Técnica, inicie sessão na Consola de Gestão Remota - a conta de Administrador da Assistência Técnica tem de ter privilégios de Assistência Técnica.
5. Navegue até à opção do menu **Recuperar dados** no painel esquerdo.
6. Introduza os códigos fornecidos pelo utilizador final.
7. Clique no botão **Gerar resposta** no canto inferior direito do ecrã.
8. Forneça ao utilizador o Código de acesso.

   NOTA:

   Certifique-se de que autentica manualmente o utilizador antes de lhe fornecer um Código de acesso. Por exemplo, faça ao utilizador uma série de perguntas pelo telefone que apenas essa pessoa saiba, como, por exemplo, "Qual é a sua ID de funcionário?". Outro exemplo: peça que o utilizador se desloque à Assistência Técnica para fornecer identificação e garantir que é o proprietário do suporte de dados. A não autenticação de um utilizador antes de fornecer um Código de acesso pelo telefone pode permitir que um intruso tenha acesso a suportes amovíveis encriptados.

9. Reponha a sua palavra-passe para o suporte de dados encriptado.

   É pedido ao utilizador que reponha a sua palavra-passe para o suporte de dados encriptado.

Autorrecuperação

A unidade deve ser inserida novamente na máquina que a encriptou originalmente para que a autorrecuperação funcione. Desde que o proprietário do suporte de dados esteja autenticado para o Mac ou PC protegido, o cliente deteta a perda do material de

chave e solicita ao utilizador a reinicialização do dispositivo. Nessa altura, o utilizador pode repor a sua palavra-passe e recuperar o acesso aos seus dados encriptados. Este processo pode resolver problemas de ficheiros multimédia parcialmente danificados.

1. Inicie a sessão numa estação de trabalho encriptada da Dell Data Security como proprietário do suporte de dados.
2. Insira o dispositivo de armazenamento amovível encriptado.
3. Quando lhe for solicitado, introduza uma nova palavra-passe para reinicializar o dispositivo de armazenamento amovível.

   Se tiver êxito, uma pequena notificação é apresentada para indicar que a palavra-passe foi aceite.

4. Navegue até ao dispositivo de armazenamento e confirme o acesso aos dados.

12

Anexo A — Transferência do ambiente de recuperação

O ambiente de recuperação pré-configurado WinPE pode ser transferido aqui ou solicitado através do Dell ProSupport. Contacte o número 877-459-7304, extensão 4310039 para obter suporte telefónico permanente (24 x 7) para o seu produto Dell. Para obter mais informações sobre a recuperação, consulte o artigo 130790 da BDC.

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

13

Anexo B - Criação de suportes de dados de arranque

Utilize este anexo para criar um suporte de dados de arranque.

Gravar o ISO do Ambiente de Recuperação em CD/DVD

A ligação seguinte contém o processo necessário para utilizar o Microsoft Windows 7 para criar um CD ou DVD de arranque para o ambiente de recuperação. Se estiver a utilizar o Windows 10 ou posterior, consulte Gravar o Ambiente de Recuperação em Suportes de Dados Amovíveis.

https://support.microsoft.com/windows/create-installation-media-for-windows

Gravar o Ambiente de Recuperação em Suportes de Dados Amovíveis

Transfira o ISO de recuperação mais recente aqui. Para criar uma unidade USB de arranque, siga as seguintes instruções:

Arranque de legado:

1. Ligue uma unidade USB ao computador.
2. Abra uma linha de comandos administrativa.
3. Aceda ao utilitário Diskpart ao digitar **diskpart**.
4. Localize o disco de destino a modificar, ao digitar **list disk**. Os discos são designados por número.
5. Selecione o disco apropriado através do comando **select disk #**, no qual # deve ser substituído por um número de disco correspondente a uma unidade, conforme indicado no passo anterior.
6. Limpe o disco através do comando **clean**. Isto irá remover completamente os dados da unidade, ao limpar a Tabela de ficheiros.
7. Crie uma partição na qual a imagem de arranque deverá residir.
   a. O comando **create partition primary** gera uma partição principal na unidade.
   b. O comando **select partition 1** seleciona a nova partição.
   c. Utilize o seguinte comando para formatar rapidamente a unidade com o sistema de ficheiros NTFS: **format FS=NTFS quick**.
8. A unidade deve estar marcada como uma unidade de arranque. Utilize o comando **active** para marcar a unidade como unidade de arranque.
9. Para mover ficheiros diretamente para a unidade, atribua uma letra disponível à unidade com o comando **assign**.
10. A unidade é montada automaticamente e os conteúdos do ficheiro ISO podem ser copiados para a raiz da unidade.

Assim que os conteúdos do ficheiro ISO forem copiados, é possível arrancar através da unidade, que pode ser utilizada para realizar uma recuperação.

Arranque EUFI:

1. Ligue uma unidade USB ao computador.
2. Abra uma linha de comandos administrativa.
3. Aceda ao utilitário Diskpart ao digitar **diskpart**.
4. Localize o disco de destino a modificar, ao digitar **list disk**. Os discos serão designados por um número.
5. Selecione o disco apropriado através do comando **select disk #**, no qual # deve ser substituído por um número de disco correspondente a uma unidade, conforme indicado no passo anterior.
6. Limpe o disco através do comando **clean**. Isto irá remover completamente os dados da unidade, ao limpar a Tabela de ficheiros.

7. Crie uma partição na qual a imagem de arranque deverá residir.
   a. O comando **create partition primary** gera uma partição principal na unidade.
   b. O comando **select partition 1** seleciona a nova partição.
   c. Utilize o seguinte comando para formatar rapidamente a unidade com o sistema de ficheiros FAT32: **format FS=FAT32 quick**.
8. A unidade deve estar marcada como uma unidade de arranque. Utilize o comando **active** para marcar a unidade como unidade de arranque.
9. Para mover ficheiros diretamente para a unidade, atribua uma letra disponível à unidade com o comando **assign**.
10. A unidade é montada automaticamente e os conteúdos do ficheiro ISO podem ser copiados para a raiz da unidade.

Assim que os conteúdos do ficheiro ISO forem copiados, é possível arrancar através da unidade, que pode ser utilizada para realizar uma recuperação.