

Dell Data Protection

Guia de Recuperação v8.13/v1.7/v1.4/v1.2



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

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

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

© 2017 Dell Inc. Todos os direitos reservados. A Dell, a EMC, e outras marcas são marcas comerciais da Dell Inc. ou suas subsidiárias. Outras marcas podem ser marcas comerciais de seus respectivos proprietários.

Marcas registradas e marcas comerciais usadas no conjunto de documentos do Dell Data Protection Encryption, Endpoint Security Suite, Endpoint Security Suite Enterprise e Dell Data Guardian: Dell™ e o logotipo da Dell, Dell Precision™, OptiPlex™, ControlVault™, Latitude™, XPS® e KACE™ são marcas comerciais da Dell Inc. Cylance®, CylancePROTECT e o logotipo da Cylance são marcas comerciais ou marcas registradas da Cylance, Inc. nos Estados Unidos e em outros países. McAfee® e o logotipo da McAfee são marcas comerciais ou marcas registradas da McAfee, Inc. nos Estados Unidos e em outros países. Intel®, Pentium®, Intel Core Inside Duo®, Itanium® e Xeon® são marcas registradas da Intel Corporation nos Estados Unidos e em outros países. Adobe®, Acrobat®, e Flash® são marcas registradas da Adobe Systems Incorporated. Authen Tec® e Eikon® são marcas registradas da Authen Tec. AMD® é marca registrada da Advanced Micro Devices, Inc. Microsoft®, Windows® e Windows Server®, Internet Explorer®, MS-DOS®, Windows Vista®, MSN®, ActiveX®, Active Directory®, Access®, ActiveSync®, BitLocker®, BitLocker To Go®, Excel®, Hyper-V®, Silverlight®, Outlook®, PowerPoint®, OneDrive®, SQL Server®, e Visual C++® são marcas comerciais ou marcas registradas da Microsoft Corporation nos Estados Unidos e/ou em outros países. VMware® é marca registrada ou marca comercial da VMware, Inc. nos Estados Unidos ou em outros países. Box® é marca comercial registrada da Box. DropboxSM é marca de serviço da Dropbox, Inc. Google™, Android™, Google™ Chrome™, Gmail™, YouTube® e Google™ Play são marcas comerciais ou marcas registradas da Google Inc. nos Estados Unidos e em outros países. Apple®, Aperture®, App StoreSM, Apple Remote Desktop™, Apple TV®, Boot Camp™, FileVault™, iCloud®SM, iPad®, iPhone®, iPhoto®, iTunes Music Store®, Macintosh®, Safari®, e Siri® são marcas de serviço, marcas comerciais ou marcas registradas da Apple, Inc. nos Estados Unidos e/ou em outros países. GO ID®, RSA®, e SecurID® são marcas registradas da Dell EMC. EnCase™ e Guidance Software® são marcas comerciais ou marcas registradas da Guidance Software. Entrust® é marca registrada da Entrust®, Inc. nos Estados Unidos e em outros países. InstallShield® é marca registrada da Flexera Software nos Estados Unidos, China, Comunidade Europeia, Hong Kong, Japão, Taiwan, e Reino Unido. Micron® e RealSSD® são marcas registradas da Micron Technology, Inc. nos Estados Unidos e em outros países. Mozilla® Firefox® é marca registrada da Mozilla Foundation nos Estados Unidos e/ou em outros países. iOS® é marca comercial ou marca registrada da Cisco Systems, Inc. nos Estados Unidos e em determinados países e é usada sob licença. Oracle® e Java® são marcas registradas da Oracle e/ou seus afiliados. Outros nomes podem ser marcas comerciais de seus respectivos proprietários. SAMSUNG™ é marca comercial da SAMSUNG nos Estados Unidos ou em outros países. Seagate® é marca registrada da Seagate Technology LLC nos Estados Unidos e/ou em outros países. Travelstar® é marca registrada da HGST, Inc. nos Estados Unidos e em outros países. UNIX® é marca registrada da The Open Group. VALIDITY™ é marca comercial da Validity Sensors, Inc. nos Estados Unidos e em outros países. VeriSign® e outras marcas relacionadas são marcas comerciais ou marcas registradas da VeriSign, Inc. ou de suas afiliadas ou subsidiárias nos Estados Unidos e em outros países e licenciadas para a Symantec Corporation. KVM on IP® é marca comercial da Video Products. Yahoo!® é marca comercial da Yahoo! Inc. Este produto usa partes do programa 7-Zip. O código-fonte pode ser encontrado em 7-zip.org. O licenciamento é feito sob a licença GNU LGPL + restrições unRAR (7-zip.org/license.txt).

Guia de Recuperação do Dell Data Protection

2017 - 04

Rev. A01

1 Introdução à recuperação.....	5
Entre em contato com o Dell ProSupport.....	5
2 Recuperação de criptografia baseada em política ou arquivo/pasta.....	6
Visão geral do processo de recuperação.....	6
Executar recuperação FFE ou criptografia baseada em política.....	6
Obter o arquivo de recuperação - Computador gerenciado remotamente.....	6
Obter o arquivo de recuperação - Computador gerenciado localmente.....	7
Executar uma recuperação.....	7
Recuperação de dados de unidade criptografada.....	8
Recuperar dados de unidade criptografada.....	8
3 Recuperação de Hardware Crypto Accelerator.....	9
Requisitos de recuperação.....	9
Visão geral do processo de recuperação.....	9
Executar recuperação de HCA.....	9
Obter o arquivo de recuperação - Computador gerenciado remotamente.....	9
Obter o arquivo de recuperação - Computador gerenciado localmente.....	10
Executar uma recuperação.....	10
4 Recuperação de Unidade de criptografia automática (SED).....	12
Requisitos de recuperação.....	12
Visão geral do processo de recuperação.....	12
Executar recuperação de SED.....	12
Obter o arquivo de recuperação - Cliente SED gerenciado remotamente.....	12
Obter o arquivo de recuperação - Cliente SED gerenciado localmente.....	13
Executar uma recuperação.....	13
5 Recuperação de Chave de uso geral.....	14
Recuperar a GPK.....	14
Obter o arquivo de recuperação.....	14
Executar uma recuperação.....	14
6 Recuperação do BitLocker Manager.....	16
Recuperar dados.....	16
7 Recuperação de senha.....	17
Perguntas de recuperação.....	17
Códigos de resposta/desafio.....	17
8 Recuperação de senha do External Media Shield.....	19
Recuperar acesso aos dados.....	19
Recuperação automática.....	19

9 Recuperação do Dell Data Guardian.....	21
Requisitos de recuperação.....	21
Execute a recuperação do Data Guardian.....	21
10 Apêndice A - Gravação do ambiente de recuperação.....	24
Gravação da ISO do ambiente de recuperação para CD/DVD.....	24
Gravação do ambiente de recuperação em mídia removível.....	24



Introdução à recuperação

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

- Cópia obtida por download do software do ambiente de recuperação - Localizada na pasta Kit de recuperação do Windows na mídia de instalação do Dell Data Protection.
- 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 Servidor do Dell Data Protection.
 - 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 Data Protection.

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

Quando telefonar, tenha em mãos o código de serviço, 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](#).



Recuperação de criptografia baseada em política ou arquivo/pasta

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 cujos dados criptografados não podem ser acessados ou cujas políticas não podem ser editadas.
- Um servidor com o Dell Data Protection | Server 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.

Visão geral do processo de recuperação

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 avançada, digite uma senha de recuperação e clique em **Fazer download**.

① 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 Personal Edition:

- 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 Personal Edition.
- 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.
 - 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 Personal Edition, 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 do dispositivo: **https://<server.organization.com>:8081/xapi**

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

Administrador Dell: O nome da conta do Administrador forense (ativado no servidor)

Senha do administrador Dell: O nome da conta do Administrador forense (ativado no servidor)

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

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

- 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
- Mídia USB ou CD/DVD inicializável

Visão geral do processo de recuperação

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

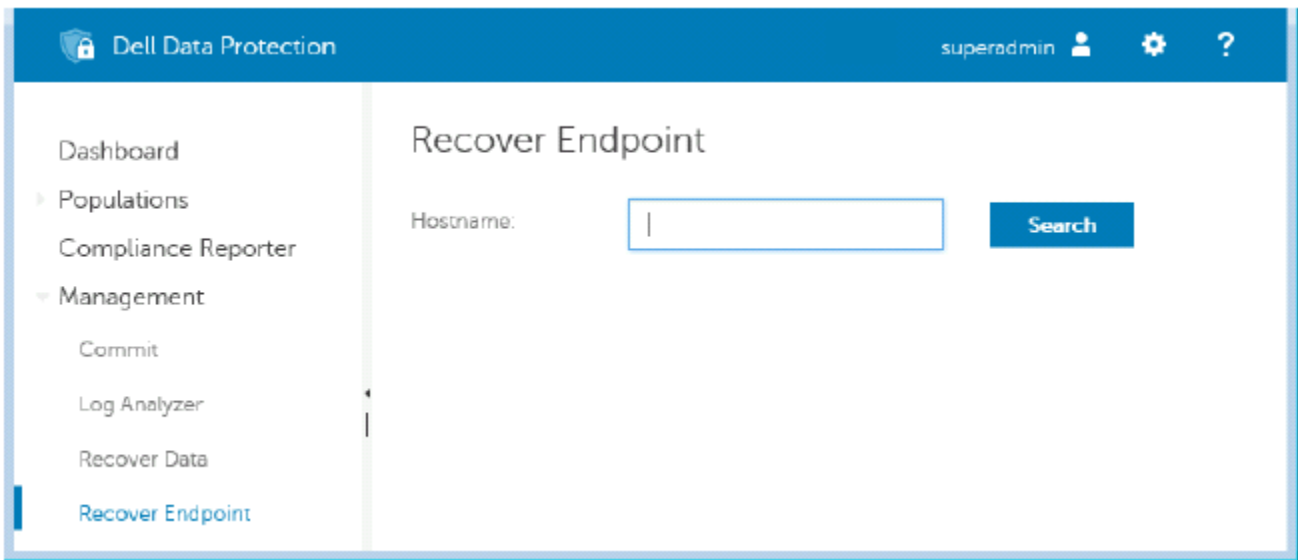
Execute este procedimento para realizar uma recuperação de HCA.

Obter o arquivo de recuperação - Computador gerenciado remotamente

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

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

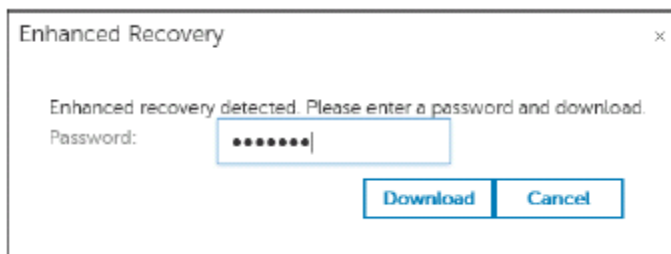




- 2 No campo Nome de host, digite o nome de domínio totalmente qualificado do endpoint e clique em **Pesquisar**.
- 3 Na janela Recuperação avançada, digite uma senha de recuperação e clique em **Fazer download**.

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 Personal Edition:

- 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 Personal Edition.
- 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.
- 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 criptografada 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 reiniciado.

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



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 e remover a Autenticação de pré-inicialização (PBA, Preboot Authentication).
 - Com um cliente SED gerenciado remotamente, posteriormente, a PBA poderá ser ativada novamente através do Remote Management Console.
 - Com um cliente SED gerenciado localmente, a PBA poderá ser ativada através do Security Tools Administrator Console.
- 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

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 Protection:

- 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 pode ser acessado a partir do local de backup que você selecionou quando o Dell Data Protection | Security Tools foi instalado 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.
- 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 e remove a PBA. Posteriormente, a PBA poderá ser ativada novamente através do Remote Management Console (para um cliente SED gerenciado remotamente) ou através do Security Tools Administrator Console (para um cliente SED gerenciado localmente).
 - **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.

① 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 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 extraíndo-a do pacote de recuperação que é obtido por download do servidor.

Recuperar a GPK

Obter o arquivo de recuperação

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

- 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 avançada, digite uma senha de recuperação e clique em **Fazer download**

① 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](#).
- 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.



Recuperação do BitLocker Manager

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 BitLocker Manager 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 BitLocker Manager, você deverá seguir o processo para recuperar o TPM desse proprietário específico ou seguir o seu próprio processo existente de recuperação do TPM.

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.

Códigos de resposta/desafio

A recuperação por desafio/resposta pode ser usada para autenticação por meio de PBA para acessar o Windows. Pode-se usar desafio/resposta nos seguintes cenários:

- Quando um usuário não lembra as respostas fornecidas no momento da inscrição das perguntas de recuperação.
- O administrador não ativou o recurso de perguntas de recuperação.
- Um usuário está remoto sem conectividade de rede e não é capaz de receber um comando de desbloqueio do Security Server por meio de controles de dispositivo SED

Um usuário pode chegar à tela Desafio/resposta clicando na opção **Problemas para fazer login** ou inserindo a senha incorretamente, excedendo o limite de falhas de senha sem o cabo de rede conectado. Se as perguntas de recuperação tiverem sido desativadas, a opção **Problemas para fazer login** abre diretamente a tela Desafio/resposta.

Requisito

- A recuperação por Desafio/resposta só está disponível para computadores de domínio que são gerenciados remotamente pela sua organização ou empreendimento.



Pré-requisitos

- Desconecte o computador da rede antes de responder as perguntas de recuperação ou inserir os códigos de Desafio/resposta.
- Antes de clicar em Problemas para fazer login, insira um nome de usuário e domínio válidos.

Para usar a recuperação por Desafio/resposta

- 1 O usuário clica no link **Opções** para exibir o menu.
- 2 O usuário clica em **Problemas para fazer login > Desafio/resposta**.

NOTA:

A opção Desafio/resposta só está disponível em computadores que são gerenciados por uma organização. Se o computador não pertencer ao domínio, a opção Desafio/resposta não aparece no menu.

- 3 Quando solicitado, o usuário entra em contato com o suporte técnico e dá ao administrador o nome do dispositivo (nome do host) e o código de desafio.
- 4 O administrador abre o console de gerenciamento remoto, clica em **Gerenciamento > Recuperar dados**, e depois em **SED** no menu superior.
- 5 Sob acesso de usuário SED de recuperação, o administrador insere o **Nome do host** obtido do usuário e clica em **Pesquisar**.
- 6 O administrador seleciona o nome de usuário que está pedindo ajuda:
- 7 Insira o código do dispositivo obtido do usuário no campo **Desafio** e clique em **Gerar resposta**.
- 8 Dê o código de resposta gerado ao usuário.

NOTA:

Esses códigos não diferenciam maiúsculas e minúsculas. Os números são mostrados em vermelho e as letras em azul.

- 9 O usuário digita o código de resposta nos campos **Código de resposta** na tela de entrada de PBA. Este é um exemplo de código de resposta inserido por usuário:
- 10 Clique na seta direita para continuar e fazer autenticação para ir além da tela de PBA.
- 11 Clique em **Enviar**.

Um usuário pode fazer autenticação e ir além da PBA usando o recurso Desafio/resposta apenas uma vez. Após a reinicialização do computador, o PBA retomará a proteção do computador e solicitará ao usuário que efetue login na tela de PBA.

NOTA:

Depois que o usuário tiver exibido a caixa de diálogo Desafio/resposta, o usuário deve concluir a sequência Desafio/resposta para recuperar o acesso ao sistema. Se o usuário desligar o computador e tentar fazer login novamente, mesmo com a senha correta, o PBA exibe novamente a caixa de diálogo de Desafio/resposta.

Recuperação de senha do External Media Shield

O External Media Shield (EMS) 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 servidor.

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 recuperação automática é o processo de redefinir a senha para um dispositivo de mídia removível criptografado, inserindo a unidade de volta em uma máquina protegida na qual o proprietário da mídia está conectado. Contudo 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.

- 1 Faça login em uma estação de trabalho Dell Data Protection 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 protegidos do Office

Isso inclui até arquivos com criptografia tripla. Como há mais de uma forma de criptografar arquivos, ocasionalmente um arquivo é criptografado duas ou três vezes. Se o usuário abrir o arquivo, uma mensagem de erro o instruirá a entrar em contato com o administrador para recuperá-lo.
- Depósito 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.

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 URL do servidor Dell neste formato:

`https://<server.domain.com>:8443/cloud`



NOTA:

Substitua <server.domain.com> pelo nome do host totalmente qualificado do servidor Dell que gerencia o Data Guardian nesse terminal. Para localizar a URL do servidor Dell, clique no ícone do Data Guardian na bandeja do sistema e clique em **Detalhes**. O canto superior esquerdo da tela Detalhes mostra o URL do servidor.

- 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**

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.

Descriptografado

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 registra as informações.

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 descryptografia foi bem-sucedida ou falhou

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



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 uma unidade USB inicializável, siga as instruções deste artigo da Microsoft:

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