Dell Data Security

Guia de Recuperação v8.17/v1.7/v1.5

Notas, avisos e advertências

NOTA: Uma NOTA indica informações importantes que ajudam você a usar melhor o seu produto.

AVISO: Um AVISO indica possíveis danos ao hardware ou perda de dados e ensina como evitar o problema.

ADVERTÊNCIA: Uma ADVERTÊNCIA indica possíveis danos à propriedade, risco de lesões corporais ou mesmo risco de vida.

Guia Recuperação

2018 - 01

Rev. A01

Índice

1

Introdução à recuperação

Esta seção detalha o que é necessário para criar o ambiente de recuperação.

- Mídia CD-R, DVD-R ou mídia USB formatada
  - Se estiver gravando um CD ou DVD, analise Gravação do ambiente ISO de recuperação para CD\DVD para obter detalhes.
  - Se estiver usando mídia USB, analise Gravação do ambiente de recuperação em mídia removível para obter detalhes.
- Pacote de recuperação para dispositivo com falha
  - Para clientes gerenciados remotamente, as instruções a seguir explicam como obter um pacote de recuperação do Dell Servidor de gerenciamento de segurança.
  - Para clientes gerenciados localmente, o pacote de recuperação foi criado durante a configuração em uma unidade de rede compartilhada ou em uma mídia externa. Encontre este pacote antes de continuar.

Entre em contato com o Dell ProSupport

Ligue para 877-459-7304, extensão 4310039 para obter suporte por telefone, 24 horas por dia, 7 dias na semana, para o seu produto Dell.

Há também disponível o serviço de suporte on-line para os produtos Dell no site dell.com/support. O suporte on-line inclui drivers, manuais, orientações técnicas, perguntas frequentes e problemas emergentes.

Quando telefonar, tenha em mãos a Etiqueta de serviço ou Código de serviço expresso, para nos ajudar a garantir que possamos direcioná-lo rapidamente ao especialista técnico correto.

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

2

Recuperação de criptografia baseada em política ou arquivo/pasta

A recuperação é necessária quando o computador criptografado não inicializará o sistema operacional. Isso ocorre quando o registro é incorretamente modificado ou quando ocorreram alterações de hardware em um computador criptografado.

Com a recuperação FFE (File/Folder Encryption - Criptografia de pastas/arquivos) ou baseada em política, você pode acessar:

- Um computador que não inicializa e que mostra um prompt para executar uma recuperação de SDE.
- Um computador exibe BSOD com um Código de parada 0x6f ou 0x74.
- Um computador cujos dados criptografados não podem ser acessados ou cujas políticas não podem ser editadas.
- Um servidor com o Dell Encryption que atenda uma das condições acima.
- Um computador com uma placa de Hardware Crypto Accelerator ou uma placa-mãe/TPM que precisa ser trocada.

NOTA: Hardware Crypto Accelerator não é suportado, a partir da v8.9.3.

Visão geral do processo de recuperação

NOTA: A recuperação exige um ambiente de 32 bits.

Para recuperar um sistema que falhou:

1 Grave o ambiente de recuperação em um CD/DVD ou crie um USB inicializável. Consulte o Apêndice A - Gravação do ambiente de recuperação.
2 Obtenha o arquivo de recuperação.
3 Execute a recuperação.

Executar recuperação FFE ou criptografia baseada em política

Execute este procedimento para realizar uma recuperação FFE ou criptografia baseada em política.

Obter o arquivo de recuperação - Computador gerenciado remotamente

Para fazer download do arquivo **<machinename_domain.com>.exe**:

1 Abra o Remote Management Console e, no painel esquerdo, selecione **Gerenciamento** > **Recuperar endpoint**.
2 No campo Nome de host, digite o nome de domínio totalmente qualificado do endpoint e clique em **Pesquisar**.
3 Na janela Recuperação, digite uma senha de recuperação e clique em **Fazer download**.

NOTA:
Você precisa memorizar essa senha para acessar as chaves de recuperação.

4 Copie o arquivo **<machinename_domain.com > .exe** para um local onde ele possa ser acessado ao ser inicializado no WinPE.

Obter o arquivo de recuperação - Computador gerenciado localmente

Para obter o arquivo de recuperação do Encryption Personal:

1 Localize o arquivo de recuperação chamado **LSARecovery_<systemname > .exe**. O arquivo estava armazenado em uma unidade de rede ou um armazenamento removível quando você acessou o Assistente de configuração durante a instalação do Encryption Personal.

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

Executar uma recuperação

1 Usando a mídia inicializável criada anteriormente, inicialize-a em um sistema de recuperação ou no dispositivo com a unidade que você está tentando recuperar. Um ambiente WinPE é aberto.

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

2 Digite **x** e pressione **Enter** para chegar a um prompt de comando.

3 Navegue até o arquivo de recuperação e abra-o.

4 Selecione uma opção:

- Meu sistema não inicializa e mostra uma mensagem solicitando a execução da Recuperação de SDE.

  Isso permitirá que você recompile as verificações de hardware que o cliente Encryption executa quando você inicializa no SO.

- Meu sistema não me permite acessar dados criptografados, editar políticas ou está sendo reinstalado.

  Use isso se a placa do Hardware Crypto Accelerator ou a placa-mãe/TPM precisar ser substituída.

5 Na caixa de diálogo Informações de backup e recuperação, confirme que as informações sobre o computador cliente a ser recuperado estão corretas e clique em **Avançar**.
Ao recuperar computadores que não sejam Dell, os campos SerialNumber e AssetTag estarão em branco.

6 Na caixa de diálogo que mostra uma lista dos volumes do computador, selecione todas as unidades aplicáveis e clique em **Avançar**.
Use as teclas Shift e Control para destacar múltiplas unidades.

Se a unidade selecionada não estiver criptografada por FFE ou baseada em política, ela não poderá ser recuperada.

7 Digite sua senha de recuperação e clique em **Avançar**.
Com um cliente gerenciado remotamente, essa é a senha fornecida na etapa 3 em Obter o arquivo de recuperação - Computador gerenciado remotamente.

No Encryption Personal, a senha é a Senha de administrador do Encryption definida para o sistema no momento em que as chaves foram depositadas.

8 Na caixa de diálogo Recuperação, clique em **Recuperar**. O processo de recuperação é iniciado.

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

NOTA:
Remova qualquer mídia USB ou CD\DVD usado para inicializar a máquina. Se não fizer isso, o computador pode ser inicializado novamente no ambiente de recuperação.

10 Após o computador ser reinicializado, ele deve funcionar plenamente. Se o problema persistir, entre em contato com o Dell ProSupport.

Recuperação de dados de unidade criptografada

Se o computador de destino não for reinicializável e não houver nenhuma falha de hardware, a recuperação de dados pode ser realizada no computador inicializado em um ambiente de recuperação. Se não for possível inicializar o computador de destino e houver falha de hardware ou for um dispositivo USB, a recuperação de dados pode ser realizada inicializando em uma unidade escrava. Quando você define uma unidade como escrava, você pode ver o sistema de arquivos e navegar pelos diretórios. Contudo, se você tentar abrir ou copiar um arquivo, ocorre um erro de *acesso negado*.

Recuperar dados de unidade criptografada

Para recuperar dados de uma unidade criptografada:

1 Para obter o DCID/ID de recuperação do computador, escolha uma das opções:
   a Executar o WSScan em uma pasta que tem dados criptografados Comuns armazenados.
   O DCID/ID de recuperação de oito dígitos é exibido após “Comum”.

   b Abra o console de gerenciamento remoto e selecione a guia **Detalhes e ações** para o terminal.
   c Na seção Detalhes do Shield da tela Detalhe do endpoint, encontre o DCID/ID de recuperação.

2 Para fazer download da chave do servidor, procure e execute o utilitário Dell Administrative Unlock (**CMGAu**).
   O utilitário Dell Administrative Unlock pode ser obtido do Dell ProSupport.

3 Na caixa de diálogo Utilitário administrativo Dell (CMGAu), digite as informações a seguir (alguns campos podem já estar preenchidos) e clique em **Avançar**.
   Servidor: Nome de host totalmente qualificado do servidor, por exemplo:

   Servidor de dispositivo (Clientes pré-8.x): **https://<server.organization.com>:8081/xapi**

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

   Administrador Dell: o nome da conta para o Administrador forense (ativado no Security Management Server/Security Management Server Virtual)

   Senha do administrador Dell: a senha da conta para o Administrador forense (ativado no Security Management Server/Security Management Server Virtual)

   MCID: Apague o campo MCID

   DCID: O DCID/ID de recuperação que você obteve anteriormente.

4 Na caixa de diálogo do utilitário administrativo Dell, selecione **Não, realizar um download a partir de um servidor agora** e clique em **Avançar**.

   NOTA:
   Se o cliente Encryption não estiver instalado, uma mensagem é exibida informando que *o desbloqueio falhou*. Mova para um computador com o cliente Encryption instalado.

5 Quando terminar o download e o desbloqueio, copie os arquivos que você precisa recuperar desta unidade. Todos os arquivos podem ser lidos. ***Não clique em Concluir até ter recuperado os arquivos***.

6 Após recuperar os arquivos e estar pronto para bloquear os arquivos novamente, clique em **Concluir**.
Após clicar em Concluir, os arquivos criptografados não estarão mais disponíveis.

Recuperação de Hardware Crypto Accelerator

NOTA: Hardware Crypto Accelerator não é suportado, a partir da v8.9.3.

Com a recuperação de Hardware Crypto Accelerator (HCA), você pode recuperar o acesso a:

- Arquivos em uma unidade com criptografia de HCA - Este método descriptografa a unidade usando as chaves fornecidas. Durante o processo de recuperação você poderá selecionar a unidade específica que precisa ser descriptografada.
- Uma unidade com criptografia de HCA após uma substituição de hardware - Este método é usado após a substituição de uma placa do Hardware Crypto Accelerator ou de uma placa-mãe/TPM. Você pode executar uma recuperação para obter acesso novamente aos dados criptografados sem descriptografar a unidade.

Requisitos de recuperação

Para uma recuperação de HCA, você precisará de:

- Acesso à ISO do ambiente de recuperação (a recuperação exige um ambiente 32 bits)
- Mídia USB ou CD\DVD inicializável

Visão geral do processo de recuperação

NOTA: A recuperação exige um ambiente de 32 bits.

Para recuperar um sistema que falhou:

1 Grave o ambiente de recuperação em um CD/DVD ou crie um USB inicializável. Consulte o Apêndice A - Gravação do ambiente de recuperação.
2 Obtenha o arquivo de recuperação.
3 Execute a recuperação.

Executar recuperação de HCA

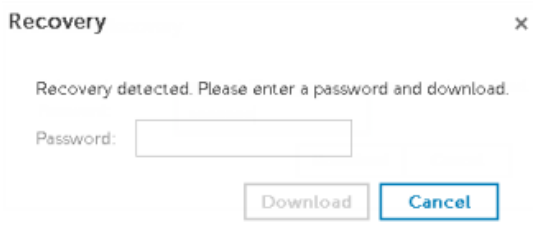
Execute este procedimento para realizar uma recuperação de HCA.

Obter o arquivo de recuperação - Computador gerenciado remotamente

Para fazer download do arquivo**<machinename_domain.com>.exe** que foi gerado quando você instalou o Dell Encryption:

1 Abra o Remote Management Console e, no painel esquerdo, selecione **Gerenciamento** > **Recuperar endpoint**.
2 No campo Nome de host, digite o nome de domínio totalmente qualificado do endpoint e clique em **Pesquisar**.
3 Na janela Recuperação, digite uma senha de recuperação e clique em **Fazer download**.

NOTA:
Você precisa memorizar essa senha para acessar as chaves de recuperação.



Obter o arquivo de recuperação - Computador gerenciado localmente

Para obter o arquivo de recuperação do Encryption Personal:

1 Localize o arquivo de recuperação chamado **LSARecovery_<systemname** > **.exe**. O arquivo estava armazenado em uma unidade de rede ou um armazenamento removível quando você acessou o Assistente de configuração durante a instalação do Encryption Personal.

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

Executar uma recuperação

1 Usando a mídia inicializável criada anteriormente, inicialize-a em um sistema de recuperação ou no dispositivo com a unidade que você está tentando recuperar.

Um ambiente WinPE é aberto.

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

2 Digite **x** e pressione **Enter** para chegar a um prompt de comando.

3 Navegue até o arquivo de recuperação salvo e abra-o.

4 Selecione uma opção:

- Desejo descriptografar minha unidade criptografada HCA.
- Desejo restaurar o acesso à minha unidade criptografada HCA.

5 Na caixa de diálogo Backup e Recuperação, confirme que a Etiqueta de serviço ou o Número do ativo está correto e clique em **Avançar**.

6 Na caixa de diálogo que mostra uma lista dos volumes do computador, selecione todas as unidades aplicáveis e clique em **Avançar**.

Use as teclas Shift e Control para destacar múltiplas unidades.

Se a unidade selecionada não estiver criptografa com HCA, ela não poderá ser recuperada.

7 Digite sua senha de recuperação e clique em **Avançar**.

Em um computador gerenciado remotamente, essa é a senha fornecida na etapa 3 em Obter o arquivo de recuperação - Computador gerenciado remotamente.

Em um computador gerenciado localmente, essa senha é a Senha de administrador do Encryption definida para o sistema no Personal Edition no momento em que as chaves foram depositadas.

8 Na caixa de diálogo Recuperação, clique em **Recuperar**. O processo de recuperação é iniciado.

9 Quando solicitado, navegue até o arquivo de recuperação salvo e clique em **OK**.

Se você estiver executando uma descriptografia completa, a caixa de diálogo a seguir mostrará o status. Esse processo pode exigir algum tempo.

10 Após ser mostrada uma mensagem indicando que a recuperação foi concluída satisfatoriamente, clique em **Concluir**. O computador será reinicializado.

Após o computador ser reinicializado, ele deve funcionar plenamente. Se o problema persistir, entre em contato com o Dell ProSupport.

4

Recuperação de Unidade de criptografia automática (SED)

Com a recuperação de SED, você pode recuperar o acesso aos arquivos em uma SED (Self-Encrypting Drive - Unidade de criptografia automática) através dos seguintes métodos:

- Execute o desbloqueio de uso único da unidade para ignorar a Autenticação de pré-inicialização (PBA).
- Desbloquear e, em seguida, remover permanentemente a PBA da unidade. O Login único não funcionará com a PBA removida.
  - Com um cliente SED gerenciado remotamente, se posteriormente for necessário reativar a PBA, a remoção da PBA exigirá que você desative o produto a partir do Remote Management Console.
  - Com um cliente SED gerenciado localmente, se posteriormente for necessário reativar a PBA, a remoção da PBA exigirá que você desative o produto dentro do SO.

Requisitos de recuperação

Para uma recuperação de SED, você precisará de:

- Acesso à ISO do ambiente de recuperação
- Mídia USB ou CD\DVD inicializável

Visão geral do processo de recuperação

NOTA: A recuperação exige um ambiente de 32 bits.

Para recuperar um sistema que falhou:

1 Grave o ambiente de recuperação em um CD/DVD ou crie um USB inicializável. Consulte o Apêndice A - Gravação do ambiente de recuperação.
2 Obtenha o arquivo de recuperação.
3 Execute a recuperação.

Executar recuperação de SED

Execute este procedimento para realizar uma recuperação de SED.

Obter o arquivo de recuperação - Cliente SED gerenciado remotamente

Obtenha o arquivo de recuperação.

O arquivo de recuperação pode ser obtido por download a partir do Remote Management Console. Para fazer download do arquivo *<hostname>-sed-recovery.dat* que foi gerado quando você instalou o Dell Data Security:

a Abra o console de gerenciamento remoto e, no painel esquerdo, selecione **Gerenciamento > Recuperar dados** e selecione a guia **SED**.

b Na tela Recuperar dados, no campo Nome de host, digite o nome de domínio totalmente qualificado do terminal e clique em **Pesquisar**.
c No campo SED, selecione uma opção.
d Clique em **Criar arquivo de recuperação**.
O arquivo **<hostname>-sed-recovery.dat** foi baixado.

Obter o arquivo de recuperação - Cliente SED gerenciado localmente

Obtenha o arquivo de recuperação.

O arquivo foi gerado e está acessível pelo local do backup selecionado ao instalar o Advanced Authentication no computador. O nome do arquivo é *OpalSPkey<systemname>.dat*.

Executar uma recuperação

1 Usando a mídia inicializável criada anteriormente, inicialize-a em um sistema de recuperação ou no dispositivo com a unidade que você está tentando recuperar. Um ambiente WinPE é aberto com o aplicativo de recuperação.

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

2 Selecione a opção um e pressione **Enter**.
3 Selecione **Procurar**, localize o arquivo de recuperação e depois clique em **Abrir**.
4 Selecione uma opção e clique em **OK**.
- **Desbloqueio único da unidade** - Este método ignora a PBA.
- **Desbloqueie a unidade e remova a PBA** - Este método permite desbloquear e, em seguida, remover permanentemente o PBA da unidade. Se posteriormente for necessário reativar a PBA, a remoção da PBA exigirá que você desative o produto a partir do Remote Management Console (para um cliente SED gerenciado remotamente) ou de dentro do SO (para um cliente SED gerenciado localmente). O Login único não funcionará com a PBA removida.

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

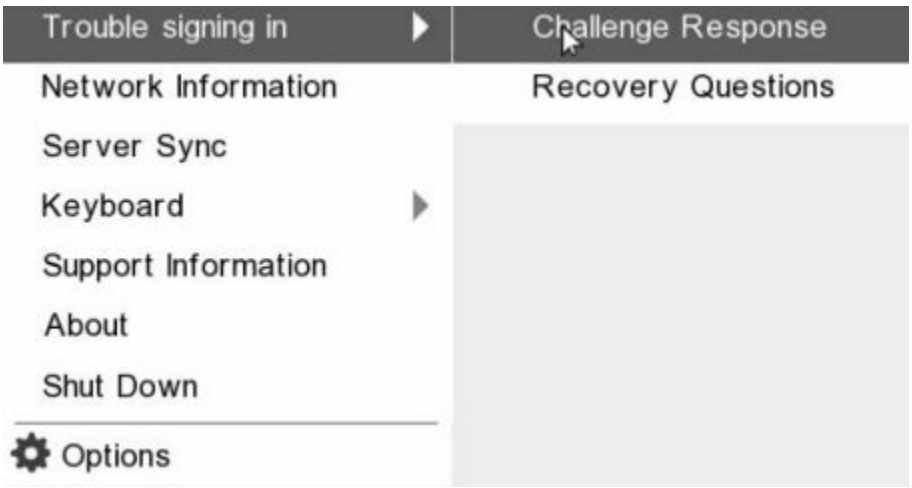
NOTA:
Remova qualquer mídia USB ou CD\DVD usado para inicializar o computador. Se não fizer isso, o computador pode ser inicializado novamente no ambiente de recuperação.

7 Após o computador ser reinicializado, ele deve funcionar plenamente. Se o problema persistir, entre em contato com o Dell ProSupport.

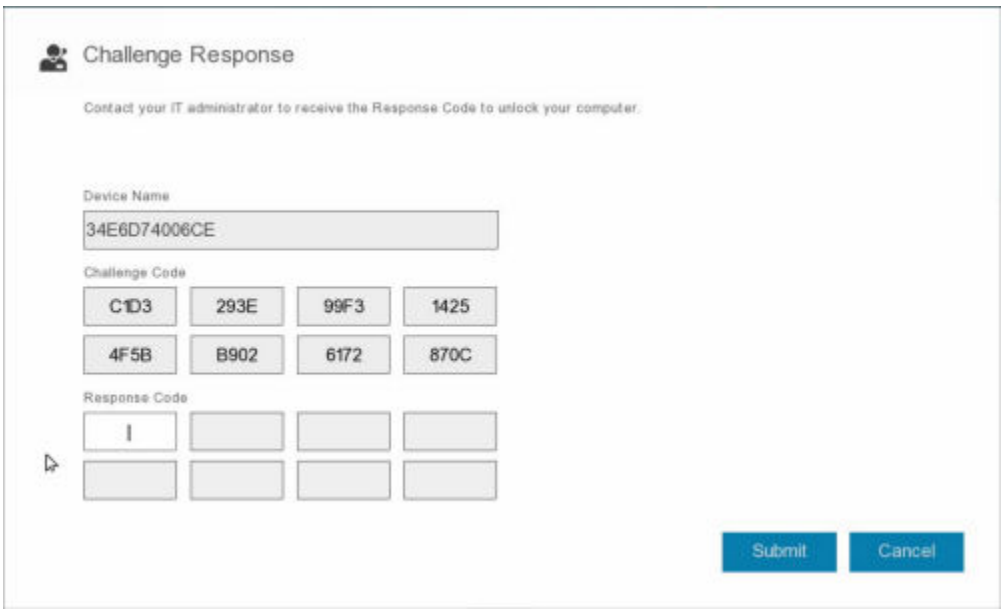
Recuperação por desafio com SED

Ignorar o ambiente de autenticação pré-inicialização

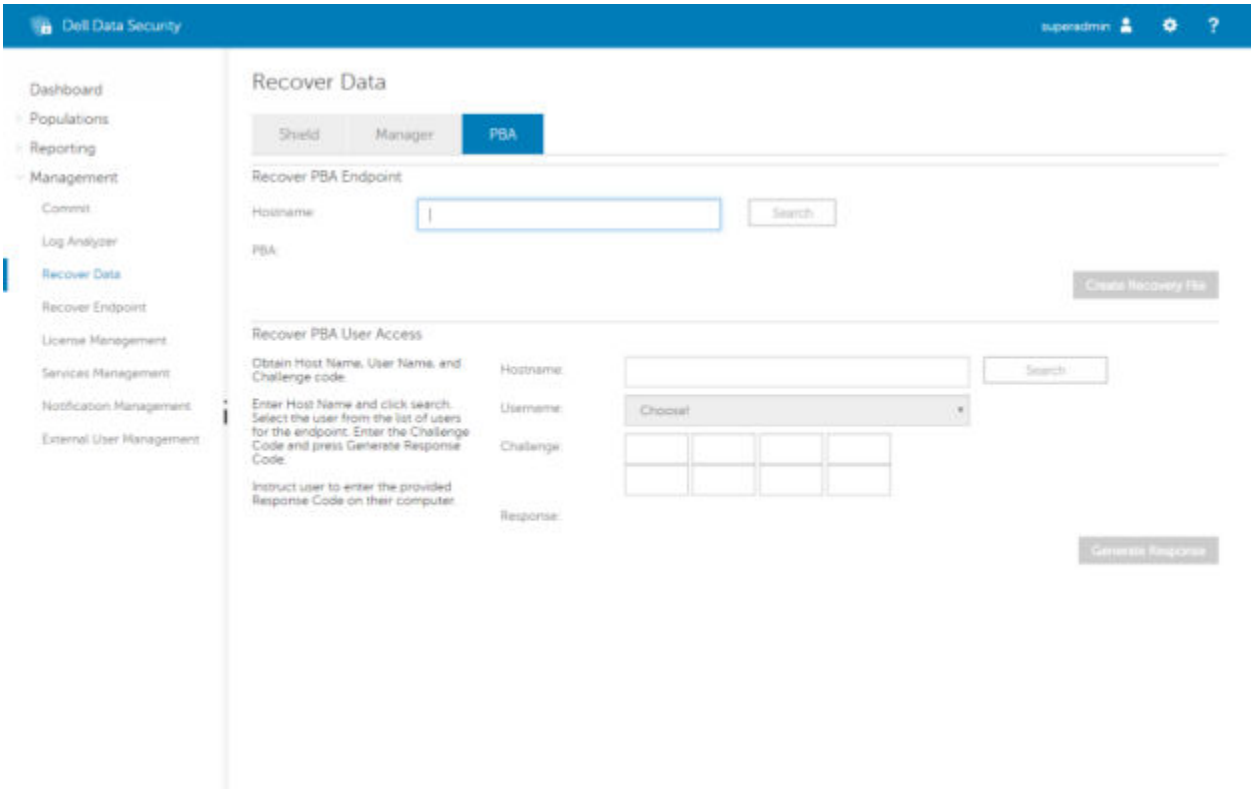
Usuários esquecem suas senhas e ligam para a assistência técnica sobre como passar pelo ambiente da PBA. Use o mecanismo de Desafio/Resposta que está incorporado no dispositivo. Este mecanismo funciona conforme o usuário com base em um conjunto rotativo de caracteres alfanuméricos. O usuário deve inserir seu nome no campo **Nome de usuário** e, em seguida, selecionar **Opções > Desafio/Resposta**.



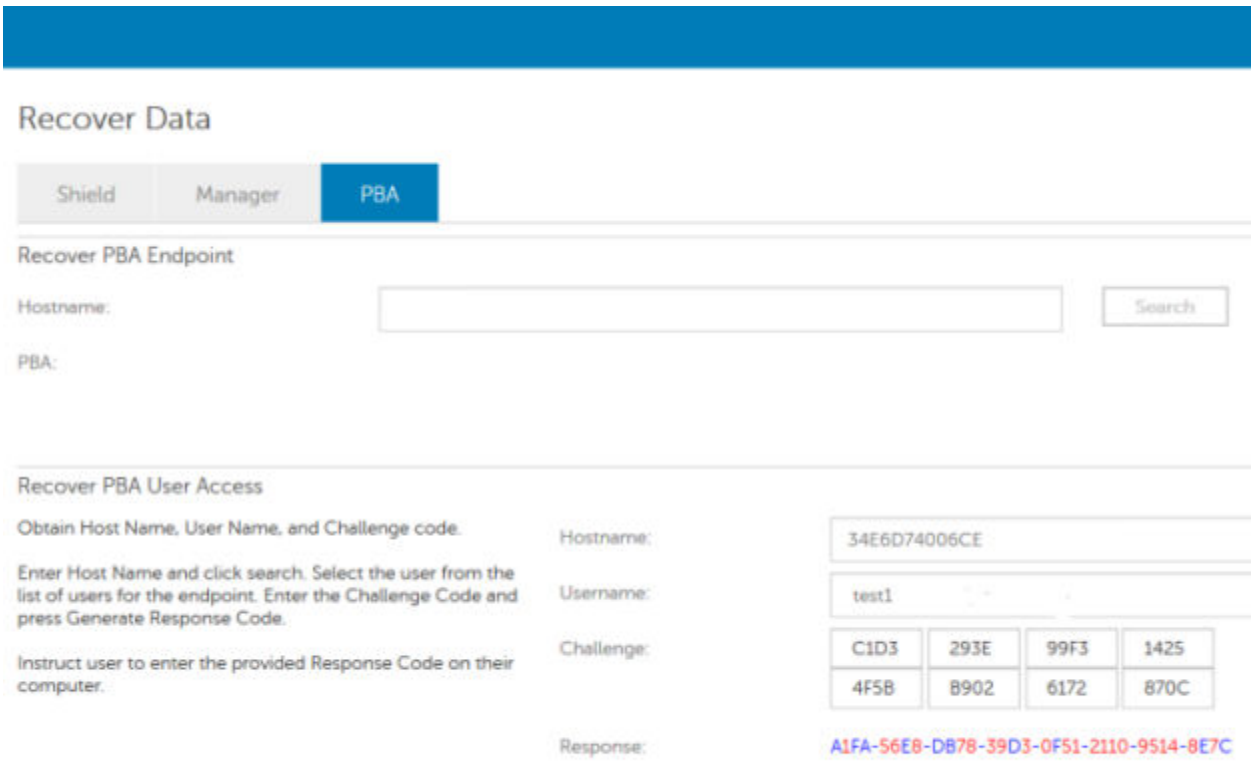
As seguintes informações são exibidas após selecionar **Desafio/Resposta**.



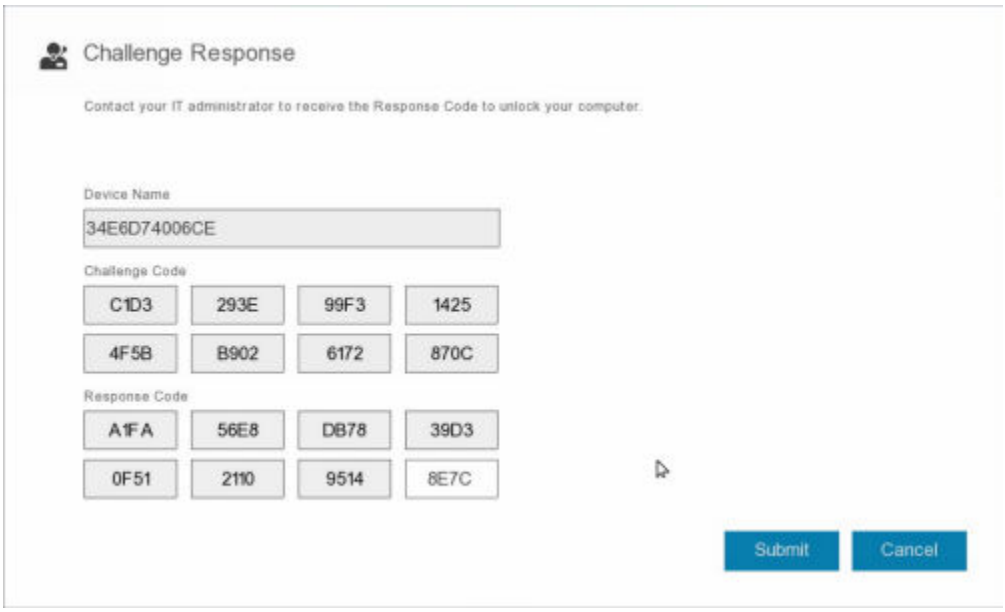
O campo **Nome do dispositivo** é usado pelo técnico da assistência técnica dentro do Remote Management Console para encontrar o dispositivo correto e, em seguida, um nome de usuário é selecionado. Isso pode ser encontrado dentro de **Gerenciamento > Recuperar dados** na guia **PBA**.



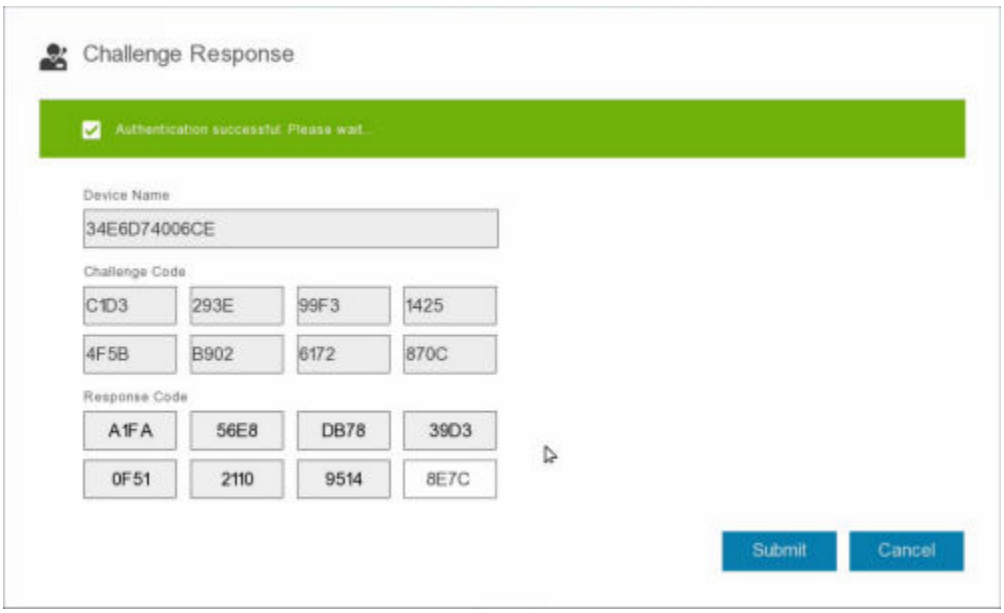
O Código de desafio é fornecido para o técnico da assistência técnica, que insere os dados e então clica no bot **Gerar resposta**.



Estes dados resultantes são coordenados por cores para ajudar a discernir os caracteres numerais (vermelho) e alfabéticos (azul). Esses dados são lidos para o usuário final, o qual entra no ambiente de PBA e, em seguida, clica no botão **Enviar**, colocando o usuário no Windows.



Após uma autenticação bem-sucedida, a seguinte mensagem será exibida:



A recuperação por desafio foi concluída.

Recuperação por criptografia completa de disco

A recuperação permite a você recuperar o acesso a arquivos em uma unidade criptografada com a Criptografia completa de disco.

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

Requisitos de recuperação

Para a recuperação por Criptografia completa de disco, você precisará do seguinte:

- Acesso à ISO do ambiente de recuperação
- Mídia USB ou CD\DVD inicializável

Visão geral do processo de recuperação

NOTA: A recuperação exige um ambiente de 32 bits.

Para recuperar um sistema que falhou:

1 Grave o ambiente de recuperação em um CD/DVD ou crie um USB inicializável. Consulte o Apêndice A - Gravação do ambiente de recuperação.
2 Obtenha o arquivo de recuperação.
3 Execute a recuperação.

Realizar a recuperação por criptografia completa de disco

Siga estas etapas para realizar uma recuperação de Criptografia completa de disco.

Obter o arquivo de recuperação - Cliente de criptografia completa de disco

Obtenha o arquivo de recuperação.

Faça o download do arquivo de recuperação a partir do Remote Management Console. Para fazer download do arquivo *<hostname>-sed-recovery.dat* que foi gerado quando você instalou o Dell Data Security:

a Abra o Remote Management Console e, no painel esquerdo, selecione **Gerenciamento > Recuperar dados** e selecione a guia **PBA**.
b Na tela Recuperar dados, no campo Nome de host, digite o nome de domínio totalmente qualificado do terminal e clique em **Pesquisar**.
c No campo SED, selecione uma opção.
d Clique em **Criar arquivo de recuperação**.

O arquivo **<hostname>-sed-recovery.dat** foi baixado.

Executar uma recuperação

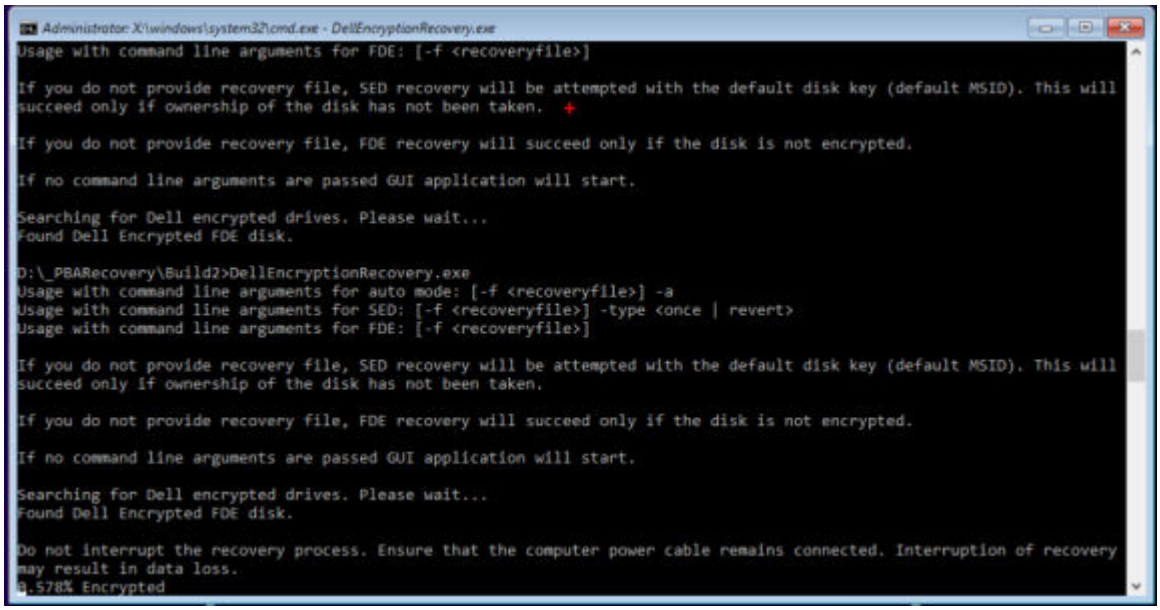
1 Usando a mídia inicializável criada anteriormente, inicialize-a em um sistema de recuperação ou no dispositivo com a unidade que você está tentando recuperar. Um ambiente WinPE é aberto com o aplicativo de recuperação.

> **NOTA: Desative o SecureBoot antes o processo de recuperação. Quando terminar, reative o SecureBoot.**

2 Selecione a opção um e pressione **Enter**.

3 Selecione **Procurar**, localize o arquivo de recuperação e depois clique em **Abrir**.

4 Clique em **OK**.



.

5 A recuperação agora está concluída. Pressione qualquer tecla para retornar ao menu.

6 Pressione **r** para reiniciar o computador.

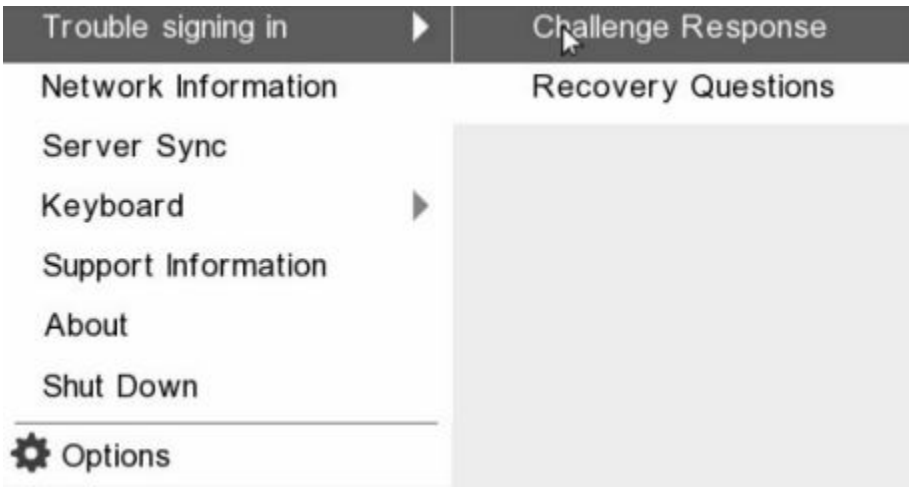
> **NOTA:**
> Remova qualquer mídia USB ou CD\DVD usado para inicializar o computador. Se não fizer isso, o computador pode ser inicializado novamente no ambiente de recuperação.

7 Após o computador ser reinicializado, ele deve funcionar plenamente. Se o problema persistir, entre em contato com o Dell ProSupport.

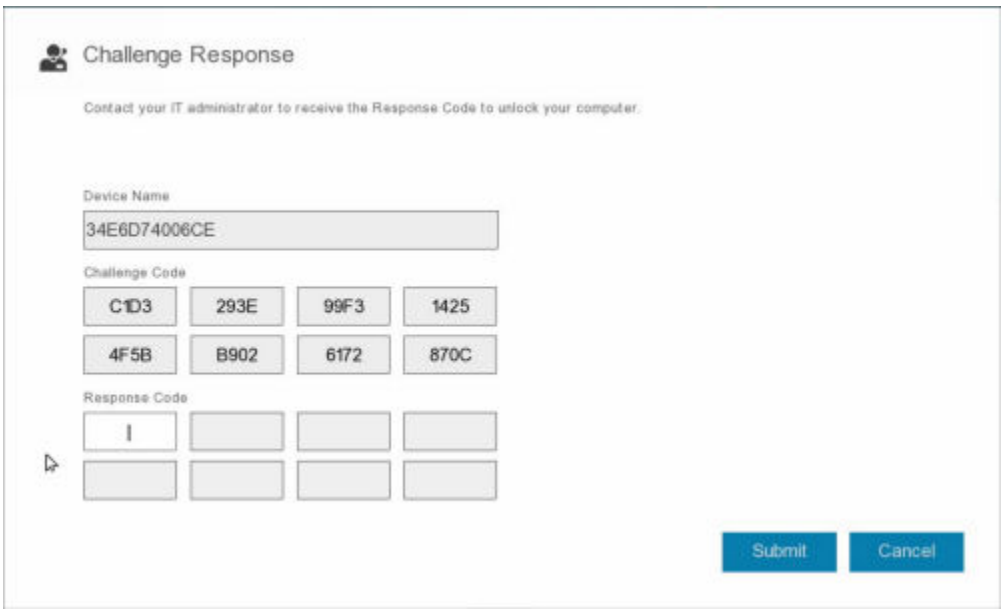
Recuperação por desafio com Criptografia completa de disco

Ignorar o Ambiente de autenticação pré-inicialização

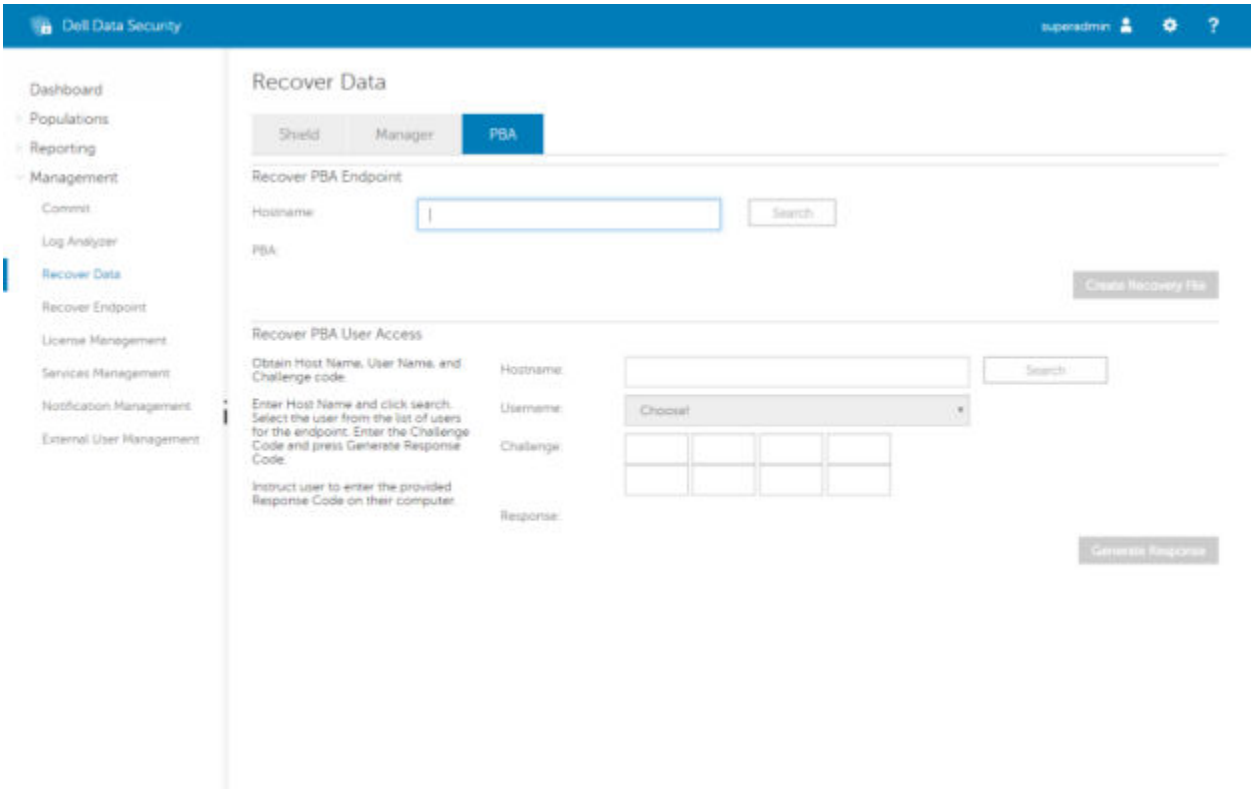
Usuários esquecem suas senhas e ligam para a assistência técnica sobre como passar pelo ambiente da PBA. Use o mecanismo de Desafio/Resposta que está incorporado no dispositivo. Este mecanismo funciona conforme o usuário com base em um conjunto rotativo de caracteres alfanuméricos. O usuário deve inserir seu nome no campo **Nome de usuário** e, em seguida, selecionar **Opções > Desafio/Resposta**.



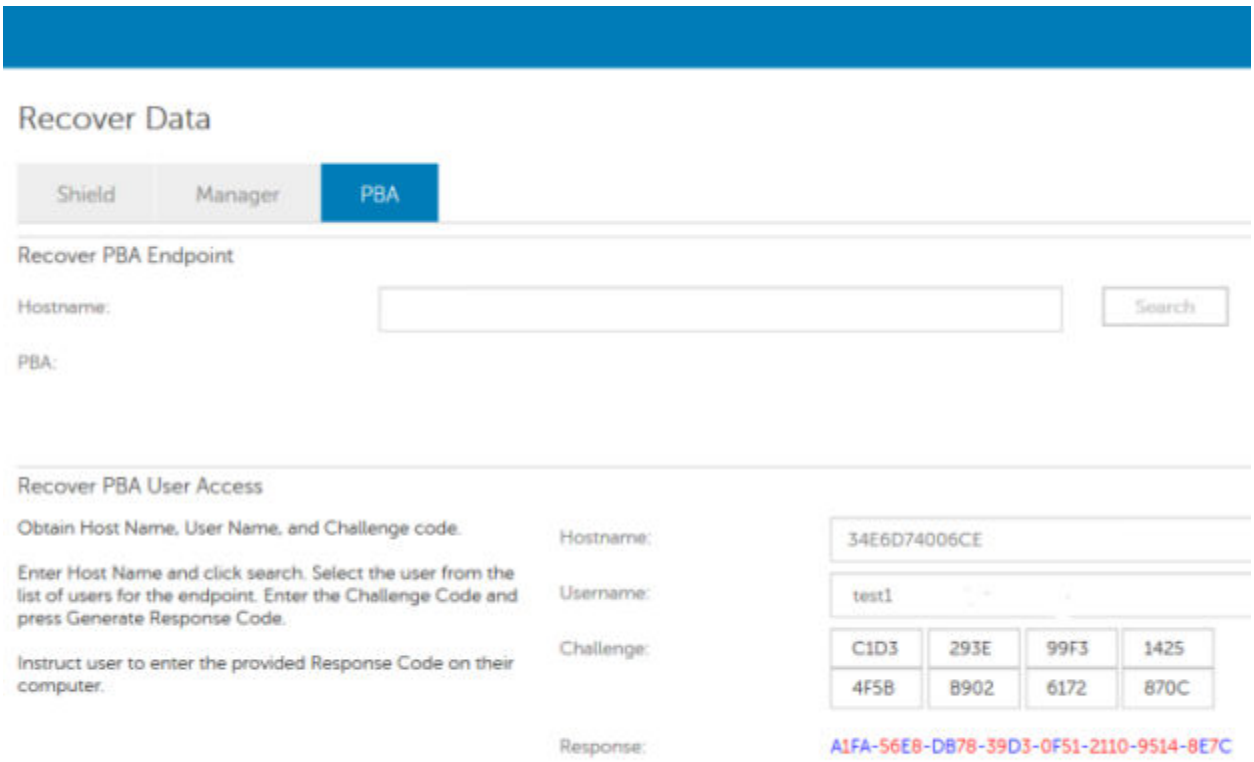
As seguintes informações são exibidas após selecionar **Desafio/Resposta**.



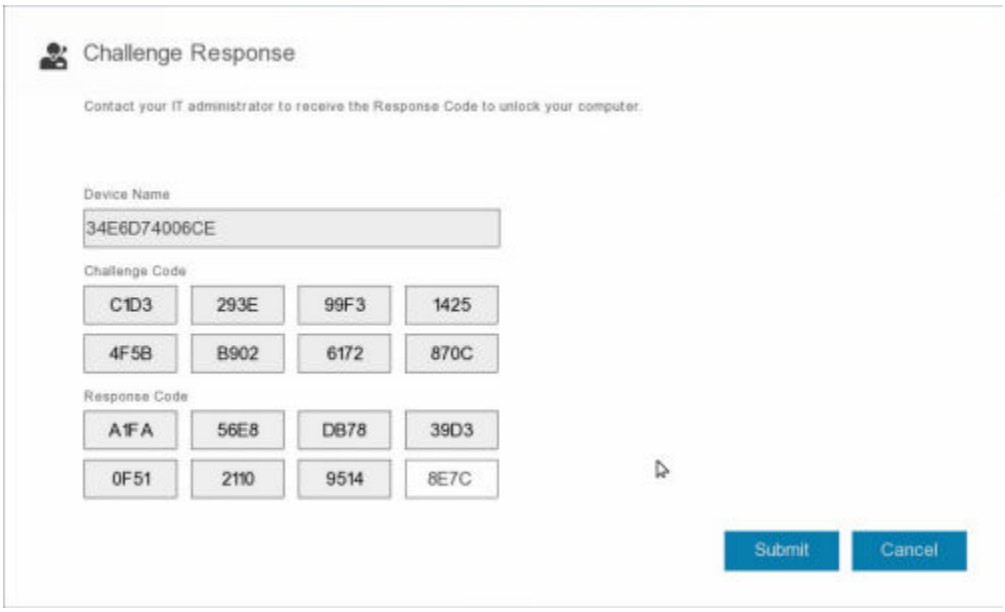
O campo **Nome do dispositivo** é usado pelo técnico da assistência técnica dentro do Remote Management Console para encontrar o dispositivo correto e, em seguida, um nome de usuário é selecionado. Isso pode ser encontrado dentro de **Gerenciamento > Recuperar dados** na guia **PBA**.



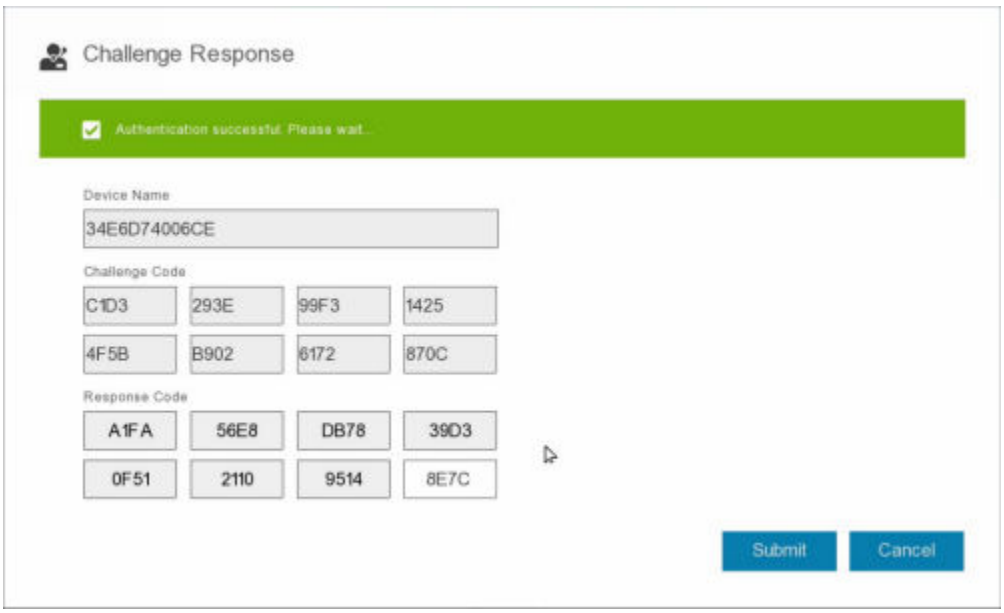
O Código de desafio é fornecido para o técnico da assistência técnica, que insere os dados e então clica no bot **Gerar resposta**.



Estes dados resultantes são coordenados por cores para ajudar a discernir os caracteres numerais (vermelho) e alfabéticos (azul). Esses dados são lidos para o usuário final, o qual entra no ambiente de PBA e, em seguida, clica no botão **Enviar**, colocando o usuário no Windows.



Após uma autenticação bem-sucedida, a seguinte mensagem será exibida:



A recuperação por desafio foi concluída.

6

Controle de dispositivos de PBA

O Controle do dispositivo PBA aplica-se aos endpoints criptografados com Criptografia completa de disco ou SED.

Uso do controle de dispositivos de PBA

Comandos de PBA para um endpoint específico são realizados na área de controle de dispositivo de PBA. Cada comando possui uma classificação de prioridade. Um comando com uma classificação de prioridade superior cancela comandos de prioridade inferior na fila de imposição. Para obter uma lista de classificações de prioridade de comando, consulte *AdminHelp* disponível, clicando no ? no Remote Management Console. Os Controles de dispositivo de PBA estão disponíveis na página Detalhes de endpoint do Remote Management Console.

Os comandos a seguir estão disponíveis no Controle de dispositivo de PBA:

- **Bloquear** - Bloqueia a tela de PBA e impede que o usuário faça login no computador.
- **Desbloquear** - Desbloqueia a tela de PBA após ela ter sido bloqueada nesse ponto de extremidade, seja enviando um comando Bloquear ou por ultrapassar o número máximo de tentativas de autenticações permitido pela política.
- **Remover usuários** - Remove todos os usuários do PBA.
- **Ignorar login** - Ignora a tela PBA uma vez para permitir um usuário no computador sem autenticação. O usuário ainda precisará fazer login no Windows após o PBA ter sido ignorado.
- **Limpar** - O comando Limpar funciona como um recurso de "restaurar para estado de fábrica" para a unidade criptografada. O comando Limpar pode ser usado para realocar um computador ou, em uma situação de emergência, limpar o computador, tornando os dados permanentemente irrecuperáveis. Certifique-se de que esse seja o comportamento desejado antes de acionar esse comando. Para a Criptografia completa de disco, o comando Limpar apaga criptograficamente a unidade e a PBA é removida. Para SED, o comando Limpar apaga criptograficamente a unidade e a PBA exibe “Dispositivo bloqueado”. Para realocar o SED, remova a PBA com o aplicativo Recuperação de SED.

Recuperação de Chave de uso geral

A Chave de uso geral (GPK - General Purpose Key) é usada para criptografar parte do registro de usuários do domínio. Entretanto, durante o processo de inicialização, em casos raros, ela pode se corromper e não desselar. Nesse caso, os seguintes erros serão mostrados no arquivo CMGShield.log no computador cliente:

```
[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 desselar, ela precisará ser recuperada extraindo-a do pacote de recuperação que é obtido por download do Dell Server.

Recuperar a GPK

Obter o arquivo de recuperação

Para fazer download do arquivo**<machinename_domain.com>.exe** que foi gerado quando você instalou o Dell Data Security:

1 Abra o Remote Management Console e, no painel esquerdo, selecione **Gerenciamento** > **Recuperar endpoint**.

2 No campo Nome de host, digite o nome de domínio totalmente qualificado do endpoint e clique em **Pesquisar**.

3 Na janela Recuperação, digite uma senha de recuperação e clique em **Fazer download**

> **NOTA:**
> Você precisa memorizar essa senha para acessar as chaves de recuperação.

O arquivo **<machinename_domain.com>.exe** é baixado.

Executar uma recuperação

1 Crie uma mídia inicializável do ambiente de recuperação. Para instruções, consulte o Apêndice A - Gravação do ambiente de recuperação.

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

2 Inicialize com essa mídia em um sistema de recuperação ou no dispositivo com a unidade que você está tentando recuperar.
Um ambiente WinPE é aberto.

3 Digite **x** e pressione **Enter** para chegar a um prompt de comando.

4 Navegue até o arquivo de recuperação e abra-o.
Uma caixa de diálogo Diagnóstico do cliente Encryption é aberta e o arquivo de recuperação é gerado em segundo plano.

5 Em um prompt de comando administrativo, execute **<machinename_domain.com** > **.exe** > **-p <password** > **-gpk**
Ele retorna o arquivo GPKRCVR.txt para o seu computador.

6 Copie o arquivo **GPKRCVR.txt** na raiz da unidade do SO do computador.

7 Reinicie o computador.
O arquivo GPKRCVR.txt será usado pelo sistema operacional para restaurar a GPK nesse computador.
8 Se for solicitado, reinicie novamente o computador.

8

Recuperação do Gerenciador BitLocker

Para recuperar dados, você obtém uma senha de recuperação ou um pacote de chaves do Remote Management Console que permitem o desbloqueio dos dados no computador.

Recuperar dados

1 Como um administrador Dell, faça login no Remote Management Console.

2 No painel esquerdo, clique em **Gerenciamento** > **Recuperar dados**.

3 Clique na guia **Gerenciador**.

4 Para BitLocker:

Digite o **ID de recuperação** recebido do BitLocker. Opcionalmente, se você inserir o Nome de host e o Volume, o ID de recuperação é preenchido.

Clique em **Obter senha de recuperação** ou em **Criar pacote de chaves**.

Dependendo de como deseja fazer a recuperação, você usará essa senha de recuperação ou o pacote de chaves para recuperar dados.

Para o *TPM*:

Insira o **nome do host**.

Clique em **Obter senha de recuperação** ou em **Criar pacote de chaves**.

Dependendo de como deseja fazer a recuperação, você usará essa senha de recuperação ou o pacote de chaves para recuperar dados.

5 Para concluir a recuperação, consulte as Instruções de recuperação da Microsoft.

NOTA:

Se o Gerenciador BitLocker não for "proprietário" do TPM, a senha do TPM e o pacote de chaves não estarão disponíveis no banco de dados Dell. Você receberá uma mensagem de erro informando que a Dell não consegue localizar a chave, que é o comportamento esperado.

Para recuperar um TPM que é "propriedade" de uma entidade que não seja o Gerenciador BitLocker, você deverá seguir o processo para recuperar o TPM desse proprietário específico ou seguir o seu próprio processo existente de recuperação do TPM.

9

Recuperação de senha

Os usuários normalmente esquecem as senhas deles. Felizmente, existem várias maneiras dos usuários recuperarem o acesso a um computador com autenticação pré-inicialização quando eles esquecerem.

- O recurso de questões de recuperação oferece autenticação baseada em pergunta e resposta.
- Os códigos de resposta/desafio permitem que o usuário trabalhe junto com o administrador para recuperar o acesso ao computador dele. Este recurso está disponível apenas para o usuário que tenham computadores que sejam gerenciados por sua organização.

Perguntas de recuperação

A primeira vez que um usuário faz login em um computador, ele é solicitado a responder a um conjunto de perguntas configuradas pelo administrador. Após adicionar respostas a essas três questões, a próxima vez que ele esquecer a senha, o usuário será solicitado a respondê-las. Supondo-se que ele tenha respondido corretamente, ele será capaz de fazer login e recuperar o acesso ao Windows.

Pré-requisitos

- As perguntas da recuperação devem ser definidas pelo administrador.
- O usuário precisa ter inserido suas respostas para as perguntas.
- Antes de clicar na opção de menu **Problemas para fazer login**, o usuário precisa inserir um nome de usuário e domínio válidos.

Para acessar as perguntas de recuperação da tela de login da PBA:

1 Digite um nome de domínio e nome de usuário válidos.
2 Na parte inferior esquerda da tela, clique em **Opções** > **Tendo problemas para entrar?**.
3 Quando a caixa de diálogo de perguntas e respostas for exibida, insira o número que você forneceu quando se inscreveu nas perguntas de recuperação na primeira vez em que fez login.

Recuperação de senha do Encryption External Media

O Encryption External Media proporciona a você a capacidade de proteger mídia de armazenamento removível dentro e fora da sua organização, permitindo que usuários criptografem suas unidades flash USB e outras mídias de armazenamento removíveis. O usuário define uma senha para cada mídia removível que deseja proteger. Esta seção descreve o processo para recuperação de acesso a um dispositivo de armazenamento USB criptografado quando um usuário esquece a senha de um dispositivo.

Recuperar acesso aos dados

Quando um usuário digita sua senha incorretamente tantas vezes que excede o número permitido de tentativas, o dispositivo USB é colocado em modo de autenticação manual.

Autenticação Manual é o processo de fornecimento dos códigos do cliente para um administrador que está conectado ao Dell Server.

Quando no modo de autenticação manual, o usuário tem duas opções para redefinir sua senha e recuperar o acesso aos seus dados.

O administrador fornece um código de acesso para o cliente, permitindo que o usuário redefina sua senha e recupere o acesso aos seus dados criptografados.

1 Quando for solicitada a senha, clique em **Eu esqueci.**

A caixa de diálogo de confirmação é exibida.

2 Clique em **Sim** para confirmar. Após a confirmação, o dispositivo entra no modo de autenticação manual.
3 Entre em contato com o administrador do suporte técnico e dê a ele os códigos que aparecem na caixa de diálogo.
4 Como administrador do suporte técnico, faça login no console de gerenciamento remoto - a conta de administrador do suporte técnico deve ser privilégios de suporte técnico.
5 Navegue até a opção **Recuperar dados** no menu no painel esquerdo.
6 Insira os códigos fornecidos pelo usuário final.
7 Clique no botão **Gerar resposta** no canto inferior direito da tela.
8 Dê ao usuário o código de acesso.

NOTA:
Certifique-se de autenticar manualmente o usuário antes de fornecer um código de acesso. Por exemplo, faça uma série de perguntas ao usuário pelo telefone que só aquela pessoa saberia responder, como “Qual é o seu número de ID de funcionário?” Outro exemplo: solicite que o usuário venha ao suporte técnico para fornecer informações para assegurar que ele é o proprietário da mídia. Não autenticar um usuário antes de conceder o código de acesso pelo telefone pode permitir que um invasor tenha acesso a mídia removível criptografada.

9 Redefina sua senha para a mídia criptografada.

É solicitado que o usuário redefina sua senha para a mídia criptografada.

Recuperação automática

A unidade deve ser inserida novamente na máquina que originalmente a criptografou para a Autorrecuperação funcionar. Contanto que o proprietário da mídia esteja autenticado no Mac ou PC protegido, o cliente detecta a perda de material importante e solicita que o usuário reinicialize o dispositivo. Nesse momento, o usuário pode redefinir sua senha e recuperar o acesso a seus dados criptografados. Este processo pode resolver problemas de mídia parcialmente corrompida.

1 Faça login em uma estação de trabalho Dell Data Security criptografada como proprietário da mídia.
2 Insira o dispositivo de armazenamento removível criptografado.
3 Quando solicitado, insira uma nova senha para reinicializar o dispositivo de armazenamento removível.

   Se bem sucedido, uma breve notificação de que a senha foi aceita será exibida.

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

Recuperação do Dell Data Guardian

A ferramenta de recuperação permite:

- Descriptografia de arquivos do Office protegidos com qualquer formato suportado

  Os arquivos que são protegidos pela criptografia de Documento do Office protegido pelo Data Guardian e sua proteção no Prestador de Serviços de Nuvem podem ser recuperados.
- Depósito manual de material importante
- Capacidade de verificar arquivos adulterados
- Capacidade de forçar a descriptografia de documentos Office quando alguém adulterou o wrapper do arquivo, por exemplo, a página de capa protegida do Office na nuvem ou em um dispositivo que não tem o Data Guardian

Requisitos de recuperação

Os requisitos incluem:

- Microsoft .Net Framework 4.5.2 em execução no terminal a ser recuperado.
- A função de administrador forense precisa ser atribuída no console de gerenciamento remoto para o administrador que está executando a recuperação.

Execute a recuperação do Data Guardian

Siga estas etapas para realizar uma recuperação de documentos do Office protegidos do Data Guardian. Você pode recuperar um computador por vez.

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

Para executar uma recuperação:

1 A partir da mídia de instalação da Dell, copie o arquivo **RecoveryTools.exe** para uma dessas opções:

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

2 Clique duas vezes em **RecoveryTools.exe** para executar a ferramenta de recuperação.

3 Na janela do Data Guardian, insira a FQDN do Dell Server neste formato:

   server.domain.com

   NOTA: Um prefixo e um sufixo são automaticamente adicionados ao FQDN.

4 Digite seu nome de usuário e senha e clique em **Login**.

   NOTA:
   Não desmarque a caixa de seleção *Ativar certificado SSL* a menos que o seu administrador diga a você para fazê-lo.

NOTA:
Se você não for um administrador forense e inserir credenciais, uma mensagem será exibida, indicando que você não tem permissão para login.

Se você for um administrador forense, ferramenta de recuperação será aberta.

5 Selecione **Origem**.

NOTA:
Você precisa procurar uma origem e um destino, mas pode selecioná-los em qualquer ordem.

6 Clique em **Procurar** para selecionar a pasta ou unidade a ser recuperada.

7 Clique em **OK**.

8 Clique em **Destino**, uma pasta vazia para os arquivos descriptografados ou recuperados.

9 Clique em **Procurar** para selecionar um destino, como um dispositivo externo, um diretório local ou a área de trabalho.

10 Clique em **OK**.

11 Marque uma ou mais caixas de seleção com base no que deseja recuperar.

Opções	Descrição
Depósito	• Recuperar chaves off-line que não podem ser depositadas no servidor Dell. • Se o disco rígido falhar enquanto o usuário está off-line da rede, use o disco escravo para recuperar dados e teclas não depositadas do computador.
Descriptografar	Aponte a ferramenta de recuperação para um diretório que contém os documentos do Office para descriptografá-los. Opcionalmente, se ocorreu qualquer adulteração, selecione uma ou ambas as opções (veja a lista abaixo para obter detalhes): • **Verificação de adulteração** - verifica a existência de arquivos adulterados, mas não os descriptografa. • **Verificação de adulteração** e **Descriptografia forçada mesmo se adulterado** - verificações à procura de arquivos adulterados e se o wrapper de um documento protegido do Office foi adulterado, o Data Guardian repara o wrapper e descriptografa o documento do Office.
Verificação de violação	Detecta arquivos que foram adulterados e os registra ou notifica você. Registra o autor que adulterou o arquivo. Ele não descriptografa os arquivos.
Forçar descriptografia mesmo se violado	Para selecionar esta opção, você também precisa selecionar **Verificação de adulteração**. Se uma pessoa autorizada adulterou o wrapper de um documento protegido do Office, como a página da capa, seja na nuvem ou em um dispositivo que não tem o Data Guardian, selecione esta opção para reparar o wrapper e para forçar a descriptografia do arquivo protegido do Office. **Nota:** Se alguém adulterar o arquivo .xen criptografado do Office dentro do wrapper, o arquivo não pode ser recuperado.

Cada documento protegido do Office tem uma marca d'água oculta que contém um histórico e o nome do computador do usuário original e o nome de qualquer outro computador que modificou o arquivo. Por padrão, a ferramenta de recuperação verifica as marcas d'água ocultas e adiciona um arquivo de texto com uma lista de todos os autores a uma pasta *HiddenWatermark* nos registros.

12 Depois que as seleções forem concluídas, clique em **Verificar**.

A área de registro exibe:

- Pastas encontradas e verificadas dentro da origem selecionada
- Se a descriptografia, por arquivo, foi bem-sucedida ou falhou
- O nome do último autor de um arquivo

A ferramenta de recuperação adiciona os arquivos recuperados ao destino selecionado. Você pode abrir e visualizar os arquivos

Visualize dados a partir da Trilha de auditoria oculta

Para o Windows, se a política de Trilha de auditoria oculta para documentos do Office protegidos estiver ativada, as informações de usuário são capturadas no metadados de arquivo. Para visualizar esses dados, use a Ferramenta de recuperação:

1 Abra a Ferramenta de recuperação.
   - Para **Fonte**, navegue até uma pasta que contenha documentos do Office protegidos com dados de auditoria ocultos. A Ferramenta de recuperação irá copiar a estrutura de pasta e subpasta, descriptografando qualquer documento do Office protegido que possuem dados de auditoria ocultos.
   - Antes de navegar pra um **Destino**, você pode criar uma pasta, descriptografar os arquivos e, em seguida, navegar até ela.
2 Selecione **Descriptografar**.
3 Depois que as seleções forem concluídas, clique em **Verificar**.

   A pasta selecionada como Destino contém uma pasta de *Arquivos recuperados* datada com o seguinte:
   - Arquivos do Office protegidos descriptografados
   - A pasta de *Trilha de auditoria*, criada pela Ferramenta de recuperação, com um arquivo .txt para cada arquivo descriptografado. Cada arquivo .txt tem um log que lista as informações do arquivo descriptografado, tais como autores, último autor, do decodificadas somente arquivo, como autores, último autor, marcação de data/hora.

Apêndice A - Gravação do ambiente de recuperação

Você pode fazer download do instalador mestre.

Gravação da ISO do ambiente de recuperação para CD/DVD

O link a seguir contém o processo necessário para usar o Microsoft Windows 7, Windows 8 ou Windows 10 para criar um CD ou DVD inicializável para o ambiente de recuperação.

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

Gravação do ambiente de recuperação em mídia removível

Para criar um USB inicializável, use as seguintes instruções:

Legacy Boot:

1 Conecte uma unidade USB ao sistema.
2 Abra um prompt de comando administrativo.
3 Acesse o utilitário Diskpart, digitando **diskpart**.
4 Encontre o disco de destino para modificar, digitando **list disk**. Os discos serão designados por número.
5 Selecione o disco apropriado usando o comando **select disk #** onde # é o número do disco para a unidade correspondente indicada na etapa anterior.
6 Limpe o disco utilizando o comando **clean**. Isso limpará a unidade de dados fazendo uma limpeza na Tabela de arquivos.
7 Crie uma partição para a imagem de inicialização residir.
   a O comando **create partition primary** gera uma partição primária na unidade.
   b O comando **select partition 1** selecione a nova partição.
   c Use o comando a seguir para formatar rapidamente a unidade com o sistema de arquivos NTFS: **format FS=NTFS quick**.
8 A unidade deve estar marcada como uma unidade inicializável. Use o comando **active** para marcar a unidade como inicializável.
9 Para mover arquivos diretamente para uma unidade, atribua um letra disponível para a unidade com o comando **assign**.
10 A unidade será montada automaticamente e o conteúdo do arquivo ISO pode ser copiado para a raiz da unidade.

Após o conteúdo do ISO ter sido completamente copiado, a unidade é inicializável e pode ser usada para recuperação.

Inicialização do EUFI:

1 Conecte uma unidade USB ao sistema.
2 Abra um prompt de comando administrativo.
3 Acesse o utilitário Diskpart, digitando **diskpart**.
4 Encontre o disco de destino para modificar, digitando **list disk**. Os discos serão designados por número.

5 Selecione o disco apropriado usando o comando **select disk #** onde # é o número do disco para a unidade correspondente indicada na etapa anterior.

6 Limpe o disco utilizando o comando **clean**. Isso limpará a unidade de dados fazendo uma limpeza na Tabela de arquivos.

7 Crie uma partição para a imagem de inicialização residir.

   a O comando **create partition primary** gera uma partição primária na unidade.

   b O comando **select partition 1** selecione a nova partição.

   c Use o comando a seguir para formatar rapidamente a unidade com o sistema de arquivos FAT32: **format FS=FAT32 quick**.

8 A unidade deve estar marcada como uma unidade inicializável. Use o comando **active** para marcar a unidade como inicializável.

9 Para mover arquivos diretamente para uma unidade, atribua um letra disponível para a unidade com o comando **assign**.

10 A unidade será montada automaticamente e o conteúdo do arquivo ISO pode ser copiado para a raiz da unidade.

Após o conteúdo do ISO ter sido completamente copiado, a unidade é inicializável e pode ser usada para recuperação.