Dell Data Guardian

Guia do Usuário v1.2

Notas, avisos e advertências

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.

Guia do Usuário do Dell Data Guardian

2017 - 04

Rev. A01

Índice

Introdução ao Dell Data Guardian

O *Guia do usuário do Dell Data Guardian* fornece as informações necessárias para instalar e usar o Dell Data Guardian.

Visão geral

Com base nas políticas definidas por um administrador, o Dell Data Guardian protege os dados, por exemplo:

- Sistemas de compartilhamento de arquivos baseados em nuvem - Computadores ou dispositivos móveis Windows capturam dados destinados a armazenamento em nuvem, criptografam estes dados e fazem upload dos dados criptografados para a nuvem.
- Documentos do Office armazenados localmente, compartilhados com outros usuários de várias maneiras ou armazenados em mídia removível. Estes documentos do Office podem ser protegidos: .docx, .pptx, .xlsx, .docm, .pptm, .xlsm.

> **NOTA:**
> O administrador informará se sua empresa usa o Data Guardian somente com armazenamento em nuvem, somente com documentos do Office ou ambos.

O Data Guardian pode ser usado nas seguintes plataformas:

- Windows
- iOS
- Android
- Tanto esse produto quanto oData Guardian para Mac pode abrir arquivos criptografados pelo outro.
  - Este documento aborda somente o Dell Data Guardian para Windows.
  - Para obter informações de usuário sobre o Dell Data Guardian para Mac, consulte a ajuda online do software.

Suporte adicional

Se precisar de suporte adicional além deste documento, entre em contato com o administrador.

2

Requisitos do Dell Data Guardian

Os requisitos de hardware e software de cliente são apresentados neste capítulo.

NOTA:
IPv6 não é compatível.

Servidor

O Data Guardian requer que o cliente esteja conectado a um Dell Enterprise Server ou Dell Enterprise Server - VE, v9.6 ou posterior. Para a finalidade deste documento, ambos os servidores são citados como Dell Server, a menos que uma versão específica precise ser citada (por exemplo, um procedimento é diferente ao ser usado o Dell Enterprise Server - VE).

Cliente Encryption

- As práticas recomendadas de TI devem ser seguidas durante a implementação. Isso inclui, sem limitações, ambientes de teste controlados para testes iniciais e implantações escalonadas para os usuários.
- A conta de usuário que executa a instalação/upgrade/desinstalação precisa ser a de um usuário Admin local ou de domínio, que pode ser temporariamente atribuída por uma ferramenta de implementação, como o Microsoft SMS ou o Dell KACE. Não há suporte para um usuário que não é administrador mas possui privilégios elevados.
- Faça backup de todos os dados importantes antes de iniciar a instalação/desinstalação.
- Não realize alterações no computador, incluindo a inserção ou a remoção de unidades externas (USB), durante a instalação.
- Embora o cliente Encryption não seja necessário, qualquer cliente Encryption usado com o Data Guardian deverá ser v8.12 ou posterior.
- O Data Guardian não é compatível com o Microsoft Office 365.
- Para criptografia na nuvem, o computador deverá ter uma unidade de disco (parâmetro de letra) disponível.
- Certifique-se de que os dispositivos de destino tenham conectividade com https://yoursecurityservername.domain.com:8443/cloudweb/register e https://yoursecurityservername.domain.com:8443/cloudweb.
- Antes de implantar o Data Guardian, será melhor se os dispositivos de destino ainda não tiverem as contas de armazenamento na nuvem configuradas.

  Se os usuários decidirem manter suas contas existentes, eles deverão garantir que todos os arquivos que precisem ser mantidos *descriptografados* sejam transferidos para fora do cliente de sincronização antes da instalação do Data Guardian.
- Os usuários finais deverão estar preparados para reiniciar seus computadores quando o cliente for instalado.
- O Data Guardian não interfere no comportamento dos clientes de sincronização. Portanto, os administradores e os usuários finais deverão se familiarizar com o modo como esses aplicativos funcionam antes de implantar o Data Guardian. Para obter mais informações, consulte suporte ao Box em https://support.box.com/home, suporte ao Dropbox em https://www.dropbox.com/help ou suporte ao OneDrive em http://windows.microsoft.com/en-us/onedrive/onedrive-help#onedrive=other.
- Se o Office 2010 estiver em execução: caso tenham sido definidas políticas para proteger documentos do Office e documentos ativados por macro, será necessário que os usuários tenham o Office 2010 Service Pack 1 ou superior (v14.0.6029 ou superior). Consulte https://support.microsoft.com/en-us/kb/2121559 para determinar se um service pack foi aplicado a um pacote do Microsoft Office 2010. Sem essa atualização, documentos protegidos não poderão ser acessados. Novos documentos do Office estarão desprotegidos independentemente da política, a menos que a funcionalidade varredura esteja ativada. A próxima varredura converterá documentos do Office em arquivos protegidos, mas os usuários não poderão acessá-los sem uma versão compatível do Office.
- O Data Guardian não oferece suporte à ferramenta de Restauração do sistema do Windows.
- Verifique periodicamente www.dell.com/support para obter a documentação e recomendações técnicas mais recentes.

Pré-requisitos do cliente

Se ainda não estiver instalado, o instalador instalará o Microsoft Visual C++ 2015 Redistributable Package (x86 e x64).

NOTA:
Para o Windows 7 e Windows 8.1, os computadores devem estar atualizados com o Windows Update. Para obter mais informações, consulte https://support.microsoft.com/en-us/help/2919355 e https://support.microsoft.com/en-us/help/2999226.

O Microsoft .Net 4.5.2 (ou posterior) é exigido para o Data Guardian. Todos os computadores enviados da fábrica da Dell têm o .Net 4.5.2. pré-instalado. No entanto, se você não estiver instalando no hardware da Dell ou atualizando o Data Guardian em equipamentos mais antigos da Dell, você deve verificar qual versão do .Net está instalada e atualizar a versão, caso seja necessário, antes de instalar o Dell Data Guardian para evitar falhas de upgrade/instalação. Para verificar a versão do .Net instalado, siga estas instruções no computador no qual ele será instalado: http://msdn.microsoft.com/en-us/library/hh925568(v=vs.110).aspx. Para instalar o Microsoft .Net Framework 4.5.2, visite https://www.microsoft.com/en-us/download/details.aspx?id=42643.

Hardware para cliente Windows

Os requisitos mínimos de hardware precisam atender às especificações mínimas do sistema operacional. A tabela a seguir detalha o hardware suportado para o cliente Windows.

Hardware Windows

- 200 MB de espaço livre em disco, dependendo do sistema operacional
- Placa de interface de rede 10/100/1000 ou Wi-Fi
- TCP/IP instalado e ativado

Se sua empresa criptografa os dados para armazenamento na nuvem, o computador deverá ter uma letra alfabética disponível para atribuir a uma unidade de disco.

Sistemas operacionais

A tabela a seguir detalha os sistemas operacionais suportados.

Sistemas operacionais Windows (32 bits e 64 bits)

- Windows 7 SP0-SP1
- Windows 8,1
- Windows 10

NOTA:
O Windows 7 não é suportado com a política de geolocalização para eventos de auditoria do Data Guardian.

Sistemas operacionais Android

- 4.4 - 4.4.4 (KitKat)
- 5.0-5.1.1 Lollipop
- 6.0-6.0.1 Marshmallow
- 7.0 Nougat

Sistemas operacionais iOS

- iOS 8.x
- iOS 9.x
- iOS 10.x - 10.3

Cliente de sincronização em nuvem

A tabela a seguir detalha os clientes de sincronização em nuvem que funcionam com o Data Guardian. Atualizações aos clientes de sincronização são liberadas com frequência. A Dell recomenda testar novas versões de clientes de sincronização com o Data Guardian antes de introduzi-las ao ambiente de produção.

Cliente de sincronização em nuvem

- DropBox
- Dropbox for Business (apenas para Windows)

  NOTA:
  Dependendo da versão do Dell Server usada por sua empresa, todos os arquivos e pastas nas contas pessoais Dropbox que estão ligados a contas da empresa podem ser criptografados.

- Box

  NOTA:
  Box Tools e o Box Edit não são suportados com o Data Guardian. O uso do Box Tools pode causar uma condição de tela azul.

- Google Drive
- OneDrive
- OneDrive for Business
- Unified OneDrive

  NOTA:
  O Unified OneDrive é um cliente de sincronização unificada para OneDrive e OneDrive for Business.

Navegadores da Web

Você pode usar o Data Guardian > Criptografia de nuvem com o Internet Explorer, Mozilla Firefox e Google Chrome.

NOTA:
O Data Guardian > Criptografia de nuvem não suporta o navegador Microsoft Edge.

Tarefas do usuário - Criptografia na nuvem e Documentos protegidos do Office

O administrador já configurou as políticas do Data Guardian e informará se sua empresa usa o Data Guardian:

- Para gerenciar o cliente de sincronização de nuvem
- Para gerenciar o cliente de sincronização de nuvem e proteção adicional a documentos do Office - Se sua empresa somente protege documentos do Office, mas não gerencia um cliente de sincronização de nuvem, siga as etapas descritas em Tarefas do usuário - Documentos protegidos do Office sem Criptografia na nuvem.

Se sua empresa usa o Data Guardian com armazenamento em nuvem:

- Antes de implantar o Data Guardian, consulte a ajuda online do seu provedor de armazenamento em nuvem/cliente de sincronização de nuvem para entender como seu aplicativo de armazenamento em nuvem funciona. Este documento descreve principalmente como usar o Data Guardian.
- De forma geral, instale e use um único cliente de sincronização de nuvem. Pode ser que sua empresa tenha um cliente de sincronização de nuvem preferido e defina uma política permitindo que você use apenas esse cliente.

Visão geral das Tarefas

Essa visão geral resume a sequência de instalação e uso do Data Guardian.

Instale o Data Guardian e um cliente de sincronização de nuvem

Tarefa	Descrição	Para obter mais informações
Se um cliente de sincronização de nuvem for instalado antes do Data Guardian	Pastas e arquivos preexistentes que sincronizam para a nuvem não são criptografados. **NOTA:** Pastas e arquivos preexistentes que sincronizam a partir da nuvem não são criptografados.	Consulte Pastas existentes com arquivos não criptografados.
Instalar o Data Guardian	Determine se: O usuário precisa instalar o Data Guardian Administrador já instalou o Data Guardian - passe para a próxima etapa.	O usuário instala: Consulte Instalar o Data Guardian no Windows. Reinicialize e vá para a próxima etapa.
Confirmar o estado de ativação	Confirme, na bandeja do sistema, se o ícone do Data Guardian tem uma marca de seleção verde  .	Se o ícone tiver um ponto de exclamação laranja, consulte Possíveis problemas com a ativação - Armazenamento em nuvem e Documentos protegidos do Office.
Se houver políticas protegendo os documentos na	Cliente de sincronização empresarial ou	Contas empresariais do cliente Cloud Sync ou

Tarefa	Descrição	Para obter mais informações
nuvem, instale um cliente de sincronização de nuvem	Cliente de sincronização básico	Contas básicas do cliente Cloud Sync

NOTA:

Se você abrir um documento do Office e for exibida uma página de rosto com informações sobre instalação ou ativação, o administrador poderá ter definido políticas para proteger documentos do Office. Confirme se o Data Guardian está instalado e ativado. Consulte Possíveis problemas com a ativação - Armazenamento em nuvem e Documentos protegidos do Office.

Usar o Data Guardian

Tarefa	Descrição	Para obter mais informações
Ver o cliente de sincronização de nuvem no Gerenciador de arquivos	Depois de instalar o Data Guardian e um cliente de sincronização de nuvem, uma DDG VDisk virtual drive é exibida no Explorador de arquivos.	Trabalhar com pastas e arquivos Acessar pastas e arquivos do cliente de sincronização no computador local
Trabalhar com o cliente de sincronização de nuvem na DDG VDisk virtual drive	Na DDG VDisk virtual drive, você pode adicionar subpastas ao cliente de sincronização de nuvem e, a seguir, arrastar ou criar arquivos nestas subpastas. Após a sincronização, os arquivos ficam protegidos na nuvem: arquivos do Office podem ser abertos, mas somente é exibida uma página de rosto; outros arquivos são criptografadas como arquivos .xen. Entretanto, na unidade virtual local, eles permanecem descriptografados e são mostrados em texto simples. Para obter mais informações, clique no link adequado referente ao seu cliente de sincronização de nuvem.	**Conta empresarial:** Dropbox for Business OneDrive for Business/Unified OneDrive **Conta básica:** DropBox Box Google Drive OneDrive
Ver o menu da bandeja do sistema	Fornece informações úteis sobre arquivos, pastas e solução de problemas.	Entender itens de menu da bandeja do sistema do Data Guardian
Documentos protegidos do Office, habilitados para macro e .pdf, se a política estiver ativada	Proteja um documento do Office (.docx, .pptx, .xlsx, .docm, .pptm, .xlsm, .pdf) quando criá-lo. O documento será protegido quando você compartilhá-lo com outros usuários ou armazená-lo em mídia removível.	Usar documentos do Office com o modo protegido do Data Guardian • Observar as opções do menu Arquivo para determinar o nível de segurança para Documentos do Office • Trabalhar com as opções do menu Arquivo
Compartilhar uma pasta da nuvem com outros usuários para colaborar em arquivos	Compartilhar uma pasta com: Usuário interno (tem um endereço de email no domínio) Usuário externo (tem um endereço de email fora do domínio) - consulte seu administrador.	Usuário interno - Consulte a ajuda on-line do seu provedor de armazenamento em nuvem. Usuário externo - Consulte Uso do Data Guardian como usuário externo.

Instalar o Data Guardian com armazenamento em nuvem e documentos protegidos do Office

Pastas existentes com arquivos não-criptografados

Antes de implantar o Dell Data Protection | Data Guardian (DDG VDisk), será melhor se os dispositivos de destino ainda não tiverem a conta do provedor de armazenamento em nuvem configurada.

Se você já tiver uma conta no provedor de armazenamento em nuvem com pastas que são sincronizadas com o computador local e instalar o Data Guardian:

- Arquivos e pastas preexistentes que sincronizam para a nuvem permanecem em texto não criptografado
- Os arquivos que você adicionar a essas pastas preexistentes permanecerão em texto não criptografado
- Arquivos que sincronizarão a partir da nuvem serão criptografados

  Se você quiser que arquivos preexistentes sejam criptografados, vá para a DDG VDisk virtual drive, crie uma nova subpasta no cliente de sincronização de nuvem e mova os arquivos preexistentes para esta pasta.

  ou

  Para grande conteúdo, um gerente ou administrador poderá temporariamente solicitar o Menu Gerenciar pastas.

Instalar o Data Guardian no Windows

Você precisa ser um administrador local do computador para instalar o Data Guardian.

O computador precisa ter disponível uma letra do alfabeto para ser atribuída a uma unidade de disco.

O computador precisará ser reiniciado depois que o Data Guardian for instalado.

1 Para fazer download do instalador do Data Guardian, acesse o local especificado pelo administrador.
2 Com base no sistema operacional, selecione o instalador de 32 bits ou 64 bits, normalmente **setup32.exe** ou **setup64.exe**, e copie-o para o computador local.
3 Clique duas vezes no arquivo para abrir o instalador.
4 Se for mostrado um aviso de segurança, clique em **Executar**.
5 Selecione um idioma e clique em **OK**.
6 Se aparecer uma mensagem perguntando se você quer instalar o Pacote Redistribuível do Microsoft Visual C++ 2010 ou o Microsoft.NET Framework 4.0 Client Profile, clique em **OK**.
7 Na página de boas-vindas, clique em **Avançar**.
8 Leia o contrato de licença, aceite os termos e condições e clique em **Avançar**.
9 Na tela Pasta de destino, clique em **Avançar** para fazer a instalação no local padrão de **C:\Arquivos de Programas\Dell\Dell Data Protection\Dell Data Guardian\.**

  Em **C:**, não instale o Data Guardian nas pastas Usuários ou Windows ou na raiz de qualquer unidade. Você provocará um erro.
10 No campo *Nome do servidor:*, digite o nome do servidor com o qual o computador irá se comunicar, como server.domain.com. Não é necessário incluir www ou http(s). Esse dado é fornecido pelo administrador.

  Não desmarque a caixa de seleção *Ativar verificação da confiabilidade do SSL*, a menos que seu administrador instrua que você o faça.
11 Clique em **Avançar**.
12 Na tela Confirmar informações do servidor de ativação, verifique se o endereço URL do servidor está correto. O instalador acrescenta www ou http(s) e a porta. Clique em **Avançar**.

13 Na janela Tipo de gerenciamento, selecione a opção:
   - Uso interno – Um usuário com endereço de e-mail no domínio da empresa.
14 Clique em **Instalar** para iniciar a instalação.
   Uma janela de status mostra o andamento da instalação.
15 Clique em **Concluir** quando a tela Instalação concluída for exibida.
16 Clique em **Sim** para reiniciar.
   A instalação doData Guardian está concluída.
17 Após a reinicialização, confirme, na bandeja do sistema, se o ícone do Data Guardian tem uma marca de seleção verde  .

Data Guardian e Criptografia na nuvem

Se sua empresa definir políticas para proteger os dados na nuvem e você já tiver instalado e se conectado a um cliente de sincronização, será exibida uma DDG VDisk virtual drive no Windows Explorer.

NOTA:
O Data Guardian não oferece suporte à desmontagem da unidade virtual.

Se você precisar instalar e fazer login em um cliente de sincronização, consulte Instalar um Cliente de sincronização de nuvem.

Instalar um cliente Cloud Sync

Fazer download e instalar

Em geral, as empresas sugerem que todos os usuários instalem o mesmo cliente de sincronização de nuvem. Se for o caso, use o cliente de sincronização de nuvem preferencial da sua empresa.

NOTA:
O computador precisa ter disponível uma letra do alfabeto para ser atribuída a uma unidade de disco.

NOTA:
Atualmente, o Data Guardian não oferece suporte a um cliente de sincronização instalado em um ponto de montagem.

1 Instale um cliente de sincronização de nuvem básico ou empresarial:
   - **Contas empresariais do cliente Cloud Sync**
     Se sua empresa oferecer uma opção de conta empresarial, o administrador fornecerá a você um link para fazer o download e instalar o cliente. As opções são:
     - **Dropbox for Business** - Se você instalar o Dropbox for Business, precisará também de Autenticar o Dropbox for Business.
     - **OneDrive for Business/Unified OneDrive** - Para conhecer as etapas detalhadas, consulte https://support.microsoft.com/en-us/kb/2903984.
   - **Contas básicas do cliente Cloud Sync**
     - **Dropbox** - consulte https://www.dropbox.com/install
     - **Box Sync** - consulte https://www.box.com/box-for-devices
     - **Google Drive** - https://www.google.com/drive/download/
     - **OneDrive/Unified OneDrive (Windows 7 e 8)** - consulte https://onedrive.live.com/about/en-us/download/
       No Windows 8.1 ou posterior, o OneDrive já vem pré-instalado. Se o Windows Update estiver ativado, o Unified OneDrive substituirá o OneDrive.
2 Depois de instalar e fazer o login, a seguinte tela é exibida:
   - No Explorador de arquivos, é adicionada uma DDG VDisk virtual drive. A pasta de cliente de sincronização de nuvem é adicionada à unidade virtual.
     Se você instalar mais de um cliente de sincronização de nuvem, cada um deles mostrará uma pasta nessa unidade.

NOTA:
O Data Guardian não oferece suporte à desmontagem da unidade virtual.

- Em Gerenciador de arquivos > Favoritos, uma pasta é adicionada para o seu cliente de sincronização de nuvem.
- Na bandeja do sistema, o ícone do cliente de sincronização é mostrado.
- Dependendo do provedor de armazenamento em nuvem, um atalho para o cliente de sincronização pode ser adicionado automaticamente à área de trabalho.
- Somente no modo Aceitar (mas não no modo Forçar protegido) - uma pasta de Documentos protegidos é adicionada à raiz da pasta Documentos. Consulte Documentos > pasta Documentos protegidos.

Alterar a letra da unidade virtual ou criar um atalho

Depois de instalar o Data Guardian e um cliente de sincronização de nuvem, o ícone da DDG VDisk virtual drive é exibido no Explorador de arquivos. A letra da unidade é atribuída usando uma letra disponível do final do alfabeto.

Para alterar a letra da unidade:

1 Na bandeja do sistema, clique no ícone do Data Guardian e selecione **Configurar unidade**.

2 Selecione uma letra disponível na lista *Atual*.

3 Clique em **Aplicar** ou em **OK**.
Para adicionar o ícone da DDG VDisk virtual drive à área de trabalho, clique com o botão direito do mouse na unidade e selecione **Criar atalho**.

Autenticar o Dropbox for Business

Se você instalar o Dropbox for Business, o Data Guardian solicitará a autenticação.

Para autenticar:

1 Após a instalação do Data Guardian, poderá ser aberta uma janela de Autenticação ou você poderá clicar no ícone do Data Guardian e selecionar **Dropbox > Conectar**.
A janela Autenticação informará que o Data Guardian precisa ter acesso à sua conta do Dropbox e poderá fornecer instruções sobre contas empresariais e pessoais.

Para o usuário, fornece opções de menu de contexto. Para a empresa e seu administrador, é essencial, pois fornece medidas de segurança adicionais.

2 Na janela de Autenticação, clique em **Avançar**.

3 Se for aberta a janela Proteção contra ameaça à rede, clique em **Sim**.

4 Na janela de Autenticação, digite seu email de domínio e senha do Dropbox.

5 Clique em **Conectar**.

6 Se você tiver vinculado suas contas empresarial e pessoal do Dropbox, você será solicitado a selecionar uma delas nesse momento. Você precisa selecionar sua conta empresarial.

7 Clique em **Concluir** ou espere a janela fechar.

Trabalhar com pastas e arquivos

O Data Guardian trabalha de modo transparente com seu cliente de sincronização de nuvem. Quando o administrador define uma política para ativar o Data Guardian, os arquivos ficam criptografados e protegidos na nuvem quando sincronizados no computador local.

Siga as instruções na ajuda do provedor de armazenamento em nuvem para fazer o seguinte:

- Criar pastas
- Fazer upload/download de pastas e arquivos

NOTA:
Para fazer upload de arquivos, copie ou arraste os arquivos para pastas na DDG VDisk virtual drive. O Data Guardian não oferece suporte ao arraste de arquivos do computador local para a web ou à criação de arquivos diretamente no site do provedor de armazenamento em nuvem.

- Usar a sincronização seletiva de pastas
- Compartilhar pastas ou arquivos com usuários internos que têm o Data Guardian. Consulte Compartilhar uma pasta com um usuário interno.
- Compartilhar pastas ou arquivos com usuários externos. Consulte Uso do Data Guardian como usuário externo.
- Descompartilhar pastas

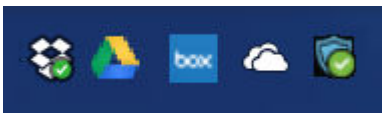
Ver pastas e arquivos no computador local e na nuvem

Acessar pastas e arquivos do cliente de sincronização no computador local

Para acessar pastas e arquivos sincronizados, clique na **DDG VDisk virtual drive** no Explorador de arquivos. Seu cliente de sincronização de nuvem é mostrado.

Há outras formas de acessar o cliente de sincronização de nuvem.

- Na bandeja do sistema, selecione o ícone do cliente de sincronização e abra a pasta do cliente de sincronização. Para obter mais informações, consulte a ajuda do provedor de armazenamento em nuvem.



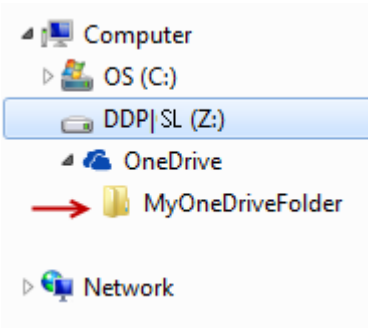
- Em Favoritos, clique no ícone do cliente de sincronização de nuvem.

  Note que, quando você clicar no ícone do cliente de sincronização na bandeja do sistema ou em Favoritos, a DDG VDisk virtual drive é destacada. O Data Guardian o redirecionará para essa unidade virtual, o que permitirá que você veja suas pastas e arquivos localmente descriptografados em texto não criptografado.

Você pode também acessar as pastas e arquivos da DDG VDisk virtual drive por meio de um atalho da área de trabalho. Consulte Alterar a letra da unidade virtual ou criar um atalho.

Adicionar pastas

Com o Data Guardian, você precisa adicionar subpastas à pasta de sincronização de nuvem. Não adicione arquivos à raiz da DDG VDisk virtual drive.



Adicionar arquivos

Quando você adiciona um arquivo a uma pasta, o Data Guardian adiciona automaticamente um arquivo à pasta na Web. O Data Guardian usa o arquivo Como acessar arquivos seguros.html quando você compartilha uma pasta com usuários externos. Você não precisa abrir nem fazer download desse arquivo. Consulte Uso do Data Guardian como usuário externo.

Ver pastas e arquivos do cliente de sincronização na nuvem

O Data Guardian criptografa seus dados na nuvem e os nomes dos arquivos têm uma extensão .xen. O ícone ao lado do arquivo pode ser diferente para cada provedor de armazenamento em nuvem, mas o conteúdo não é mostrado. Você não pode abrir arquivos na nuvem. Portanto, se alguém conseguir acessar sua conta de armazenamento na nuvem, a pessoa não conseguirá abrir nem ver seus arquivos. Isso aumenta a segurança na nuvem. Você só pode exibir arquivos em texto não criptografado na DDG VDisk virtual drive.

Ocasionalmente, quando você fizer download de um arquivo .xen para sua área de trabalho e ele for descriptografado, uma cópia do arquivo com uma extensão .xen permanecerá. Você pode apagar a cópia do arquivo .xen obtida por download.

Se sua empresa precisar de proteção adicional para pastas e arquivos na nuvem, o administrador poderá definir uma política para ofuscar os nomes dos arquivos na nuvem e ao fazer download. Se alguém conseguir acessar sua conta de armazenamento em nuvem, a pessoa não conseguirá abrir os arquivos nem ler os nomes dos arquivos.

Ver pastas e arquivos do cliente de sincronização em um computador local com o Data Guardian e uma unidade virtual instalados

Para tornar o Data Guardian fácil de usar no computador local, quando você abrir uma pasta da DDG VDisk virtual drive, os arquivos da nuvem serão automaticamente descriptografados em texto não criptografado mesmo se eles forem protegidos como arquivos criptografados na nuvem.

Proteger pastas e arquivos em Dispositivos que não têm o Data Guardian

Se uma pessoa não autorizada fizer download de um arquivo protegido da nuvem para um dispositivo que **não** tenha o Data Guardian instalado, esta pessoa não poderá acessar seus dados. Com base nas políticas definidas pelo administrador:

- Documentos do Office - o documento é aberto, mas será exibida somente uma página de rosto com uma mensagem específica para a empresa.
- Documentos não Office - o arquivo é obtido por download como um arquivo .xen. A pessoa não poderá abrir o arquivo.

> **NOTA:**
> Para usuários internos, se você fizer download de um arquivo de um computador que tenha o Data Guardian para um dispositivo que não tenha o aplicativo, você não poderá ver este arquivo a menos que instale o Data Guardian como usuário externo.

Em algumas situações, um arquivo .xen pode ser exibido em um computador que tenha o Data Guardian instalado. Por exemplo, se a conexão à Internet for perdida antes de terminar o download, a chave para abrir o arquivo poderá não estar disponível. Uma caixa de diálogo indica que não é possível descriptografar o arquivo.

O Data Guardian não permite a edição de arquivos sem extensões. Esses arquivos são tratados como arquivos somente leitura. Para editar um arquivo sem extensão, obtenha-o por download do site do provedor de armazenamento em nuvem, edite-o e transfira-o por upload através da DDG VDisk virtual drive.

Pesquisar nomes e conteúdo na DDG VDisk virtual drive

Se você quiser procurar por nomes de arquivo ou conteúdo na DDG VDisk virtual drive, precisará ativar a indexação do Windows Search para essa unidade.

> **NOTA:**
> A indexação de pesquisa do Windows está ativa apenas para as pastas de usuários.

Para ativar a indexação do Windows Search para a DDG VDisk virtual drive:

1 No Painel de controle, digite **Indexação de pesquisa** no campo de Pesquisa.
2 Selecione **Opções de indexação**.

3 Em *Alterar locais selecionados*, marque a caixa de seleção da DDG VDisk virtual drive.

> **NOTA:**
> As etapas restantes podem variar dependendo do seu sistema operacional.

4 Clique em **OK**.

5 Em Opções de indexação, clique em **Fechar**.

Agora, você pode realizar uma pesquisa na DDG VDisk virtual drive.

Compartilhar uma pasta com um usuário interno

Um usuário interno tem um endereço de email dentro do domínio da empresa.

Para compartilhar uma pasta com um usuário interno, é necessário acessar o site do provedor de armazenamento em nuvem e selecionar **Compartilhar**. Consulte a ajuda on-line do provedor de armazenamento em nuvem.

Como compartilhar uma pasta usando o Data Guardian e o Box.

No site do Box, selecione uma das opções a seguir.

Opção do site do Box	Opções	Descrição
Compartilhar	Disponível para pastas e arquivos Ver acesso	Quando a janela Compartilhar abrir, certifique-se de que a opção Permitir download esteja definida como **Sim**. Após fazer download de pastas ou arquivos, os usuários que estiverem fazendo compartilhamento precisarão extrair a pasta compactada e transferir a pasta e os arquivos para a DDG VDisk virtual drive.
Convidar Colaboradores	Disponível para pastas Ver ou Editar acesso	Quando a janela Convidar abrir, selecione **Editor** ou **Visualizador**. Os usuários que estiverem fazendo compartilhamento poderão sincronizar a pasta com seu respectivo computador. Ela será sincronizada com a DDG VDisk virtual drive.

Usar documentos do Office com o modo protegido do Data Guardian

Para melhorar a segurança da empresa, o administrador pode ativar uma política para proteger arquivos para os seguintes aplicativos do Office:

- .docx, .pptx, .xlsx
- .docm, .pptm, .xlsm

Se uma pessoa não autorizada acessar um arquivo protegido, o arquivo permanecerá criptografado, por exemplo quando você:

- Anexá-lo a um email
- Movê-lo em um navegador - em alguns clientes de sincronização de nuvem, é possível clicar com o botão direito do mouse em um nome de arquivo e selecionar **Mover**.
- Compartilhá-lo na rede
- Fazer upload do arquivo em um provedor de armazenamento em nuvem
- Armazená-lo em mídia removível

Em documentos do Office, pode ser exibida uma página de rosto com instruções para instalação ou ativação do Data Guardian, por exemplo:

- Você precisa instalar o Data Guardian.
- Você precisa ativar o Data Guardian.
- Você abre um documento protegido do Office na nuvem.
- Você fez download de um arquivo do Office do computador que tem o Data Guardian para um dispositivo pessoal que não tem o aplicativo.
- Um usuário não autorizado acessa um dos seus arquivos do Office - a página de rosto é exibida com uma mensagem específica para a empresa, mas o usuário não consegue ver o conteúdo do arquivo.

Se sua empresa usar o modo protegido do Data Guardian, observe o seguinte:

Observar as opções do menu Arquivo para determinar o nível de segurança para Documentos do Office

Para determinar se o administrador ativou as políticas do Data Guardian, abra um documento do Office e selecione **Arquivo**. Se for exibido *Salvar como protegido* no painel esquerdo, você tem proteção adicional nos documentos do Office.

Para determinar o nível de segurança, observe as opções que estão ativadas ou desativadas:

- **Modo Aceitar** - Você tem algumas opções para determinar que documentos do Office serão protegidos.
  - *Salvar e Salvar como protegido estão ativados* - Se você optar por proteger um documento do Office, selecione **Salvar como protegido**.
  - *Imprimir* e *Exportar* podem estar ativados ou desativados, dependendo da política.
  - *Compartilhar* (*Salvar e Enviar* para o Office 2010) está ativado.
  - Pasta **Documentos > Documentos protegidos** - No modo Aceitar (mas não no modo Forçar protegido) - uma pasta de Documentos protegidos é adicionada à raiz da pasta Documentos. Os documentos do Office nessa pasta estão criptografadas. Se você remover um documento protegido do Office dessa pasta, ele permanecerá criptografado. Se você renomear a pasta, o conteúdo da pasta renomeada estará criptografado. Se você apagar a pasta, ela será recriada.
- **Modo Forçar protegido** - sua empresa precisa de um nível mais alto de segurança.
  - *Salvar como* está desativado e *Salvar como protegido* está ativado - Você precisa salvar todos os documentos do Office no modo protegido.
  - *Imprimir* e *Exportar* podem estar ativados ou desativados, com base na política.
  - *Compartilhar* (*Salvar e Enviar* para o Office 2010) está desativado.

    NOTA:
    Com o modo Force-Protected, a política também ativa horários específicos para verificar seu computador e localizar arquivos desprotegidos do Office, e alterá-los para o modo Protegido. Você precisa estar conectado à rede para que o Data Guardian verifique todos os arquivos do Office desprotegidos.

- Se você selecionar **Salvar como protegido**, a única opção do campo *Salvar como tipo* será *Protegido do Office*.

- **Arquivo > Info** é diferente, por exemplo:
  - Para os modos Aceitar e Forçar protegido: é exibido *Adicionar restrição de data* caso o administrador tenha ativado esta política. Consulte Melhorar a segurança ao *Adicionar restrição de data*.
  - Para os modos Aceitar e Forçar protegido: as informações sobre propriedades relativas a esse documento do Office, como autor e data, estão ocultas para maior segurança.

- Status somente leitura: consulte a seguir para obter mais informações.

  NOTA:
  A opção *Proteger documento* em Arquivo > Info está relacionada ao Microsoft Office e não ao modo protegido do Data Guardian.

Se você abrir um documento do Office e ele indicar modo somente leitura, verifique o seguinte:

- Se *Salvar como protegido* não for exibido no painel esquerdo, o modo somente leitura não estará relacionado às políticas doData Guardian.
- Se o administrador definir políticas para o modo Forçar protegido com um nível de segurança mais alto, documentos desprotegidos do Office abrirão no modo somente leitura.

  NOTA:
  Para OneDrive, se você abrir um documento protegido do Office por meio de **Arquivo > Abrir > OneDrive** e o documento for somente leitura, confirme se você instalou e configurou o cliente de sincronização do OneDrive.

Trabalhar com as opções do menu Arquivo

Esta tabela lista as opções do menu Arquivo para documentos do Office. Dependendo do nível de segurança, algumas opções são esmaecidas.

NOTA:
Atualmente, documentos integrados do Office não são suportados pelo modo Documentos protegidos do Office.

Menu Arquivo	Modo Aceitar e documentos protegidos do Office	Modo Forçar protegido para documentos protegidos e desprotegidos
Abra	**Os arquivos abrem normalmente**	**Documentos desprotegidos abertos no modo somente leitura.**
Salvar	• Opções: Documento já protegido - Salva como protegido. Desprotegido - Salva como desprotegido. Para protegê-lo, clique em **Salvar como protegido**. • Documento somente leitura - Uma caixa de diálogo indica que não é possível salvar um documento desprotegido. A janela Salvar como é exibida e é preciso salvá-lo com outro nome de arquivo. • Arquivo xen - Você pode abri-lo e salvá-lo no modo protegido, mas o arquivo .xen é removido da nuvem. O documento do Office tem sua extensão usual, mas está protegido. **NOTA:** **Na unidade virtual, se o usuário clicar com o botão direito do mouse para criar um novo documento do Office, ele será um arquivo .xen. Você precisa salvá-lo manualmente como protegido.**	• O documento está protegido. • Documento somente leitura - Você pode editá-lo, mas não poderá salvar o original. Quando você clicar em Salvar, a janela Salvar como protegido será exibida e você precisará salvar o documento no modo protegido com um novo nome. • Documentos remotos - Se você abrir um documento em um local remoto e ele não estiver protegido, precisará salvá-lo na unidade local para modificar e salvar. Você não pode salvar o documento no local remoto. **NOTA:** **Clicar em Salvar abre a janela Salvar como, e a única opção no campo Salvar como tipo é Protegido do Office (documentos, apresentação, ou pasta de trabalho).** • Arquivo xen - Você pode abri-lo e salvá-lo no modo protegido, mas o arquivo .xen é removido da nuvem. O documento do Office tem sua extensão usual, mas está protegido.
Salvar como	**Tem as opções padrão (mas não o modo protegido)**	**Desativado**
Salvar de forma protegida como	**A única opção no campo Salvar como tipo é Protegido do Office**	**A única opção no campo Salvar como tipo é Protegido do Office**
Imprimir	**Pode estar ativado ou esmaecido com base nas políticas definidas pelo administrador. Se a opção de menu estiver ativada, uma política poderá colocar uma marca d'água contendo nome de usuário, nome de domínio e ID do computador em cada página que você imprimir.**	**Dependendo da política, essa opção poderá estar ativada ou esmaecida.** **Se a opção de menu estiver ativada, uma política poderá colocar uma marca d'água contendo nome de usuário, nome de domínio e ID do computador em cada página que você imprimir.**
Compartilhar	**Ativado**	**Desativado**
Salvar e enviar (Office 2010)	**Ativado**	**Desativado** **Se a opção Imprimir estiver ativada, você poderá selecionar Imprimir para imprimir o documento como PDF.**
Exportar (Office 2013 e superior)	**Pode estar ativado ou esmaecido com base nas políticas definidas pelo administrador.**	**Pode estar ativado ou esmaecido com base nas políticas definidas pelo administrador.**
Exportação protegida (Office 2013 e superior)	Se a opção de menu Exportar estiver esmaecida e Exportação protegida estiver ativada, o documento exportará com uma marca d'água, contendo nome de usuário, nome de domínio e ID do computador em cada página. **NOTA:** Se você exportar um documento no modo protegido para um usuário externo, ele poderá abrir e ver o documento, mas não poderá exportar ou imprimi-lo.	Se a opção de menu Exportar estiver esmaecida e Exportação protegida estiver ativada, o documento exportará com uma marca d'água, contendo nome de usuário, nome de domínio e ID do computador em cada página. **NOTA:** Se você exportar um documento no modo protegido para um usuário externo, ele poderá abrir e ver o documento, mas não poderá exportar ou imprimi-lo.

Trabalhar online com documentos protegidos do Office

Ao criar documentos protegidos do Office, recomenda-se trabalhar online, pois são geradas chaves para esses documentos. Se tiver sido necessário recriar a imagem do seu computador e você tiver criado documentos protegidos do Office offline, informe o administrador.

Trabalhar online com documentos protegidos habilitados para macro

Com um documento protegido habilitado para macro, a macro existe, mas está bloqueada. No entanto, atualmente, o Data Guardian só pode controlar um documento habilitado para macro depois que o documento recém-protegido (.docm, .pptm, .xlsm) seja fechado e reaberto. Além disso, se você salvar um documento protegido com uma macro como desprotegido, precisará fechar e reabrir a documento, para que a macro seja executada.

Anexar um documento protegido do Office a um email do Outlook

Ao anexar um documento protegido do Office a um email do Outlook, selecione **Inserir** em vez de *inserir como texto*. *Inserir como texto* cola o conteúdo do documento diretamente no corpo do email e o conteúdo não estará mais protegido.

Solução de problemas para o modo Aceitar

Em Arquivo > Info, se sua opção Imprimir está esmaecida, significa que uma política do Data Guardian desativou a impressão de documentos protegidos do Office. No entanto, atualmente, quando você clica com o botão direito do mouse em uma arquivo protegido do Office no Windows Explorer, a opção de Imprimir não está esmaecida. Porém, se você selecionar Imprimir, ocorrerá o seguinte:

- Word - Uma caixa de diálogo indica que o Word parou de funcionar.
- Excel - Uma caixa de diálogo indica que a opção Imprimir está desativada por uma política.
- PowerPoint - Uma caixa de diálogo indica que a opção Imprimir está desativada por uma política. Se você clicar em OK, uma página de rosto será impressa, informando que o documento está protegido.

Determinar que documentos do modo Aceitar estão protegidos

Se você tiver o modo Forçar protegido, todos os documentos do Office estarão protegidos. Se você tiver o modo Aceitar e quiser confirmar se um documento está protegido ou não, abra o documento e a barra de título o mostrará como protegido.

Opções de menu adicionais para documentos protegidos do Office

O tipo de documento do Office, protegido ou desprotegido, pode afetar o seguinte.

Clicar com o botão direito do mouse > Proteger

Você pode clicar com o botão direito do mouse em um documento do Office e selecionar **Proteger**. Você precisa adicionar conteúdo para que a opção de menu seja exibida. Você não pode proteger um documento em branco.

Guia Propriedades do arquivo > Dell Data Guardian

Com documentos protegidos do Office, clique com o botão direito do mouse e selecione **Propriedades**; a guia **Dell Data Guardian** será exibida com informações, como a identificação da chave do arquivo e dados de acesso e embargo.

Colar

Se o administrador definir uma política para proteger documentos do Office:

- Você poderá copiar e colar dados no documento protegido original.
- Você não poderá copiar ou colar de um documento protegido para um documento desprotegido. Nada será mostrado na área de transferência, e uma mensagem de texto específica para a empresa informará que não é possível colar no documento desprotegido ou não gerenciado.

  NOTA:
  Se você cortar texto de um documento protegido e receber a mensagem em um documento desprotegido, clique em **Desfazer** no documento protegido para recuperar o texto.

Arrastar e soltar no modo protegido

Você pode arrastar e soltar conteúdo em um documento protegido do Word. Atualmente, a opção arrastar e soltar está desativada para arquivos protegidos do PowerPoint e do Excel.

Impressão de envelopes e etiquetas

Se o administrador tiver definido uma política para adicionar uma marca d'água quando você imprimir um documento protegido do Office, siga estas etapas para imprimir envelopes ou etiquetas:

1 Em um documento do Word, selecione a guia **Correspondências**.
2 Selecione a opção **Envelopes** ou **Etiquetas**.
3 Depois que você digitar o endereço ou o endereço do remetente, clique em **Imprimir**.

> **NOTA: Se você usar outra opção para imprimir e o administrador definir uma política para adicionar uma marca d'água para documentos impressos do Office, será exibida uma marca d'água no envelope ou na etiqueta.**

Documentos Office protegidos e adulterados

O Data Guardian pode analisar documentos protegidos do Office para detectar algumas formas de adulteração.

Se um usuário interno adulterar um documento protegido do Office:

- O Data Guardian poderá reparar ou restaurar parte da adulteração.
- Para a adulteração que não puder ser reparada, uma caixa de diálogo será exibida informando que o arquivo foi adulterado e solicitando que você entre em contato com o administrador.

Se um usuário não autorizado abrir um documento protegido do Office, apenas a página de rosto será exibida. Se o usuário não autorizado modificar a página de rosto, o Data Guardian restaurará a página de rosto quando um usuário autorizado salvar novamente o documento como protegido.

Usuários externos e documentos protegidos do Office

Melhorar a segurança ao adicionar restrições de data

Com o Data Guardian, faça upload de um documento protegido do Office para a nuvem e compartilhe-o:

- Todos os usuários internos do Data Guardian poderão vê-lo.
- Com base na política, os usuários externos poderão vê-lo.

Opcionalmente, para a segurança aprimorada com os usuários externos, você pode adicionar uma restrição de data para limitar o tempo em que um usuário externo pode ver uma documento protegido do Office.

1 Selecione **Arquivo > Info > Restringir data**.
2 Na lista suspensa, selecione uma Data de início e uma Data de término e a hora para um usuário externo ver o documento.

> **NOTA:**
> A data de início e a hora poderão estar no futuro se você quiser enviar o documento, mas impeça que o usuário externo o veja até a data e a hora determinadas.

3 Clique em **OK**.
O documento será salvo, protegido, fechado e, em seguida, reaberto.

> **NOTA:**
> Se você modificar as datas para um documento desprotegido do Office e, em seguida, clicar em Cancelar, o Data Guardian ainda protegerá o arquivo.

NOTA:
Atualmente, ao adicionar restrições de data a um documento protegido do Office e planejar salvá-lo em uma unidade de rede, será preciso salvar o arquivo localmente e, em seguida, copiá-lo para a rede.

Se um usuário externo abrir um arquivo depois do intervalo de data e hora, uma caixa de diálogo informará que o arquivo tem restrições de acesso e que o usuário do arquivo poderá entrar em contato com o autor do arquivo. A caixa de diálogo não exibirá qualquer data para o usuário externo.

Se você definir o campo Data de início para uma data ou hora futura e o usuário externo abrir o arquivo antes dessa hora, uma caixa de diálogo será exibida indicando que o arquivo não poderá ser aberto antes da data e da hora determinadas devido a restrições de acesso.

Trabalhar sem conexão de Internet

Sem uma conexão de Internet, ainda é possível ver arquivos de sincronização de nuvem na unidade local por meio do Explorador de arquivos. Entretanto, a DDG VDisk virtual drive não é exibida. Além disso, as alterações não serão sincronizadas na nuvem até que você se conecte à Internet.

Limite de caracteres para nomes de caminho de pastas

Os nomes de caminho do Windows têm um limite de 248 caracteres.

Na nuvem, esse limite não existe. Portanto, você pode criar pastas e subpastas com um nome de caminho além do limite. Contudo, localmente, no Windows, para qualquer nome de caminho que exceda esse limite, as pastas não são criadas. Portanto, não use mais de 248 caracteres para o caminho de pastas e subpastas.

Dropbox for Business

O Dropbox for Business tem requisitos específicos. Consulte Instalar um cliente Cloud Sync.

Ajuda do provedor de armazenamento em nuvem

Antes de usar o Data Guardian, saiba mais sobre o provedor de armazenamento em nuvem. O suporte do Dropbox for Business está em:

https://www.dropbox.com/help.

Embora você possa fazer upload de arquivos no site do provedor de armazenamento em nuvem, é aconselhável trabalhar com pastas e arquivos na DDG VDisk virtual drive.

Conectar o Data Guardian e o Dropbox for Business

Se sua empresa usa o Dropbox for Business, é preciso permitir que o Data Guardian permaneça conectado.

Para conectar:

1. Na bandeja do sistema, clique no ícone do Data Guardian e selecione **Dropbox > Conectar**.
2. Na janela Autenticação do Dropbox, leia as informações e, em seguida, clique em **Avançar**.
3. Se você tiver vinculado suas contas empresarial e pessoal do Dropbox, você será solicitado a selecionar uma delas nesse momento. Você precisa selecionar sua conta empresarial.
4. No prompt para permitir o acesso do Data Guardian aos seus arquivos e pastas do Dropbox, clique em **Permitir**.

5 Clique em **Concluir**.

Definir sincronização seletiva para pastas

Para sincronizar pastas seletivamente:

1 Na bandeja do sistema, clique no ícone do **Dropbox for Business**.
2 Clique no ícone de **Configurações** e selecione **Preferências**.
3 Clique na guia **Conta** e, em seguida, clique em **Sincronização seletiva**.
4 Selecione apenas as pastas ou subpastas que você quer sincronizar a partir de seu computador.
5 Clique em **Atualizar**.
6 Na caixa de diálogo de confirmação de Atualização, clique em **OK**.
7 Na janela Preferências do Dropbox, clique em **OK**.
Uma mensagem pop-up na bandeja do sistema mostra que as pastas estão sendo sincronizadas.

Sua empresa determinará se você pode ter uma conta empresarial apenas ou se você pode usar tanto a pasta empresarial como a pessoal. Se você quiser que pastas preexistentes contendo arquivos ou dados pessoais não sejam criptografadas, desmarque a seleção dessas pastas antes de instalar o Data Guardian. Caso contrário, seus dados pessoais poderão ser criptografados.

Usar o ícone do Dropbox for Business na bandeja do sistema

Na bandeja do sistema, clique no ícone do Dropbox.

- Para o site, selecione o ícone de globo.

> **NOTA:**
> Se você usar o Chrome ou o Firefox para abrir Dropbox.com, certifique-se de fechá-lo depois de terminar de trabalhar com arquivos e pastas. Mesmo se você abrir outra guia no navegador, o conteúdo será criptografado. Isso pode incluir emails, anexos ou uploads que estejam usando o navegador.

- Para a pasta - selecione o ícone da pasta do Dropbox. Isso redirecionará você para a DDG VDisk virtual drive.

Usar o menu contextual do Dropbox for Business

No Windows Explorer, quando o Data Guardian é instalado, o Dropbox for Business tem um menu contextual.

> **NOTA:**
> É necessário conectar o Data Guardian ao Dropbox.

No Windows Explorer, para acessar o menu contextual, abra uma pasta do Dropbox e clique com o botão direito em um arquivo. O ícone da nuvem tem as seguintes opções:

- Compartilhar o link seguro do Dropbox
- Mostrar no Dropbox.com
- Ver versões anteriores

Usar contas empresariais e pessoais do Dropbox

Se seu computador tiver Dropbox for Business e também permitir que você vincule uma conta pessoal do Dropbox a sua conta empresarial, certifique-se de entender as políticas estabelecidas por seu administrador para essas contas. Por exemplo, uma empresa pode estabelecer as seguintes políticas:

- Tanto arquivos empresariais como pessoais são criptografados.

  ou

- Apenas arquivos e pastas empresariais são criptografados. Arquivos pessoais permanecem descriptografados.

  Por segurança, sua empresa pode ter uma política de auditoria. Nomes de arquivos da pasta pessoal são registrados e enviados ao Dell Data Protection Server.

Se você usar contas empresariais e pessoais do Dropbox, não armazene arquivos empresariais em sua pasta pessoal do Dropbox.

Decriptografar pastas em uma conta pessoal

Se uma pasta pessoal for acidentalmente criptografada, o administrador poderá lhe conceder acesso temporário para que você gerencie a criptografia das suas pastas. Desmarque as pastas que devem ser decriptografadas. Além disso, você pode remover pastas da sincronização desvinculando a conta ou desfazendo a sincronização das pastas pessoais que devem permanecer decriptografadas.

OneDrive for Business/ Unified OneDrive

NOTA:
O Data Guardian não é compatível com o Microsoft Office 365.

NOTA:
O compartilhamento de dados no OneDrive for Business não é suportado.

Ajuda do provedor de armazenamento em nuvem

Antes de usar o Data Guardian, saiba mais sobre o provedor de armazenamento em nuvem. O suporte do OneDrive for Business está em

http://windows.microsoft.com/en-us/onedrive/onedrive-help#onedrive=other.

Embora você possa fazer upload de arquivos no site do provedor de armazenamento em nuvem, é aconselhável trabalhar com pastas e arquivos na DDG VDisk virtual drive.

Definir sincronização seletiva para pastas

Para sincronizar pastas seletivamente:

1. Na bandeja do sistema, clique com o botão direito do mouse no ícone do **OneDrive for Business/ Unified OneDrive** e clique em **Sincronizar uma nova biblioteca**.
2. Digite o URL da sua biblioteca.
3. Selecione **Sincronizar agora**.
4. Selecione **Mostrar meus arquivos**.

Usar o ícone do OneDrive for Business na bandeja do sistema

Na bandeja do sistema:

- Para o site - clique com o botão direito do mouse e selecione **Ir para OneDrive.com**.
- Para a pasta - clique com o botão direita ou esquerdo do mouse e selecione **Abrir a pasta do OneDrive for Business**. Essa ação redirecionará você para a DDG VDisk virtual drive.

Considerações de segurança com o Data Guardian e o OneDrive ou OneDrive for Business

O Dell Data Guardian criptografa pastas e arquivos para tornar os dados protegidos. Como o Data Guardian funciona com clientes de sincronização, leve em conta as considerações a seguir.

- Ao fazer download, não selecione Cancelar. Isso causará um erro. Se você quiser apagar o arquivo, aguarde o download terminar.
- No Windows 8.1, o Microsoft OneDrive tem arquivos de espaço reservado que parecem existir no cliente de sincronização, mas cujo download realmente não ocorreu. Portanto, o Dell Data Guardian não pode criptografá-los. Se você abrir um arquivo de espaço reservado, o Data Guardian exibirá uma caixa de diálogo indicando que o arquivo não estará protegido. É possível clicar com o botão direito do mouse e selecionar **Download** e, em seguida, o **Data Guardian** o converterá em um arquivo .xen.

DropBox

Ajuda do provedor de armazenamento em nuvem

Antes de usar o Data Guardian, saiba mais sobre o provedor de armazenamento em nuvem. O suporte para Dropbox está no endereço https://www.dropbox.com/help.

Embora você possa criar arquivos na nuvem ou fazer upload de arquivos no site do provedor de armazenamento em nuvem, é aconselhável trabalhar com pastas e arquivos na DDG VDisk virtual drive.

NOTA:
No Dropbox e no Data Guardian, se você criar um arquivo do Office na nuvem e sincronizá-lo, ele será criptografado como um arquivo .xen. Portanto, na unidade virtual, ele abre no modo somente leitura. Não é possível editá-lo.

Se você apagar todas as pastas da unidade virtual, os arquivos serão apagados, mas as pastas poderão permanecer. Nesse caso, apague as pastas na nuvem.

Definir sincronização seletiva para pastas

Para sincronizar pastas seletivamente:

1. Na bandeja do sistema, clique no ícone do **Dropbox**.
2. Clique no ícone de **Configurações** e selecione **Preferências**.
3. Clique na guia **Conta** e, em seguida, clique em **Sincronização seletiva**.
4. Selecione apenas as pastas ou subpastas que você quer sincronizar a partir de seu computador.
5. Clique em **Atualizar**.
6. Na caixa de diálogo de confirmação de Atualização, clique em **OK**.
7. Na janela Preferências do Dropbox, clique em **OK**.
   Uma mensagem pop-up na bandeja do sistema mostra que as pastas estão sendo sincronizadas.

Usar o ícone do Dropbox na bandeja do sistema

Na bandeja do sistema, clique no ícone do Dropbox.

- Para o site, selecione o ícone de globo.

NOTA:
Se você usar o Chrome ou o Firefox para abrir Dropbox.com, certifique-se de fechá-lo depois de terminar de trabalhar com arquivos e pastas. Mesmo se você abrir outra guia no navegador, o conteúdo será criptografado. Isso pode incluir emails, anexos ou uploads que estejam usando o navegador.

- Para a pasta - selecione o ícone da pasta do Dropbox. Isso redirecionará você para a DDG VDisk virtual drive.

Considerações de segurança com o Data Guardian e o Dropbox

Se você estiver executando em uma máquina virtual, não arraste um arquivo da área de trabalho do servidor para o navegador. O arquivo não estará protegido. Execute uma destas opções: no navegador, use a opção Upload ou, na área de trabalho, arraste o arquivo para a DDG VDisk virtual drive.

Perguntas frequentes do Dropbox

Pergunta

Minha conta do Dropbox possui muitos arquivos com conflito. Quando eu os apago da nuvem, eles continuam a ser criados.

Resposta

Às vezes, quando uma pasta já tiver sido compartilhada e múltiplas contas do Data Guardian forem ativadas ao mesmo tempo, esses arquivos serão vistos como tendo sido criados ao mesmo tempo. Em um esforço para preservar o original, o Dropbox cria múltiplos arquivos com o mesmo nome e tipo e os coloca na nuvem. Portanto, o Data Guardian permitirá que todos os arquivos sejam criados sem interferir.

Solução

1 Todas as pessoas que estiverem compartilhando esse arquivo precisam colaborar para desmarcar essa pasta para sincronização a partir do aplicativo Dropbox. Consulte Dropbox for Business.
2 Depois de todos os arquivos e a pasta serem removidas de cada máquina local, uma pessoa precisa acessar a nuvem e apagar os arquivos duplicados.

A seguir, cada pessoa pode usar a sincronização seletiva para adicionar novamente a pasta a ser sincronizada.

Box

Ajuda do provedor de armazenamento em nuvem

Antes de usar o Data Guardian, saiba mais sobre o provedor de armazenamento em nuvem. O suporte para Box está no endereço https://support.box.com/home.

Embora você possa fazer upload de arquivos no site do provedor de armazenamento em nuvem, é aconselhável trabalhar com pastas e arquivos na DDG VDisk virtual drive.

NOTA:
Se você usar o Internet Explorer para fazer upload de arquivos para o provedor de armazenamento em nuvem do Box ou para abrir um arquivo, poderá ocorrer um atraso na janela do Explorador de arquivos.

NOTA:
O Box Tools e o Box Edit não são suportados pelo Data Guardian. O uso do Box Tools pode causar uma condição de tela azul.

Definir sincronização seletiva para pastas

Para sincronizar pastas seletivamente:

1 Na bandeja do sistema, clique com o botão direito no ícone do Box e selecione **Abrir o site do Box**.

2 No site do cliente de sincronização de nuvem, clique com o botão direito do mouse em uma pasta e selecione **Sincronizar pasta com o computador**.

3 Na janela Sincronizar pasta, clique em **Sincronizar pasta**.

O ícone da bandeja do sistema indica que as configurações estão sendo aplicadas. Isso pode levar vários minutos.

4 Quando concluir, navegue para **Windows Explorer** > **Sincronização do Box**. As pastas sincronizadas serão mostradas com uma marca de seleção.

Usar o ícone do Box na bandeja do sistema

Na bandeja do sistema, clique no ícone do Box.

- Para o site - Selecione **Abrir site do Box**.
- Para a pasta - Selecione a pasta **Abrir sincronização do Box**. Essa ação redirecionará você para a DDG VDisk virtual drive.

Perguntas frequentes sobre o cliente de sincronização do Box

Pergunta

Estou usando o cliente de sincronização do Box. Criei uma nova pasta localmente e adicionei alguns arquivos. O cliente de sincronização parece estar funcionando, mas nada foi criado na nuvem.

Resposta

O cliente de sincronização do Box pode necessitar de algum tempo para coletar informações sobre pastas e arquivos novos. O processo pode levar vários minutos, em comparação com outros clientes de sincronização. Certifique-se de aguardar vários minutos para o cliente de sincronização concluir antes de criar pastas e arquivos novos.

Pergunta

Estou usando o cliente de sincronização do Box. Eu fiquei sem espaço na minha partição primária, então eu passei a usar outra unidade. Agora, a pasta Meus arquivos do Box tem uma ou mais pastas criadas e com o nome de **Nova pasta**.

Resposta

Atualmente, quando estão sendo sincronizados arquivos entre dois computadores no mesmo arquivo de compartilhamento, se alguém transferir essa pasta para outro local, toda nova pasta que outras pessoas criarem naquele arquivo será criado naquele arquivo de compartilhamento será uma pasta vazia com o nome de **Nova pasta**.

Solução

Apague a Nova pasta diretamente da nuvem. Ela será removida de todos os sistemas que estiverem compartilhando essa pasta.

Considerações de segurança com o Data Guardian e o Box

Se você criar um arquivo no site Box Cloud, ele será sincronizado. Entretanto, o download será obtido como um arquivo criptografado.

O Internet Explorer poderá provocar um atraso quando fizer upload ou for aberto no Box.

Google Drive

Ajuda do provedor de armazenamento em nuvem

Antes de usar o Data Guardian, saiba mais sobre o provedor de armazenamento em nuvem. O suporte para o Google Drive está no endereço https://support.google.com/drive/?hl=en#topic=14940.

Embora você possa fazer upload de arquivos no site do provedor de armazenamento em nuvem, é aconselhável trabalhar com pastas e arquivos na DDG VDisk virtual drive.

Definir sincronização seletiva para pastas

Para sincronizar pastas seletivamente:

1 Na bandeja do sistema, clique no ícone do **Google Drive**.
2 Selecione o ícone Configurações.
3 Selecione **Preferences** (Preferências).
4 Para sincronizar seletivamente, clique em **Somente essas pastas**.
5 Limpe a caixa de seleção das pastas que não precisam de proteção na nuvem.
6 Clique em **Aplicar**.
7 Para confirmar, clique em **Continuar**.

Usar o ícone do Google Drive na bandeja do sistema

Na bandeja do sistema, clique no ícone do Google Drive.

- Para o site - Selecione **Visitar o Google Drive na Web**.
- Para a pasta - Selecione a pasta**Abrir o Google Drive**. Essa ação redirecionará você para a DDG VDisk virtual drive

Considerações de segurança com o Data Guardian e o Google Drive

O Data Guardian criptografa pastas e arquivos para proteger os dados. Como o Data Guardian funciona com clientes de sincronização, leve em conta as considerações a seguir.

- A política de segurança da empresa proíbe o uso do Google Docs com o Data Guardian. Quando você instala o Data Guardian, uma caixa de diálogo fornece informações sobre essa política. Para obter mais informações, entre em contato com o administrador de TI.

  O Google Drive contém um aplicativo Google Docs que permite aos usuários colaborar em documentos em tempo real. Entretanto, a colaboração ocorre em um servidor do Google e os arquivos não são criptografados. Para o Windows e o Data Guardian, qualquer documento do Google Docs que for criado será exibido nas pastas do cliente de sincronização do Google Docs.

  Entretanto, se você abrir a pasta, uma caixa de diálogo alertará você de que o Data Guardian não poderá criptografar o documento. Além disso, para garantir a proteção dos dados, o administrador poderá executar relatórios para identificar os documentos do Google Docs que estão sendo sincronizados para oferecer maior segurança.
- A opções do Google Drive incluem **Remover** (remove para a lixeira) e **Apagar**. O Google Drive com Data Guardian tem apenas a opção Apagar, para ser consistente com outra funcionalidade do Data Guardian.

NOTA:
Se você apagar múltiplos arquivos da unidade virtual do Data Guardian e alguns continuarem a ser exibidos no navegador ou na linha de comando, apague-os do navegador ou da linha de comando.

- No Google Drive, você poderá receber o aviso de que as propriedades serão retiradas ao serem copiados arquivos para a DDG VDisk virtual drive. Esses são atributos de segurança.

OneDrive

NOTA:
O Data Guardian não é compatível com o Microsoft Office 365.

Ajuda do provedor de armazenamento em nuvem

Antes de usar o Data Guardian, saiba mais sobre o provedor de armazenamento em nuvem. Suporte para OneDrive no endereço http://windows.microsoft.com/en-us/onedrive/onedrive-help#onedrive=other.

Embora você possa fazer upload de arquivos no site do provedor de armazenamento em nuvem, é aconselhável trabalhar com pastas e arquivos na DDG VDisk virtual drive.

Definir sincronização seletiva para pastas

Para sincronizar pastas seletivamente:

1. Na bandeja do sistema, clique com o botão direito do mouse no ícone do **OneDrive** e clique em **Configurações**.
2. Selecione a guia **Escolher pastas** e clique em **Escolher pastas**.
3. Em seguida, selecione **Escolher pastas para sincronizar**.
4. É mostrada uma lista de pastas. Marque ou desmarque caixas de seleção para sincronizar essas pastas. Clique em **OK**.
5. Clique em **OK**.
6. O ícone da bandeja do sistema indica que as configurações estão sendo aplicadas. Isso pode levar vários minutos.
7. Quando concluir, navegue para **Windows Explorer** > **OneDrive**. As pastas sincronizadas serão mostradas com uma marca de seleção.

Usar o ícone do OneDrive na bandeja do sistema

Na bandeja do sistema:

- Para o site - clique com o botão direito do mouse e selecione **Ir para OneDrive.com**.
- Para a pasta - clique com o botão direita ou esquerdo do mouse e selecione **Abrir a pasta do OneDrive**. Essa ação redirecionará você para a DDG VDisk virtual drive.

Considerações de segurança com o Data Guardian e o OneDrive ou OneDrive for Business

Consulte Considerações de segurança com o Data Guardian e clientes de sincronização.

Entender itens de menu da bandeja do sistema do Data Guardian

Tela de detalhes

A tela Detalhes do Data Guardian fornece informações úteis; por exemplo:

- Para obter suporte técnico, você pode fornecer informações de status ou de versão.
- Para visualizar um nome de arquivo não obscurecido que está associado a um arquivo .xen, selecione **Arquivos** > **Estado do arquivo**.
- Para procurar por um nome de arquivo, selecione a opção Copiar no canto inferior direito e cole o conteúdo em um arquivo Word.
- Para ver quem é o proprietário de uma pasta, selecione Pastase role até à coluna PROPRIEDADE DE PASTA.

Para ter acesso à tela Detalhes:

Clique no ícone da bandeja de sistema do **Data Guardian** e, a seguir, clique em **Detalhes...**

O canto superior esquerdo da tela Detalhes mostra as seguintes informações:

Status do serviço: status do Serviço Windows do Data Guardian. Os valores são: Interrompido, IniciarPendente, PararPendente, Em execução, ContinuarPendente, PausarPendente, Pausado

Estado de execução: o status de ativação do dispositivo. Os valores são: Ativo, Reativando, Suspenso, Suspendendo

Modo de usuário: usuário interno - um usuário dentro desse endereço de domínio

Usuário externo - usuário fora desse endereço de domínio

Email de registro: para usuários internos, este é o endereço de email de domínio. Para usuários externos, este é o endereço de e-mail para o qual os usuários estão registrados.

URL do servidor: o DDP EE Server/VE Server que se comunica com esse cliente.

Data da última modificação da política: data e carimbo de data/hora em que a política foi modificada pela última vez e consumida pelo cliente.

Versão da política: versão da política gerada pelo DDP EE Server/VE Server.

A área **Arquivos** da tela Detalhes exibe as seguintes informações:

Nome: nome do arquivo

Nuvem: mostra em uma lista o nome de arquivo ofuscado ou se o arquivo está *Desprotegido*.

Estado do arquivo: esse valor indica o proprietário da pasta. O valor é determinado pela ID da chave.

Estado do processamento: mostra se o arquivo precisa de uma chave ou se está *Concluído*.

Empresa: mostra o servidor padrão. Se for mostrada uma mensagem nessa coluna, *Erro: a chave não é do seu servidor*, a chave não pertence ao servidor da sua empresa. A chave de um arquivo criptografado precisa pertencer ao servidor da empresa.

Chave: identificação da chave atribuída a essa pasta (os arquivos novos usam essa chave para criptografia).

Pasta: nome do caminho completo da pasta.

Data da última modificação: data na qual o arquivo foi modificado.

Estado de persistência: indica se o arquivo está no disco.

Leitura de arquivo XEN: *Verdadeiro* ou *Falso.*

Criado pelo navegador: *Verdadeiro* ou *Falso*.

Para ver arquivos de registro, clique em **Ver registro** no canto inferior esquerdo da tela.

NOTA:
Os arquivos de registro podem ser encontrados também em **C:\ProgramData\Dell\Dell Data Protection\Dell Data Guardian.**

A área **Pastas** da tela Detalhes exibe as seguintes informações:

Nome: nome da pasta

Chave: identificação da chave atribuída a essa pasta (os arquivos novos usam essa chave para criptografia).

Cliente de sincronização: o último cliente de sincronização a sincronizar essa pasta (Clientes de sincronização de nuvem.)

Propriedade da pasta: esse valor indica o proprietário da pasta. O valor é determinado pela ID da chave.

Anular: as opções são *Nenhum* e *Preexistente.* Os arquivos preexistentes não são protegidos. Além disso, se você tiver acesso ao Gerenciamento de pastas e tiver alguns arquivos desprotegidos, essa coluna indica que eles não estão protegidos.

Tipo de Ofuscação: se sua empresa gerencia seu armazenamento em nuvem, essa é a política definida em cada pasta indicando que tipos de arquivos .xen serão criados na nuvem. Essa é uma política definida pelo administrador. Se o administrador selecionar *Somente extensão*, será exibido o nome real do arquivo com a extensão ".xen". Se o administrador selecionar *Guid*, será exibido um nome de arquivo misturado com a extensão ".xen". Essa é uma definição de política aplicada apenas em pastas novas. O padrão é *Extensão apenas*.

Menu de Gerenciar pastas

Alguns gerentes ou administradores podem temporariamente precisar solucionar problemas em pastas compartilhadas por mais de um usuário. Você pode solicitar permissão do seu administrador para a opção Gerenciar pastas. Normalmente, essa é uma opção temporária.

Verificar atualizações de política

Se o administrador modificar uma política e notificá-lo sobre uma atualização da política, acesse a bandeja do sistema, clique no ícone **Dell Data Protection | Data Guardian** e selecione **Verificar atualizações de política**.

Se o administrador modificar uma política para proteger arquivos criados no Microsoft Word, você precisará fechar o Word para que a atualização seja aplicada.

Localizar arquivos de log

Para solução de problemas, talvez o administrador solicite os arquivos de registro.

Para localizar os arquivos de log:

1 Navegue até
2 Selecione **Xendow.Service.log**.

NOTA:
Após o Xendow.Service.log atingir 3 MB, ele será salvo como Xendow.Service1.log e, depois, Xendow.Service2.log.

Atualizar o Data Guardian

A prática recomendada é desinstalar as versões anteriores e, em seguida, instalar a versão atual. Consulte Desinstalar o Data Guardian.

Fornecer feedback à Dell

Se seu administrador tiver habilitado uma política de feedback, você poderá fornecer feedback à Dell sobre este produto. O pequeno formulário contém duas perguntas sobre o seu nível de satisfação, com escalas de classificação (onde 10 indica o mais alto nível de satisfação) e um campo de comentário.

Para acessar o formulário, clique no ícone do Data Guardian na bandeja do sistema e selecione **Enviar feedback**.

Se esse recurso não for ativado por política, essa opção não será mostrada.

Possíveis problemas com a ativação - Armazenamento em nuvem e Documentos protegidos do Office

Se você tiver instalado o Data Guardian, mas o ícone do Data Guardian na bandeja do sistema não tiver uma marca de seleção verde,  , lembre-se do seguinte, dependendo de você ter criptografia em nuvem, documentos protegidos do Office ou ambos:

- O acesso é bloqueado para sites de sincronização em nuvem
- Os aplicativos de sincronização em nuvem são bloqueados de se conectar a seus serviços Web
- Pastas locais sincronizadas não são atualizadas durante esse período
- O Data Guardian pode converter documentos existentes do Office para o modo protegido antes de serem ativados. Nesse caso, quando você abrir um documento do Office, uma página de rosto exibirá informações sobre como ativar.

Execute um destes processos:

- Reinicialize e faça login novamente com um sufixo UPN, como user_name@domain.com.
- Confirme com o administrador se você deverá ou não selecionar a caixa de seleção **Ativar verificação da confiabilidade do SSL** quanto tiver instalado o Data Guardian.
- Entre em contato com o administrador do sistema quanto a configurar o computador para ativar manualmente. Consulte Ativar o Data Guardian.

Ativar o Data Guardian

Tipicamente, o Data Guardian é ativado automaticamente após a instalação e a reinicialização. Se o administrador pedir que você faça a ativação manual, siga estas etapas:

1 Faça login no Windows.

A bandeja do sistema mostra um ícone de blindagem com um ponto de exclamação laranja.

2 Clique no ícone do **Data Guardian** na bandeja do sistema e selecione **Ativação do usuário**.

3 Digite seu endereço de e-mail de domínio e sua senha de domínio e clique em **Ativar**.

Se você for usuário interno (com um endereço de email no domínio), ignore o botão Registrar. Apenas usuários externos precisam se registrar.

Após o término da ativação, uma marca verde é exibida no ícone da bandeja do sistema do Data Guardian  .

4 Confirme seu status de modo de usuário. Clique no ícone da bandeja do sistema do e selecione **Detalhes**.

5 Na parte superior, confirme o modo de usuário:

Interno: um usuário com um endereço de email no domínio da empresa.

Externo: um usuário com um endereço de email fora do domínio da empresa. Para obter mais informações, consulte Uso do Data Guardian como usuário externo.

Tarefas do usuário - Documentos protegidos do Office sem Criptografia na nuvem

O administrador já configurou as políticas do Data Guardian para proteger documentos do Office.

NOTA:
Se sua empresa também gerenciar seu cliente de sincronização de nuvem, consulte Tarefas do usuário - Criptografia na nuvem e Documentos protegidos do Office.

Visão geral das Tarefas

Essa visão geral resume a sequência de instalação e uso do Data Guardian.

Instalar o Data Guardian

Tarefa	Descrição	Para obter mais informações
Instalar o Data Guardian	Determine se: O usuário precisa instalar o Data Guardian Administrador já instalou o Data Guardian - passe para a próxima etapa.	O usuário instala: Consulte Instalar o Data Guardian no Windows. Reinicialize e vá para a próxima etapa.
Confirmar o estado de ativação	Confirme, na bandeja do sistema, se o ícone do Data Guardian tem uma marca de seleção verde  .	Se o ícone tiver um ponto de exclamação laranja, consulte Possíveis problemas com a ativação - Documentos protegidos do Office.

Usar o Data Guardian

Tarefa	Descrição	Para obter mais informações
Ver o menu da bandeja do sistema	Fornece informações úteis sobre arquivos, pastas e solução de problemas.	Entender itens de menu da bandeja do sistema do Data Guardian
Documentos protegidos do Office e habilitados para macro, se a política estiver ativada	Proteja um documento do Office (.docx, .pptx, .xlsx, .docm, .pptm, .xlsm) quando criá-lo. O documento será protegido quando você compartilhá-lo com outros usuários ou armazená-lo em mídia removível.	Usar documentos do Office com o modo protegido do Data Guardian • Observar as opções do menu Arquivo para determinar o nível de segurança para Documentos do Office • Trabalhar com as opções do menu Arquivo
Compartilhar uma pasta com outros usuários para colaborar em arquivos	Compartilhar uma pasta com: Usuário interno (tem um endereço de email no domínio)	Usuário interno - Consulte a ajuda on-line do seu provedor de armazenamento em nuvem. Usuário externo - Consulte Uso do Data Guardian como usuário externo.

Tarefa	Descrição	Para obter mais informações
	Usuário externo (tem um endereço de email fora do domínio) - consulte seu administrador.	

NOTA:
Se você abrir um documento do Office e for exibida uma página de rosto com informações sobre instalação ou ativação, o administrador poderá ter definido políticas para proteger documentos do Office. Confirme se o Data Guardian está instalado e ativado. Consulte Possíveis problemas com a ativação - Documentos protegidos do Office.

Instalar o Data Guardian para documentos protegidos do Office

Instalar o Data Guardian no Windows

Você precisa ser um administrador local do computador para instalar o Data Guardian.

O computador precisa ter disponível uma letra do alfabeto para ser atribuída a uma unidade de disco.

O computador precisará ser reiniciado depois que o Data Guardian for instalado.

1 Para fazer download do instalador do Data Guardian, acesse o local especificado pelo administrador.
2 Com base no sistema operacional, selecione o instalador de 32 bits ou 64 bits, normalmente **setup32.exe** ou **setup64.exe**, e copie-o para o computador local.
3 Clique duas vezes no arquivo para abrir o instalador.
4 Se for mostrado um aviso de segurança, clique em **Executar**.
5 Selecione um idioma e clique em **OK**.
6 Se aparecer uma mensagem perguntando se você quer instalar o Pacote Redistribuível do Microsoft Visual C++ 2010 ou o Microsoft.NET Framework 4.0 Client Profile, clique em **OK**.
7 Na página de boas-vindas, clique em **Avançar**.
8 Leia o contrato de licença, aceite os termos e condições e clique em **Avançar**.
9 Na tela Pasta de destino, clique em **Avançar** para fazer a instalação no local padrão de **C:\Arquivos de Programas\Dell\Dell Data Protection\Dell Data Guardian\.**

   Em **C:**, não instale o Data Guardian nas pastas Usuários ou Windows ou na raiz de qualquer unidade. Você provocará um erro.
10 No campo *Nome do servidor:*, digite o nome do servidor com o qual o computador irá se comunicar, como server.domain.com. Não é necessário incluir www ou http(s). Esse dado é fornecido pelo administrador.

   Não desmarque a caixa de seleção *Ativar verificação da confiabilidade do SSL*, a menos que seu administrador instrua que você o faça.
11 Clique em **Avançar**.
12 Na tela Confirmar informações do servidor de ativação, verifique se o endereço URL do servidor está correto. O instalador acrescenta www ou http(s) e a porta. Clique em **Avançar**.
13 Na janela Tipo de gerenciamento, selecione a opção:
   - Uso interno – Um usuário com endereço de e-mail no domínio da empresa.
14 Clique em **Instalar** para iniciar a instalação.

   Uma janela de status mostra o andamento da instalação.
15 Clique em **Concluir** quando a tela Instalação concluída for exibida.
16 Clique em **Sim** para reiniciar.

   A instalação doData Guardian está concluída.
17 Após a reinicialização, confirme, na bandeja do sistema, se o ícone do Data Guardian tem uma marca de seleção verde  .

Usar documentos do Office com o modo protegido do Data Guardian

Para melhorar a segurança da empresa, o administrador pode ativar uma política para proteger arquivos para os seguintes aplicativos do Office:

- .docx, .pptx, .xlsx
- .docm, .pptm, .xlsm

Se uma pessoa não autorizada acessar um arquivo protegido, o arquivo permanecerá criptografado, por exemplo quando você:

- Anexá-lo a um email
- Movê-lo em um navegador - em alguns clientes de sincronização de nuvem, é possível clicar com o botão direito do mouse em um nome de arquivo e selecionar **Mover**.
- Compartilhá-lo na rede
- Fazer upload do arquivo em um provedor de armazenamento em nuvem
- Armazená-lo em mídia removível

Em documentos do Office, pode ser exibida uma página de rosto com instruções para instalação ou ativação do Data Guardian, por exemplo:

- Você precisa instalar o Data Guardian.
- Você precisa ativar o Data Guardian.
- Você abre um documento protegido do Office na nuvem.
- Você fez download de um arquivo do Office do computador que tem o Data Guardian para um dispositivo pessoal que não tem o aplicativo.
- Um usuário não autorizado acessa um dos seus arquivos do Office - a página de rosto é exibida com uma mensagem específica para a empresa, mas o usuário não consegue ver o conteúdo do arquivo.

Se sua empresa usar o modo protegido do Data Guardian, observe o seguinte:

- Observar as opções do menu Arquivo para determinar o nível de segurança para Documentos do Office
- Trabalhar com as opções do menu Arquivo
- Determinar que documentos do modo Aceitar estão protegidos
- Opções de menu adicionais para documentos protegidos do Office
- Usuários externos e documentos protegidos do Office

Observar as opções do menu Arquivo para determinar o nível de segurança para Documentos do Office

Para determinar se o administrador ativou as políticas do Data Guardian, abra um documento do Office e selecione **Arquivo**. Se for exibido *Salvar como protegido* no painel esquerdo, você tem proteção adicional nos documentos do Office.

Para determinar o nível de segurança, observe as opções que estão ativadas ou desativadas:

- **Modo Aceitar** - Você tem algumas opções para determinar que documentos do Office serão protegidos.
  - *Salvar e Salvar como protegido estão ativados* - Se você optar por proteger um documento do Office, selecione **Salvar como protegido**.
  - *Imprimir* e *Exportar* podem estar ativados ou desativados, dependendo da política.
  - *Compartilhar* (*Salvar e Enviar* para o Office 2010) está ativado.
  - Pasta **Documentos > Documentos protegidos** - No modo Aceitar (mas não no modo Forçar protegido) - uma pasta de Documentos protegidos é adicionada à raiz da pasta Documentos. Os documentos do Office nessa pasta estão criptografadas. Se

você remover um documento protegido do Office dessa pasta, ele permanecerá criptografado. Se você renomear a pasta, o conteúdo da pasta renomeada estará criptografado. Se você apagar a pasta, ela será recriada.

- **Modo Forçar protegido** - sua empresa precisa de um nível mais alto de segurança.
  - *Salvar como* está desativado e *Salvar como protegido* está ativado - Você precisa salvar todos os documentos do Office no modo protegido.
  - *Imprimir* e *Exportar* podem estar ativados ou desativados, com base na política.
  - *Compartilhar* (*Salvar e Enviar* para o Office 2010) está desativado.

    NOTA:
    Com o modo Force-Protected, a política também ativa horários específicos para verificar seu computador e localizar arquivos desprotegidos do Office, e alterá-los para o modo Protegido. Você precisa estar conectado à rede para que o Data Guardian verifique todos os arquivos do Office desprotegidos.

- Se você selecionar **Salvar como protegido**, a única opção do campo *Salvar como tipo* será *Protegido do Office*.

- **Arquivo > Info** é diferente, por exemplo:
  - Para os modos Aceitar e Forçar protegido: é exibido *Adicionar restrição de data* caso o administrador tenha ativado esta política. Consulte Melhorar a segurança ao *Adicionar restrição de data*.
  - Para os modos Aceitar e Forçar protegido: as informações sobre propriedades relativas a esse documento do Office, como autor e data, estão ocultas para maior segurança.
  - Status somente leitura: consulte a seguir para obter mais informações.

    NOTA:
    A opção *Proteger documento* em Arquivo > Info está relacionada ao Microsoft Office e não ao modo protegido do Data Guardian.

Se você abrir um documento do Office e ele indicar modo somente leitura, verifique o seguinte:

- Se *Salvar como protegido* não for exibido no painel esquerdo, o modo somente leitura não estará relacionado às políticas doData Guardian.
- Se o administrador definir políticas para o modo Forçar protegido com um nível de segurança mais alto, documentos desprotegidos do Office abrirão no modo somente leitura.

  NOTA:
  Para OneDrive, se você abrir um documento protegido do Office por meio de **Arquivo > Abrir > OneDrive** e o documento for somente leitura, confirme se você instalou e configurou o cliente de sincronização do OneDrive.

Trabalhar com as opções do menu Arquivo

Esta tabela lista as opções do menu Arquivo para documentos do Office. Dependendo do nível de segurança, algumas opções são esmaecidas.

NOTA:
Atualmente, documentos integrados do Office não são suportados pelo modo Documentos protegidos do Office.

Menu Arquivo	Modo Aceitar e documentos protegidos do Office	Modo Forçar protegido para documentos protegidos e desprotegidos
Abra	**Os arquivos abrem normalmente**	**Documentos desprotegidos abertos no modo somente leitura.**
Salvar	• Opções: Documento já protegido - Salva como protegido. Desprotegido - Salva como desprotegido. Para protegê-lo, clique em **Salvar como protegido**. • Documento somente leitura - Uma caixa de diálogo indica que não é possível salvar um documento desprotegido. A janela Salvar como é exibida e é preciso salvá-lo com outro nome de arquivo. • Arquivo xen - Você pode abri-lo e salvá-lo no modo protegido, mas o arquivo .xen é removido da nuvem. O documento do Office tem sua extensão usual, mas está protegido. **NOTA:** **Na unidade virtual, se o usuário clicar com o botão direito do mouse para criar um novo documento do Office, ele será um arquivo .xen. Você precisa salvá-lo manualmente como protegido.**	• O documento está protegido. • Documento somente leitura - Você pode editá-lo, mas não poderá salvar o original. Quando você clicar em Salvar, a janela Salvar como protegido será exibida e você precisará salvar o documento no modo protegido com um novo nome. • Documentos remotos - Se você abrir um documento em um local remoto e ele não estiver protegido, precisará salvá-lo na unidade local para modificar e salvar. Você não pode salvar o documento no local remoto. **NOTA:** **Clicar em Salvar abre a janela Salvar como, e a única opção no campo Salvar como tipo é Protegido do Office (documentos, apresentação, ou pasta de trabalho).** • Arquivo xen - Você pode abri-lo e salvá-lo no modo protegido, mas o arquivo .xen é removido da nuvem. O documento do Office tem sua extensão usual, mas está protegido.
Salvar como	**Tem as opções padrão (mas não o modo protegido)**	**Desativado**
Salvar de forma protegida como	**A única opção no campo Salvar como tipo é Protegido do Office**	**A única opção no campo Salvar como tipo é Protegido do Office**
Imprimir	**Pode estar ativado ou esmaecido com base nas políticas definidas pelo administrador. Se a opção de menu estiver ativada, uma política poderá colocar uma marca d'água contendo nome de usuário, nome de domínio e ID do computador em cada página que você imprimir.**	**Dependendo da política, essa opção poderá estar ativada ou esmaecida.** **Se a opção de menu estiver ativada, uma política poderá colocar uma marca d'água contendo nome de usuário, nome de domínio e ID do computador em cada página que você imprimir.**
Compartilhar	**Ativado**	**Desativado**
Salvar e enviar (Office 2010)	**Ativado**	**Desativado** **Se a opção Imprimir estiver ativada, você poderá selecionar Imprimir para imprimir o documento como PDF.**
Exportar (Office 2013 e superior)	**Pode estar ativado ou esmaecido com base nas políticas definidas pelo administrador.**	**Pode estar ativado ou esmaecido com base nas políticas definidas pelo administrador.**
Exportação protegida (Office 2013 e superior)	Se a opção de menu Exportar estiver esmaecida e Exportação protegida estiver ativada, o documento exportará com uma marca d'água, contendo nome de usuário, nome de domínio e ID do computador em cada página. **NOTA:** Se você exportar um documento no modo protegido para um usuário externo, ele poderá abrir e ver o documento, mas não poderá exportar ou imprimi-lo.	Se a opção de menu Exportar estiver esmaecida e Exportação protegida estiver ativada, o documento exportará com uma marca d'água, contendo nome de usuário, nome de domínio e ID do computador em cada página. **NOTA:** Se você exportar um documento no modo protegido para um usuário externo, ele poderá abrir e ver o documento, mas não poderá exportar ou imprimi-lo.

Trabalhar online com documentos protegidos do Office

Ao criar documentos protegidos do Office, recomenda-se trabalhar online, pois são geradas chaves para esses documentos. Se tiver sido necessário recriar a imagem do seu computador e você tiver criado documentos protegidos do Office offline, informe o administrador.

Trabalhar online com documentos protegidos habilitados para macro

Com um documento protegido habilitado para macro, a macro existe, mas está bloqueada. No entanto, atualmente, o Data Guardian só pode controlar um documento habilitado para macro depois que o documento recém-protegido (.docm, .pptm, .xlsm) seja fechado e reaberto. Além disso, se você salvar um documento protegido com uma macro como desprotegido, precisará fechar e reabrir a documento, para que a macro seja executada.

Anexar um documento protegido do Office a um email do Outlook

Ao anexar um documento protegido do Office a um email do Outlook, selecione **Inserir** em vez de *inserir como texto*. *Inserir como texto* cola o conteúdo do documento diretamente no corpo do email e o conteúdo não estará mais protegido.

Solução de problemas para o modo Aceitar

Em Arquivo > Info, se sua opção Imprimir está esmaecida, significa que uma política do Data Guardian desativou a impressão de documentos protegidos do Office. No entanto, atualmente, quando você clica com o botão direito do mouse em uma arquivo protegido do Office no Windows Explorer, a opção de Imprimir não está esmaecida. Porém, se você selecionar Imprimir, ocorrerá o seguinte:

- Word - Uma caixa de diálogo indica que o Word parou de funcionar.
- Excel - Uma caixa de diálogo indica que a opção Imprimir está desativada por uma política.
- PowerPoint - Uma caixa de diálogo indica que a opção Imprimir está desativada por uma política. Se você clicar em OK, uma página de rosto será impressa, informando que o documento está protegido.

Determinar que documentos do modo Aceitar estão protegidos

Se você tiver o modo Forçar protegido, todos os documentos do Office estarão protegidos. Se você tiver o modo Aceitar e quiser confirmar se um documento está protegido ou não, abra o documento e a barra de título o mostrará como protegido.

Opções de menu adicionais para documentos protegidos do Office

O tipo de documento do Office, protegido ou desprotegido, pode afetar o seguinte.

Clicar com o botão direito do mouse > Proteger

Você pode clicar com o botão direito do mouse em um documento do Office e selecionar **Proteger**. Você precisa adicionar conteúdo para que a opção de menu seja exibida. Você não pode proteger um documento em branco.

Guia Propriedades do arquivo > Dell Data Guardian

Com documentos protegidos do Office, clique com o botão direito do mouse e selecione **Propriedades**; a guia **Dell Data Guardian** será exibida com informações, como a identificação da chave do arquivo e dados de acesso e embargo.

Colar

Se o administrador definir uma política para proteger documentos do Office:

- Você poderá copiar e colar dados no documento protegido original.
- Você não poderá copiar ou colar de um documento protegido para um documento desprotegido. Nada será mostrado na área de transferência, e uma mensagem de texto específica para a empresa informará que não é possível colar no documento desprotegido ou não gerenciado.

> **NOTA:**
> Se você cortar texto de um documento protegido e receber a mensagem em um documento desprotegido, clique em **Desfazer** no documento protegido para recuperar o texto.

Arrastar e soltar no modo protegido

Você pode arrastar e soltar conteúdo em um documento protegido do Word. Atualmente, a opção arrastar e soltar está desativada para arquivos protegidos do PowerPoint e do Excel.

Impressão de envelopes e etiquetas

Se o administrador tiver definido uma política para adicionar uma marca d'água quando você imprimir um documento protegido do Office, siga estas etapas para imprimir envelopes ou etiquetas:

1 Em um documento do Word, selecione a guia **Correspondências**.
2 Selecione a opção **Envelopes** ou **Etiquetas**.
3 Depois que você digitar o endereço ou o endereço do remetente, clique em **Imprimir**.

> **NOTA: Se você usar outra opção para imprimir e o administrador definir uma política para adicionar uma marca d'água para documentos impressos do Office, será exibida uma marca d'água no envelope ou na etiqueta.**

Documentos Office protegidos e adulterados

O Data Guardian pode analisar documentos protegidos do Office para detectar algumas formas de adulteração.

Se um usuário interno adulterar um documento protegido do Office:

- O Data Guardian poderá reparar ou restaurar parte da adulteração.
- Para a adulteração que não puder ser reparada, uma caixa de diálogo será exibida informando que o arquivo foi adulterado e solicitando que você entre em contato com o administrador.

Se um usuário não autorizado abrir um documento protegido do Office, apenas a página de rosto será exibida. Se o usuário não autorizado modificar a página de rosto, o Data Guardian restaurará a página de rosto quando um usuário autorizado salvar novamente o documento como protegido.

Usuários externos e documentos protegidos do Office

Melhorar a segurança ao adicionar restrições de data

Com o Data Guardian, faça upload de um documento protegido do Office para a nuvem e compartilhe-o:

- Todos os usuários internos do Data Guardian poderão vê-lo.
- Com base na política, os usuários externos poderão vê-lo.

Opcionalmente, para a segurança aprimorada com os usuários externos, você pode adicionar uma restrição de data para limitar o tempo em que um usuário externo pode ver uma documento protegido do Office.

1 Selecione **Arquivo > Info > Restringir data**.
2 Na lista suspensa, selecione uma Data de início e uma Data de término e a hora para um usuário externo ver o documento.

> **NOTA:**
> A data de início e a hora poderão estar no futuro se você quiser enviar o documento, mas impeça que o usuário externo o veja até a data e a hora determinadas.

3 Clique em **OK**.
O documento será salvo, protegido, fechado e, em seguida, reaberto.

NOTA:
Se você modificar as datas para um documento desprotegido do Office e, em seguida, clicar em Cancelar, o Data Guardian ainda protegerá o arquivo.

NOTA:
Atualmente, ao adicionar restrições de data a um documento protegido do Office e planejar salvá-lo em uma unidade de rede, será preciso salvar o arquivo localmente e, em seguida, copiá-lo para a rede.

Se um usuário externo abrir um arquivo depois do intervalo de data e hora, uma caixa de diálogo informará que o arquivo tem restrições de acesso e que o usuário do arquivo poderá entrar em contato com o autor do arquivo. A caixa de diálogo não exibirá qualquer data para o usuário externo.

Se você definir o campo Data de início para uma data ou hora futura e o usuário externo abrir o arquivo antes dessa hora, uma caixa de diálogo será exibida indicando que o arquivo não poderá ser aberto antes da data e da hora determinadas devido a restrições de acesso.

Entender itens de menu da bandeja do sistema do Data Guardian

Tela de detalhes

A tela Detalhes do Data Guardian fornece informações úteis; por exemplo:

- Para obter suporte técnico, você pode fornecer informações de status ou de versão.
- Para visualizar um nome de arquivo não obscurecido que está associado a um arquivo .xen, selecione **Arquivos** > **Estado do arquivo**.
- Para procurar por um nome de arquivo, selecione a opção Copiar no canto inferior direito e cole o conteúdo em um arquivo Word.
- Para ver quem é o proprietário de uma pasta, selecione Pastase role até à coluna PROPRIEDADE DE PASTA.

Para ter acesso à tela Detalhes:

Clique no ícone da bandeja de sistema do **Data Guardian** e, a seguir, clique em **Detalhes...**

O canto superior esquerdo da tela Detalhes mostra as seguintes informações:

Status do serviço: status do Serviço Windows do Data Guardian. Os valores são: Interrompido, IniciarPendente, PararPendente, Em execução, ContinuarPendente, PausarPendente, Pausado

Estado de execução: o status de ativação do dispositivo. Os valores são: Ativo, Reativando, Suspenso, Suspendendo

Modo de usuário: usuário interno - um usuário dentro desse endereço de domínio

Usuário externo - usuário fora desse endereço de domínio

Email de registro: para usuários internos, este é o endereço de email de domínio. Para usuários externos, este é o endereço de e-mail para o qual os usuários estão registrados.

URL do servidor: o DDP EE Server/VE Server que se comunica com esse cliente.

Data da última modificação da política: data e carimbo de data/hora em que a política foi modificada pela última vez e consumida pelo cliente.

Versão da política: versão da política gerada pelo DDP EE Server/VE Server.

A área **Arquivos** da tela Detalhes exibe as seguintes informações:

Nome: nome do arquivo

Nuvem: mostra em uma lista o nome de arquivo ofuscado ou se o arquivo está *Desprotegido*.

Estado do arquivo: esse valor indica o proprietário da pasta. O valor é determinado pela ID da chave.

Estado do processamento: mostra se o arquivo precisa de uma chave ou se está *Concluído*.

Empresa: mostra o servidor padrão. Se for mostrada uma mensagem nessa coluna, *Erro: a chave não é do seu servidor*, a chave não pertence ao servidor da sua empresa. A chave de um arquivo criptografado precisa pertencer ao servidor da empresa.

Chave: identificação da chave atribuída a essa pasta (os arquivos novos usam essa chave para criptografia).

Pasta: nome do caminho completo da pasta.

Data da última modificação: data na qual o arquivo foi modificado.

Estado de persistência: indica se o arquivo está no disco.

Leitura de arquivo XEN: *Verdadeiro* ou *Falso.*

Criado pelo navegador: *Verdadeiro* ou *Falso*.

Para ver arquivos de registro, clique em **Ver registro** no canto inferior esquerdo da tela.

NOTA:
Os arquivos de registro podem ser encontrados também em **C:\ProgramData\Dell\Dell Data Protection\Dell Data Guardian.**

A área **Pastas** da tela Detalhes exibe as seguintes informações:

Nome: nome da pasta

Chave: identificação da chave atribuída a essa pasta (os arquivos novos usam essa chave para criptografia).

Cliente de sincronização: o último cliente de sincronização a sincronizar essa pasta (Clientes de sincronização de nuvem.)

Propriedade da pasta: esse valor indica o proprietário da pasta. O valor é determinado pela ID da chave.

Anular: as opções são *Nenhum* e *Preexistente.* Os arquivos preexistentes não são protegidos. Além disso, se você tiver acesso ao Gerenciamento de pastas e tiver alguns arquivos desprotegidos, essa coluna indica que eles não estão protegidos.

Tipo de Ofuscação: se sua empresa gerencia seu armazenamento em nuvem, essa é a política definida em cada pasta indicando que tipos de arquivos .xen serão criados na nuvem. Essa é uma política definida pelo administrador. Se o administrador selecionar *Somente extensão*, será exibido o nome real do arquivo com a extensão ".xen". Se o administrador selecionar *Guid*, será exibido um nome de arquivo misturado com a extensão ".xen". Essa é uma definição de política aplicada apenas em pastas novas. O padrão é *Extensão apenas*.

Menu de Gerenciar pastas

Alguns gerentes ou administradores podem temporariamente precisar solucionar problemas em pastas compartilhadas por mais de um usuário. Você pode solicitar permissão do seu administrador para a opção Gerenciar pastas. Normalmente, essa é uma opção temporária.

Localizar arquivos de log

Para solução de problemas, talvez o administrador solicite os arquivos de registro.

Para localizar os arquivos de log:

1 Navegue até
2 Selecione **Xendow.Service.log**.

NOTA:
Após o Xendow.Service.log atingir 3 MB, ele será salvo como Xendow.Service1.log e, depois, Xendow.Service2.log.

Verificar atualizações de política

Se o administrador modificar uma política e notificá-lo sobre uma atualização da política, acesse a bandeja do sistema, clique no ícone **Dell Data Protection | Data Guardian** e selecione **Verificar atualizações de política**.

Se o administrador modificar uma política para proteger arquivos criados no Microsoft Word, você precisará fechar o Word para que a atualização seja aplicada.

Atualizar o Data Guardian

A prática recomendada é desinstalar as versões anteriores e, em seguida, instalar a versão atual. Consulte Desinstalar o Data Guardian.

Fornecer feedback à Dell

Se seu administrador tiver habilitado uma política de feedback, você poderá fornecer feedback à Dell sobre este produto. O pequeno formulário contém duas perguntas sobre o seu nível de satisfação, com escalas de classificação (onde 10 indica o mais alto nível de satisfação) e um campo de comentário.

Para acessar o formulário, clique no ícone do Data Guardian na bandeja do sistema e selecione **Enviar feedback**.

Se esse recurso não for ativado por política, essa opção não será mostrada.

Possíveis problemas com a ativação - Documentos protegidos do Office

Se você tiver instalado o Data Guardian, mas o ícone do Data Guardian na bandeja do sistema não tiver uma marca de seleção verde,  , lembre-se do seguinte:

- O Data Guardian pode converter documentos existentes do Office para o modo protegido antes de serem ativados. Nesse caso, quando você abrir um documento do Office, uma página de rosto exibirá informações sobre como ativar.

Execute um destes processos:

- Reinicialize e faça login novamente com um sufixo UPN, como user_name@domain.com.
- Confirme com o administrador se você deverá ou não selecionar a caixa de seleção **Ativar verificação da confiabilidade do SSL** quanto tiver instalado o Data Guardian.
- Entre em contato com o administrador do sistema quanto a configurar o computador para ativar manualmente. Consulte Ativar o Data Guardian.

Ativar o Data Guardian

Tipicamente, o Data Guardian é ativado automaticamente após a instalação e a reinicialização. Se o administrador pedir que você faça a ativação manual, siga estas etapas:

1 Faça login no Windows.
A bandeja do sistema mostra um ícone de blindagem com um ponto de exclamação laranja.
2 Clique no ícone do **Data Guardian** na bandeja do sistema e selecione **Ativação do usuário**.

3 Digite seu endereço de e-mail de domínio e sua senha de domínio e clique em **Ativar**.

Se você for usuário interno (com um endereço de email no domínio), ignore o botão Registrar. Apenas usuários externos precisam se registrar.

Após o término da ativação, uma marca verde é exibida no ícone da bandeja do sistema do Data Guardian  .

4 Confirme seu status de modo de usuário. Clique no ícone da bandeja do sistema do e selecione **Detalhes**.

5 Na parte superior, confirme o modo de usuário:

Interno: um usuário com um endereço de email no domínio da empresa.

Externo: um usuário com um endereço de email fora do domínio da empresa. Para obter mais informações, consulte Uso do Data Guardian como usuário externo.

Uso do Data Guardian Mobile com iOS ou Android

Esta seção descreve informações básicas sobre como usar o Data Guardian Mobile com dispositivos iOS ou Android. Quando o administrador define uma política para ativar o Data Guardian, os arquivos ficam criptografados e protegidos na nuvem. No entanto, você pode usar o aplicativo Data Guardian Mobile para vê-los no seu dispositivo móvel.

Pré-requisito

Antes de usar o aplicativo Data Guardian, você precisará do nome do Dell Data Protection Server da sua empresa, como server.domain.com. Esse dado é fornecido pelo administrador.

Introdução ao Data Guardian Mobile

Siga esta sequência quando usar o Data Guardian Mobile.

Tarefa	Descrição	Veja esta seção
Instalar o Data Guardian	Determine se: O administrador já instalou O usuário precisa instalar	Instalado pelo administrador: toque no aplicativo Data Guardian e faça login. O usuário instala: veja uma destas opções: Instalar em um dispositivo iOS Instalar em um dispositivo Android
Acessar sua conta no provedor de armazenamento em nuvem	No dispositivo, vá para a página inicial do aplicativo Data Guardian e toque no seu provedor de armazenamento em nuvem.	Veja uma dessas opções: Acessar sua conta do Provedor de armazenamento em nuvem para IOS Acessar sua conta do Provedor de armazenamento em nuvem para Android

O aplicativo Data Guardian Mobile lista o cliente de sincronização de nuvem usado na sua empresa e permite que você faça download do mesmo.

NOTA:
Se você fizer download do aplicativo do cliente de sincronização de nuvem para seu dispositivo, o Data Guardian não criptografará qualquer pasta ou arquivo obtidos por upload diretamente deste aplicativo. Para criptografar e proteger arquivos, você precisará usar o aplicativo Data Guardian para fazer upload.

Para proteger seus dados na nuvem, eles serão criptografados pelo Data Guardian. Portanto, é preciso que o aplicativo Data Guardian seja instalado no seu dispositivo móvel para ver arquivos criptografados.

- Arquivos protegidos do Office files (.docx, .pptx, .xlsx) mantêm sua extensão.
- Os arquivos não Office na nuvem têm a extensão .xen.

Se uma pessoa não autorizada acessar sua conta de armazenamento em nuvem e fizer download de um arquivo para um dispositivo móvel que **não** tenha o Data Guardian instalado, a pessoa não poderá abrir ou ver seus arquivos. Se essa pessoa abrir um arquivo protegido do

Office, será exibida somente uma página de rosto indicando que a pessoa não poderá ver o documento sem o Data Guardian. Isso torna seus dados mais seguros.

Em dispositivos móveis, você pode:

- Criar pastas
- Fazer upload e download de arquivos

  NOTA:
  Com o Data Guardian, você precisará iniciar o upload e o download no dispositivo. Para que os arquivos sejam criptografados quando forem transferidos por upload para a nuvem, você precisará fazer o upload a partir da página inicial do Data Guardian e não de um aplicativo de cliente de sincronização de nuvem. Quando você tocar em um arquivo, o Data Guardian automaticamente o descriptografará e o exibirá em texto não criptografado dentro do aplicativo. Entretanto, na nuvem, o arquivo permanece seguro como um arquivo .xen.

- Adicionar um arquivo aos Favoritos
  - No iOS, use a gaveta de navegação. No Android, mantenha pressionado o nome do arquivo.
- Apagar pastas e arquivos
- Aceitar uma pasta compartilhada de um usuário interno

  NOTA:
  Se um usuário interno compartilhar uma pasta com você através do Data Guardian, você deverá ir para o site de armazenamento em nuvem e movê-la para a pasta raiz ou fazer download da pasta compartilhada para vê-la no dispositivo.

- Compartilhar um documento com um usuário externo (se a política estiver ativada para visualizadores externos) - Para iOS, consulte Ver as políticas de Armazenamento em nuvem do Data Guardian para seu dispositivo iOS.
- Editar arquivos .docx e .ppt do Office.

  NOTA:
  Atualmente, arquivos .csv e .csv.xen não podem ser editadas em dispositivos móveis.

Documentos protegidos do Office quando estiver offline

Quando você criar um documento protegido do Office ou um documento protegido habilitado para macro e estiver offline, será criada uma chave para este documento. Quando o dispositivo entrar online, será feito o upload das chaves para o Dell Server. Se um dispositivo ficar offline por três dias, uma notificação informará que o Data Guardian não conseguiu entrar em contato com o Dell Server. A notificação será exibida diariamente até que você se conecte à rede. Para ver os arquivos criptografados, o dispositivo móvel deverá estar online.

Proteção adicional por Cerca geográfica

Com base nas políticas definidas pelo administrador, dispositivos móveis podem ter proteção adicional tal que documentos protegidos do Office e arquivos .xen não possam ser abertos fora de uma região específica. Você precisa estar em uma região aprovada para abrir arquivos protegidos. Atualmente, as regiões são os Estados Unidos e Canadá. Você precisa ativar os serviços de localização no dispositivo para que a cerca geográfica funcione. Se o recurso de cerca geográfica estiver ativado pelo administrador e os serviços de localização forem definidos como Desligado, o acesso aos arquivos será negado.

Usar um PIN

O administrador poderá definir uma política que exija um PIN.

Data Guardian em um dispositivo IOS

Instalar em um dispositivo iOS

1 No seu dispositivo, toque em App Store e procure por **Data Guardian Mobile**.
2 Selecione e instale o aplicativo **Data Guardian**.

3 Para o campo Servidor na tela de login, digite o nome do host do Dell Data Protection Server da sua empresa, como server.domain.com.

4 Digite o nome de usuário e a senha.

5 Toque em **Login**.

Acessar sua conta do Provedor de armazenamento em nuvem para IOS

Após fazer login no Data Guardian, uma política do Data Guardian determina quais provedores de armazenamento em nuvem são exibidos na tela inicial. Seu administrador talvez determine um provedor de armazenamento em nuvem específico para uso na empresa.

A gaveta de navegação tem opções adicionais.

Para acessar uma conta:

1 Na página inicial do Data Guardian, toque no provedor de armazenamento em nuvem.

2 Execute uma das seguintes ações seguindo as instruções on-line:

- Crie uma conta no provedor de armazenamento em nuvem.
- Faça login em uma conta existente do provedor de armazenamento em nuvem.

> **NOTA:**
> Para obter mais informações, consulte a ajuda do provedor de armazenamento em nuvem.

Desvincular um provedor de armazenamento em nuvem

Se você tiver mais de uma conta no mesmo provedor de armazenamento em nuvem, você não poderá se conectar nas duas simultaneamente. Será necessário desmarcar a caixa de seleção para desvincular e encerrar a sessão da conta atual e, em seguida, fazer login com as outras credenciais.

1 Abra a gaveta de navegação do Data Guardian e toque em **Configurações**.

2 Toque em **Desvincular**.

Ver as políticas de Armazenamento em nuvem do Data Guardian para seu dispositivo IOS

1 Na gaveta de navegação do Data Guardian, toque em **Configurações**.

2 Toque em **Política**.

A lista pode conter:

- Revisão - o número de políticas revisadas
- Obscurecer nomes de arquivos - por padrão, configurado como **Não**
- Cliente de sincronização de nuvem - a política deve ser configurada para **Criptografar**
- Visualizadores externos - se configurado como **Sim**, a política de compartilhamento estará ativada. Quando você abre um documento no aplicativo, uma opção do menu permite que você compartilhe o arquivo.

Desinstalar o aplicativo Data Guardian

1 Na gaveta Aplicativos iOS, toque e segure o ícone do Data Guardian.

2 Toque em **x**.

3 Toque em **Excluir**.

Solução de problemas do iOS e do Data Guardian

Em um dispositivo iOS, se você abrir um documento protegido do Office maior do que 25 MB e for exibida uma caixa de diálogo indicando baixa memória, a advertência será proveniente do Polaris Office, não do Data Guardian. Se o dispositivo tiver memória suficiente, feche o arquivo e abra-o novamente.

Com o Dropbox for Business, se você marcar um arquivo como disponível offline e depois renomeá-lo no site do Dropbox, o arquivo não abrirá no dispositivo iOS com o aplicativo Data Guardian.

Data Guardian em um dispositivo Android

Instalar em um dispositivo Android

1 No seu dispositivo, toque em **Google Play** e procure por **Data Guardian Mobile**.
2 Selecione e instale o aplicativo **Data Guardian**.
3 Para o campo Servidor na tela de login, digite o nome do servidor do Dell Data Protection da sua empresa, como server.domain.com.
4 Digite o nome de usuário e a senha.
5 Toque em **Login**.

Sua conta agora está ativa.

Acessar sua conta do Provedor de armazenamento em nuvem para Android

Após fazer login no Data Guardian, uma política do Data Guardian determina quais provedores de armazenamento em nuvem são exibidos. Seu administrador talvez determine um provedor de armazenamento em nuvem específico para uso na empresa e bloqueie os demais.

Para acessar uma conta:

1 Na página inicial do Data Guardian, toque no provedor de armazenamento em nuvem.
2 Execute uma das seguintes ações seguindo as telas on-line:
   - Crie uma conta no provedor de armazenamento em nuvem.
   - Faça login em uma conta existente do provedor de armazenamento em nuvem.

   NOTA:
   Para obter mais informações, consulte a ajuda do provedor de armazenamento em nuvem.
3 Depois de acessar sua conta, abra a gaveta de navegação e toque em **Configurações.** Quando o acesso a um provedor de armazenamento em nuvem for concedido a você, uma marca de seleção será mostrada na caixa de seleção.

NOTA:
Se você tiver mais de uma conta no mesmo provedor de armazenamento em nuvem, você não poderá se conectar nas duas simultaneamente. Será necessário desmarcar a caixa de seleção para desvincular e encerrar a sessão da conta atual e, em seguida, fazer login com as outras credenciais.

NOTA:
No OneDrive e no Dropbox, se não for possível compartilhar um arquivo de Aplicativos e o arquivo compartilhar um link com o aplicativo Data Guardian, compartilhe o arquivo a partir do aplicativo Navegador de arquivos do dispositivo.

Desinstalar o aplicativo Data Guardian

1 Na gaveta de aplicativos do Android, toque em **Configurações**.
2 Em **Configurações**, toque em **Aplicativos**.
3 Pressione o ícone do **Data Guardian**.
4 Arraste o ícone para a opção Desinstalar.
5 Clique em **OK**.

Considerações de segurança com o Data Guardian e clientes de sincronização

O Data Guardian criptografa pastas e arquivos para tornar os dados protegidos. Como o Data Guardian funciona com clientes de sincronização, leve em conta as considerações a seguir.

Google Drive

O Google Drive contém um aplicativo Google Docs que permite aos usuários colaborar em documentos em tempo real. Entretanto, a colaboração ocorre em um servidor do Google, não no Dell Data Protection EE Server/VE Server. Portanto, esses arquivos não são criptografados. Para dispositivos Android e iOS com o Data Guardian, o acesso a esses documentos do Google está bloqueado. É um pouco diferente em cada plataforma:

- Android
- iOS - Uma mensagem é mostrada.

OneDrive e OneDrive for Business

No OneDrive for Business, se, após iniciar o download de vários arquivos, você cancelar o download, o OneDrive for Business cancelará o download dos arquivos que ainda não foram baixados, mas continuará o download do arquivo em processamento. Esse é um problema da Microsoft. Por isso, espere terminar o download dos arquivos antes de cancelar.

Logs

Por motivos de segurança, não há arquivos de log disponíveis em dispositivos móveis.

Enviar feedback à Dell

Se seu administrador tiver habilitado uma política de feedback, você poderá fornecer feedback à Dell sobre este produto. Se esse recurso não for ativado por política, essa opção não será mostrada.

Para enviar feedback:

1 Na gaveta de navegação do Data Guardian, toque em **Feedback**.
2 Algumas perguntas breves permitirão que você classifique o seu nível de satisfação (10 indica o mais alto nível de satisfação) e faça um comentário.

Uso do Data Guardian como Usuário externo

Um usuário externo com um endereço de e-mail fora do domínio também pode usar o Data Guardian. Veja alguns exemplos:

- Você instalou e ativou o Data Guardian. na sua empresa, mas precisa compartilhar arquivos protegidos ou usá-los de forma colaborativa com um usuário fora da empresa.
- O endereço de email da sua empresa está dentro do domínio da empresa, mas você também quer instalar e ativar o Data Guardian. em um computador ou dispositivo móvel com seu endereço de email pessoal fora do domínio. Esse procedimento permite que você interaja com os arquivos protegidos usando um endereço de email fora do domínio da empresa.

Para usuários externos, consulte Requisitos de servidor. Além disso, o domínio ou o usuário não pode estar na lista negra da empresa.

NOTA:
Os usuários externos que tiverem sido registrados com o Secure Lifecycle 1.0 ou superior serão migrados se a empresa fizer a atualização.

Tarefas do usuário interno

Para compartilhar arquivos protegidos com um usuário externo, você pode enviar um documento protegido do Office ou um arquivo .xen por meio de um email do Outlook. Um aviso de confirmação lembra a você que a chave do arquivo protegido será compartilhada.

NOTA:
Se um usuário externo enviar um arquivo protegido por email, as chaves não serão compartilhadas.

Você também pode usar a opção Conceder acesso para compartilhar arquivos protegidos com um usuário externo. Você precisará:

- Disponibilize um ou mais arquivos protegidos para o usuário externo.
  - Documentos protegidos do Office - Conceda acesso a um ou mais arquivos protegido usando:
    - Pasta local ou unidade de rede
    - E-mail
    - Mídia removível
    - Compartilhamento de rede
  - Arquivos .xen não Office - Crie uma pasta para compartilhar no cliente de sincronização e adicione arquivos.
- Conceda ao usuário externo acesso a um ou mais arquivos.

Se você pretende compartilhar arquivos .xen não Office, precisa adicioná-los a uma pasta de cliente de sincronização e, em seguida, conceder o acesso. Para arquivos protegidos do Office, você precisa conceder acesso. As etapas podem variar, dependendo do método que você usar ou do cliente de sincronização usado.

Compartilhar uma pasta no cliente de sincronização para compartilhar arquivos .xen

1 No Windows Explorer, acesse seu cliente de sincronização, crie uma pasta e faça upload de um arquivo para compartilhá-lo com um usuário externo. Consulte Ver pastas e arquivos no computador local e na nuvem.

Documentos protegidos do Office podem estar na DDG VDisk virtual drive, na pasta do Data Guardian ou na área de trabalho.

NOTA:
Com arquivos protegidos do Office, você não pode selecionar uma pasta.

É aberta a página *Compartilhamento de acesso a documentos protegidos* com uma coluna que exibe os arquivos selecionados.

2 No site do cliente de sincronização, confirme que a pasta e o arquivo foram criados e criptografados.

Quando você adiciona um arquivo .xen a uma nova pasta na DDG VDisk virtual drive, o Data Guardian adiciona um documento, *Como acessar arquivos protegidos.html*, à pasta no site. Esse arquivo é usado apenas quando uma pasta é compartilhada com um usuário externo.

3 No site do cliente de sincronização, clique com o botão direito do mouse na pasta criada por você e clique em **Compartilhar**.

Uma janela é aberta para que você digite a conta de email do usuário externo. As etapas variam dependendo do cliente de sincronização usado. Para acessar links para informações sobre o cliente de sincronização, consulte Trabalhar com o cliente de sincronização de nuvem na unidade virtual DDG VDisk.

4 Conceda acesso aos arquivos individuais dentro da pasta que você quer compartilhar.

Conceder acesso a um ou mais arquivos protegidos do Office

É necessário conceder acesso a todos os arquivos que você compartilhar com usuários externos.

1 Clique com o botão direito do mouse e selecione **Conceder acesso a arquivos protegidos**. Você pode selecionar de um até 50 arquivos.
2 No campo *Email para compartilhar*, digite o endereço de email do usuário sem domínio e clique em **Adicionar**.
3 Repita essa etapa para adicionar até dez endereços de email.
4 Clique em **OK**.

Uma caixa de diálogo informa que o compartilhamento foi bem-sucedido ou que o endereço de email não está autorizado a receber arquivos protegidos.

5 Como prática recomendável, informe o usuário externo de que ele receberá um email de você com instruções para permitir que ele se registre em um Dell Server, faça download e ative o Dell Data Protection | Data Guardian e, a seguir, veja os arquivos protegidos compartilhados.

Aprovar ou negar acesso quando um usuário externo solicitar acesso

Um usuário externo que tenha o Data Guardian instalado pode solicitar acesso a um documento protegido caso não tenha a chave desse documento.

1 Se você receber um email de um usuário externo, solicitando acesso a um documento protegido, poderá ver o nome do usuário externo e o arquivo solicitado.
2 Selecione **Aprovar** ou **Negar**.

Um email é enviado ao usuário externo. Se você aprovar, a chave do documento protegido será compartilhada.

Se você não estiver disponível, o administrador também terá a opção de aprovar ou negar acesso.

Tarefas de usuário externo

Para abrir e ver um documento do Data Guardian, o usuário externo precisará:

- Registrar-se no Data Guardian

- Instalar o Data Guardian - o usuário externo precisa ter direitos de administrador no computador
- Se o usuário interno compartilhar uma pasta por meio de um cliente de sincronização, o usuário externo precisará ter uma conta de cliente de sincronização. Consulte Instalar um cliente de sincronização de nuvem e, em seguida, Trabalhar com o cliente de sincronização de nuvem na unidade virtual DDG VDisk.

Registrar-se no Data Guardian

Na primeira vez em que um usuário interno compartilhar um arquivo, o usuário externo precisará se registrar.

Para se registrar no Data Guardian:

1 No email de Verificação da conta do Dell Enterprise Server, clique no hiperlink.
2 Continue para a página da Web.
3 Na página de confirmação, clique em **Continuar para fazer login**.
4 Na página de login, clique em **Esqueci a senha**.

> **NOTA:**
> O Dell Server atribuiu uma senha aleatória, que você deverá redefinir.

5 Na página Redefinição da senha, digite e confirme sua senha e clique em **Registrar**.
A caixa de diálogo Confirmação de registro é exibida e um email é enviado ao endereço informado pelo usuário interno.
6 Abra o email de ativação da conta e clique no link.
O email também informa o nome do servidor a ser usado durante a instalação do Data Guardian.
7 Na página Login, digite o endereço de email e a senha usados para se registrar.
8 Clique em **Fazer login**.
A página Download do Data Guardian é exibida.
9 Faça download e instale o Data Guardian.
É exibida uma página de download com opções para Windows, iOS, Android e Mac OS X. Para o Enterprise Server, a página de download é exibida. Para o Dell Enterprise Server - VE, clicar no Windows levará você para o site dell.com/support (em inglês).

As etapas a seguir descrevem como instalar o Data Guardian no Windows. Consulte também Tarefas do usuário - Documentos protegidos do Office sem Criptografia na nuvem.

> **NOTA:**
> A página de download também mostra o nome do servidor que você usará nestas etapas.

10 No Windows, clique em **Download (32 bits)** ou **Download (64 bits)**, dependendo do sistema operacional do computador.
11 Faça download do arquivo de instalação para um diretório no seu computador.
12 Clique duas vezes no arquivo de instalação para abrir o instalador.
13 Selecione um idioma e clique em **OK**.
14 Se você for solicitado a instalar o Pacote redistribuível do Microsoft Visual C++ 2010, clique em **OK**.
15 Na página de boas-vindas, clique em **Avançar**.
16 Leia o contrato de licença, aceite os termos e condições e clique em **Avançar**.
17 Na tela Pasta de destino, clique em **Avançar** para fazer a instalação no local padrão de **C:\Arquivos de Programas\Dell\Dell Data Protection\Dell Data Guardian\.**
18 No campo *Nome do servidor:*, digite o nome do servidor com o qual o computador irá se comunicar. Esse nome está no email de ativação recebido ou no topo da página de download.
19 Clique em **Avançar**.
20 Na tela Confirmar servidor de ativação, certifique-se de que o endereço URL do servidor está correto. O instalador acrescenta www ou http(s) e a porta. Clique em **Avançar**.
21 Na janela Tipo de gerenciamento, selecione a opção:
- Uso externo - Um usuário com endereço de e-mail fora do domínio da empresa.

22 Clique em **Instalar** para iniciar a instalação.

Uma janela de status mostra o andamento da instalação.

23 Clique em **Concluir** quando a tela Instalação concluída for exibida.

24 Clique em **Sim** para reiniciar.

A instalação doData Guardian está concluída.

25 Consulte Ativar o Data Guardian.

Ativar o Data Guardian

Depois de instalar o Data Guardian e reiniciar o computador, execute este procedimento para fazer a ativação:

1 Faça login no Windows.

A bandeja do sistema mostra um ícone de nuvem com um ponto de exclamação laranja.

2 Quando uma caixa de diálogo for exibida na bandeja do sistema, clique em **Clique aqui para ativar**.

Se a caixa de diálogo não aparecer, clique no ícone do **Data Guardian** na bandeja do sistema e selecione **Ativação do usuário**.

3 Digite o endereço de email e a senha usados durante o registro e clique em **Ativar**.

Após o término da ativação, uma marca verde é exibida no ícone da bandeja do sistema do Data Guardian  .

4 Confirme seu status de modo de usuário. Clique no ícone da bandeja do sistema do e selecione **Detalhes**.

Na parte superior, o modo de usuário é:

Externo: um usuário com um endereço de email fora do domínio da empresa.

Se você já tiver instalado e feito login em um cliente de sincronização, a DDG VDisk virtual drive será exibida no Windows Explorer.

Solicitar acesso a um usuário interno

Com o Windows e o Mobile, se um usuário externo tiver instalado e ativado o Data Guardian, poderá solicitar a um usuário interno acesso a um arquivo. O usuário externo precisará fazer uma solicitação separada para cada arquivo.

1 Se você abrir um arquivo protegido do Office e ele informar que você precisa solicitar acesso, clique em **Sim** ou **Não**.

Uma caixa de diálogo indica que a solicitação foi enviada com sucesso. O usuário interno poderá conceder ou negar acesso e o usuário externo receberá um e-mail com o resultado. Se o usuário externo abrir o arquivo protegido antes que o usuário interno aprove o acesso, será mostrada uma mensagem informando que a solicitação está pendente.

2 Depois de 48 horas, o usuário externo poderá novamente solicitar o acesso.

Na bandeja do sistema, o usuário externo deverá clicar com o botão direito do mouse no ícone do Data Guardian e selecionar a página **Detalhes**. Clique na guia **Segurança**. Quando o tempo para uma solicitação retornar para *Nenhum*, o usuário externo poderá solicitar acesso novamente.

Exibir um documento protegido do Office

Se uma empresa ativar um política para proteger documentos do Office e um usuário interno enviar um arquivo protegido a um usuário externo, o usuário externo deverá estar conectado ao Dell Server quando abrir o documento pela primeira vez. Depois disso, ele poderá abrir e ver o documento offline por um período especificado, por exemplo, uma vez por semana. O usuário externo precisará, a seguir, se conectar ao servidor e reabrir o documento protegido.

Para fins de segurança, um usuário externo não pode fazer o seguinte com um documento protegido do Office.

- Imprimir
- Exportar
- Salvar como
- Compartilhar

Desinstalar o Sync Client ou o Data Guardian

Se o administrador tiver instalado o Data Guardian, somente o administrador poderá desinstalar o produto. Um usuário externo que tenha convidado a compartilhar uma pasta e tenha direitos de administrador em um computador externo também poderá desinstalar o Data Guardian deste computador externo.

Desinstalar um Cliente de sincronização de nuvem

Se você desinstalar o cliente de sincronização de nuvem mas ainda tiver o Data Guardian no computador, ainda poderá ver seus arquivos em texto não criptografado na DDG VDisk virtual drive.

No entanto, se você reinstalar o mesmo cliente de sincronização de nuvem, precisará de uma nova chave para abri-lo na DDG VDisk virtual drive e terá de fazer download dos seus arquivos do site do cliente de sincronização.

Desinstalar o Data Guardian

Você precisa ser um Administrador local do computador para desinstalar o Data Guardian.

Copiar arquivos para a unidade local

Se você desinstalar o Data Guardian do seu computador ou dispositivo, os arquivos no site do cliente de sincronização ainda precisarão estar protegidos para permanecerem criptografados.

1 Antes de desinstalar, determine se há arquivos que você precisa acessar.
2 Copie esses arquivos da DDG VDisk virtual drive para a unidade local.

Esses arquivos, copiados da DDG VDisk virtual drive, serão exibidos em texto não criptografado. As pastas e os arquivos no site do cliente de sincronização permanecerão criptografados, mesmo que você faça download deles. Para vê-los, será preciso reinstalar o Data Guardian.

Desinstalar o Data Guardian

1 Use o Painel de controle do Windows para desinstalar o programa.
2 Selecione Dell Data Protection | Data Guardian e clique em **Alterar** no menu superior.
3 Clique em **Avançar** quando a tela Boas-vindas for mostrada.
4 Selecione **Remover** e clique em **Avançar**.
5 É exibida uma advertência para confirmar se você quer desinstalar o Dell Data Protection | Data Guardian. Caso positivo, clique em **Avançar.**
6 Na tela Remover o programa, clique em **Remover**.
A janela de status mostrará o andamento.
7 Se for exibida uma caixa de diálogo de erro do cliente de sincronização, clique em **Continuar**.
8 Clique em **Concluir** quando a tela Concluído for exibida.
9 Clique em **Sim** para reiniciar.

A desinstalação do Dell Data Protection | Data Guardian foi concluída.

Perguntas frequentes

Perguntas frequentes de disposição geral

Pergunta

Removi a pasta de sincronização do provedor de nuvem para Arquivos de programas e agora não consigo descriptografar os arquivos que estão sendo obtidos por download para minha pasta de sincronização a partir da nuvem.

Resposta

Conforme o projeto, a pasta Arquivos de programas ou outras pastas apagadas não são protegidas, com base na política. O Data Guardian não descriptografará qualquer arquivo obtido por download nessa pasta ou nas suas subpastas.

Solução

Desvincule ou desinstale o cliente de sincronização e reponha a pasta de sincronização em seu local padrão ou em um local alternativo gerenciado.

NOTA:
Para obter uma lista de locais gerenciados e não gerenciados, entre em contato com o administrador.

Pergunta

Eu tinha alguns arquivos .xen files arquivados e os copiei para minha área de trabalho. Alguns deles foram criptografados, outros não.

Resposta

Durante a sincronização, o Data Guardian foi projetado para ser descriptografado diretamente na unidade virtual ou ser descriptografado quando estiver fazendo download por um navegador da Web. Para arquivos que tiverem sido copiados de outro local, use o Windows Explorer e mova o arquivo .xen para a unidade virtual a ser descriptografada.

Solução

Remova os arquivos .xen para a pasta da unidade virtual e faça upload dos mesmos para a nuvem. Depois eles serão descriptografados localmente.

Pergunta

Renomeei meu computador. Agora, não estou recebendo atualizações de políticas e não consigo criptografar na nuvem.

Resposta

Atualmente, o servidor reconhece apenas o endpoint em relação ao qual você originalmente ativou. Se você alterar o nome do ponto de extremidade, o servidor não reconhecerá mais o local para enviar a política e o Data Guardian tampouco funcionará conforme esperado.

Solução

1 Pare de sincronizar arquivos para o computador local.

NOTA:
Se você não parar de sincronizar antes de desinstalar, dados importantes podem ficar desprotegidos na nuvem ou talvez sejam apagados.

2 Desinstale e depois reinstale o Data Guardian. Você precisa ter direitos de administrador para desinstalar.

Pergunta

Em dispositivos suspensos do Windows, quando tento fazer upload de arquivos para a nuvem, nada acontece. Quando fecho as janelas que já estão abertas, aparece uma mensagem de erro indicando Acesso negado.

Resposta

A mensagem de erro não vem do Data Guardian. Você pode acessar os arquivos localmente, mas não obterá as próximas atualizações dos arquivos.

Perguntas frequentes sobre documentos do Office e modo protegido

Pergunta

Tentei abrir um documento do Office (.docx, .pptx, .xlsx, .docm, .pptm, .xlsm) e foi exibida uma página de rosto.

Resposta

Se o administrador tiver definido uma política para proteger documentos do Office, você ou o administrador precisará instalar o Data Guardian. Confirme que o ícone do Data Guardian na bandeja do sistema tenha uma marca de seleção verde, indicando que o aplicativo está ativado.

Solução

Determine se você precisa instalar ou ativar o Data Guardian. Consulte Instalar Data Guardian ou Possíveis problemas com a ativação.

Pergunta

Não consigo abrir um documento protegido do Office (Word, PowerPoint ou Excel).

Resposta

Verifique o seguinte:

- Configurações do Bloqueio avançado de arquivo - Se o administrador definir políticas para proteger documentos do Office, não use esta configuração em **Arquivo > Opções**.

Solução

Para verificar as Configurações do Bloqueio avançado de arquivo:

1 Em um documento do Office, selecione **Arquivo > Opções**.
2 Selecione **Central de confiabilidade** na lista.
3 À direita,clique em **Configurações da Central de confiabilidade**.
4 Selecione **Configurações do Bloqueio avançado de arquivo** na lista.
5 Para *Word/Excel/PowerPoint 2007 e documentos e modelos posteriores*, certifique-se de que a caixa de seleção *Abrir* esteja desmarcada.
6 Clique em **OK**.