Recuperação de Encryption

Encryption v10.0 / Data Guardian v2.0

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.

© 2012-2018 Dell Inc. Todos os direitos reservados. Dell, EMC e outras marcas comerciais pertencem à Dell Inc ou às suas subsidiárias. Outras marcas comerciais podem pertencer aos seus respetivos proprietários.Marcas comerciais e marcas comerciais registadas utilizadas no Dell Encryption, Endpoint Security Suite Enterprise e no conjunto de aplicações de documentos Data Guardian: Dell™ e o logótipo Dell, Dell Precision™, OptiPlex™, ControlVault™, Latitude™, XPS® e KACE™ são marcas comerciais da Dell Inc. Cylance®, CylancePROTECT e o logótipo Cylance são marcas comerciais registadas da Cylance, Inc. nos EUA e noutros países. McAfee® e o logótipo da McAfee são marcas comerciais ou marcas comerciais registadas da McAfee, Inc. nos Estados Unidos e noutros países. Intel®, Pentium®, Intel Core Inside Duo®, Itanium® e Xeon® são marcas comerciais registadas da Intel Corporation nos EUA e noutros países. Adobe®, Acrobat®, e Flash® são marcas registadas da Adobe Systems Incorporated. Authen Tec® e Eikon® são marcas comerciais registadas da Authen Tec. AMD® é marca registada da Advanced Micro Devices, Inc. Microsoft®, Windows® e Windows Server®, Internet Explorer®, Windows Vista®, Windows 7®, Windows 10®, Active Directory®, Access®, BitLocker®, BitLocker To Go®, Excel®, Hyper-V®, Outlook®, PowerPoint®, Word®, OneDrive®, SQL Server® e Visual C++® são marcas comerciais ou marcas comerciais registadas da Microsoft Corporation nos Estados Unidos e/ou noutros países. VMware® é marca registada ou marca comercial da VMware, Inc. nos Estados Unidos ou noutros países. Box® é marca registada da Box. Dropbox℠ é uma marca de serviço da Dropbox, Inc. Google™, Android™, Google™ Chrome™, Gmail™ e Google™ Play são marcas comerciais ou marcas comerciais registadas da Google Inc. nos Estados Unidos e noutros países. Apple®, App Store℠, Apple Remote Desktop™, Boot Camp™, FileVault™, iPad®, iPhone®, iPod®, iPod touch®, iPod shuffle® e iPod nano®, Macintosh® e Safari® são marcas de serviço, marcas comerciais ou marcas comerciais registadas da Apple, Inc. nos Estados Unidos e/ou noutros países. EnCase™ e Guidance Software® são marcas comerciais ou marcas registradas da Guidance Software. Entrust® é marca registada da Entrust®, Inc. nos Estados Unidos e noutros países. Mozilla® Firefox® é uma marca comercial registada da Mozilla Foundation nos Estados Unidos e/ou noutros países. iOS® é uma marca comercial ou marca comercial registada da Cisco Systems, Inc. nos Estados Unidos e outros países e é utilizada sob licença. Oracle® e Java® são marcas registadas da Oracle e/ou suas afiliadas. Travelstar® é marca registada da HGST, Inc. nos Estados Unidos e noutros países. UNIX® é marca registada da The Open Group. VALIDITY™ é uma marca comercial da Validity Sensors, Inc. nos Estados Unidos e noutros países. VeriSign® e outras marcas similares são marcas comerciais ou marcas comerciais registadas da VeriSign, Inc. ou respetivas filiais ou subsidiárias nos Estados Unidos e noutros países e licenciadas à Symantec Corporation. KVM on IP® é marca registada da Video Products. Yahoo!® é marca registada da Yahoo! Inc. Bing® é uma marca comercial registada da Microsoft Inc. Ask® é uma marca registada da IAC Publishing, LLC. Os outros nomes podem ser marcas comerciais dos respetivos proprietários.

Encryption v10.0 / Data Guardian v2.0

2018 - 08

Rev. A01

Índice

1

Como começar a recuperação

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

- Suporte de CD-R, DVD-R ou USB formatado
  - Se gravar um CD ou DVD, consulte Gravar o ISO do ambiente de recuperação em CD\DVD para obter detalhes.
  - Se utilizar um suporte USB, consulte Gravar o ambiente de recuperação em suporte de dados amovível 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

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, 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 ou Código de serviço expresso disponível quando nos contactar.

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

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.

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.

Efetuar a encriptação Policy-based ou FFE

Siga estes passos para realizar uma recuperação Policy-Based ou FFE.

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

Para transferir o ficheiro de recuperação:

1 Transfira o pacote de instalação Dell Encryption em http://www.dell.com/support/home/us/en/19/product-support/product/dell-data-protection-encryption/drivers . Aceda à pasta **AdminUtilities** no pacote de instalação e abra o **CMGAd.exe**.
2 No campo **Servidor Dell**, introduza o Security Management Server/Security Management Server Virtual utilizado para ativar o utilizador.
3 No campo **Administrador Dell**, introduza um nome de conta de utilizador com privilégios de administrador forense.
4 No campo **Palavra-passe**, introduza a palavra-passe para o administrador forense.
5 No campo **MCID**, introduza o FQDN do dispositivo em recuperação.

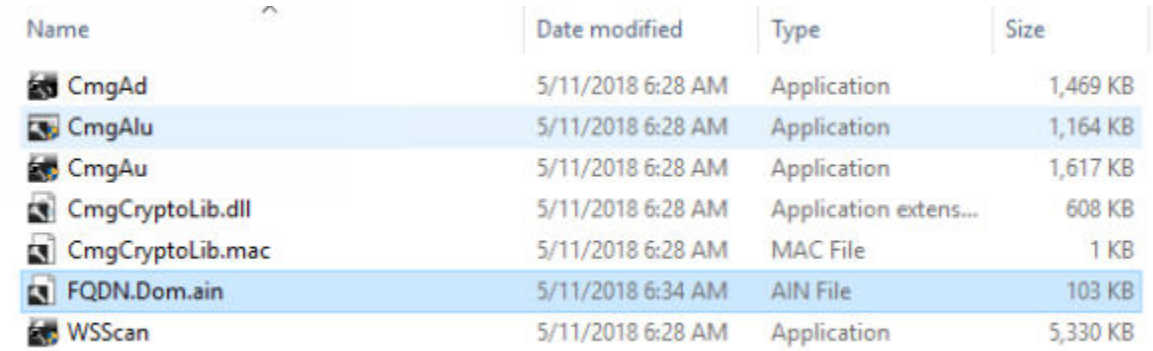
- O campo **DCID** é a ID de recuperação do dispositivo a ser recuperado.

6 Selecione **Seguinte**.

7 Defina e confirme a **Frase de acesso** para o ficheiro a ser recuperado. Esta frase de acesso é necessária para realizar a recuperação.

8 No campo **Transferir para:**, introduza um local de destino para o pacote de recuperação e, em seguida, selecione **Seguinte**. Por predefinição, estará no diretório a partir do qual o CMGAd.exe foi executado.

9 O pacote de recuperação é transferido para a pasta especificada em **Transferir para:**.



10 Copie o ficheiro do pacote de recuperação para uma localização onde possa ser acedido 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 3 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 reinicializar o computador de destino e não existir falha de hardware, pode ser realizada recuperação de dados no computador inicializado 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, ao tentar abrir ou copiar um ficheiro, ocorre um erro de *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 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.

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

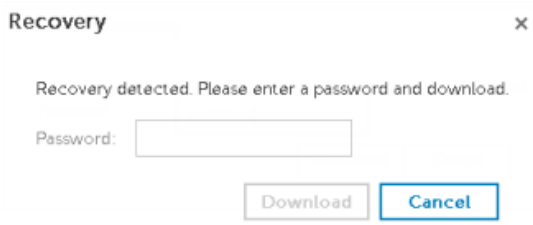
Siga estes passos para realizar uma recuperação do HCA.

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: A recuperação requer um ambiente de 64 ou de 32 bits com base no modo de arranque da BIOS.

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.

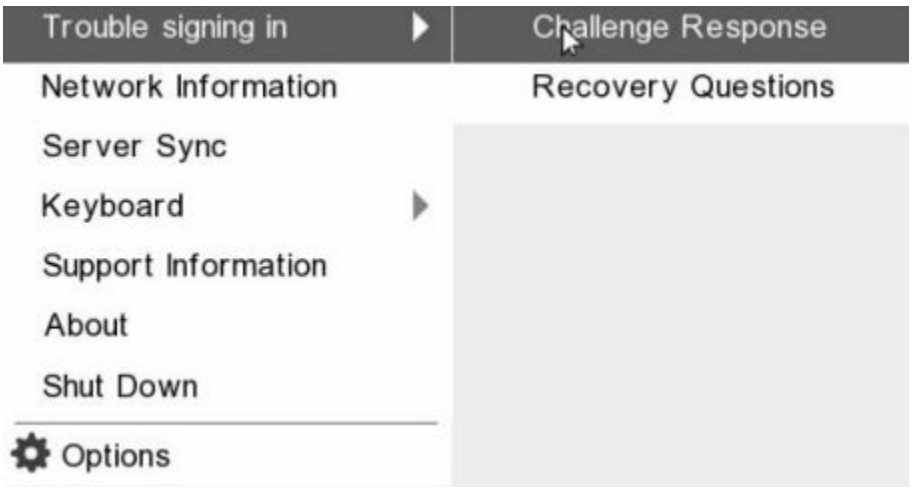
NOTA:
Certifique-se de que retira qualquer suporte USB ou CD/DVD usado para inicializar o computador. O incumprimento deste princípio poderá resultar na inicialização novamente no ambiente de recuperação.

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

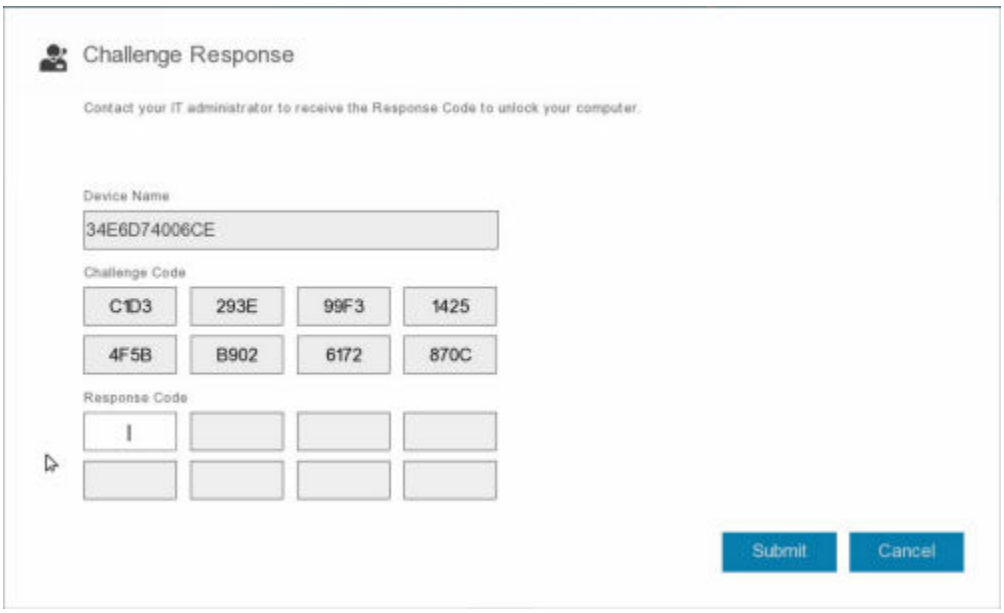
Recuperação de Desafio com SED

Ignorar o Ambiente de Autenticação de pré-arranque

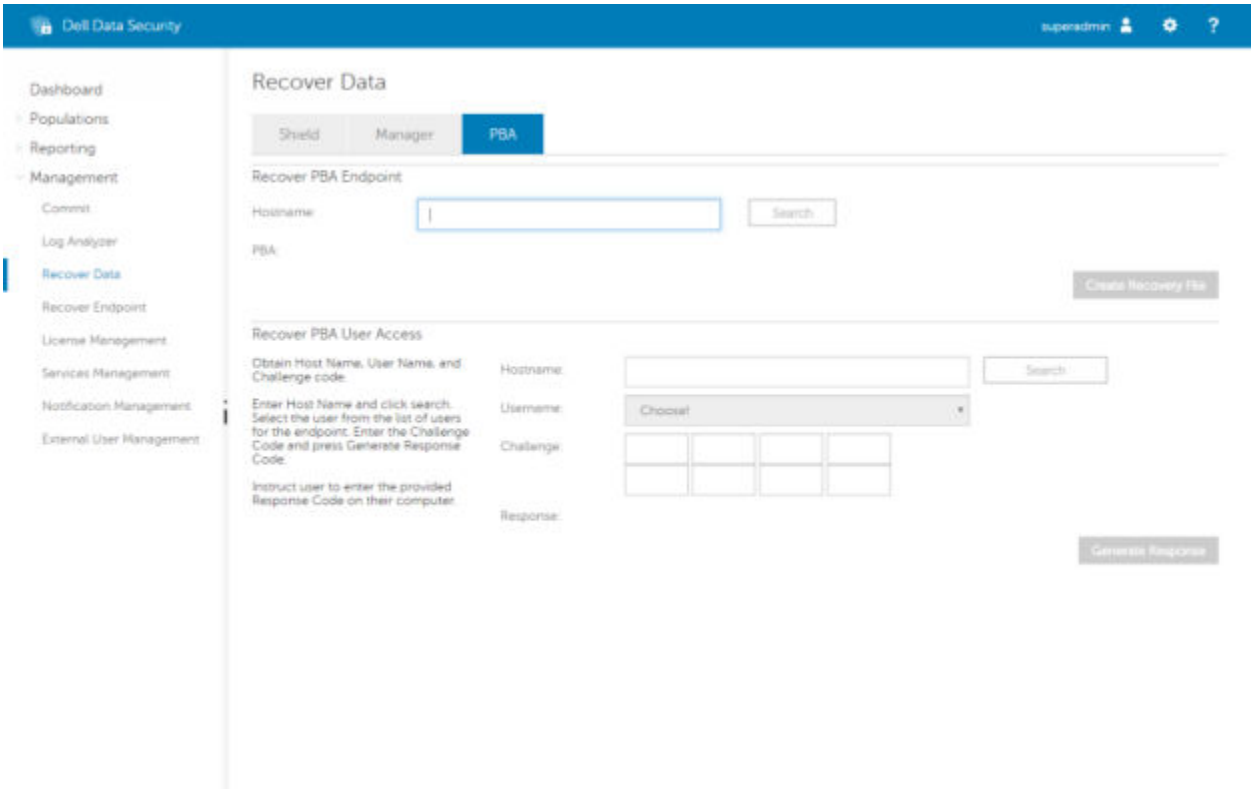
Os utilizadores esquecem-se das palavras-passe e telefonam para o Suporte Técnico para obter assistência para ultrapassar o ambiente PBA. Utilize o mecanismo de Desafio/Resposta que está incorporado no dispositivo. Este mecanismo é configurado por utilizador e tem por base um conjunto rotativo de caracteres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



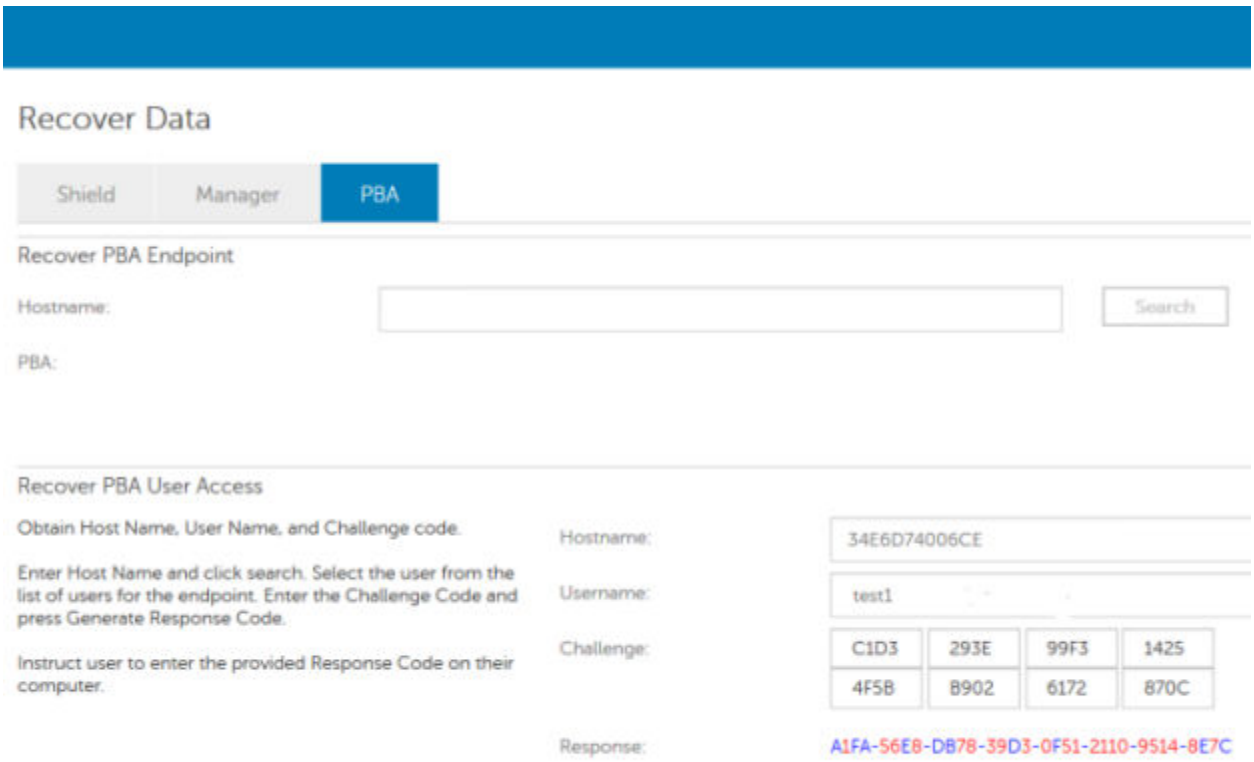
A seguinte informação é apresentada após selecionar **Desafio Resposta**.



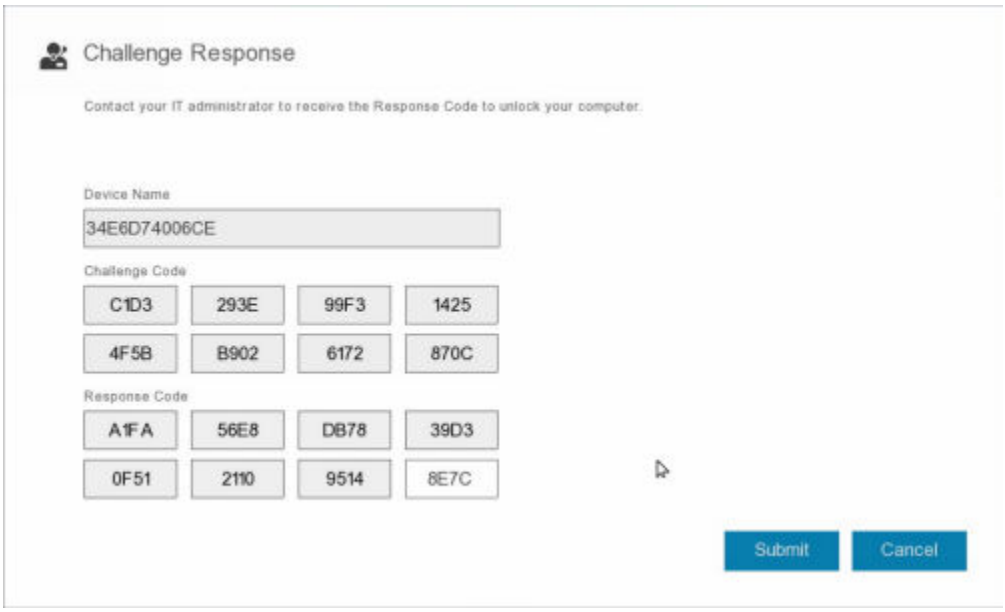
O campo **Nome do dispositivo** é utilizado pelo técnico de Suporte Técnico na Remote Management Console para encontrar o dispositivo correto e, em seguida, é selecionado um nome de utilizador. Isto pode ser encontrado em **Gestão > Recuperar dados** no separador **PBA**.



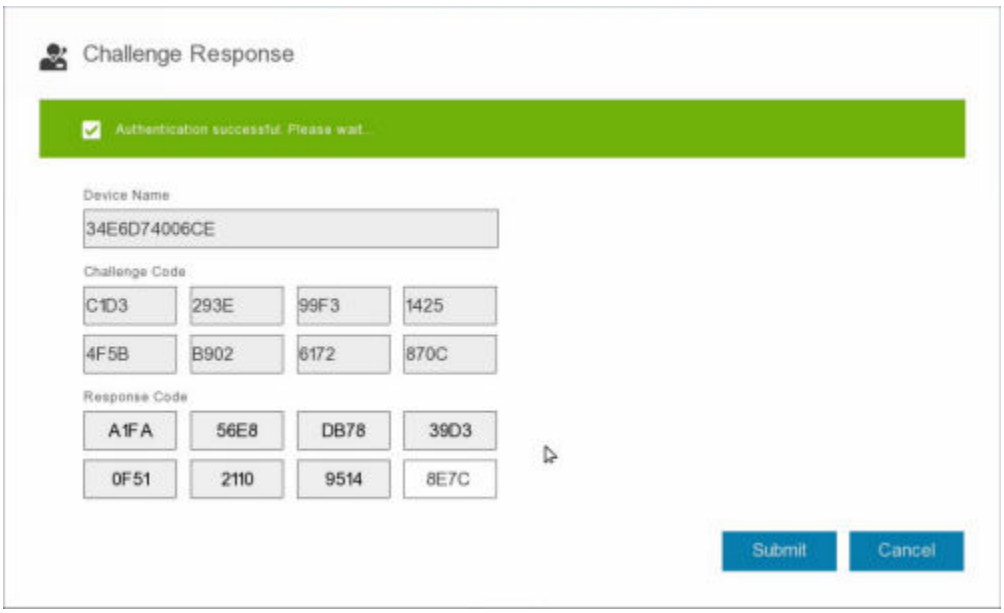
O código de desafio é fornecido ao técnico de Suporte Técnico, que introduz os dados e, em seguida, clica no botão **Gerar resposta**.



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

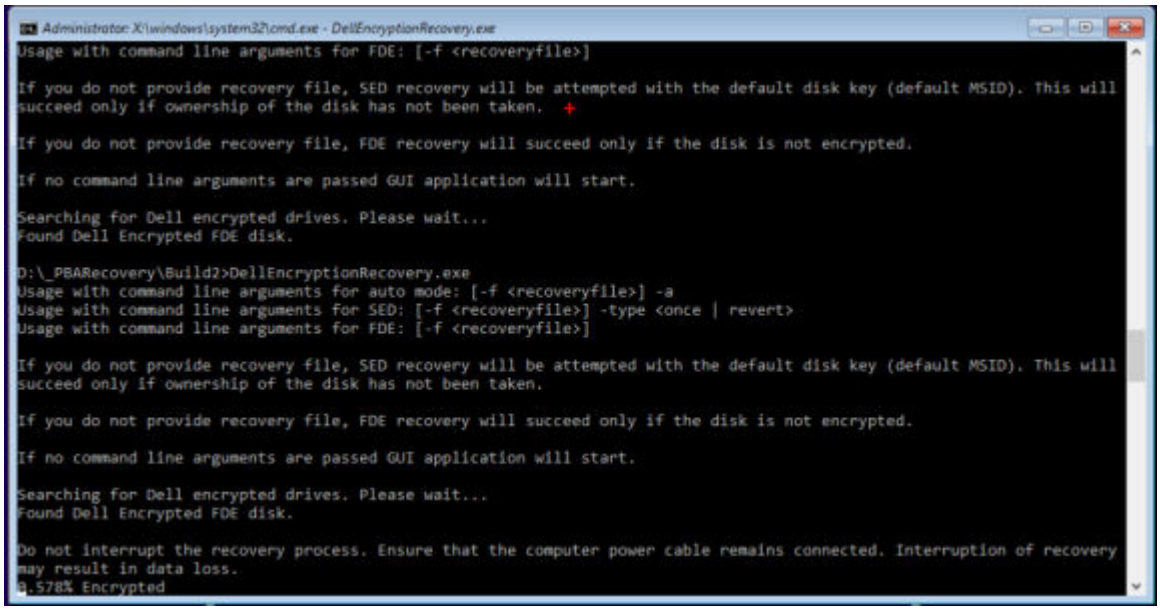
1 Usando o suporte multimédia de arranque criado anteriormente, arranque num sistema de recuperação ou no dispositivo onde se encontra a unidade que deseja recuperar. Abre-se um ambiente WinPE com a aplicação de recuperação.

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.

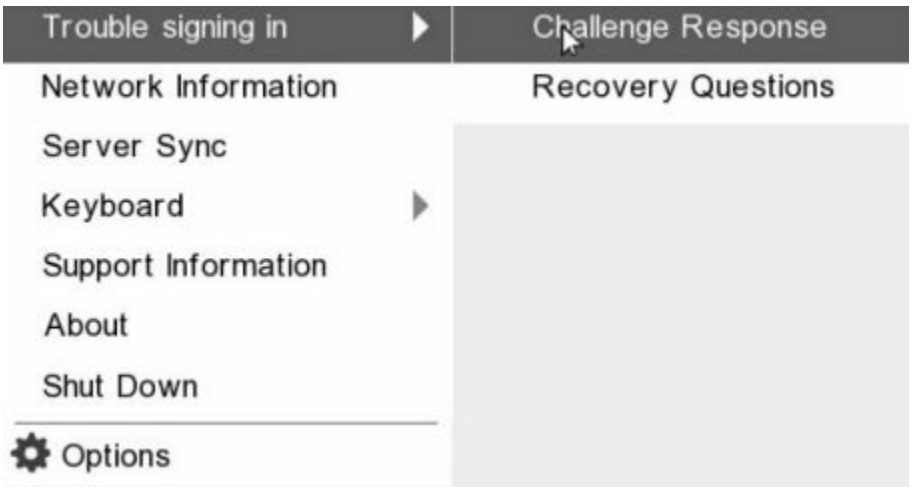
NOTA:
Certifique-se de que retira qualquer suporte USB ou CD/DVD usado para inicializar o computador. O incumprimento deste princípio poderá resultar na inicialização novamente no ambiente de recuperação.

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

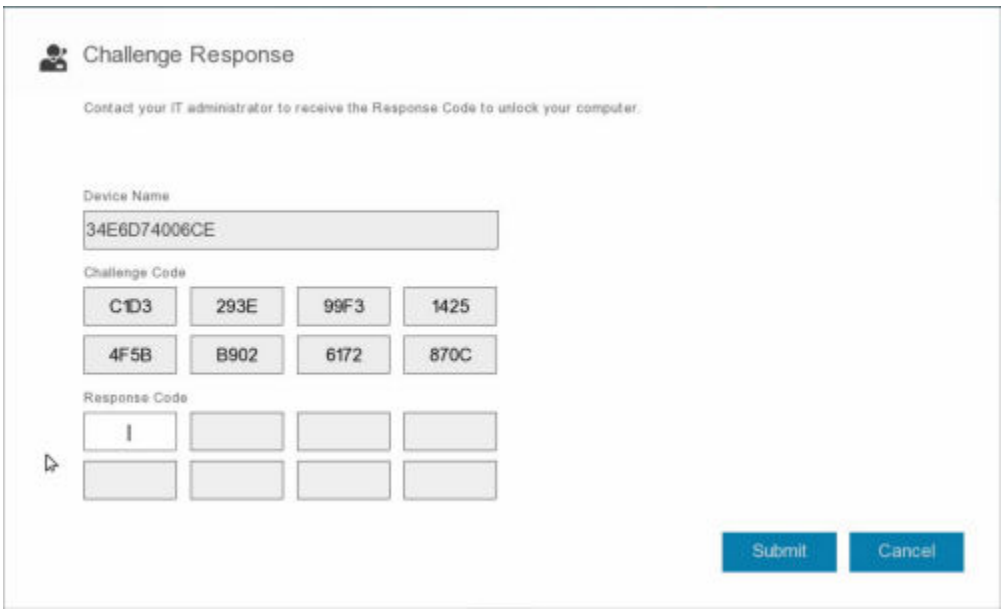
Recuperação de Desafio com Full Disk Encryption

Ignorar o ambiente de Autenticação de pré-arranque

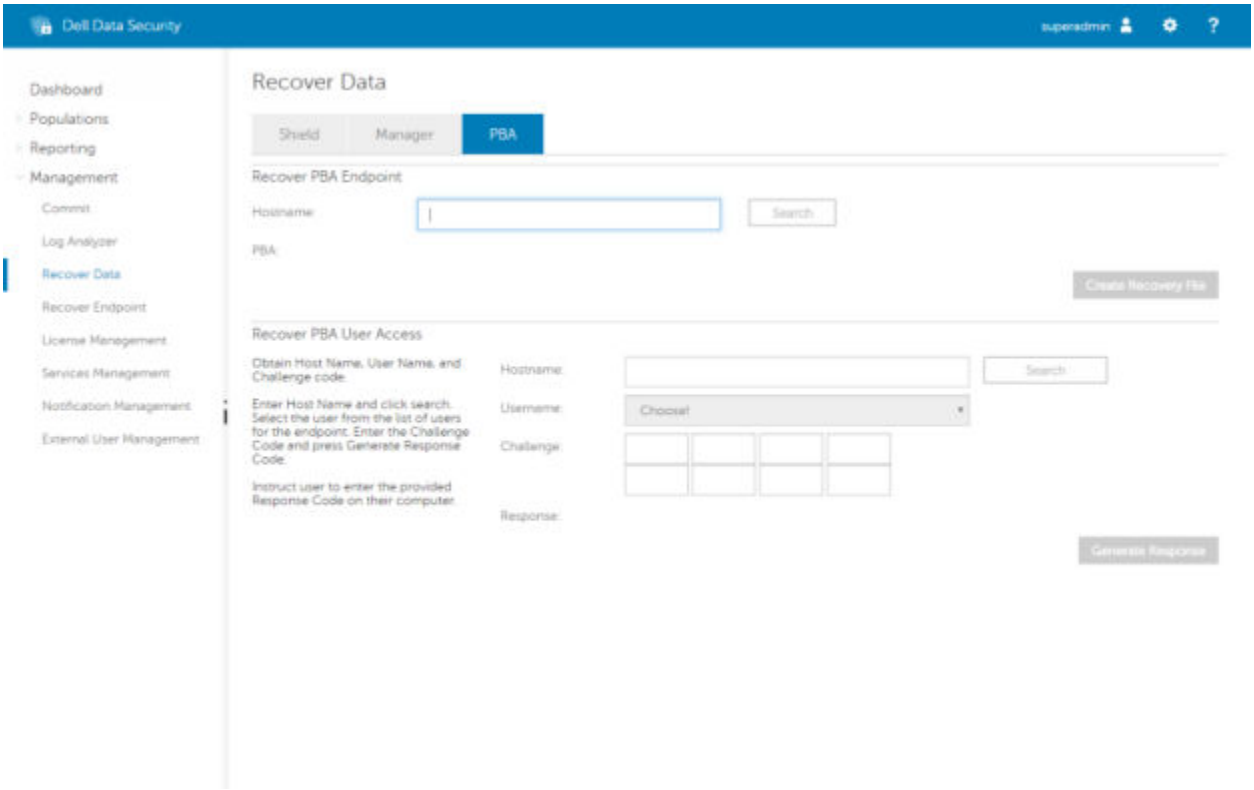
Os utilizadores esquecem-se das palavras-passe e telefonam para o Suporte Técnico para obter assistência para ultrapassar o ambiente PBA. Utilize o mecanismo de Desafio/Resposta que está incorporado no dispositivo. Este mecanismo é configurado por utilizador e tem por base um conjunto rotativo de caracteres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



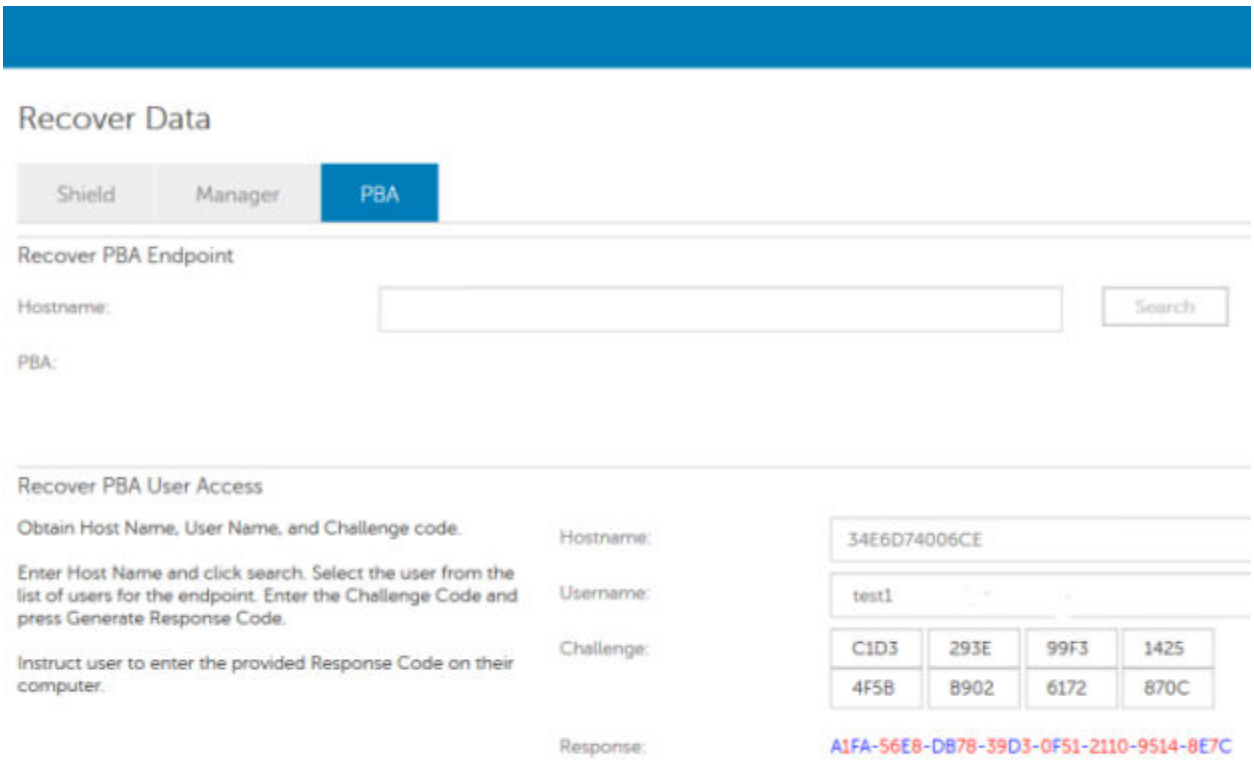
A seguinte informação é apresentada após selecionar **Desafio Resposta**.



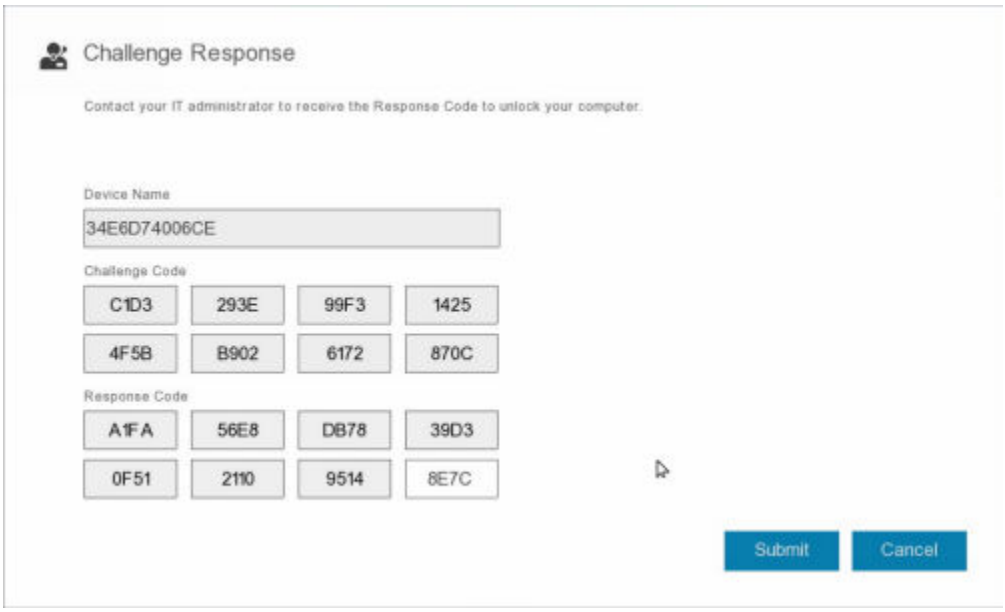
O campo **Nome do dispositivo** é utilizado pelo técnico de Suporte Técnico na Remote Management Console para encontrar o dispositivo correto e, em seguida, é selecionado um nome de utilizador. Isto pode ser encontrado em **Gestão > Recuperar dados** no separador **PBA**.



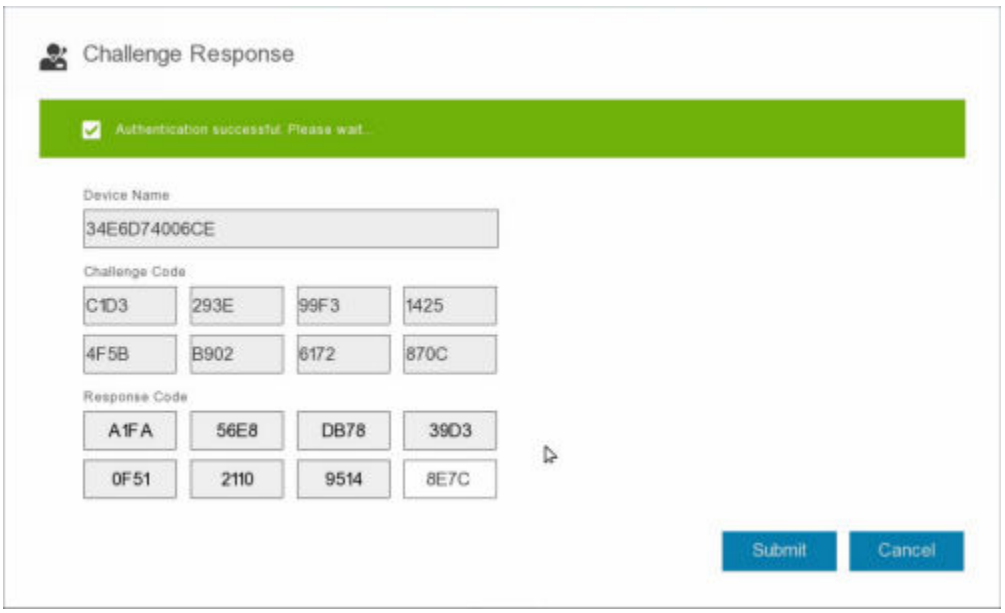
O código de desafio é fornecido ao técnico de Suporte Técnico, que introduz os dados e, em seguida, clica no botão **Gerar resposta**.



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 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 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.

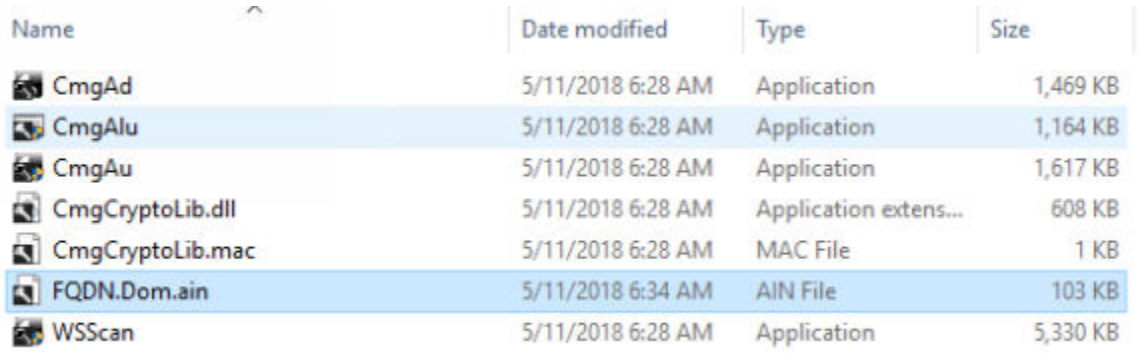
d Clique em **Criar ficheiro de recuperação**.
É transferido o ficheiro **<nome do anfitrião>-sed-recovery.dat**.

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

Para transferir o ficheiro de recuperação:

1 Transfira o pacote de instalação Dell Encryption em http://www.dell.com/support/home/us/en/19/product-support/product/dell-data-protection-encryption/drivers . Aceda à pasta **AdminUtilities** no pacote de instalação e abra o **CMGAd.exe**.
2 No campo **Servidor Dell**, introduza o Security Management Server/Security Management Server Virtual utilizado para ativar o utilizador.
3 No campo **Administrador Dell**, introduza um nome de conta de utilizador com privilégios de administrador forense.
4 No campo **Palavra-passe**, introduza a palavra-passe para o administrador forense.
5 No campo **MCID**, introduza o FQDN do dispositivo em recuperação.
   - O campo **DCID** é a ID de recuperação do dispositivo a ser recuperado.
6 Selecione **Seguinte**.
7 Defina e confirme a **Frase de acesso** para o ficheiro a ser recuperado. Esta frase de acesso é necessária para realizar a recuperação.
8 No campo **Transferir para:**, introduza um local de destino para o pacote de recuperação e, em seguida, selecione **Seguinte**. Por predefinição, estará no diretório a partir do qual o CMGAd.exe foi executado.

9 O pacote de recuperação é transferido para a pasta especificada em **Transferir para:**.

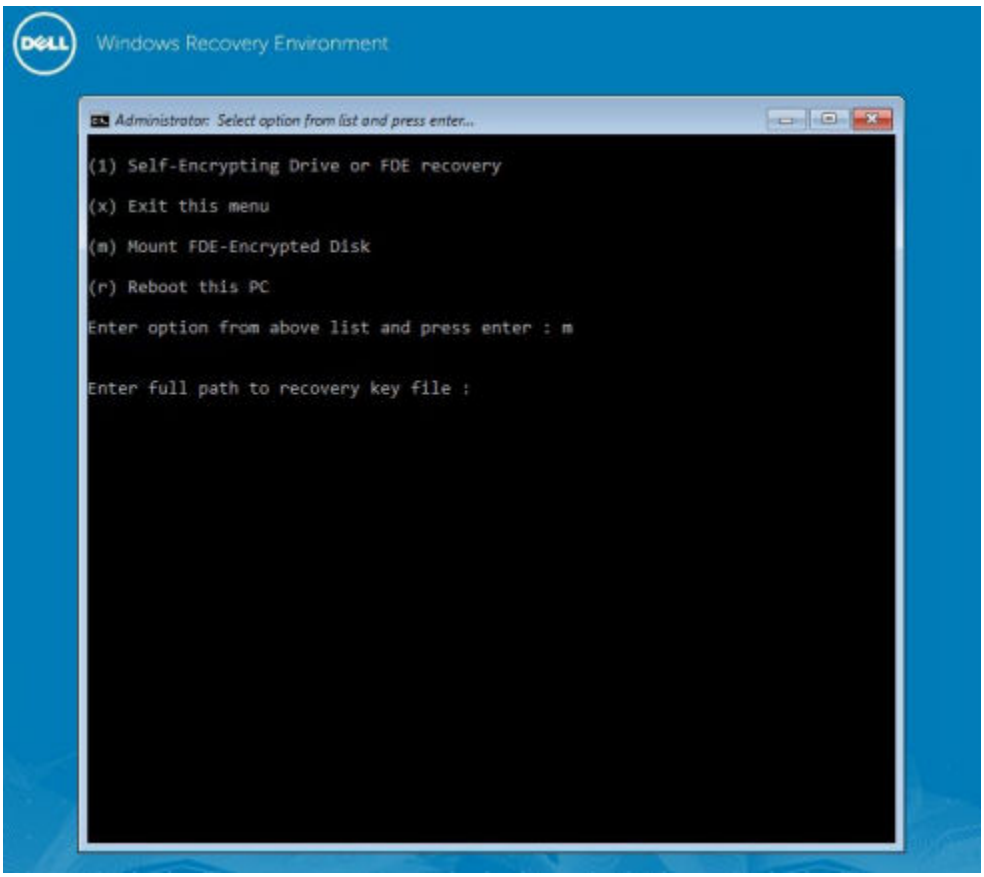


10 Copie o ficheiro do pacote de recuperação para uma localização onde possa ser acedido ao reinicializar em WinPE.

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.

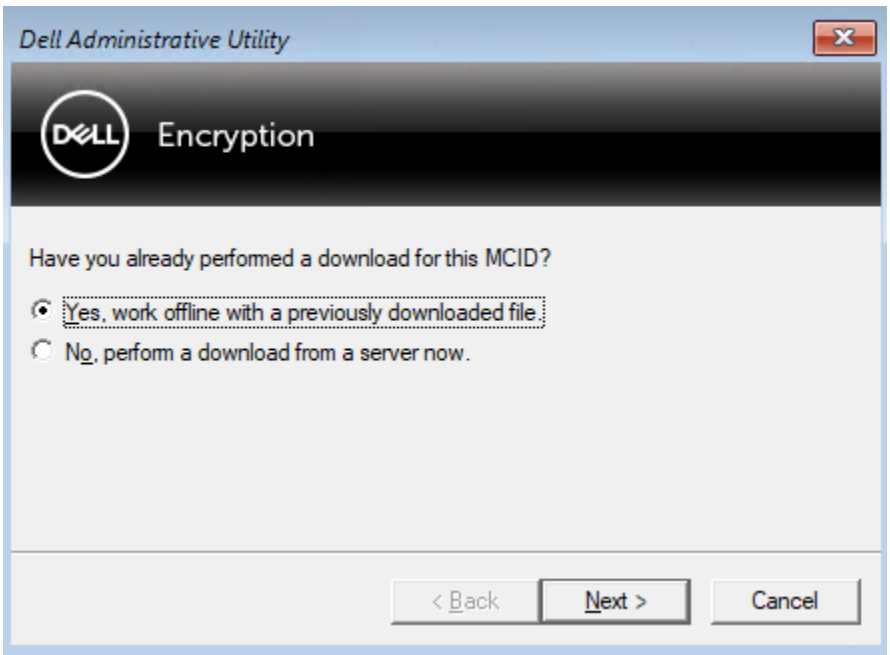
```
Enter option from above list and press enter : m

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**.

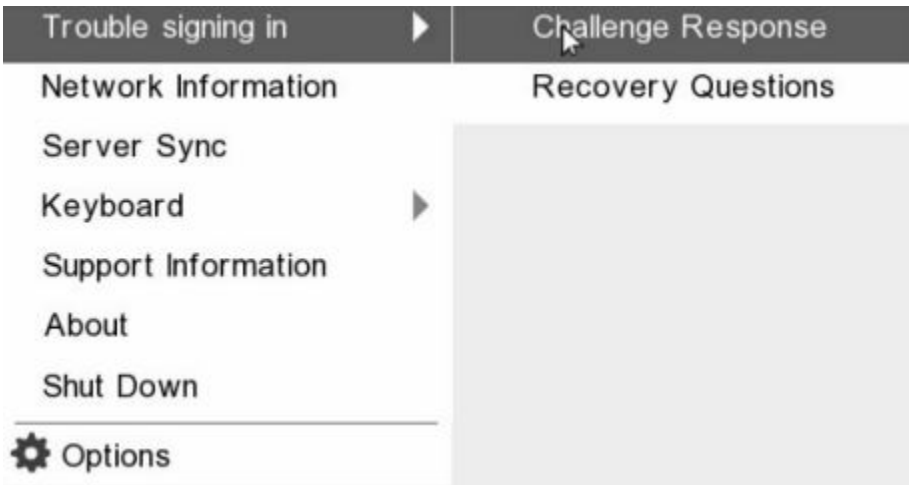
NOTA:
Certifique-se de que retira qualquer suporte USB ou CD/DVD usado para inicializar o computador. O incumprimento deste princípio poderá resultar na inicialização novamente no ambiente de recuperação.

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

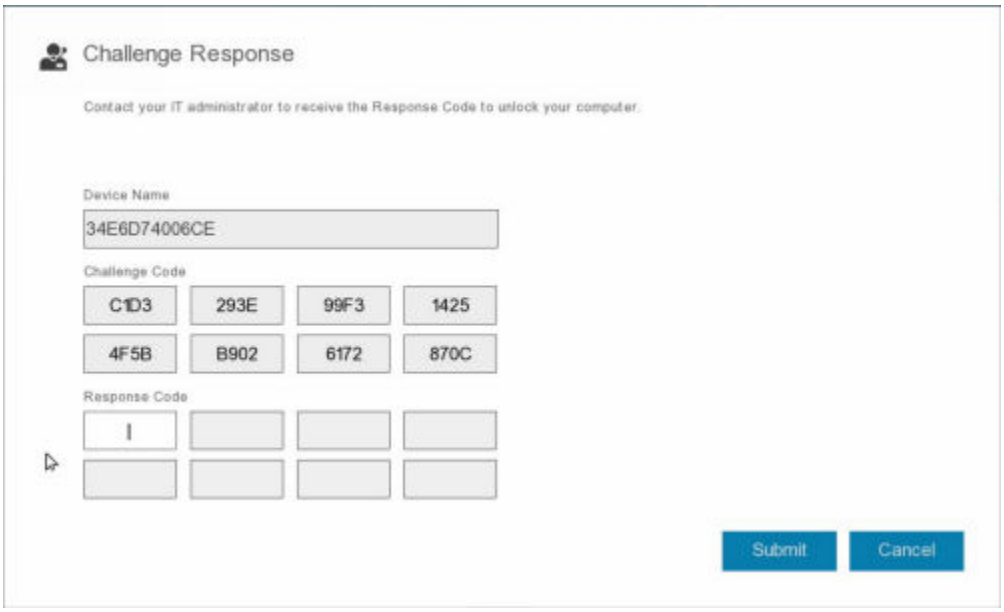
Recuperação de Desafio com Full Disk Encryption

Ignorar o ambiente de Autenticação de pré-arranque

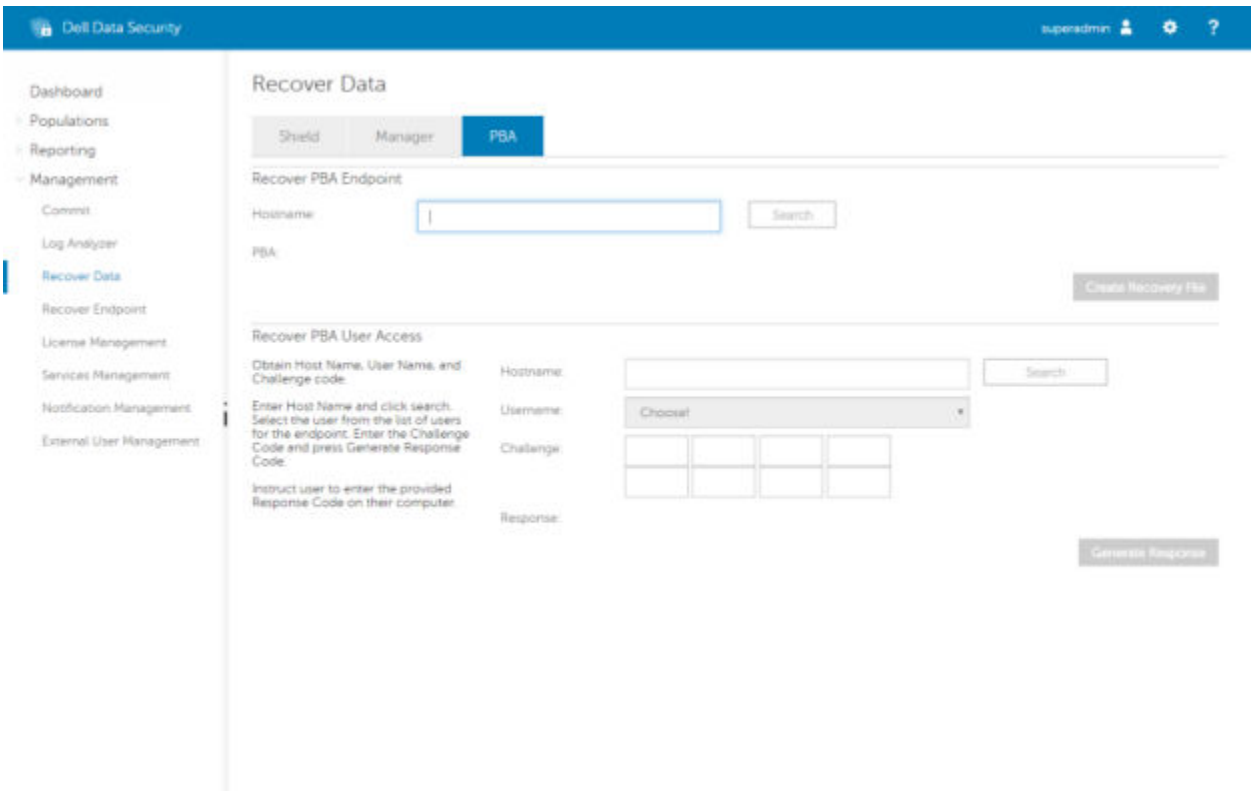
Os utilizadores esquecem-se das palavras-passe e telefonam para o Suporte Técnico para obter assistência para ultrapassar o ambiente PBA. Utilize o mecanismo de Desafio/Resposta que está incorporado no dispositivo. Este mecanismo é configurado por utilizador e tem por base um conjunto rotativo de caracteres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



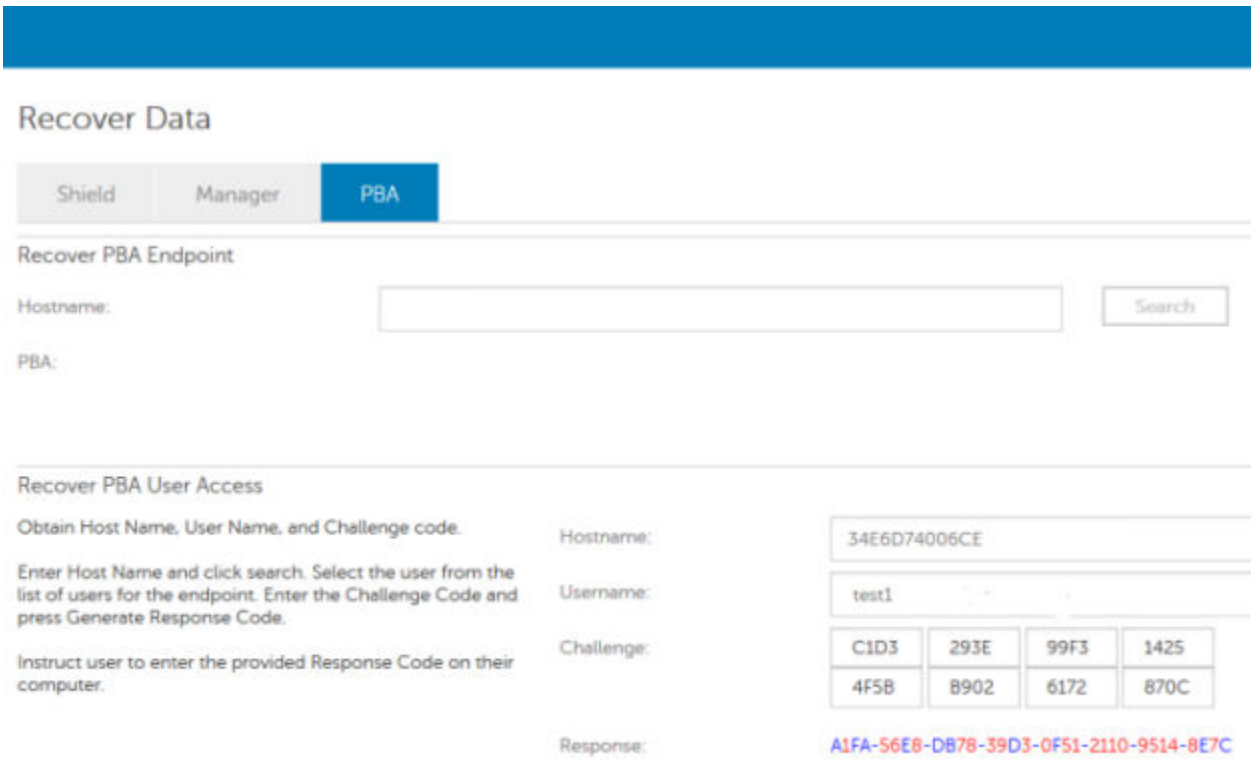
A seguinte informação é apresentada após selecionar **Desafio Resposta**.



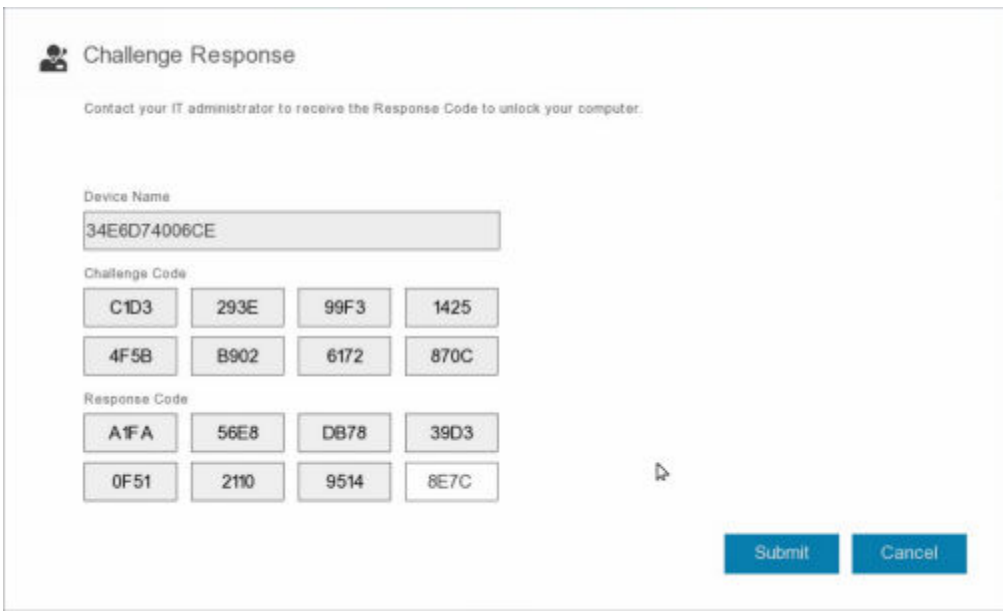
O campo **Nome do dispositivo** é utilizado pelo técnico de Suporte Técnico na Remote Management Console para encontrar o dispositivo correto e, em seguida, é selecionado um nome de utilizador. Isto pode ser encontrado em **Gestão > Recuperar dados** no separador **PBA**.



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 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 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 as Instruções de recuperação da Microsoft.

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.

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.

Recuperação do Dell Data Guardian

A ferramenta de recuperação permite:

- Desencriptação de:
  - Ficheiros protegidos do Office com qualquer formato suportado - ficheiros que estão protegidos pela encriptação de Documentos protegidos do Office do Data Guardian e pela proteção do respetivo Fornecedor de serviços em nuvem podem ser recuperados.
  - Formatos de ficheiros listados na política de proteção básica de ficheiros, se ativada.
- Caucionamento manual do material de chave
- Capacidade para procurar ficheiros adulterados
- Capacidade para forçar a desencriptação de documentos do Office protegidos cujo invólucro, como a página de capa do ficheiro de Office protegido, tenha sido adulterado, na nuvem ou num dispositivo sem Data Guardian

NOTA:
Pode utilizar a ferramenta de recuperação do Windows com ficheiros criados num Mac, telemóvel ou em plataformas do Portal Web.

Pré-requisitos

Os pré-requisitos incluem:

- Microsoft .Net Framework 4.5.2 em execução no ponto final a recuperar.
- A função de administrador forense tem de ser atribuída na Consola de Gestão para o administrador que efetua a recuperação.

Realizar a recuperação do Data Guardian

Siga estes passos para executar uma recuperação dos documentos do Office protegidos do Data Guardian. Pode realizar a recuperação de um computador de cada vez.

IMPORTANTE:
Para evitar a perda de conteúdos em caso de danos, desencripte cópias dos ficheiros e não os ficheiros originais.

Executar uma recuperação a partir do Windows, de unidade USB ou de uma unidade de rede

Para executar uma recuperação:

1 A partir do suporte de instalação Dell, copie**RecoveryTools.exe** para uma destas localizações:

- Computador - Copie o .exe para o computador no qual serão recuperados os documentos de Office.
- USB - Copie o .exe para a unidade USB e execute-o a partir desta.
- Unidade de rede

IMPORTANTE:
Enquanto administrador, certifique-se de que copia apenas o **RecoveryTools.exe** e não o instalador. O **RecoveryTools.exe** funciona melhor se nenhum varrimento ou desencriptação estiver a ser executado.

2 Faça duplo clique em **RecoveryTools.exe** para iniciar a ferramenta de recuperação.

3 Na janela da Ferramenta de recuperação Data Guardian, selecione **Início de sessão no domínio**.

> **NOTA:**
> A opção de início de sessão SaaS para uma solução alojada destina-se a um lançamento futuro.

4 Introduza o FQDN do Dell Server neste formato:
server.domain.com

> **NOTA:**
> São adicionados automaticamente um prefixo e um sufixo ao FQDN.

5 Introduza o nome de utilizador e palavra-passe e clique em **Iniciar sessão**.

> **NOTA:**
> Não desmarque a caixa de verificação *Ativar confiança SSL*, exceto se for instruído pelo administrador.

> **NOTA:**
> Se não for um administrador forense e introduzir as credenciais, é apresentada uma mensagem indicando que não têm direitos de início de sessão.

6 Se for um administrador forense, a ferramenta de recuperação abre.

7 Selecione a **Origem**.

> **NOTA:**
> Deve procurar para uma origem e um destino, mas pode selecioná-las em qualquer ordem.

8 Clique em **Procurar** para selecionar a pasta ou a unidade a recuperar.

9 Clique em **OK**.

10 Clique em **Destino**, uma pasta vazia para os ficheiros desencriptados ou recuperados.

11 Clique em **Procurar** para selecionar um destino, como um dispositivo externo, a localização de um diretório ou o Ambiente de trabalho.

12 Clique em **OK**.

13 Selecione uma ou mais caixas de verificação com base no que pretende recuperar.

Opções	Descrição
Caução	• Recupere chaves geradas offline que não foi possível caucionar para o Dell Server. • Se um disco rígido falhar enquanto o utilizador está offline da rede, utilize a unidade secundária para recuperar dados e chaves não caucionadas do computador.
Desencriptar	Aponte a ferramenta de recuperação para um diretório que contenha documentos do Office protegidos para o desencriptar. **NOTA:** Como prática recomendada, desencripte cópias dos ficheiros, não os originais, para a eventualidade de ocorrer corrupção dos ficheiros. Opcionalmente, se tiver ocorrido sabotagem, selecione uma ou mais das seguintes opções (consulte os detalhes abaixo): • **Verificação de adulteração** - verifica se existem ficheiros adulterados, mas não os desencripta.

Opções	Descrição
	• **Verificação de adulteração** e **Forçar desencriptação mesmo se adulterado** - verifica se existem ficheiros adulterados e se foi adulterado o invólucro do documento do Office; o Data Guardian repara o invólucro e desencripta o documento do Office.
Verificar adulteração	Deteta os ficheiros adulterados e regista-os ou notifica-o. Regista o autor que adulterou o ficheiro. Não desencripta os ficheiros.
Forçar desencriptação, mesmo se adulterado	Para selecionar esta opção, terá de selecionar também **Verificação de adulteração**. Se uma pessoa não autorizada tiver adulterado o invólucro de um documento do Office protegido, como a página de rosto, tanto na nuvem como num dispositivo sem Data Guardian, selecione esta opção para reparar o invólucro e para forçar a desencriptação do ficheiro do Office protegido. **NOTA:** Se alguém tiver adulterado a encriptação do ficheiro .xen do Office dentro do invólucro, o ficheiro não pode ser recuperado.

Cada documento do Office protegido tem uma marca de água oculta que contém um histórico do utilizador e do nome do computador original, assim como o nome de qualquer outro computador que tenha efetuado alterações ao ficheiro. Por predefinição, a ferramenta de recuperação verifica as marcas de água ocultas e adiciona um ficheiro de texto com uma lista de todos os autores a uma pasta *HiddenWatermark* nos registos.

14 Após a realização das seleções, clique em **Analisar**.

A área de Registo exibe:

- Pastas encontradas e analisadas dentro da origem selecionada
- A desencriptação, por ficheiro, foi concluída com êxito ou falhou
- O nome do último autor de um ficheiro

A ferramenta de recuperação adiciona os ficheiros recuperados ao destino selecionado. É possível abrir e visualizar os ficheiros

Visualizar dados de Registo de auditoria oculto

No Windows, se a política do Registo de auditoria oculto para documentos protegidos do Office estiver ativada, as informações do utilizador são registadas nos metadados do ficheiro. Para visualizar estes dados, utilize a Ferramenta de recuperação:

1 Inicie a Ferramenta de recuperação.
   - Para selecionar a **Origem**, aceda a uma pasta que contenha documentos protegidos do Office com dados de auditoria ocultos. A Ferramenta de recuperação copia a estrutura de pastas e subpastas, desencriptando quaisquer documentos protegidos do Office que possuam dados de auditoria ocultos.
   - Antes de aceder a um **Destino**, pode criar uma pasta para os ficheiros desencriptados e, em seguida, aceder a esta pasta.

2 Selecione **Desencriptar**.

3 Após a realização das seleções, clique em **Analisar**.

A pasta selecionada como Destino contém uma pasta *Ficheiros recuperados* datada com o seguinte:

- Ficheiros protegidos do Office desencriptados
- Pasta *Registo de auditoria*, criada pela Ferramenta de recuperação, com um ficheiro .txt para cada ficheiro desencriptado. Cada ficheiro .txt tem um registo com uma lista das informações dos ficheiros desencriptados, como, por exemplo, os autores, o último autor e o carimbo de data/hora.

Anexo A - Gravação do ambiente de recuperação

É possível efetuar a transferência do programa de instalação principal.

Gravar o ISO Ambiente de recuperação em CD/DVD

A ligação seguinte contém o processo necessário para utilizar o Microsoft Windows 7, Windows 8 ou Windows 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

Gravar o ambiente de recuperação em suportes de dados amovíveis

Para criar uma unidade USB de arranque, siga as seguintes instruções:

Arranque de legado:

1 Ligue uma unidade USB ao sistema.
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 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 será montada automaticamente e os conteúdos do ficheiro ISO podem ser copiados para a raiz da unidade.

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

Arranque UEFI:

1 Ligue uma unidade USB ao sistema.
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 será montada automaticamente e os conteúdos do ficheiro ISO podem ser copiados para a raiz da unidade.

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