# Dell Data Guardian

Guia do utilizador v1.2

## Notas, avisos e advertências

**NOTA: Uma NOTA indica informações importantes que ajudam a melhorar a utilização do produto.**

**AVISO: Um AVISO indica potenciais danos do hardware ou a perda de dados e explica como evitar o problema.**

**ADVERTÊNCIA: Uma ADVERTÊNCIA indica potenciais danos no equipamento, lesões pessoais ou mesmo morte.**



**Guia do utilizador do Dell Data Guardian**

2017 - 04

Rev. A01

# Índice

# Introdução ao Dell Data Guardian

O *Guia do utilizador do Dell Data Guardian* fornece as informações necessárias para a instalação e utilização do Dell Data Guardian.

## Descrição geral

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

- Sistemas de partilha de ficheiros baseados na nuvem - Os computadores Windows ou dispositivos móveis captam dados destinados ao armazenamento na nuvem, encriptam esses dados e, em seguida, carregam os dados encriptados para a nuvem.
- Documentos do Office armazenados localmente, partilhados com outros utilizadores de várias formas ou guardados em suportes de dados amovíveis. Podem ser protegidos os seguintes tipos de documentos do Office: .docx, .pptx, .xlsx, .docm, .pptm, .xlsm.

> **NOTA:**
> O seu administrador irá informá-lo se a sua empresa utiliza o Data Guardian apenas com armazenamento na nuvem, apenas com documentos do Office ou com ambos.

Pode utilizar o Data Guardian nas seguintes plataformas:

- Windows
- iOS
- Android
- Tanto este produto como o Data Guardian para Mac conseguem abrir ficheiros encriptados pelo outro.
    - Este documento trata do Dell Data Guardian apenas para Windows.
    - Para obter informações sobre o Dell Data Guardian para Mac, consulte a ajuda online do software.

## Suporte adicional

Se necessitar de suporte adicional além deste documento, contacte o seu administrador.

2

# Requisitos do Dell Data Guardian

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

**NOTA:**
O IPv6 não é suportado.

## Servidor

O Data Guardian obriga o cliente a estar ligado a um Dell Enterprise Server ou Dell Enterprise Server - VE, v9.6 ou superior. Neste documento, ambos os servidores estão assinalados como Dell Server, a não ser que seja necessário indicar uma versão específica (por exemplo, um procedimento que seja diferente ao utilizar o Dell Enterprise Server - VE).

## Cliente de encriptação

- Durante a implementação, devem ser seguidas as melhores práticas de TI. Estas incluem, entre outras, ambientes de teste controlados para os testes iniciais e a implementação progressiva para os utilizadores.
- A conta de utilizador que realiza a instalação/atualização/desinstalação deve ser um utilizador administrador local ou de domínio, que poderá ser atribuído temporariamente por uma ferramenta de implementação, como o Microsoft SMS ou Dell KACE. Não são suportados utilizadores não administradores com privilégios elevados.
- Realize uma cópia de segurança de todos os dados importantes antes de iniciar a instalação/desinstalação.
- Não realize alterações no computador, incluindo inserir ou remover unidades externas (USB) durante a instalação.
- Apesar de não ser necessário o cliente de encriptação, qualquer cliente de encriptação utilizado com o Data Guardian deve ser v8.12 ou posterior.
- O Data Guardian não é compatível com o Microsoft Office 365.
- Para encriptação na nuvem, o computador deve ter uma (letra) unidade de disco atribuível disponível.
- Certifique-se de que os dispositivos de destino estão ligados a https://yoursecurityservername.domain.com:8443/cloudweb/register https://yoursecurityservername.domain.com:8443/cloudweb
- Antes de implementar o Data Guardian, é preferível que os dispositivos de destino não tenham ainda contas de armazenamento na nuvem configuradas.

  Se os utilizadores decidirem manter as respetivas contas existentes, devem certificar-se de que quaisquer ficheiros que devam permanecer *sem encriptação* são retirados do cliente de sincronização antes de instalar o Data Guardian.
- Os utilizadores devem estar preparados para reiniciarem os respetivos computadores depois de instalarem o cliente.
- O Data Guardian não interfere no comportamento de clientes de sincronização. Por conseguinte, os administradores e utilizadores finais devem familiarizar-se com o funcionamento destas aplicações antes de implementarem o Data Guardian. Para obter mais informações, consulte o apoio técnico do Box em https://support.box.com/home, o apoio técnico do Dropbox em https://www.dropbox.com/help ou o apoio técnico do OneDrive em http://windows.microsoft.com/en-us/onedrive/onedrive-help#onedrive=other.
- Se estiver em execução o Office 2010: caso tenham sido definidas políticas para proteger documentos do Office e documentos com permissão para macros, os utilizadores têm de ter o Service Pack 1 do Office 2010 ou superior (v14.0.6029 ou superior). Consulte https://support.microsoft.com/en-us/kb/2121559 para determinar se foi aplicado um service pack a uma suite do Microsoft Office 2010. Sem esta atualização, não é possível aceder a documentos protegidos. Os novos documentos do Office estão desprotegidos, independentemente da política, exceto se a funcionalidade de varrimento estiver ativada. O próximo varrimento converte os documentos do Office em ficheiros protegidos, mas os utilizadores não podem aceder aos mesmos sem uma versão compatível do Office.
- O Data Guardian não suporta a ferramenta de restauro do sistema Windows.

- Assegure-se de verificar periodicamente a página www.dell.com/support para procurar a documentação mais atual e Conselhos técnicos.

# Pré-requisitos do cliente

Se ainda não estiver instalado, o programa de instalação instala o Pacote Redistribuível do Microsoft Visual C++ 2015 (x86 e x64).

**NOTA:**
No 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.

É necessário Microsoft .Net 4.5.2 (ou posterior) para o Data Guardian. Todos os computadores enviados da fábrica da Dell estão previamente equipados com o .Net 4.5.2. No entanto, se não instalar no hardware Dell ou se atualizar o Data Guardian num hardware Dell mais antigo, deve verificar qual a versão do .Net instalada e atualizar a versão, antes de instalar o Dell Data Guardian para impedir falhas na instalação/atualização. Para verificar a versão instalada do .Net, siga estas instruções no computador onde pretende efetuar a instalação: http://msdn.microsoft.com/en-us/library/hh925568(v=vs.110).aspx Para instalar o Microsoft .Net Framework 4.5.2, aceda a https://www.microsoft.com/en-us/download/details.aspx?id=42643.

# Hardware para um cliente Windows

Os requisitos mínimos de hardware necessitam atender as especificações mínimas do sistema operativo. A tabela seguinte apresenta o hardware suportado para o cliente Windows.

**Hardware Windows**

- 200 MB de espaço livre no disco, dependendo do sistema operativo
- Placa de rede 10/100/1000 ou Wi-Fi
- TCP/IP instalado e ativado

Se o seu Enterprise encriptar os dados para o armazenamento na nuvem, o seu computador tem de ter uma letra do alfabeto disponível para atribuir a um disco rígido.

# Sistemas operativos

A tabela seguinte apresenta os sistemas operativos suportados.

**Sistemas operativos 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 dos eventos de auditoria do Data Guardian.

**Sistemas operativos para Android**

- 4.4 - 4.4.4 KitKat
- 5.0 -5.1.1 Lollipop
- 6.0-6.0.1 Marshmallow

- 7.0 Nougat

**Sistemas operativos iOS**

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

# Clientes Cloud Edition

A tabela seguinte detalha os clientes de sincronização na nuvem que trabalham com o Data Guardian. As atualizações do cliente de sincronização são lançadas frequentemente. A Dell recomenda que proceda a testes das novas versões do cliente de sincronização com o Data Guardian antes de as incorporar no ambiente de produção.

**Clientes Cloud Edition**

- DropBox
- DropBox for Business (apenas para Windows)

  **NOTA:**
  Dependendo da versão do servidor Dell utilizada pela sua empresa, é possível encriptar todos os ficheiros e pastas nas contas pessoais Dropbox que estão ligados a contas da empresa.

- Box

  **NOTA:**
  O Box Tools e Box Edit não são suportados pelo Data Guardian. Utilizar o Box Tools pode provocar a apresentação de um ecrã azul.

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

  **NOTA:**
  O Unified OneDrive consiste num cliente de sincronização unificado para o OneDrive e para o OneDrive para Empresas.

# Web browsers

Pode utilizar o Data Guardian > Encriptação na nuvem com Internet Explorer, Mozilla Firefox e Google Chrome.

**NOTA:**
Data Guardian > Encriptação na nuvem não suporta o browser Microsoft Edge.

# Tarefas do utilizador - Encriptação na nuvem e Office protegido

O seu administrador já configurou as políticas para o Data Guardian e irá informá-lo se a sua empresa utilizar o Data Guardian:

- Para gerir o seu cliente de sincronização na nuvem
- Para gerir o seu cliente de sincronização na nuvem e ter proteção adicional para os seus documentos do Office - Se a sua empresa apenas protege documentos do Office, mas não gere um cliente de sincronização na nuvem, siga os passos apresentados em Tarefas do utilizador - Office protegido sem encriptação na nuvem.

Se a sua empresa utiliza o Data Guardian com armazenamento na nuvem:

- Antes de implementar o Data Guardian, consulte a ajuda online do seu fornecedor de armazenamento na nuvem/cliente de sincronização na nuvem para compreender o funcionamento da sua aplicação de armazenamento na nuvem. Este documento explica essencialmente como utilizar o Data Guardian.
- Normalmente, instale e funcione com um cliente de sincronização na nuvem. A sua empresa pode ter um cliente de sincronização na nuvem preferencial e estabelecer uma política para permitir que utilize apenas esse.

## Descrição geral das tarefas

Esta descrição geral resume a sequência de instalação e utilização do Data Guardian.

**Instalar o Data Guardian e um cliente de sincronização na nuvem**

| Tarefa | Descrição | Para obter mais informações |
|---|---|---|
| Se um cliente de sincronização na nuvem for instalado antes do Data Guardian | As pastas e ficheiros preexistentes que são sincronizados para a nuvem não são encriptados.<br><br>**NOTA:**<br>As pastas e ficheiros preexistentes que são sincronizados a partir da nuvem são encriptados. | Consulte Pastas preexistentes com ficheiros não encriptados. |
| Instalar o Data Guardian | Determinar o seguinte:<br><br>O utilizador tem de instalar o Data Guardian<br><br>O administrador já instalou o Data Guardian - continue para o passo seguinte. | Instalações pelo utilizador: consulte Instalar o Data Guardian no Windows. Reiniciar e continuar para o passo seguinte. |
| Confirmar o estado de ativação | Confirmar no tabuleiro do sistema se o ícone do Data Guardian tem uma marca de verificação verde  . | Se o ícone apresentar um ponto de exclamação laranja, consulte Possíveis problemas na ativação - Nuvem e Office protegido. |
| Se as políticas protegerem os documentos na | Cliente de sincronização empresarial<br><br>ou | Contas de clientes de sincronização na nuvem empresarial<br><br>ou |

| Tarefa | Descrição | Para obter mais informações |
|---|---|---|
| nuvem, instale um cliente de sincronização na nuvem | Cliente de sincronização básica | Contas de clientes de sincronização na nuvem básica |

**NOTA:**
Se ao abrir um documento do Office for apresentada uma página de rosto com informações de instalação ou ativação, o seu administrador poderá ter definido políticas para proteger os documentos do Office. Confirme se o Data Guardian está instalado e ativado. Consulte Possíveis problemas na ativação - Nuvem e Office protegido.

**Utilizar o Data Guardian**

| Tarefa | Descrição | Para obter mais informações |
|---|---|---|
| Visualizar o cliente de sincronização na nuvem no Explorador de Ficheiros | Depois de ter instalado o Data Guardian e um cliente de sincronização na nuvem, é apresentada uma Unidade virtual DDG VDisk no Explorador de ficheiros. | Trabalhar com pastas e ficheiros<br><br>Aceder a pastas e ficheiros do cliente de sincronização no computador local |
| Trabalhar com o cliente de sincronização na nuvem na Unidade virtual DDG VDisk | Na Unidade virtual DDG VDisk, pode adicionar subpastas ao cliente de sincronização na nuvem e, em seguida, arrastar ficheiros ou criar ficheiros nessas subpastas.<br><br>Após a sincronização, os ficheiros ficam seguros na nuvem: os ficheiros do Office podem ser abertos, mas apenas é apresentada uma página de rosto; os outros ficheiros são encriptados como ficheiros .xen.<br><br>No entanto, na unidade virtual, são desencriptados e exibidos como texto legível.<br><br>Para obter mais informações, clique na ligação adequada para o seu cliente de sincronização na nuvem. | **Conta empresarial:**<br><br>Dropbox para empresas<br><br>OneDrive for Business/OneDrive unificado<br><br>**Conta básica:**<br><br>DropBox<br><br>Box<br><br>Google Drive<br><br>OneDrive |
| Visualizar o menu do tabuleiro do sistema | Fornece informações úteis sobre ficheiros, pastas e resolução de problemas. | Compreender os itens de menu do tabuleiro do sistema do Data Guardian |
| Proteger documentos do Office, com permissão para macros e .pdf, se a política estiver ativada | Proteger um documento do Office (.docx, .pptx, .xlsx, .docm, .pptm, .xlsm, .pdf ) no momento da sua criação. Está seguro quando o partilhar com outras pessoas ou quando o guardar num suporte de dados amovível. | Utilizar documentos do Office com o modo protegido do Data Guardian<br>• Observar as opções do menu Ficheiro para determinar o nível de segurança para documentos do Office<br>• Trabalhar com opções do menu Ficheiro |
| Partilhar uma pasta na nuvem com outros para colaborarem em ficheiros | Partilhar uma pasta com:<br><br>Utilizador interno (com um endereço de e-mail do domínio)<br><br>Utilizador externo (com um endereço de e-mail fora do domínio) - trabalhe com o seu administrador. | Utilizador interno - Consulte a ajuda online do seu fornecedor de armazenamento na nuvem.<br><br>Utilizador externo - Consulte Utilizar o Data Guardian como utilizador externo. |

# Instalar o Data Guardian com nuvem e Office protegido

## Pastas preexistentes com ficheiros não encriptados

Antes de implementar o Dell Data Protection | Data Guardian (DDG VDisk), é preferível que os dispositivos de destino não tenham ainda uma conta de fornecedor de armazenamento na nuvem configurada.

Caso já disponha de uma conta de fornecedor de armazenamento na nuvem com pastas sincronizadas com o seu computador local e depois instale o Data Guardian:

- Os ficheiros e pastas preexistentes que são sincronizados para a nuvem permanecem em texto desencriptado
- Os ficheiros que adicionar a essas pastas preexistentes permanecem em texto desencriptado
- Os ficheiros que são sincronizados a partir da nuvem são encriptados

  Se pretende que os ficheiros preexistentes sejam encriptados, navegue até à Unidade virtual DDG VDisk, crie uma nova subpasta dentro do cliente de sincronização na nuvem e mova os ficheiros preexistentes para essa pasta.

  ou

  Para conteúdos de grande dimensão, um gestor ou administrador pode solicitar temporariamente o Menu Gerir pastas.

## Instalar o Data Guardian no Windows

Apenas um administrador local do computador tem permissão para instalar o Data Guardian.

O computador deve ter uma letra do alfabeto disponível para atribuir a uma unidade de disco.

Prepare-se para reiniciar o computador, assim que o Data Guardian estiver instalado.

1. Para transferir o instalador do Data Guardian, aceda à localização especificada pelo seu administrador.
2. Com base no seu sistema operativo, selecione o instalador de 32 bits ou de 64 bits, normalmente **setup32.exe** ou **setup64.exe**, e copie-o para o computador local.
3. Clique duas vezes no ficheiro para iniciar o programa de instalação.
4. Se for apresentado um aviso de segurança, clique em **Executar**.
5. Selecione um idioma e clique em **OK**.
6. Se aparecer uma mensagem a questionar se deseja instalar o Pacote redistribuível do Microsoft Visual C++ 2010 ou o Microsoft .NET Framework 4.0 Client Profile, clique em **OK**.
7. No ecrã de boas-vindas, clique em **Seguinte**.
8. Leia o contrato de licença, aceite os termos e condições e clique em **Seguinte**.
9. No ecrã Pasta de destino, clique em **Seguinte** para instalar na localização predefinida de C:\Program Files\Dell\Dell Data Protection \Dell Data Guardian\.

   Em C:\, não instale o Data Guardian nas pastas Utilizadores ou Windows, nem na raiz de qualquer unidade. Nesse caso, é obtido um erro.
10. No campo *Nome do servidor:*, introduza o nome do servidor com o qual este computador vai comunicar, como, por exemplo, servidor.domínio.com. Não é necessário incluir web ou http(s). Esta informação é fornecida pelo seu administrador.

    Não desmarque a caixa de verificação *Ativar verificação de confiança SSL* exceto se tal for instruído pelo administrador.
11. Clique em **Seguinte**.
12. No ecrã Confirmar informações do servidor de ativação, certifique-se de que o endereço URL do servidor está correto. O instalador adiciona www ou http(s) e, de seguida, a porta. Clique em **Seguinte**.

13 Na janela Tipo de gestão, selecione esta opção:
   - Uso interno - Um utilizador com um endereço de e-mail dentro do domínio da empresa.
14 Clique em **Instalar** para dar início à instalação.
   Uma janela de estado apresenta o progresso da instalação.
15 Clique em **Concluir** quando for apresentado o ecrã de Instalação concluída.
16 Clique em **Sim** para reiniciar.
   A instalação do Data Guardian está concluída.
17 Depois de reiniciar, confirme no tabuleiro do sistema se o ícone do Data Guardian tem uma marca de verificação verde  .

# O Data Guardian e encriptação na nuvem

Se a sua empresa definir políticas para proteger os dados na nuvem e já tiver instalado e iniciado sessão num cliente de sincronização, é apresentada uma Unidade virtual DDG VDisk no Explorador do Windows.

**NOTA:**
O Data Guardian não suporta a desmontagem da unidade virtual.

Se precisar de instalar e iniciar sessão num cliente de sincronização, consulte Instalar um cliente de sincronização na nuvem.

# Instalar um Cliente de sincronização na nuvem

**Transferir e Instalar**

Normalmente, uma empresa sugere que todos os utilizadores instalem o mesmo cliente de sincronização na nuvem. Se aplicável, use o cliente de sincronização na nuvem preferido da sua empresa.

**NOTA:**
O computador deve ter uma letra do alfabeto disponível para atribuir a uma unidade de disco.

**NOTA:**
Atualmente, o Data Guardian não suporta um cliente de sincronização instalado num ponto de montagem.

1 Instale um cliente de sincronização na nuvem empresarial ou básico:
   - **Contas de clientes de sincronização na nuvem empresarial**
     Se a sua empresa disponibilizar uma opção de conta empresarial, o seu administrador irá fornecer-lhe uma ligação para a respetiva transferência e instalação. As opções são:
     - **Dropbox for Business** - Se instalar o Dropbox for Business, também terá de Autenticar o Dropbox for Business.
     - **OneDrive for Business/OneDrive unificado**- Para os passos detalhados, consulte https://support.microsoft.com/en-us/kb/2903984.
   - **Contas de clientes de sincronização na nuvem básica**
     - **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/OneDrive unificado (Windows 7 e 8)** - consulte https://onedrive.live.com/about/en-us/download/
       No Windows 8.1 e posterior, o OneDrive está pré-instalado. Se tiver as Atualizações do Windows ativadas, o OneDrive unificado substitui o OneDrive.
2 Depois de instalar e iniciar a sessão, é apresentado o seguinte:
   - Em Explorador de ficheiros, uma Unidade virtual DDG VDisk é adicionada. A pasta de cliente de sincronização na nuvem é adicionada a esta unidade virtual.
     Se instalar mais de um cliente de sincronização na nuvem, cada um deles exibe uma pasta nesta unidade virtual.

**NOTA:**
O Data Guardian não suporta a desmontagem da unidade virtual.

- Em Explorador de Ficheiros > Favoritos, é adicionada uma pasta para o seu cliente de sincronização na nuvem.
- No tabuleiro do sistema, é exibido o ícone do cliente de sincronização na nuvem.
- Dependendo do fornecedor de armazenamento na nuvem, pode ser automaticamente adicionado um atalho do cliente de sincronização na nuvem no ambiente de trabalho.
- Apenas no modo opcional (mas não no modo de proteção forçada) - uma pasta de Documentos seguros é adicionada à raiz da pasta de Documentos. Consulte Documentos > Pasta de documentos seguros.

**Alterar a letra da unidade virtual ou criar um atalho**

Depois de instalar o Data Guardian e um cliente de sincronização na nuvem, o ícone da Unidade virtual DDG VDisk é apresentado no Explorador de ficheiros. A letra da unidade é atribuída utilizando uma letra disponível, escolhida a partir do final do alfabeto.

Para alterar a letra da unidade:

1 No tabuleiro 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 **OK**.
Para adicionar o ícone da Unidade virtual DDG VDisk ao ambiente de trabalho, clique com o botão direito na unidade e selecione **Criar atalho**.

**Autenticar Dropbox para Empresas**

Caso instale o Dropbox for Business, o Data Guardian irá solicitar uma autenticação.

Para autenticar:

1 Após a instalação do Data Guardian, poderá abrir-se uma janela Autenticação ou então clique no ícone do Data Guardian e, em seguida, selecione **Dropbox > Ligar**.
A janela Autenticação irá informá-lo de que o Data Guardian necessita ter acesso à sua conta Dropbox e poderá fornecer instruções sobre contas empresariais e pessoais.

Para o utilizador, isto proporciona opções de menu de contexto. Para a empresa e o seu administrador, isto é essencial, uma vez que proporciona medidas de segurança adicionais.

2 Na janela Autenticação, clique em **Seguinte**.

3 Caso se abra uma janela do Threat Protection para rede, clique em **Sim**.

4 Na janela Autenticação, introduza o seu e-mail de domínio e palavra-passe do Dropbox.

5 Clique em **Iniciar sessão**.

6 Se tem a sua conta empresarial e a pessoal do Dropbox associadas, ser-lhe-á pedido para selecionar uma delas. Deve selecionar a sua conta empresarial.

7 Clique em **Concluir** ou aguarde até a janela fechar.

# Trabalhar com pastas e ficheiros

O Data Guardian trabalha de forma transparente com o seu cliente de sincronização na nuvem. Quando o seu administrador define uma política para ativar o Data Guardian, os ficheiros são encriptados e protegidos na nuvem quando são sincronizados a partir do seu computador local.

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

- Criar pastas
- Carregar/transferir pastas e ficheiros

**NOTA:**
Para carregar ficheiros, copie ou arraste ficheiros para pastas na Unidade virtual DDG VDisk. O Data Guardian não suporta a função de arrastar ficheiros do seu computador local para a Web nem a criação de ficheiros diretamente no website do fornecedor de armazenamento na nuvem.

- Utilizar sincronização seletiva de pastas
- Partilhar pastas ou ficheiros com utilizadores internos possuidores do Data Guardian. Consulte Partilhar uma pasta com um utilizador interno.
- Partilhar pastas ou ficheiros com utilizadores externos. Consulte Utilizar o Data Guardian como utilizador externo.
- Deixar de partilhar pastas

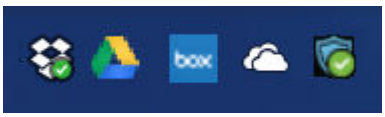
# Visualizar pastas e ficheiros no computador local e na nuvem

### Aceder a pastas e ficheiros do cliente de sincronização no computador local

Para aceder a pastas e ficheiros sincronizados, clique na **Unidade virtual DDG VDisk** no Explorador de ficheiros. O seu cliente de sincronização na nuvem é exibido.

Seguem-se outras formas para aceder ao seu cliente de sincronização na nuvem.

- No tabuleiro do sistema, selecione o ícone do cliente de sincronização na nuvem e abra a pasta do cliente de sincronização. Para obter mais informações, consulte a ajuda do fornecedor de armazenamento na nuvem.

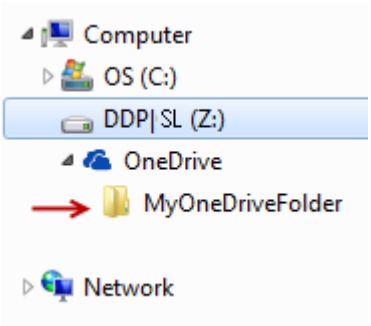



- Em Favoritos, clique no ícone do cliente de sincronização.
  Quando clicar no ícone do cliente de sincronização no tabuleiro do sistema ou em Favoritos, confirme se a Unidade virtual DDG VDisk está realçada. O Data Guardian redireciona-o para esta unidade virtual, que lhe permite visualizar as suas pastas e ficheiros desencriptados localmente como texto desencriptado.

Também pode aceder às pastas e ficheiros da Unidade virtual DDG VDisk através de um atalho no ambiente de trabalho. Consulte Alterar a letra da unidade virtual ou criar um atalho.

### Adicionar pastas

Com o Data Guardian, tem de adicionar subpastas à pasta de sincronização na nuvem. Não adicione ficheiros à raiz da Unidade virtual DDG VDisk.




### Adicionar ficheiros

Quando adiciona um ficheiro a uma pasta, o Data Guardian adiciona automaticamente um ficheiro na pasta na Internet. O Data Guardian utiliza o ficheiro Como aceder a ficheiros protegidos.html quando partilha uma pasta com utilizadores externos. Não será necessário abrir ou transferir este ficheiro. Consulte Utilizar o Data Guardian como utilizador externo.

### *Visualizar pastas e ficheiros do cliente de sincronização na nuvem*

O Data Guardian encripta os seus dados na nuvem e os nomes dos ficheiros têm uma extensão .xen. O ícone junto ao ficheiro pode ser diferente para cada fornecedor de armazenamento na nuvem, mas não exibe o conteúdo. Não pode abrir os ficheiros na nuvem. Por esse motivo, se alguém obtiver acesso à sua conta de armazenamento na nuvem, não poderá abrir ou visualizar os seus ficheiros. Esta funcionalidade aumenta a segurança na nuvem. Só é possível visualizar os ficheiros como texto desencriptado na Unidade virtual DDG VDisk.

Ocasionalmente, quando transferir um ficheiro .xen para o seu ambiente de trabalho e este é desencriptado, subsiste uma cópia do ficheiro com uma extensão .xen. Pode eliminar a cópia transferida do ficheiro .xen.

Se a sua empresa pretender proteção adicional para pastas e ficheiros na nuvem, o seu administrador pode definir uma política para ocultar os nomes de ficheiros na nuvem e quando forem transferidos. Se alguém obtiver acesso à sua conta de armazenamento na nuvem, não poderá abrir os ficheiros nem ler os nomes dos ficheiros.

### *Visualizar pastas e ficheiros do cliente de sincronização num computador local com o Data Guardian e uma unidade virtual instalada*

Para facilitar a utilização do Data Guardian no seu computador local, quando abre uma pasta na Unidade virtual DDG VDisk, os ficheiros da nuvem são automaticamente desencriptados e apresentados como texto desencriptado, mesmo estando protegidos como ficheiros encriptados na nuvem.

### *Proteger pastas e ficheiros em dispositivos que não têm o Data Guardian*

Se uma pessoa não autorizada transferir um ficheiro protegido a partir da nuvem para um dispositivo que **não** tenha o Data Guardian instalado, essa pessoa não consegue aceder aos seus dados. Com base nas políticas definidas pelo seu administrador:

- Documentos do Office - o documento abre-se, mas apenas é apresentada uma página de rosto com uma mensagem empresarial específica.
- Documentos não Office - o ficheiro é transferido como um ficheiro .xen. A pessoa não consegue abrir o ficheiro.

> **NOTA:**
> Com os utilizadores internos, se transferirem um ficheiro de um computador que tenha o Data Guardian para um dispositivo que não o tenha, não é possível visualizar o ficheiro a menos que instalem o Data Guardian como utilizador externo.

Ocasionalmente, um ficheiro .xen poderá ser exibido num computador que tenha o Data Guardian instalado. Por exemplo, se ocorrer um corte na ligação à Internet antes da transferência estar concluída, a chave pode não ficar disponível para abrir o ficheiro. Uma caixa de diálogo informa que o ficheiro não pode ser desencriptado.

O Data Guardian não permite edições a ficheiros sem extensões. Estes ficheiros são tratados como ficheiros só de leitura. Para editar um ficheiro sem uma extensão, transfira-o do website do fornecedor de armazenamento na nuvem, edite-o e, em seguida, carregue-o através da Unidade virtual DDG VDisk.

### Pesquisar nomes de ficheiros e conteúdos na Unidade virtual DDG VDisk

Se pretender pesquisar nomes de ficheiros ou conteúdos na Unidade virtual DDG VDisk, terá de ativar a Indexação de pesquisa do Windows para esta unidade.

> **NOTA:**
> A Indexação de Pesquisa do Windows está ativada apenas para as pastas dos utilizadores.

Para ativar a Indexação de pesquisa do Windows para a Unidade virtual DDG VDisk:

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

3 Em *Alterar localizações selecionadas*, selecione a caixa de verificação para a Unidade virtual DDG VDisk.

> **NOTA:**
> Os restantes passos podem variar, dependendo do seu sistema operativo.

4 Clique em **OK**.

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

Pode agora efetuar uma pesquisa na Unidade virtual DDG VDisk.

# Partilhar uma pasta com um utilizador interno

Um utilizador interno dispõe de um endereço de e-mail dentro do domínio da empresa.

Para partilhar uma pasta com um utilizador interno, deve aceder ao website do seu fornecedor de armazenamento na nuvem e selecionar **Partilhar**. Consulte a ajuda online do fornecedor de armazenamento na nuvem.

**Partilhar uma pasta através do Data Guardian e do Box**

No website do Box, selecione uma das seguintes opções.

| Opção do website do Box | Opções | Descrição |
|---|---|---|
| Partilhar | Disponível para pastas e ficheiros<br><br>Visualizar o acesso | Quando a janela Partilhar abrir, certifique-se de que Permitir a transferência está definido como **Sim**.<br><br>Depois de transferir ficheiros ou pastas, quem partilha tem de extrair a pasta comprimida e, em seguida, mover a pasta e os ficheiros para a Unidade virtual DDG VDisk. |
| Convidar colaboradores | Disponível para pastas<br><br>Visualizar ou Editar o acesso | Quando a janela Convidar abrir, pode selecionar **Editor** ou **Visualizador**.<br><br>Quem partilha pode sincronizar a pasta para o seu computador e este é sincronizado com a Unidade virtual DDG VDisk. |

# Utilizar documentos do Office com o modo protegido do Data Guardian

Para melhorar a segurança empresarial, o seu administrador pode ativar uma política para proteger ficheiros para as seguintes aplicações do Office:

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

Se uma pessoa não autorizada aceder a um ficheiro protegido, o ficheiro permanece encriptado quando, por exemplo:

- É enviado como anexo num e-mail
- É movido num browser - em alguns clientes de sincronização na nuvem, pode clicar com o botão direito do rato num nome de ficheiro e selecionar **Mover**.
- É partilhado na rede
- É carregado para um fornecedor de armazenamento na nuvem
- É guardado num suporte de dados amovível

Para documentos do Office, pode ser apresentada uma página de rosto com instruções para instalar ou ativar o Data Guardian, por exemplo:

- É necessário instalar o Data Guardian.
- É necessário ativar o Data Guardian.
- O utilizador abre um documento protegido do Office na nuvem.
- Transferiu um ficheiro do Office do seu computador que tem o Data Guardian para um dispositivo pessoal que não o tem.
- Um utilizador não autorizado acede a um dos seus ficheiros do Office - A página de rosto é apresentada com uma mensagem empresarial específica, mas o utilizador não consegue visualizar o conteúdo do ficheiro.

Se a sua empresa utilizar o modo protegido do Data Guardian, consulte:


- Observar as opções do menu Ficheiro para determinar o nível de segurança para documentos do Office
- Trabalhar com opções do menu Ficheiro
- Determinar que documentos no modo opcional estão protegidos
- Opções do menu adicionais para documentos do Office protegidos
- Utilizadores externos e documentos do Office protegidos


# Observar as opções do menu Ficheiro para determinar o nível de segurança para documentos do Office

Para determinar se o seu administrador ativou políticas do Data Guardian, abra um documento do Office e selecione **Ficheiro**. Se a opção *Guardar como protegido* for apresentada no painel esquerdo, tem proteção adicional em documentos do Office.

Para determinar o nível de segurança, verifique as opções ativadas ou desativadas:

- **Modo opcional** - O utilizador dispõe de algumas opções para determinar os documentos Office que pretende proteger.
  - As opções *Guardar como* e *Guardar como protegido* estão ativadas - Se optar por proteger um documento do Office, selecione **Guardar como protegido**.
  - *Imprimir* e *Exportar* podem estar ativadas ou desativadas, consoante a política.
  - *Partilhar* (*Guardar e enviar* no Office 2010) está ativada.
  - **Documentos > pasta de Documentos seguros** - No modo opcional (mas não no modo de proteção forçada), uma pasta de Documentos seguros é adicionada à raiz da pasta de Documentos. Os documentos do Office nesta pasta estão encriptados. Se remover um documento do Office protegido desta pasta, o documento mantém-se encriptado. Se mudar o nome da pasta, o conteúdo da pasta com o novo nome é encriptado. Se eliminar a pasta, a mesma é recriada.
- **Modo de proteção forçada** - A sua empresa exige um maior nível de segurança.
  - A opção *Guardar como* está desativada e *Guardar como protegido* está ativada - Deve guardar todos os documentos do Office no modo protegido.
  - *Imprimir* e *Exportar* podem estar ativadas ou desativadas, com base na política.
  - *Partilhar* (*Guardar e enviar* no Office 2010) está desativada.

    **NOTA:**
    Com o modo de proteção forçada, a política também define períodos específicos de varrimento do computador para localizar todos os ficheiros do Office desprotegidos e alterar o respetivo modo para Protegido. Para que o Data Guardian possa varrer todos os ficheiros do Office desprotegidos, tem de ter sessão iniciada e ligação à rede.

- Se selecionar **Guardar como protegido**, a única opção no campo *Guardar como tipo* é *Office protegido*.

- **Ficheiro > Informações** varia, por exemplo:
  - Tanto no modo opcional como no modo de proteção forçada: é apresentada a opção *Adicionar restrição de data*, se o seu administrador tiver ativado essa política. Consulte Melhorar a segurança adicionando restrições de data.
  - Tanto no modo opcional como no modo de proteção forçada: as informações sobre as Propriedades deste documento do Office, como o autor e data, estão ocultas para maior segurança.

- Estado Só de leitura: consulte abaixo para obter mais informações.

  **NOTA:**
  A opção *Proteger documento* em Ficheiro > Informações refere-se ao Microsoft Office e não ao modo protegido do Data Guardian.

Se abrir um documento do Office e este indicar o modo só de leitura, verifique o seguinte:

- Se a opção *Guardar como protegido* não for apresentada no painel esquerdo, o modo só de leitura não está relacionado com as políticas do Data Guardian.
- Se o seu administrador definir políticas para o modo de proteção forçada, com um maior nível de segurança, os documentos do Office desprotegidos abrem em modo só de leitura.

  **NOTA:**
  Para o OneDrive, se abrir um documento do Office protegido através de **Ficheiro > Abrir > OneDrive** e o documento for só de leitura, confirme se instalou e configurou o cliente de sincronização OneDrive.

# Trabalhar com opções do menu Ficheiro

Esta tabela apresenta as opções do menu Ficheiro para documentos do Office. Dependendo do nível de segurança, algumas opções encontram-se desativadas.

**NOTA:**
Atualmente, os documentos do Office incorporados não são compatíveis com o modo Office protegido.

| Menu Ficheiro | Modo opcional e documentos do Office protegidos | Modo de proteção forçada para protegidos e desprotegidos |
|---|---|---|
| **Abra** | **Os ficheiros abrem como de costume** | **Os documentos sem proteção são abertos no modo só de leitura.** |
| **Guardar** | • Opções:<br>Documento já protegido - É guardado como protegido.<br>Desprotegido - É guardado como desprotegido.<br>Para protegê-lo, clique em **Guardar como protegido**.<br>• Documento só de leitura - Uma caixa de diálogo indica que não é possível guardar um documento desprotegido. A janela Guardar como abre-se e terá de guardá-lo com um nome de ficheiro diferente.<br>• Ficheiro xen - Pode abrir e guardá-lo no modo protegido, mas o ficheiro .xen será removido da nuvem. O documento Office tem a extensão habitual, mas está protegido.<br>**NOTA:**<br>**Na unidade virtual, se clicar com o botão direito do rato para criar um novo documento Office, este é um ficheiro .xen. Deve guardá-lo manualmente como protegido.** | • O documento está protegido.<br>• Documento só de leitura - Pode editá-lo, mas não é possível guardar o original. Quando clicar em Guardar, a janela Guardar como protegido abre-se e terá de guardá-lo no modo protegido com um novo nome.<br>• Documentos remotos - se abrir um documento que não esteja protegido numa localização remota, tem de guardá-lo na sua unidade local para poder modificar e guardar esse documento. Não é possível guardar na localização remota.<br>**NOTA:**<br>**Clicar em Guardar abre uma janela Guardar como e a única opção no campo Guardar como tipo é Office protegido (Documentos, Apresentação ou Livro).**<br>• Ficheiro .xen - Pode abrir e guardá-lo no modo protegido, mas o ficheiro .xen será removido da nuvem. O documento Office tem a extensão habitual, mas está protegido. |
| **Guardar como** | **Tem as opções padrão (mas não o modo protegido)** | **Desativado** |
| **Guardar como protegido** | **A única opção no campo Guardar como tipo é Office protegido** | **A única opção no campo Guardar como tipo é Office protegido** |
| **Imprimir** | **Pode ser ativado ou desativado com base nas políticas definidas pelo seu administrador. Se a opção do menu estiver ativada, uma política poderá colocar uma marca de água (com o nome do utilizador, o nome do domínio e a ID do computador) em cada página que imprimir.** | **Dependendo da política, esta opção poderá estar ativada ou desativada.**<br>**Se a opção do menu estiver ativada, uma política poderá colocar uma marca de água (com o nome do utilizador, o nome do domínio e a ID do computador) em cada página que imprimir.** |
| **Partilhar** | **Ativada** | **Desativado** |
| **Guardar e enviar (Office 2010)** | **Ativada** | **Desativado**<br>**Se a opção Imprimir estiver ativada, pode selecionar Imprimir para imprimir o documento em formato PDF.** |
| **Exportar (Office 2013 e versões superiores)** | **Pode ser ativado ou desativado com base nas políticas definidas pelo seu administrador.** | **Pode ser ativado ou desativado com base nas políticas definidas pelo seu administrador.** |
| **Exportar protegido**<br>(Office 2013 e versões superiores) | Se a opção do menu Exportar estiver desativada e a Exportação protegida estiver ativada, o documento exporta com uma marca de água (com o nome do utilizador, o nome do domínio e a ID do computador) em cada página.<br>**NOTA:**<br>Se exportar um documento em modo protegido para um utilizador externo, este pode abrir e visualizar o documento, mas não o pode exportar ou imprimir. | Se a opção do menu Exportar estiver desativada e a Exportação protegida estiver ativada, o documento exporta com uma marca de água (com o nome do utilizador, o nome do domínio e a ID do computador) em cada página.<br>**NOTA:**<br>Se exportar um documento em modo protegido para um utilizador externo, este pode abrir e visualizar o documento, mas não o pode exportar ou imprimir. |

**Trabalhar online com documentos do Office protegidos**

Ao criar documentos do Office protegidos, o ideal é trabalhar online, pois são geradas chaves para esses documentos. Se o seu computador necessitava de ter a imagem recriada e criou documentos do Office protegidos offline, certifique-se de que informa o seu administrador.

**Trabalhar online com documentos com permissão para macros protegidos**

Num documento com permissão para macros protegido, a macro existe mas está bloqueada. No entanto, atualmente, o Data Guardian apenas consegue controlar um documento com permissão para macros após o documento recentemente protegido (.docm, .pptm, .xlsm) ser fechado e aberto novamente. Além disso, se guardar um documento protegido com uma macro como desprotegido, é necessário fechar e voltar a abrir o documento, para que a macro seja executada.

**Anexar um documento do Office protegido a um e-mail do Outlook**

Quando anexar um documento do Office protegido a um e-mail do Outlook, selecione **Inserir** em vez de *Inserir como texto*. A opção *Inserir como texto* cola o conteúdo do documento diretamente no corpo do e-mail e o conteúdo deixa de estar protegido.

**Solução de problemas para o modo opcional**

Se em Ficheiro > Informações, a opção Imprimir estiver desativada, uma política do Data Guardian desativou a impressão para os documentos do Office protegidos. Atualmente, contudo, quando clica com o botão direito sobre um ficheiro do Office protegido no Explorador do Windows, a opção Imprimir não está desativada. No entanto, se selecionar Imprimir, ocorre o seguinte:

- Word - Uma caixa de diálogo indica que o Word deixou de funcionar.
- Excel - Uma caixa de diálogo indica que a opção Imprimir foi desativada pela política.
- Powerpoint - Uma caixa de diálogo indica que a opção Imprimir foi desativada pela política. Se clicar em OK, é impressa uma página de rosto a indicar que o documento está protegido.

# Determinar que documentos no modo opcional estão protegidos

Se tiver o modo de proteção forçada, todos os documentos do Office estão protegidos. Se tiver o modo opcional e pretender confirmar se um documento está protegido ou não, abra o documento e verifique se é apresentado como protegido na barra de título.

# Opções do menu adicionais para documentos do Office protegidos

O tipo de documento do Office, protegido ou desprotegido, pode afetar os seguintes pontos.

***Clique com o botão direito > Proteger***

Pode clicar com o botão direito num documento do Office e selecionar **Proteger**. Tem de adicionar conteúdo para que a opção do menu seja apresentada. Não é possível proteger um documento em branco.

***Propriedades do ficheiro > Separador do Dell Data Guardian***

Com documentos do Office protegidos, pode clicar com o botão direito e selecionar **Propriedades** e é apresentado um separador do **Dell Data Guardian** com informações, como a ID da chave do ficheiro e dados de acesso e embargo.

***Colar***

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

- Pode copiar e colar dados no documento protegido original.
- Não é possível copiar ou colar a partir de um documento protegido para um documento desprotegido. Não é apresentado qualquer conteúdo na Área de transferência e uma mensagem empresarial específica indica que não é possível colar no documento desprotegido ou não gerido.

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

***Arrastar e largar no modo protegido***

Pode arrastar e largar conteúdo num documento Word protegido. Atualmente, arrastar e largar estão desativadas em ficheiros PowerPoint e Excel protegidos.

***Imprimir para envelopes e etiquetas***

Se o seu administrador tiver definido uma política para adicionar uma marca de água quando imprime um documento do Office protegido, siga estes passos para imprimir envelopes ou etiquetas:

1 Num documento Word, selecione o separador **Correio**.

2 Selecione a opção **Envelopes** ou **Etiquetas**.

3 Depois de introduzir o endereço ou o endereço do remetente, clique em **Imprimir**.

> **NOTA: Se utilizar outra opção para imprimir e o seu administrador tiver definido uma política para adicionar uma marca de água em documentos do Office impressos, será apresentada uma marca de água no seu envelope ou etiqueta.**

# Adulteração e documentos do Office protegidos

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

Se um utilizador interno adulterar um documento do Office protegido:

- O Data Guardian consegue reparar e restaurar alguns dos elementos adulterados.
- Nas formas de adulteração que não possam ser reparadas, pode ser apresentada uma caixa de diálogo a indicar que o ficheiro foi adulterado e que deve entrar em contacto com o seu administrador.

Se um utilizador não autorizado abrir um documento do Office protegido, é apresentada apenas a página de rosto. Se o utilizador não autorizado modificar a página de rosto, o Data Guardian restaura a página de rosto quando um utilizador autorizado a guardar novamente como protegida.

# Utilizadores externos e documentos do Office protegidos

**Melhorar a segurança adicionando restrições de data**

Com o Data Guardian, carrega um documento do Office protegido para a nuvem e partilha-o:

- Todos os utilizadores internos do Data Guardian o podem visualizar.
- Com base na política, os utilizadores externos podem visualizá-lo.

Opcionalmente, para uma maior segurança com utilizadores externos, pode adicionar uma restrição de data para limitar o tempo durante o qual um utilizador externo pode visualizar um documento do Office protegido.

1 Selecione **Ficheiro > Informações > Restrição de data**.

2 A partir da lista pendente, selecione a data e hora de Início e Fim em que um utilizador externo poderá visualizar o documento.

> **NOTA:**
> A data e hora de Início pode ser futura se pretender enviar o documento, mas evitar que o utilizador externo o veja antes da data e hora especificada.

3 Clique em **OK**.
O documento é guardado, protegido, fechado e, em seguida, aberto novamente.

> **NOTA:**
> Se modificar as datas de um documento do Office desprotegido e, em seguida, clicar em Cancelar, o Data Guardian protege o ficheiro.

> **NOTA:**
> Atualmente, quando adiciona restrições de data a documentos do Office protegidos e planeia guardá-los numa unidade de rede, tem de guardar o ficheiro localmente e depois copiá-lo para a rede.

Se um utilizador externo abrir um ficheiro após o intervalo de data e hora especificado, é apresentada uma caixa de diálogo a indicar que o ficheiro tem restrições de acesso e que o utilizador externo pode contactar o autor do ficheiro. A caixa de diálogo não apresenta quaisquer datas ao utilizador externo.

Se definir o campo da data de Início para uma data ou hora futura e o utilizador externo abrir o ficheiro antes dessa data e hora, é apresentada uma caixa de diálogo a indicar que não é possível abrir o ficheiro antes dessa data e hora devido a restrições de acesso.

# Trabalhar sem uma ligação à Internet

Sem uma ligação à Internet, poderá continuar a visualizar ficheiros de sincronização na nuvem na sua unidade local através do Explorador de ficheiros. No entanto, a Unidade virtual DDG VDisk não é apresentada. Além disso, as alterações não serão sincronizadas na nuvem enquanto não estabelecer uma ligação à Internet.

# Limite de caracteres para nomes de caminhos de pastas

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

Na Nuvem, esse limite não existe. Assim, pode criar pastas e subpastas com um nome de caminho que ultrapasse esse limite. No entanto, localmente, no Windows, se quaisquer nomes de caminhos ultrapassarem esse limite, as pastas não são criadas. Por conseguinte, certifique-se de que limita os nomes de caminhos de pastas e subpastas a 248 caracteres.

# Dropbox para empresas

O DropBox for Business tem requisitos específicos. Consulte Instalar um cliente de sincronização na nuvem.

## Ajuda do fornecedor de armazenamento na nuvem

Antes de utilizar o Data Guardian, recomendamos que procure obter mais informações sobre o fornecedor de armazenamento na nuvem. O Apoio Técnico do DropBox for Business encontra-se em:

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

Embora possa carregar ficheiros para o website do fornecedor de armazenamento na nuvem, a melhor prática é trabalhar com as pastas e ficheiros na Unidade virtual DDG VDisk.

## Ligar o Data Guardian e o Dropbox for Business

Se a sua empresa utiliza o Dropbox for Business, tem de permitir que o Data Guardian permaneça ligado.

Para ligar:

1. No tabuleiro do sistema, clique no ícone do Data Guardian e, em seguida, selecione **Dropbox > Ligar**.
2. Na janela Autenticação do Dropbox, leia as informações e, em seguida, clique em **Seguinte**.
3. Se tem a sua conta empresarial e a pessoal do Dropbox associadas, ser-lhe-á pedido para selecionar uma delas. Deve selecionar a sua conta empresarial.
4. Na janela seguinte, para permitir o acesso do Data Guardian aos seus ficheiros e pastas no Dropbox, clique em **Permitir**.
5. Clique em **Concluir**.

# Configurar sincronização seletiva para pastas

Para sincronizar pastas seletivamente:

1 No tabuleiro do sistema, clique no ícone do **Dropbox for Business**.
2 Clique no ícone **Definições** e selecione **Preferências**.
3 Clique no separador **Conta** e, em seguida, clique em **Sincronização seletiva**.
4 Selecione apenas as pastas ou subpastas que desejar sincronizar no seu computador.
5 Clique em **Update** (Atualizar).
6 Na caixa de diálogo de confirmação de Atualização, clique em **OK**.
7 Na janela Preferências do Dropbox, clique em **OK**.
Um pop-up indica na bandeja do sistema que pastas estão a ser sincronizadas.

A sua empresa irá determinar se apenas pode ter uma conta empresarial ou se pode utilizaram ambas as pastas empresarial e pessoal. Se pretende pastas preexistentes, com dados ou ficheiros pessoais que não necessitam de ser encriptados, anule a seleção dessas pastas antes de instalar o Data Guardian. Caso contrário, os seus dados pessoais poderão ficar encriptados.

# Utilizar o ícone do DropBox for Business no tabuleiro do sistema

No tabuleiro do sistema, clique no ícone do Dropbox.

- Para o website - Selecione o ícone do Globo.

  **NOTA:**
  Se utiliza o Chrome ou o Firefox para abrir o Dropbox.com, certifique-se de que os fecha depois de terminar de trabalhar com os ficheiros e as pastas. Mesmo que abra um outro separador no navegador, o conteúdo será encriptado. Isto inclui e-mails, anexos ou carregamentos feitos com o navegador.

- Para a pasta - Selecione o ícone da pasta do Dropbox. Será reencaminhado para a Unidade virtual DDG VDisk.

# Utilize o menu de contexto do Dropbox para Empresas

No Explorador do Windows quando o Data Guardian está a ser instalado, o Dropbox for Business tem um menu de contexto.

**NOTA:**
Tem de ligar o Data Guardian ao Dropbox.

Para aceder ao menu de contexto, no Windows Explorer, abra a pasta Dropbox e clique com o botão direito num ficheiro. O ícone de nuvem tem as seguintes opções:

- Partilhar ligação segura do Dropbox
- Ver em Dropbox.com
- Ver versões anteriores

# Utilizar contas do Dropbox pessoais e para negócios

Se a sua empresa tem o DropBox for Business e também lhe permite ligar-se a uma conta pessoal do Dropbox com a sua conta para negócios, certifique-se de que entende as políticas estabelecidas pelo seu administrador para aquelas contas. Por exemplo, uma empresa pode estabelecer as seguintes políticas:

- Tanto os ficheiros empresariais como pessoais estão encriptados.

*ou*

- Apenas os ficheiros e pastas empresariais estão encriptados. Os ficheiros pessoais permanecem não encriptados.

  Por segurança, a sua empresa pode ter uma política de auditoria. Os nomes dos ficheiros na pasta pessoal são registados e enviados para o servidor do Dell Data Protection.

Se utiliza contas do Dropbox para profissionais e pessoais, não guarde ficheiros de negócios na sua pasta pessoal do Dropbox.

**Desencriptar pastas numa Conta Pessoal**

Se uma pasta pessoal for encriptada acidentalmente, o administrador pode conceder-lhe acesso temporário para que possa gerir a encriptação das suas pastas. Desmarque as pastas que devem ser desencriptadas. Além disso, pode remover pastas de sincronização desvinculando a conta ou não sincronizando pastas pessoais que devem permanecer não encriptadas.

# OneDrive for Business/ OneDrive unificado

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

**NOTA:**
A partilha de dados no OneDrive for Business não é suportada.

## Ajuda do fornecedor de armazenamento na nuvem

Antes de utilizar o Data Guardian, recomendamos que procure obter mais informações sobre o fornecedor de armazenamento na nuvem. O Apoio Técnico do OneDrive for Business encontra-se em:

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

Embora possa carregar ficheiros para o website do fornecedor de armazenamento na nuvem, a melhor prática é trabalhar com as pastas e ficheiros na Unidade virtual DDG VDisk.

## Configurar sincronização seletiva para pastas

Para sincronizar pastas seletivamente:

1. No tabuleiro do sistema, clique com o botão direito no ícone do **OneDrive for Business/ OneDrive unificado** e clique em **Sincronizar uma nova biblioteca**.
2. Introduza o URL da sua biblioteca.
3. Selecione **Sincronizar agora**.
4. Selecione **Mostrar os meus ficheiros**.

## Utilizar o ícone do OneDrive for Business no tabuleiro do sistema

No tabuleiro do sistema:

- Para o website - Clique com o botão direito e selecione **Ir para OneDrive.com**.
- Para a pasta - Clique com o botão direito ou esquerdo e selecione **Abrir a sua pasta OneDrive for Business**. Esta opção redireciona-o para a Unidade virtual DDG VDisk.

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

O Dell Data Guardian encripta pastas e ficheiros para tornar os dados seguros. Uma vez que o Data Guardian funciona com clientes de sincronização, tenha em atenção estas considerações.

- Durante as transferências, não selecione Cancelar. Caso contrário, provocará um erro. Se pretender eliminar o ficheiro, aguarde pela conclusão da transferência.
- Para o Windows 8.1, o Microsoft OneDrive possui ficheiros marcadores de posição que aparentam existir no cliente de sincronização, mas que não são realmente transferidos. Por conseguinte, o Dell Data Guardian não os pode encriptar. Se abrir um ficheiro marcador de posição, o Data Guardian apresenta uma caixa de diálogo a indicar que o ficheiro não será protegido. Pode clicar com o botão direito e selecionar **Transferir** e, em seguida, o **Data Guardian** converte-o num ficheiro .xen.

# DropBox

## Ajuda do fornecedor de armazenamento na nuvem

Antes de utilizar o Data Guardian, recomendamos que procure obter mais informações sobre o fornecedor de armazenamento na nuvem. O Apoio Técnico do Dropbox encontra-se em https://www.dropbox.com/help.

Embora possa criar ficheiros na nuvem ou carregar ficheiros para o site do fornecedor de armazenamento na nuvem, o ideal é trabalhar com as pastas e ficheiros na Unidade virtual DDG VDisk.

**NOTA:**
Com o Dropbox e o Data Guardian, se criar um ficheiro do Office na nuvem e o sincronizar a partir dessa localização, o mesmo é encriptado como um ficheiro .xen. Por conseguinte, na unidade virtual, o ficheiro abre em modo só de leitura. Não é possível editá-lo.

Se eliminar todas as pastas na unidade virtual, os ficheiros serão eliminados, mas é possível que as pastas não desapareçam. Se isso acontecer, elimine as pastas na nuvem.

## Configurar sincronização seletiva para pastas

Para sincronizar pastas seletivamente:

1. No tabuleiro do sistema, clique no ícone do **Dropbox**.
2. Clique no ícone **Definições** e selecione **Preferências**.
3. Clique no separador **Conta** e, em seguida, clique em **Sincronização seletiva**.
4. Selecione apenas as pastas ou subpastas que desejar sincronizar no seu computador.
5. Clique em **Update** (Atualizar).
6. Na caixa de diálogo de confirmação de Atualização, clique em **OK**.
7. Na janela Preferências do Dropbox, clique em **OK**.
   Um pop-up indica na bandeja do sistema que pastas estão a ser sincronizadas.

## Utilizar o ícone do Dropbox no tabuleiro do sistema

No tabuleiro do sistema, clique no ícone do Dropbox.

- Para o website - Selecione o ícone do Globo.

**NOTA:**
Se utiliza o Chrome ou o Firefox para abrir o Dropbox.com, certifique-se de que os fecha depois de terminar de trabalhar com os ficheiros e as pastas. Mesmo que abra um outro separador no navegador, o conteúdo será encriptado. Isto inclui e-mails, anexos ou carregamentos feitos com o navegador.

- Para a pasta - Selecione o ícone da pasta do Dropbox. Será reencaminhado para a Unidade virtual DDG VDisk.

## Considerações de segurança com o Data Guardian e o Dropbox

Se estiver a trabalhar numa máquina virtual, não arraste ficheiros do ambiente de trabalho do servidor para o navegador. O ficheiro não ficará protegido. Execute uma das seguintes ações: no browser, utilize a opção Carregar ou, no ambiente de trabalho, arraste o ficheiro para a Unidade virtual DDG VDisk.

## Perguntas mais frequentes sobre o Dropbox

**Pergunta**

A minha conta do Dropbox tem muitos ficheiros em conflito. Os ficheiros continuam a ser criados, mesmo depois de os eliminar da nuvem

***Resposta***

Por vezes, quando uma pasta já foi partilhada e, em seguida, são ativadas várias contas do Data Guardian ao mesmo tempo, estes ficheiros são vistos como tendo sido criados ao mesmo tempo. Num esforço para preservar o original, o Dropbox cria vários ficheiros com o mesmo nome e tipo e coloca-os na nuvem. Por conseguinte, o Data Guardian irá permitir que todos os ficheiros sejam criados sem interferir.

***Solução***

1 Todos os que estão a partilhar o ficheiro devem colaborar na desmarcação da pasta para sincronização a partir da aplicação do Dropbox. Consulte Dropbox for Business.
2 Depois de todos os ficheiros e pastas terem sido removidos de cada computador local, o utilizador deve aceder à nuvem e eliminar os ficheiros duplicados.

Em seguida, cada pessoa pode utilizar a sincronização seletiva para adicionar novamente a pasta a sincronizar.

# Box

## Ajuda do fornecedor de armazenamento na nuvem

Antes de utilizar o Data Guardian, recomendamos que procure obter mais informações sobre o fornecedor de armazenamento na nuvem. O Apoio Técnico do Box encontra-se em https://support.box.com/home.

Embora possa carregar ficheiros para o website do fornecedor de armazenamento na nuvem, a melhor prática é trabalhar com as pastas e ficheiros na Unidade virtual DDG VDisk.

**NOTA:**
Se utilizar o Internet Explorer para transferir ficheiros para o fornecedor de armazenamento na nuvem do Box ou abrir um ficheiro, pode ocorrer um atraso na janela do Explorador de ficheiros.

**NOTA:**
O Box Tools e o Box Edit não são suportados pelo Data Guardian. Utilizar o Box Tools pode provocar uma condição de ecrã azul.

# Configurar sincronização seletiva para pastas

Para sincronizar pastas seletivamente:

1 No tabuleiro do sistema, clique com o botão direito no ícone do Box e selecione **Abrir o website do Box**.

2 No website do cliente de sincronização na nuvem, clique com o botão direito numa pasta e selecione **Sincronizar pasta com o computador**.

3 Na janela Pasta de sincronização, clique em **Pasta de sincronização**.

O ícone do tabuleiro do sistema indica que estão a ser aplicadas definições. Isto poderá demorar vários minutos.

4 Quando terminar, navegue até **Explorador do Windows** > **Box Sync**. As pastas sincronizadas são exibidas com uma marca de verificação.

# Utilizar o ícone do Box no tabuleiro do sistema

No tabuleiro do sistema, clique com o botão direito do rato no ícone do Box.

- Para o website - Selecione **Abrir o website do Box**.
- Para a pasta - Selecione **Abrir pasta Box Sync**. Esta opção redireciona-o para a Unidade virtual DDG VDisk.

# Perguntas frequentes sobre o cliente de sincronização do Box

**Pergunta**

Estou a utilizar o cliente de sincronização do Box. Criei uma nova pasta localmente e adicionei alguns ficheiros. O cliente de sincronização parece estar a funcionar, mas nada foi criado na nuvem.

***Resposta***

O cliente de sincronização do Box poderá necessitar de algum tempo para recolher a informação sobre as novas pastas e ficheiros. O processo pode demorar vários minutos, em comparação com outros clientes de sincronização. Certifique-se de que aguarda vários minutos até o cliente de sincronização estar concluído antes de criar novas pastas ou ficheiros.

**Pergunta**

Estou a utilizar o cliente de sincronização do Box. Fiquei sem espaço na partição primária e movi-o para outra unidade. Agora, a pasta Os meus ficheiros no Box tem uma ou mais pastas adicionais criadas e com o nome **Nova pasta**.

***Resposta***

Atualmente, quando os ficheiros estão a ser sincronizados entre dois computadores para a mesma partilha de ficheiros, se uma pessoa mover essa pasta para outra localização, todas as novas pastas criadas por outras pessoas nessa partilha de ficheiros criarão uma pasta vazia com o nome **Nova pasta**.

***Solução***

Elimine diretamente a Nova pasta da nuvem. Esta será removida de todos os sistemas que estão a partilhar essa pasta.

# Considerações de segurança com o Data Guardian e o Box

Se criar um ficheiro no website do Box Cloud, será sincronizado. No entanto, será transferido como ficheiro encriptado.

O Internet Explorer pode provocar um atraso ao carregar ou abrir no Box.

# Google Drive

## Ajuda do fornecedor de armazenamento na nuvem

Antes de utilizar o Data Guardian, recomendamos que procure obter mais informações sobre o fornecedor de armazenamento na nuvem. O Apoio Técnico do Google Drive encontra-se em https://support.google.com/drive/?hl=en#topic=14940.

Embora possa carregar ficheiros para o website do fornecedor de armazenamento na nuvem, a melhor prática é trabalhar com as pastas e ficheiros na Unidade virtual DDG VDisk.

## Configurar sincronização seletiva para pastas

Para sincronizar pastas seletivamente:

1 No tabuleiro do sistema, clique no ícone do **Google Drive**.
2 Selecione o ícone de Definições.
3 Selecione **Preferências**.
4 Para realizar uma sincronização seletiva, clique em **Apenas estas pastas**.
5 Anule a seleção das caixas de verificação de pastas que não necessitam de proteção na nuvem.
6 Clique em **Aplicar**.
7 Para confirmar, clique em **Continuar**.

## Utilizar o ícone do Google Drive no tabuleiro do sistema

No tabuleiro do sistema, clique no ícone do Google Drive.

- Para o website - Selecione **Visitar o Google Drive na Web**.
- Para a pasta - Selecione a pasta **Abrir Google Drive**. Esta opção redireciona-o para a Unidade virtual DDG VDisk

## Considerações de segurança com o Data Guardian e o Google Drive

O Data Guardian encripta pastas e ficheiros para proteger os dados. Uma vez que o Data Guardian funciona com clientes de sincronização, tenha em atenção estas considerações.

- A política de segurança da empresa proíbe a utilização do Google Docs com o Data Guardian. Quando instala o Data Guardian, uma caixa de diálogo informa-o desta política. Para obter mais informações, contacte o seu administrador de TI.

  O Google Drive inclui uma aplicação Google Docs que permite aos utilizadores colaborarem em documentos, em tempo real. No entanto, a colaboração ocorre num servidor Google e os ficheiros não são encriptados. Para Windows e Data Guardian, todos os Google Docs que criar são apresentados nas suas pastas de cliente de sincronização Google Docs.

  No entanto, se abrir a pasta, uma caixa de diálogo avisa-o de que o Data Guardian não pode encriptar esse documento. Além disso, para garantir a proteção dos dados, o seu administrador pode executar relatórios para identificar os Google Docs que estão a ser sincronizados, para ajudar a garantir a segurança.
- As opções do Google Drive contêm **Remover** (remove para o lixo) e **Eliminar**. O Google Drive com Data Guardian apenas contém Eliminar, para ser consistente com outras funcionalidades do Data Guardian.

**NOTA:**
Se eliminar vários ficheiros a partir da unidade virtual do Data Guardian e alguns continuarem a aparecer no browser ou na linha de comando, elimine-os no browser ou a partir da linha de comando.

- Com o Google Drive, poderá receber uma mensagem a avisar que as propriedades são desmontadas ao copiar ficheiros para a Unidade virtual DDG VDisk. Estes são atributos de segurança.

# OneDrive

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

## Ajuda do fornecedor de armazenamento na nuvem

Antes de utilizar o Data Guardian, recomendamos que procure obter mais informações sobre o fornecedor de armazenamento na nuvem. Apoio técnico do OneDrive em http://windows.microsoft.com/en-us/onedrive/onedrive-help#onedrive=other.

Embora possa carregar ficheiros para o website do fornecedor de armazenamento na nuvem, a melhor prática é trabalhar com as pastas e ficheiros na Unidade virtual DDG VDisk.

## Configurar sincronização seletiva para pastas

Para sincronizar pastas seletivamente:

1. No tabuleiro do sistema, clique com o botão direito do rato no ícone do **OneDrive** e clique em **Definições**.
2. Selecione o separador **Selecionar pastas** e, em seguida, clique em **Selecionar pastas**.
3. Em seguida, selecione **Selecionar pastas para sincronizar**.
4. Uma lista de pastas é exibida. Selecione ou desmarque as caixas de verificação para sincronizar aquelas pastas. Clique em **OK**.
5. Clique em **OK**.
6. O ícone do tabuleiro do sistema indica que estão a ser aplicadas definições. Isto poderá demorar vários minutos.
7. Quando terminar, navegue até **Explorador do Windows** > **OneDrive**. As pastas sincronizadas são exibidas com uma marca de verificação.

## Utilizar o ícone do OneDrive no tabuleiro do sistema

No tabuleiro do sistema:

- Para o website - Clique com o botão direito e selecione **Ir para OneDrive.com**.
- Para a pasta - Clique com o botão direito ou esquerdo e selecione **Abrir a sua pasta OneDrive**. Esta opção redireciona-o para a Unidade virtual DDG VDisk.

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

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

# Compreender os itens de menu do tabuleiro do sistema do Data Guardian

Ecrã de detalhes

O Ecrã de detalhes do Data Guardian fornece informações úteis, como por exemplo:

- Para obter suporte técnico, pode fornecer informações de estado ou da versão.
- Para visualizar o nome de um ficheiro não oculto associado a um ficheiro .xen, selecione **Ficheiros** > **Estado do ficheiro**.
- Para procurar por um nome de ficheiro, seleccione Copiar no lado direito inferior e cole o conteúdo num ficheiro Word.
- Para ver quem é o proprietário de uma pasta, seleccione Pastas e percorra o texto até à coluna PROPRIETÁRIO DA PASTA.

Para aceder ao ecrã Detalhes:

Clique no ícone do tabuleiro do sistema do **Data Guardian** e, em seguida, clique em **Detalhes...**

O canto superior esquerdo do ecrã Detalhes apresenta as seguintes informações:

**Estado do serviço**: estado do Serviço Windows do Data Guardian. Os valores são: Parado, StartPending, StopPending, Em execução, ContinuePending, PausePending, Em pausa

**Estado de execução**: o estado de ativação do dispositivo. Os valores são: Activo, A Reactivar, Suspenso, A Suspender

**Modo de utilizador**: Utilizador interno - um utilizador dentro deste endereço de domínio

**Utilizador externo** - um utilizador fora deste endereço de domínio

**E-mail de registo**: para utilizadores internos, este é o endereço de e-mail do domínio. Para utilizadores externos, este é o endereço de e-mail para o qual os utilizadores estão registados.

**URL do servidor**: o DDP EE Server/VE Server que comunica com este cliente.

**Data da última modificação da política**: data e hora em que a política foi modificada pela última vez e utilizada pelo cliente.

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

A área **Ficheiros** do ecrã Detalhes apresenta as seguintes informações:

**Nome**: nome do ficheiro

**Nuvem**: indica o nome de ficheiro oculto ou se o ficheiro está *Desprotegido*.

**Estado do ficheiro**: este valor indica o proprietário da pasta. O valor é determinado pela ID da chave.

**Estado de processamento**: indica se o ficheiro necessita de uma chave ou se está *Concluído*.

**Empresa**: indica o servidor predefinido. Se a mensagem *Erro: chave não pertencente ao seu servidor* for apresentada nesta coluna, a chave não pertence ao servidor da sua empresa. A chave de um ficheiro encriptado deve pertencer ao servidor da sua empresa.

**Chave**: ID da chave atribuída a essa pasta (os ficheiros novos utilizam esta chave para encriptação).

**Pasta**: o nome do caminho completo da pasta.

**Última modificação**: a data de modificação do ficheiro.

**Estado de persistência**: indica se o ficheiro se encontra no disco.

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

**Browser criado**: *Verdadeiro* ou *Falso*.

Para visualizar os ficheiros de registo, no canto inferior esquerdo do ecrã Detalhes, clique em **Ver registo**.

**NOTA:**
Os ficheiros de registo estão também disponíveis em **C:\ProgramData\Dell\Dell Data Protection\Dell Data Guardian.**

A área **Pastas** do ecrã Detalhes apresenta as seguintes informações:

**Nome**: nome da pasta

**Chave**: ID da chave atribuída a essa pasta (os ficheiros novos utilizam esta chave para encriptação).

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

**Proprietário da pasta**: este valor indica o proprietário da pasta. O valor é determinado pela ID da chave.

**Substituir**: as opções são *Nenhum* e *Preexistente*. Os ficheiros preexistentes não estão protegidos. Além disso, se aceder à Gestão de pastas e desproteger alguns ficheiros, esta coluna indica que os mesmos não estão protegidos.

**Tipo de ocultação**: se a sua empresa gerir o seu armazenamento na nuvem, esta é uma política definida em cada pasta que indica que tipo de ficheiros .xen é criado na nuvem. Esta é uma política definida pelo seu administrador. Caso o seu administrador selecione *Apenas extensão*, será exibido o nome real do ficheiro com a extensão ".xen". Caso o seu administrador selecione *Guid*, será exibido um nome de ficheiro codificado com a extensão ".xen". Esta é uma definição de política aplicada apenas a novas pastas. A predefinição é *Apenas extensão*.

# Menu Gerir pastas

Alguns gestores ou administradores podem ter de efetuar temporariamente a solução de problemas de pastas partilhadas por mais do que um utilizador. Pode solicitar permissão ao seu administrador para a opção Gerir pastas. Normalmente, esta é uma opção temporária.

# Verificar actualizações de política

Se o seu administrador modificar uma política e o notificar de uma atualização de política, aceda ao tabuleiro do sistema do Windows, clique no ícone **Dell Data Protection | Data Guardian** e selecione **Verificar atualizações de política**.

Se o seu administrador modificar uma política para proteger ficheiros criados no Microsoft Word, é necessário fechar o Word para que essa atualização seja aplicada.

# Localizar ficheiros de registo

Para a solução de problemas, o seu administrador pode solicitar ficheiros de registo.

Para localizar ficheiros de registo:

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

**NOTA:**
Quando o Xendow.Service.log atinge 3 MB, é guardado como Xendow.Service1.log, e depois Xendow.Service2.log.

# Atualizar o Data Guardian

A melhor prática consiste em desinstalar a versão anterior e, e, em seguida, instalar a versão atual. Consulte Desinstalar o Data Guardian.

# Fornecer feedback à Dell

Se o seu administrador tiver ativado uma política de feedback, poderá fornecer feedback à Dell sobre este produto. O breve formulário inclui duas perguntas sobre o seu grau de satisfação, com escalas de classificação (onde 10 indica o mais alto grau de satisfação) e um campo para comentários.

Para aceder ao formulário, clique no ícone do Data Guardian no tabuleiro do sistema e selecione **Enviar feedback**.

Se esta funcionalidade não estiver ativada devido à política da empresa, a opção não será exibida.

# Possíveis problemas na ativação - Nuvem e Office protegido

Se tiver instalado o Data Guardian, mas o ícone do Data Guardian no tabuleiro do sistema não apresentar uma marca de verificação verde  , tenha em atenção o seguinte, consoante tenha encriptação na nuvem, Office protegido ou ambos:

- O acesso está bloqueado aos websites de sincronização na nuvem
- As aplicações de sincronização na nuvem estão bloqueadas para ligação aos respetivos serviços na Internet.
- As pastas sincronizadas locais não são atualizadas durante este período de tempo
- O Data Guardian pode converter documentos do Office existentes no modo protegido antes de proceder à ativação. Se for o caso, quando abrir um documento do Office, é apresentada uma página de rosto com informações sobre o processo de ativação.

Proceda da seguinte forma:

- Reinicie e volte a iniciar sessão com um sufixo UPN, por exemplo: nome_utilizador@domínio.com.
- Confirme com o seu administrador se deve ou não selecionar a caixa de verificação **Ativar verificação de confiança SSL** ao instalar o Data Guardian.
- Contacte o seu administrador de sistema quanto à configuração do seu computador para ativar manualmente. Consulte Ativar o Data Guardian.

# Ativar o Data Guardian

Normalmente, o Data Guardian ativa-se automaticamente depois da instalação e reinicialização. Se o seu administrador lhe indicar que deve proceder à ativação manual, siga os seguintes passos:

1 Inicie a sessão no Windows.
   No tabuleiro do sistema, é apresentado um ícone de proteção com um ponto de exclamação laranja.
2 Clique no ícone do **Data Guardian** no tabuleiro do sistema e selecione **Ativação do utilizador**.
3 Introduza o seu endereço de e-mail e palavra-passe do domínio e clique em **Ativar**.
   Se é um utilizador interno (com um endereço de e-mail do domínio), ignore o botão Registar. Apenas os utilizadores externos necessitam de se registar.

   Depois de concluída a ativação, uma marca de verificação verde é apresentada no ícone do tabuleiro do sistema do Data Guardian  .
4 Confirme o seu estado de modo de utilizador. Clique na ligação no tabuleiro de sistema e selecione **Detalhes**.

5 Na parte superior, confirme

**Interno**: um utilizador com um endereço de e-mail dentro do domínio da empresa.

**Externo**: um utilizador com um endereço de e-mail fora do domínio. Para obter mais informações, consulte Utilizar o Data Guardian como utilizador externo.

# Tarefas do utilizador - Office protegido sem encriptação na nuvem

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

**NOTA:**
Se a sua empresa também gerir o seu cliente de sincronização na nuvem, consulte Tarefas do utilizador - Encriptação na nuvem e Office protegido.

## Descrição geral das tarefas

Esta descrição geral resume a sequência de instalação e utilização do Data Guardian.

**Instalar o Data Guardian**

| Tarefa | Descrição | Para obter mais informações |
|---|---|---|
| Instalar o Data Guardian | Determinar o seguinte:<br><br>O utilizador tem de instalar o Data Guardian<br><br>O administrador já instalou o Data Guardian - continue para o passo seguinte. | Instalações pelo utilizador: consulte Instalar o Data Guardian no Windows. Reiniciar e continuar para o passo seguinte. |
| Confirmar o estado de ativação | Confirmar no tabuleiro do sistema se o ícone do Data Guardian tem uma marca de verificação verde  . | Se o ícone apresentar um ponto de exclamação laranja, consulte Possíveis problemas na ativação - Office protegido. |

**Utilizar o Data Guardian**

| Tarefa | Descrição | Para obter mais informações |
|---|---|---|
| Visualizar o menu do tabuleiro do sistema | Fornece informações úteis sobre ficheiros, pastas e resolução de problemas. | Compreender os itens de menu do tabuleiro do sistema do Data Guardian |
| Proteger documentos do Office e com permissão para macros, se a política estiver ativada | Proteger um documento do Office (.docx, .pptx, .xlsx, .docm, .pptm, .xlsm) no momento da sua criação. Está seguro quando o partilhar com outras pessoas ou quando o guardar num suporte de dados amovível. | Utilizar documentos do Office com o modo protegido do Data Guardian<br>• Observar as opções do menu Ficheiro para determinar o nível de segurança para documentos do Office<br>• Trabalhar com opções do menu Ficheiro |
| Partilhar uma pasta com outros para colaborar em ficheiros | Partilhar uma pasta com:<br><br>Utilizador interno (com um endereço de e-mail do domínio) | Utilizador interno - Consulte a ajuda online do seu fornecedor de armazenamento na nuvem.<br><br>Utilizador externo - Consulte Utilizar o Data Guardian como utilizador externo. |

| Tarefa | Descrição | Para obter mais informações |
|---|---|---|
| | Utilizador externo (com um endereço de e-mail fora do domínio) - trabalhe com o seu administrador. | |

**NOTA:**
Se ao abrir um documento do Office for apresentada uma página de rosto com informações de instalação ou ativação, o seu administrador poderá ter definido políticas para proteger os documentos do Office. Confirme se o Data Guardian está instalado e ativado. Consulte Possíveis problemas na ativação - Office protegido.

# Instalar o Data Guardian para o Office protegido

## Instalar o Data Guardian no Windows

Apenas um administrador local do computador tem permissão para instalar o Data Guardian.

O computador deve ter uma letra do alfabeto disponível para atribuir a uma unidade de disco.

Prepare-se para reiniciar o computador, assim que o Data Guardian estiver instalado.

1. Para transferir o instalador do Data Guardian, aceda à localização especificada pelo seu administrador.
2. Com base no seu sistema operativo, selecione o instalador de 32 bits ou de 64 bits, normalmente **setup32.exe** ou **setup64.exe**, e copie-o para o computador local.
3. Clique duas vezes no ficheiro para iniciar o programa de instalação.
4. Se for apresentado um aviso de segurança, clique em **Executar**.
5. Selecione um idioma e clique em **OK**.
6. Se aparecer uma mensagem a questionar se deseja instalar o Pacote redistribuível do Microsoft Visual C++ 2010 ou o Microsoft .NET Framework 4.0 Client Profile, clique em **OK**.
7. No ecrã de boas-vindas, clique em **Seguinte**.
8. Leia o contrato de licença, aceite os termos e condições e clique em **Seguinte**.
9. No ecrã Pasta de destino, clique em **Seguinte** para instalar na localização predefinida de **C:\Program Files\Dell\Dell Data Protection \Dell Data Guardian\.**

   Em **C:**, não instale o Data Guardian nas pastas Utilizadores ou Windows, nem na raiz de qualquer unidade. Nesse caso, é obtido um erro.
10. No campo *Nome do servidor:*, introduza o nome do servidor com o qual este computador vai comunicar, como, por exemplo, servidor.domínio.com. Não é necessário incluir web ou http(s). Esta informação é fornecida pelo seu administrador.

    Não desmarque a caixa de verificação *Ativar verificação de confiança SSL* exceto se tal for instruído pelo administrador.
11. Clique em **Seguinte**.
12. No ecrã Confirmar informações do servidor de ativação, certifique-se de que o endereço URL do servidor está correto. O instalador adiciona www ou http(s) e, de seguida, a porta. Clique em **Seguinte**.
13. Na janela Tipo de gestão, selecione esta opção:
    - Uso interno - Um utilizador com um endereço de e-mail dentro do domínio da empresa.
14. Clique em **Instalar** para dar início à instalação.

    Uma janela de estado apresenta o progresso da instalação.
15. Clique em **Concluir** quando for apresentado o ecrã de Instalação concluída.
16. Clique em **Sim** para reiniciar.

    A instalação do Data Guardian está concluída.
17. Depois de reiniciar, confirme no tabuleiro do sistema se o ícone do Data Guardian tem uma marca de verificação verde  .

# Utilizar documentos do Office com o modo protegido do Data Guardian

Para melhorar a segurança empresarial, o seu administrador pode ativar uma política para proteger ficheiros para as seguintes aplicações do Office:

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

Se uma pessoa não autorizada aceder a um ficheiro protegido, o ficheiro permanece encriptado quando, por exemplo:

- É enviado como anexo num e-mail
- É movido num browser - em alguns clientes de sincronização na nuvem, pode clicar com o botão direito do rato num nome de ficheiro e selecionar **Mover**.
- É partilhado na rede
- É carregado para um fornecedor de armazenamento na nuvem
- É guardado num suporte de dados amovível

Para documentos do Office, pode ser apresentada uma página de rosto com instruções para instalar ou ativar o Data Guardian, por exemplo:

- É necessário instalar o Data Guardian.
- É necessário ativar o Data Guardian.
- O utilizador abre um documento protegido do Office na nuvem.
- Transferiu um ficheiro do Office do seu computador que tem o Data Guardian para um dispositivo pessoal que não o tem.
- Um utilizador não autorizado acede a um dos seus ficheiros do Office - A página de rosto é apresentada com uma mensagem empresarial específica, mas o utilizador não consegue visualizar o conteúdo do ficheiro.

Se a sua empresa utilizar o modo protegido do Data Guardian, consulte:

- Observar as opções do menu Ficheiro para determinar o nível de segurança para documentos do Office
- Trabalhar com opções do menu Ficheiro
- Determinar que documentos no modo opcional estão protegidos
- Opções do menu adicionais para documentos do Office protegidos
- Utilizadores externos e documentos do Office protegidos

# Observar as opções do menu Ficheiro para determinar o nível de segurança para documentos do Office

Para determinar se o seu administrador ativou políticas do Data Guardian, abra um documento do Office e selecione **Ficheiro**. Se a opção *Guardar como protegido* for apresentada no painel esquerdo, tem proteção adicional em documentos do Office.

Para determinar o nível de segurança, verifique as opções ativadas ou desativadas:

- **Modo opcional** - O utilizador dispõe de algumas opções para determinar os documentos Office que pretende proteger.
  - As opções *Guardar como* e *Guardar como protegido* estão ativadas - Se optar por proteger um documento do Office, selecione **Guardar como protegido**.
  - *Imprimir* e *Exportar* podem estar ativadas ou desativadas, consoante a política.
  - *Partilhar* (*Guardar e enviar* no Office 2010) está ativada.
  - **Documentos > pasta de Documentos seguros** - No modo opcional (mas não no modo de proteção forçada), uma pasta de Documentos seguros é adicionada à raiz da pasta de Documentos. Os documentos do Office nesta pasta estão encriptados. Se

remover um documento do Office protegido desta pasta, o documento mantém-se encriptado. Se mudar o nome da pasta, o conteúdo da pasta com o novo nome é encriptado. Se eliminar a pasta, a mesma é recriada.

- **Modo de proteção forçada** - A sua empresa exige um maior nível de segurança.
  - A opção *Guardar como* está desativada e *Guardar como protegido* está ativada - Deve guardar todos os documentos do Office no modo protegido.
  - *Imprimir* e *Exportar* podem estar ativadas ou desativadas, com base na política.
  - *Partilhar* (*Guardar e enviar* no Office 2010) está desativada.

    **NOTA:**
    Com o modo de proteção forçada, a política também define períodos específicos de varrimento do computador para localizar todos os ficheiros do Office desprotegidos e alterar o respetivo modo para Protegido. Para que o Data Guardian possa varrer todos os ficheiros do Office desprotegidos, tem de ter sessão iniciada e ligação à rede.

- Se selecionar **Guardar como protegido**, a única opção no campo *Guardar como tipo* é *Office protegido*.

- **Ficheiro > Informações** varia, por exemplo:
  - Tanto no modo opcional como no modo de proteção forçada: é apresentada a opção *Adicionar restrição de data*, se o seu administrador tiver ativado essa política. Consulte Melhorar a segurança adicionando restrições de data.
  - Tanto no modo opcional como no modo de proteção forçada: as informações sobre as Propriedades deste documento do Office, como o autor e data, estão ocultas para maior segurança.
  - Estado Só de leitura: consulte abaixo para obter mais informações.

    **NOTA:**
    A opção *Proteger documento* em Ficheiro > Informações refere-se ao Microsoft Office e não ao modo protegido do Data Guardian.

Se abrir um documento do Office e este indicar o modo só de leitura, verifique o seguinte:

- Se a opção *Guardar como protegido* não for apresentada no painel esquerdo, o modo só de leitura não está relacionado com as políticas do Data Guardian.
- Se o seu administrador definir políticas para o modo de proteção forçada, com um maior nível de segurança, os documentos do Office desprotegidos abrem em modo só de leitura.

  **NOTA:**
  Para o OneDrive, se abrir um documento do Office protegido através de **Ficheiro > Abrir > OneDrive** e o documento for só de leitura, confirme se instalou e configurou o cliente de sincronização OneDrive.

# Trabalhar com opções do menu Ficheiro

Esta tabela apresenta as opções do menu Ficheiro para documentos do Office. Dependendo do nível de segurança, algumas opções encontram-se desativadas.

**NOTA:**
Atualmente, os documentos do Office incorporados não são compatíveis com o modo Office protegido.

| Menu Ficheiro | Modo opcional e documentos do Office protegidos | Modo de proteção forçada para protegidos e desprotegidos |
|---|---|---|
| **Abra** | **Os ficheiros abrem como de costume** | **Os documentos sem proteção são abertos no modo só de leitura.** |
| **Guardar** | • Opções:<br>Documento já protegido - É guardado como protegido.<br>Desprotegido - É guardado como desprotegido.<br>Para protegê-lo, clique em **Guardar como protegido**.<br>• Documento só de leitura - Uma caixa de diálogo indica que não é possível guardar um documento desprotegido. A janela Guardar como abre-se e terá de guardá-lo com um nome de ficheiro diferente.<br>• Ficheiro xen - Pode abrir e guardá-lo no modo protegido, mas o ficheiro .xen será removido da nuvem. O documento Office tem a extensão habitual, mas está protegido.<br>**NOTA:**<br>**Na unidade virtual, se clicar com o botão direito do rato para criar um novo documento Office, este é um ficheiro .xen. Deve guardá-lo manualmente como protegido.** | • O documento está protegido.<br>• Documento só de leitura - Pode editá-lo, mas não é possível guardar o original. Quando clicar em Guardar, a janela Guardar como protegido abre-se e terá de guardá-lo no modo protegido com um novo nome.<br>• Documentos remotos - se abrir um documento que não esteja protegido numa localização remota, tem de guardá-lo na sua unidade local para poder modificar e guardar esse documento. Não é possível guardar na localização remota.<br>**NOTA:**<br>**Clicar em Guardar abre uma janela Guardar como e a única opção no campo Guardar como tipo é Office protegido (Documentos, Apresentação ou Livro).**<br>• Ficheiro .xen - Pode abrir e guardá-lo no modo protegido, mas o ficheiro .xen será removido da nuvem. O documento Office tem a extensão habitual, mas está protegido. |
| **Guardar como** | **Tem as opções padrão (mas não o modo protegido)** | **Desativado** |
| **Guardar como protegido** | **A única opção no campo Guardar como tipo é Office protegido** | **A única opção no campo Guardar como tipo é Office protegido** |
| **Imprimir** | **Pode ser ativado ou desativado com base nas políticas definidas pelo seu administrador. Se a opção do menu estiver ativada, uma política poderá colocar uma marca de água (com o nome do utilizador, o nome do domínio e a ID do computador) em cada página que imprimir.** | **Dependendo da política, esta opção poderá estar ativada ou desativada.**<br>**Se a opção do menu estiver ativada, uma política poderá colocar uma marca de água (com o nome do utilizador, o nome do domínio e a ID do computador) em cada página que imprimir.** |
| **Partilhar** | **Ativada** | **Desativado** |
| **Guardar e enviar (Office 2010)** | **Ativada** | **Desativado**<br>**Se a opção Imprimir estiver ativada, pode selecionar Imprimir para imprimir o documento em formato PDF.** |
| **Exportar (Office 2013 e versões superiores)** | **Pode ser ativado ou desativado com base nas políticas definidas pelo seu administrador.** | **Pode ser ativado ou desativado com base nas políticas definidas pelo seu administrador.** |
| **Exportar protegido**<br>(Office 2013 e versões superiores) | Se a opção do menu Exportar estiver desativada e a Exportação protegida estiver ativada, o documento exporta com uma marca de água (com o nome do utilizador, o nome do domínio e a ID do computador) em cada página.<br>**NOTA:**<br>Se exportar um documento em modo protegido para um utilizador externo, este pode abrir e visualizar o documento, mas não o pode exportar ou imprimir. | Se a opção do menu Exportar estiver desativada e a Exportação protegida estiver ativada, o documento exporta com uma marca de água (com o nome do utilizador, o nome do domínio e a ID do computador) em cada página.<br>**NOTA:**<br>Se exportar um documento em modo protegido para um utilizador externo, este pode abrir e visualizar o documento, mas não o pode exportar ou imprimir. |

**Trabalhar online com documentos do Office protegidos**

Ao criar documentos do Office protegidos, o ideal é trabalhar online, pois são geradas chaves para esses documentos. Se o seu computador necessitava de ter a imagem recriada e criou documentos do Office protegidos offline, certifique-se de que informa o seu administrador.

**Trabalhar online com documentos com permissão para macros protegidos**

Num documento com permissão para macros protegido, a macro existe mas está bloqueada. No entanto, atualmente, o Data Guardian apenas consegue controlar um documento com permissão para macros após o documento recentemente protegido (.docm, .pptm, .xlsm) ser fechado e aberto novamente. Além disso, se guardar um documento protegido com uma macro como desprotegido, é necessário fechar e voltar a abrir o documento, para que a macro seja executada.

**Anexar um documento do Office protegido a um e-mail do Outlook**

Quando anexar um documento do Office protegido a um e-mail do Outlook, selecione **Inserir** em vez de *Inserir como texto*. A opção *Inserir como texto* cola o conteúdo do documento diretamente no corpo do e-mail e o conteúdo deixa de estar protegido.

**Solução de problemas para o modo opcional**

Se em Ficheiro > Informações, a opção Imprimir estiver desativada, uma política do Data Guardian desativou a impressão para os documentos do Office protegidos. Atualmente, contudo, quando clica com o botão direito sobre um ficheiro do Office protegido no Explorador do Windows, a opção Imprimir não está desativada. No entanto, se selecionar Imprimir, ocorre o seguinte:

- Word - Uma caixa de diálogo indica que o Word deixou de funcionar.
- Excel - Uma caixa de diálogo indica que a opção Imprimir foi desativada pela política.
- Powerpoint - Uma caixa de diálogo indica que a opção Imprimir foi desativada pela política. Se clicar em OK, é impressa uma página de rosto a indicar que o documento está protegido.

# Determinar que documentos no modo opcional estão protegidos

Se tiver o modo de proteção forçada, todos os documentos do Office estão protegidos. Se tiver o modo opcional e pretender confirmar se um documento está protegido ou não, abra o documento e verifique se é apresentado como protegido na barra de título.

# Opções do menu adicionais para documentos do Office protegidos

O tipo de documento do Office, protegido ou desprotegido, pode afetar os seguintes pontos.

***Clique com o botão direito > Proteger***

Pode clicar com o botão direito num documento do Office e selecionar **Proteger**. Tem de adicionar conteúdo para que a opção do menu seja apresentada. Não é possível proteger um documento em branco.

***Propriedades do ficheiro > Separador do Dell Data Guardian***

Com documentos do Office protegidos, pode clicar com o botão direito e selecionar **Propriedades** e é apresentado um separador do **Dell Data Guardian** com informações, como a ID da chave do ficheiro e dados de acesso e embargo.

***Colar***

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

- Pode copiar e colar dados no documento protegido original.
- Não é possível copiar ou colar a partir de um documento protegido para um documento desprotegido. Não é apresentado qualquer conteúdo na Área de transferência e uma mensagem empresarial específica indica que não é possível colar no documento desprotegido ou não gerido.

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

***Arrastar e largar no modo protegido***

Pode arrastar e largar conteúdo num documento Word protegido. Atualmente, arrastar e largar estão desativadas em ficheiros PowerPoint e Excel protegidos.

***Imprimir para envelopes e etiquetas***

Se o seu administrador tiver definido uma política para adicionar uma marca de água quando imprime um documento do Office protegido, siga estes passos para imprimir envelopes ou etiquetas:

1 Num documento Word, selecione o separador **Correio**.
2 Selecione a opção **Envelopes** ou **Etiquetas**.
3 Depois de introduzir o endereço ou o endereço do remetente, clique em **Imprimir**.

> **NOTA: Se utilizar outra opção para imprimir e o seu administrador tiver definido uma política para adicionar uma marca de água em documentos do Office impressos, será apresentada uma marca de água no seu envelope ou etiqueta.**

# Adulteração e documentos do Office protegidos

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

Se um utilizador interno adulterar um documento do Office protegido:

- O Data Guardian consegue reparar e restaurar alguns dos elementos adulterados.
- Nas formas de adulteração que não possam ser reparadas, pode ser apresentada uma caixa de diálogo a indicar que o ficheiro foi adulterado e que deve entrar em contacto com o seu administrador.

Se um utilizador não autorizado abrir um documento do Office protegido, é apresentada apenas a página de rosto. Se o utilizador não autorizado modificar a página de rosto, o Data Guardian restaura a página de rosto quando um utilizador autorizado a guardar novamente como protegida.

# Utilizadores externos e documentos do Office protegidos

**Melhorar a segurança adicionando restrições de data**

Com o Data Guardian, carrega um documento do Office protegido para a nuvem e partilha-o:

- Todos os utilizadores internos do Data Guardian o podem visualizar.
- Com base na política, os utilizadores externos podem visualizá-lo.

Opcionalmente, para uma maior segurança com utilizadores externos, pode adicionar uma restrição de data para limitar o tempo durante o qual um utilizador externo pode visualizar um documento do Office protegido.

1 Selecione **Ficheiro > Informações > Restrição de data**.
2 A partir da lista pendente, selecione a data e hora de Início e Fim em que um utilizador externo poderá visualizar o documento.

> **NOTA:**
> A data e hora de Início pode ser futura se pretender enviar o documento, mas evitar que o utilizador externo o veja antes da data e hora especificada.

3 Clique em **OK**.
O documento é guardado, protegido, fechado e, em seguida, aberto novamente.

**NOTA:**
Se modificar as datas de um documento do Office desprotegido e, em seguida, clicar em Cancelar, o Data Guardian protege o ficheiro.

**NOTA:**
Atualmente, quando adiciona restrições de data a documentos do Office protegidos e planeia guardá-los numa unidade de rede, tem de guardar o ficheiro localmente e depois copiá-lo para a rede.

Se um utilizador externo abrir um ficheiro após o intervalo de data e hora especificado, é apresentada uma caixa de diálogo a indicar que o ficheiro tem restrições de acesso e que o utilizador externo pode contactar o autor do ficheiro. A caixa de diálogo não apresenta quaisquer datas ao utilizador externo.

Se definir o campo da data de Início para uma data ou hora futura e o utilizador externo abrir o ficheiro antes dessa data e hora, é apresentada uma caixa de diálogo a indicar que não é possível abrir o ficheiro antes dessa data e hora devido a restrições de acesso.

# Compreender os itens de menu do tabuleiro do sistema do Data Guardian

Ecrã de detalhes

O Ecrã de detalhes do Data Guardian fornece informações úteis, como por exemplo:

- Para obter suporte técnico, pode fornecer informações de estado ou da versão.
- Para visualizar o nome de um ficheiro não oculto associado a um ficheiro .xen, selecione **Ficheiros** > **Estado do ficheiro**.
- Para procurar por um nome de ficheiro, seleccione Copiar no lado direito inferior e cole o conteúdo num ficheiro Word.
- Para ver quem é o proprietário de uma pasta, seleccione Pastas e percorra o texto até à coluna PROPRIETÁRIO DA PASTA.

Para aceder ao ecrã Detalhes:

Clique no ícone do tabuleiro do sistema do **Data Guardian** e, em seguida, clique em **Detalhes...**

O canto superior esquerdo do ecrã Detalhes apresenta as seguintes informações:

**Estado do serviço**: estado do Serviço Windows do Data Guardian. Os valores são: Parado, StartPending, StopPending, Em execução, ContinuePending, PausePending, Em pausa

**Estado de execução**: o estado de ativação do dispositivo. Os valores são: Activo, A Reactivar, Suspenso, A Suspender

**Modo de utilizador**: Utilizador interno - um utilizador dentro deste endereço de domínio

**Utilizador externo** - um utilizador fora deste endereço de domínio

**E-mail de registo**: para utilizadores internos, este é o endereço de e-mail do domínio. Para utilizadores externos, este é o endereço de e-mail para o qual os utilizadores estão registados.

**URL do servidor**: o DDP EE Server/VE Server que comunica com este cliente.

**Data da última modificação da política**: data e hora em que a política foi modificada pela última vez e utilizada pelo cliente.

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

A área **Ficheiros** do ecrã Detalhes apresenta as seguintes informações:

**Nome**: nome do ficheiro

**Nuvem**: indica o nome de ficheiro oculto ou se o ficheiro está *Desprotegido*.

**Estado do ficheiro**: este valor indica o proprietário da pasta. O valor é determinado pela ID da chave.

**Estado de processamento**: indica se o ficheiro necessita de uma chave ou se está *Concluído*.

**Empresa**: indica o servidor predefinido. Se a mensagem *Erro: chave não pertencente ao seu servidor* for apresentada nesta coluna, a chave não pertence ao servidor da sua empresa. A chave de um ficheiro encriptado deve pertencer ao servidor da sua empresa.

**Chave**: ID da chave atribuída a essa pasta (os ficheiros novos utilizam esta chave para encriptação).

**Pasta**: o nome do caminho completo da pasta.

**Última modificação**: a data de modificação do ficheiro.

**Estado de persistência**: indica se o ficheiro se encontra no disco.

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

**Browser criado**: *Verdadeiro* ou *Falso*.

Para visualizar os ficheiros de registo, no canto inferior esquerdo do ecrã Detalhes, clique em **Ver registo**.

**NOTA:**
Os ficheiros de registo estão também disponíveis em **C:\ProgramData\Dell\Dell Data Protection\Dell Data Guardian.**

A área **Pastas** do ecrã Detalhes apresenta as seguintes informações:

**Nome**: nome da pasta

**Chave**: ID da chave atribuída a essa pasta (os ficheiros novos utilizam esta chave para encriptação).

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

**Proprietário da pasta**: este valor indica o proprietário da pasta. O valor é determinado pela ID da chave.

**Substituir**: as opções são *Nenhum* e *Preexistente*. Os ficheiros preexistentes não estão protegidos. Além disso, se aceder à Gestão de pastas e desproteger alguns ficheiros, esta coluna indica que os mesmos não estão protegidos.

**Tipo de ocultação**: se a sua empresa gerir o seu armazenamento na nuvem, esta é uma política definida em cada pasta que indica que tipo de ficheiros .xen é criado na nuvem. Esta é uma política definida pelo seu administrador. Caso o seu administrador selecione *Apenas extensão*, será exibido o nome real do ficheiro com a extensão ".xen". Caso o seu administrador selecione *Guid*, será exibido um nome de ficheiro codificado com a extensão ".xen". Esta é uma definição de política aplicada apenas a novas pastas. A predefinição é *Apenas extensão*.

# Menu Gerir pastas

Alguns gestores ou administradores podem ter de efetuar temporariamente a solução de problemas de pastas partilhadas por mais do que um utilizador. Pode solicitar permissão ao seu administrador para a opção Gerir pastas. Normalmente, esta é uma opção temporária.

# Localizar ficheiros de registo

Para a solução de problemas, o seu administrador pode solicitar ficheiros de registo.

Para localizar ficheiros de registo:

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

**NOTA:**
Quando o Xendow.Service.log atinge 3 MB, é guardado como Xendow.Service1.log, e depois Xendow.Service2.log.

# Verificar actualizações de política

Se o seu administrador modificar uma política e o notificar de uma atualização de política, aceda ao tabuleiro do sistema do Windows, clique no ícone **Dell Data Protection | Data Guardian** e selecione **Verificar atualizações de política**.

Se o seu administrador modificar uma política para proteger ficheiros criados no Microsoft Word, é necessário fechar o Word para que essa atualização seja aplicada.

# Atualizar o Data Guardian

A melhor prática consiste em desinstalar a versão anterior e, e, em seguida, instalar a versão atual. Consulte Desinstalar o Data Guardian.

# Fornecer feedback à Dell

Se o seu administrador tiver ativado uma política de feedback, poderá fornecer feedback à Dell sobre este produto. O breve formulário inclui duas perguntas sobre o seu grau de satisfação, com escalas de classificação (onde 10 indica o mais alto grau de satisfação) e um campo para comentários.

Para aceder ao formulário, clique no ícone do Data Guardian no tabuleiro do sistema e selecione **Enviar feedback**.

Se esta funcionalidade não estiver ativada devido à política da empresa, a opção não será exibida.

# Possíveis problemas na ativação - Office protegido

Se tiver instalado o Data Guardian, mas o ícone do Data Guardian no tabuleiro do sistema não apresentar uma marca de verificação verde  , tenha em atenção o seguinte:

- O Data Guardian pode converter documentos do Office existentes no modo protegido antes de proceder à ativação. Se for o caso, quando abrir um documento do Office, é apresentada uma página de rosto com informações sobre o processo de ativação.

Proceda da seguinte forma:

- Reinicie e volte a iniciar sessão com um sufixo UPN, por exemplo: nome_utilizador@domínio.com.
- Confirme com o seu administrador se deve ou não selecionar a caixa de verificação **Ativar verificação de confiança SSL** ao instalar o Data Guardian.
- Contacte o seu administrador de sistema quanto à configuração do seu computador para ativar manualmente. Consulte Ativar o Data Guardian.

# Ativar o Data Guardian

Normalmente, o Data Guardian ativa-se automaticamente depois da instalação e reinicialização. Se o seu administrador lhe indicar que deve proceder à ativação manual, siga os seguintes passos:

1 Inicie a sessão no Windows.
No tabuleiro do sistema, é apresentado um ícone de proteção com um ponto de exclamação laranja.
2 Clique no ícone do **Data Guardian** no tabuleiro do sistema e selecione **Ativação do utilizador**.
3 Introduza o seu endereço de e-mail e palavra-passe do domínio e clique em **Ativar**.

Se é um utilizador interno (com um endereço de e-mail do domínio), ignore o botão Registar. Apenas os utilizadores externos necessitam de se registar.

Depois de concluída a ativação, uma marca de verificação verde é apresentada no ícone do tabuleiro do sistema do Data Guardian  .

4 Confirme o seu estado de modo de utilizador. Clique na ligação no tabuleiro de sistema e selecione **Detalhes**.

5 Na parte superior, confirme

**Interno**: um utilizador com um endereço de e-mail dentro do domínio da empresa.

**Externo**: um utilizador com um endereço de e-mail fora do domínio. Para obter mais informações, consulte Utilizar o Data Guardian como utilizador externo.

# Utilizar o Data Guardian Mobile com iOS ou Android

Esta secção descreve informações básicas acerca da utilização do Data Guardian Mobile com dispositivos iOS ou Android. Quando o seu administrador define uma política para ativar o Data Guardian, os ficheiros são encriptados e protegidos na nuvem. No entanto, pode utilizar a aplicação do Data Guardian Mobile para visualizá-los no seu dispositivo móvel.

## Pré-requisito

Antes de utilizar a aplicação do Data Guardian, deve saber o nome do servidor do Dell Data Protection da sua empresa, apresentado no formato servidor.domínio.com. Esta informação é fornecida pelo seu administrador.

## Introdução ao Data Guardian Mobile

Siga esta sequência ao utilizar o Data Guardian Mobile.

| Tarefa | Descrição | Consultar esta seção |
|---|---|---|
| Instalar o Data Guardian | Determinar o seguinte:<br><br>Administrador já instalado<br><br>O utilizador deve instalar | Instalado pelo administrador: toque na aplicação do Data Guardian e inicie a sessão.<br><br>Instalações pelo utilizador: consulte um dos seguintes:<br><br>Instalação num dispositivo iOS<br><br>Instalação num dispositivo Android |
| Aceda à sua conta do fornecedor de armazenamento na nuvem | No dispositivo, navegue até à página Inicial da aplicação do Data Guardian e toque no seu fornecedor de armazenamento na nuvem. | Consulte uma das seguintes opções:<br><br>Aceda à sua conta de fornecedor de armazenamento na nuvem para iOS<br><br>Aceda à sua conta de fornecedor de armazenamento na nuvem para Android |

A aplicação Data Guardian Mobile apresenta o cliente de sincronização na nuvem utilizado na sua empresa e permite-lhe a respetiva transferência.

**NOTA:**
Se transferir a aplicação do cliente de sincronização na nuvem para o seu dispositivo, o Data Guardian não irá encriptar quaisquer pastas ou ficheiros que carregue diretamente dessa aplicação. Para encriptar e proteger ficheiros, tem de utilizar a aplicação do Data Guardian para proceder ao respetivo carregamento.

Para proteger os seus dados na nuvem, o Data Guardian encripta-os. Por conseguinte, a aplicação do Data Guardian tem de estar instalada no seu dispositivo móvel para poder visualizar ficheiros encriptados.

- Os ficheiros do Office protegidos (.docx, .pptx, .xlsx) mantêm a respetiva extensão de ficheiro.

- Os ficheiros não Office na nuvem têm uma extensão .xen.

Se uma pessoa não autorizada aceder à sua conta de armazenamento na nuvem e transferir um ficheiro para um dispositivo móvel que **não** tenha o Data Guardian instalado, essa pessoa não consegue abrir ou visualizar os seus ficheiros. Se abrirem um ficheiro do Office protegido, é apresentada apenas uma página de rosto a indicar que não é possível visualizar o documento sem o Data Guardian. Esta funcionalidade torna os seus dados mais seguros.

Em dispositivos móveis, pode:

- Criar pastas
- Carregar e transferir ficheiros

  **NOTA:**
  Com o Data Guardian, o utilizador tem de iniciar os carregamentos e transferências no dispositivo. Os ficheiros a encriptar quando carregados para a nuvem devem ser carregados a partir do ecrã inicial do Data Guardian e não da aplicação do cliente de sincronização na nuvem. Quando toca num ficheiro, o Data Guardian desencripta-o automaticamente e apresenta-o como texto desencriptado dentro da aplicação. No entanto, na nuvem, o ficheiro permanece protegido como ficheiro .xen.
- Adicionar um ficheiro a Favoritos
  - Para iOS, consulte o esquema de navegação. Para Android, mantenha premido o nome do ficheiro.
- Eliminar pastas e ficheiros
- Aceitar uma pasta partilhada proveniente de um utilizador interno

  **NOTA:**
  Se um utilizador interno partilhar uma pasta consigo através do Data Guardian, deve aceder ao website de armazenamento na nuvem e movê-la para a pasta raiz ou transferir a pasta partilhada, para poder visualizá-la no dispositivo.
- Partilhar um documento com um utilizador externo (se a política estiver ativada para visualizadores externos) - Para iOS, consulte Visualizar políticas de armazenamento na nuvem do Data Guardian para o seu dispositivo iOS.
- Editar ficheiros .docx e .ppt do Office.

  **NOTA:**
  Atualmente, os ficheiros .csv e .csv.xen não podem ser editados em dispositivos móveis.

**Documentos do Office protegidos quando estiver offline**

Quando cria um documento do Office protegido ou um documento com permissão para macros protegido e está offline, é criada uma chave para esse documento. Quando o dispositivo ficar online, as chaves são transferidas para o servidor Dell. Se um dispositivo estiver offline durante três dias, uma notificação indica que o Data Guardian não conseguiu contactar o servidor Dell. A notificação é apresentada diariamente até se ligar à rede. Para poder visualizar os ficheiros encriptados, o dispositivo móvel tem de estar online.

**Proteção adicional através de geofencing**

Com base nas políticas definidas pelo seu administrador, os dispositivos móveis podem ter proteção adicional que determine que os documentos do Office protegidos e os ficheiros .xen não podem ser abertos fora dos limites de uma região específica. O utilizador tem de estar numa região aprovada para poder abrir ficheiros protegidos. Atualmente, estas regiões são os Estados Unidos e o Canadá. O utilizador tem de ativar os serviços de Localização no dispositivo para que o geofencing funcione. Se a função de geofencing for ativada pelo seu administrador e os serviços de Localização estiverem definidos como Desligado, o acesso aos ficheiros é negado.

**Utilizar um PIN**

O seu administrador pode definir uma política que exija um PIN.

# O Data Guardian num dispositivo iOS

**Instalação num dispositivo iOS**

1 No seu dispositivo, toque em **App Store** e procure por **Data Guardian Mobile**.
2 Selecione e instale a aplicação do **Data Guardian**.
3 No campo Servidor, no ecrã de início de sessão, introduza o nome de anfitrião do servidor do Dell Data Protection da sua empresa, apresentado no formato servidor.domínio.com.
4 Introduza o seu nome de utilizador e a palavra-passe.
5 Toque em **Início de sessão**.

**Aceda à sua conta de fornecedor de armazenamento na nuvem para iOS**

Depois de iniciar sessão no Data Guardian, uma política do Data Guardian determina quais os fornecedores de armazenamento na nuvem exibidos no ecrã Inicial. O seu administrador pode designar um fornecedor de armazenamento na nuvem específico para utilizar na empresa.

O esquema de navegação apresenta opções adicionais.

Para aceder a uma conta:

1 Na página Inicial do Data Guardian, toque no fornecedor de armazenamento na nuvem.
2 Proceda de acordo com uma das seguintes opções, seguindo as instruções online:
- Crie uma conta com o fornecedor de armazenamento na nuvem.
- Inicie sessão numa conta de fornecedor de armazenamento na nuvem existente.

> **NOTA:**
> Para obter mais informações, consulte a ajuda do seu fornecedor de armazenamento na nuvem.

**Desassociar um fornecedor de armazenamento na nuvem**

Se possuir mais do que uma conta com o mesmo fornecedor de armazenamento na nuvem, não é possível iniciar sessão simultaneamente em ambas as contas. Deve desmarcar a caixa de verificação para desassociar e terminar sessão na conta atual e, depois, iniciar com as outras credenciais.

1 Abra o esquema de navegação do Data Guardian e toque em **Definições**.
2 Toque em **Desassociar**.

**Ver as políticas de armazenamento na nuvem do Data Guardian para o seu dispositivo iOS**

1 No esquema de navegação do Data Guardian, toque em **Definições**.
2 Toque em **Política**.
A lista pode incluir:
- Revisão - número de políticas que foram revistas
- Ocultar nomes de ficheiros - a predefinição está definida como **Não**
- Cliente de sincronização na nuvem - a política deve estar definida como **Encriptar**
- Visualizadores externos - se definido como **Sim**, a política de partilha está ativada. Quando abrir um documento na aplicação, uma opção de menu permite-lhe partilhar o ficheiro.

**Desinstalar a aplicação do Data Guardian**

1 No esquema de aplicações do iOS, toque sem soltar no ícone do **Data Guardian**.
2 Toque em **x**.
3 Toque em **Eliminar**.

# Solução de problemas iOS e o Data Guardian

Num dispositivo iOS, se abrir um documento do Office protegido superior a 25 MB e for apresentada uma caixa de diálogo a indicar pouca memória, este aviso é do Polaris Office e não do Data Guardian. Se o dispositivo tiver memória suficiente, feche o ficheiro e volte a abri-lo.

Com o Dropbox for Business, se marcar um ficheiro como disponível offline e posteriormente mudar o nome do ficheiro no website do Dropbox, o ficheiro não irá abrir no dispositivo iOS com a aplicação do Data Guardian.

# O Data Guardian num dispositivo Android

### Instalação num dispositivo Android

1 No seu dispositivo, aceda ao **Google Play** e procure por **Data Guardian Mobile**.
2 Selecione e instale a aplicação do **Data Guardian**.
3 No campo Servidor, no ecrã de início de sessão, introduza o nome do servidor do Dell Data Protection da sua empresa, apresentado no formato servidor.domínio.com.
4 Introduza o seu nome de utilizador e a palavra-passe.
5 Toque em **Início de sessão**.

A sua conta já está ativada.

### Aceda à sua conta de fornecedor de armazenamento na nuvem para Android

Depois de iniciar sessão no Data Guardian, uma política do Data Guardian determina quais os fornecedores de armazenamento na nuvem exibidos. O seu administrador pode designar um fornecedor de armazenamento na nuvem específico para utilizar na empresa e bloquear os restantes.

Para aceder a uma conta:

1 Na página Inicial do Data Guardian, toque no fornecedor de armazenamento na nuvem.
2 Proceda de acordo com uma das seguintes opções, seguindo os ecrãs online:
   - Crie uma conta com o fornecedor de armazenamento na nuvem.
   - Inicie sessão numa conta de fornecedor de armazenamento na nuvem existente.

> **NOTA:**
> Para obter mais informações, consulte a ajuda do seu fornecedor de armazenamento na nuvem.

3 Depois de aceder à sua conta, abra o esquema de navegação e toque em **Definições**. Quando obtiver o acesso a um fornecedor de armazenamento na nuvem, é exibida uma marca de verificação na caixa de diálogo.

> **NOTA:**
> Se possuir mais do que uma conta com o mesmo fornecedor de armazenamento na nuvem, não é possível iniciar sessão simultaneamente em ambas as contas. Deve desmarcar a caixa de verificação para desassociar e terminar sessão na conta atual e, depois, iniciar com as outras credenciais.

> **NOTA:**
> Para o OneDrive e o Dropbox, se não conseguir partilhar um ficheiro a partir de Aplicações e o ficheiro partilhar uma ligação com a aplicação do Data Guardian, partilhe o ficheiro a partir da aplicação File Browser no dispositivo.

### Desinstalar a aplicação do Data Guardian

1 No esquema das Aplicações Android, toque em **Definições**.
2 Em **Definições**, toque em **Aplicações**.
3 Prima 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 encripta pastas e ficheiros para tornar os dados seguros. Uma vez que o Data Guardian funciona com clientes de sincronização, tenha em atenção estas considerações.

**Google Drive**

O Google Drive inclui uma aplicação Google Docs que permite aos utilizadores colaborarem em documentos, em tempo real. No entanto, a colaboração ocorre num servidor Google, não no Dell Data Protection EE Server/VE Server. Por este motivo, os ficheiros não são encriptados. Para dispositivos Android e iOS com Data Guardian, o acesso a estes Google Docs está bloqueado. É ligeiramente diferente para cada plataforma:

- Android
- iOS - É exibida uma mensagem.

**OneDrive e OneDrive for Business**

Com o OneDrive for Business, se transferir diversos ficheiros e cancelar a transferência, o OneDrive for Business irá cancelar os que ainda não tiverem sido transferidos, mas irá prosseguir com o que estiver em processo de transferência. Este é um problema da Microsoft. Por este motivo, permita que os ficheiros sejam totalmente transferidos antes de cancelar.

# Registos históricos

Por razões de segurança, não estão disponíveis ficheiros de registo em dispositivos móveis.

# Enviar feedback à Dell

Se o seu administrador tiver ativado uma política de feedback, poderá fornecer feedback à Dell sobre este produto. Se esta funcionalidade não estiver ativada devido à política da empresa, a opção não será exibida.

Para enviar feedback:

1 No esquema de navegação do Data Guardian, toque em **Feedback**.
2 As questões breves permitem-lhe classificar o seu nível de satisfação (10 indica o nível de satisfação mais elevado) e introduzir um comentário.

# Utilizar o Data Guardian como utilizador externo

Um utilizador externo que tenha um endereço de e-mail fora do domínio também pode utilizar o Data Guardian. Eis alguns exemplos.

- Instalou e ativou o Data Guardian enquanto membro da sua empresa, mas precisa de partilhar ficheiros protegidos ou colaborar em ficheiros protegidos com um utilizador fora da sua empresa.
- O seu endereço de e-mail faz parte do domínio da empresa, mas também quer instalar e ativar o Data Guardian num computador ou dispositivo móvel com o seu endereço de e-mail pessoal, fora do domínio. Isto permite-lhe interagir com os seus ficheiros protegidos a partir de um endereço de e-mail fora do domínio da empresa.

Para utilizadores externos, consulte Requisitos do servidor. Além disso, o domínio ou utilizador não pode constar na lista negra da empresa.

**NOTA:**
Os utilizadores externos registados com o Secure Lifecycle 1.0 ou superior serão migrados se a empresa proceder a atualizações.

# Tarefas dos utilizadores internos

Para partilhar ficheiros seguros com um utilizador externo, pode enviar um documento do Office protegido ou um ficheiro .xen através de um e-mail do Outlook. Um pedido de confirmação lembra o utilizador de que a chave para o ficheiro protegido será partilhada.

**NOTA:**
Se um utilizador externo enviar um ficheiro protegido por e-mail, as chaves não são partilhadas.

Também pode utilizar a opção Conceder acesso para partilhar ficheiros seguros com um utilizador externo. É necessário:

- Disponibilizar um ou mais ficheiros seguros ao utilizador externo.
  - Documentos do Office protegidos - Conceder acesso a um ou mais ficheiros seguros através de:
    - Pasta local ou unidade de rede
    - Email
    - Suporte de dados amovível
    - Partilha de rede
  - Ficheiros .xen não Office - Crie uma pasta para partilhar no cliente de sincronização e adicione ficheiros.
- Conceder acesso ao utilizador externo a um ou mais ficheiros.

Se pretender partilhar ficheiros .xen não Office, tem de os adicionar a uma pasta no cliente de sincronização e, em seguida, conceder acesso aos mesmos. Para ficheiros do Office protegidos, tem de conceder acesso. Os passos podem variar de acordo com o método que utilizar ou do cliente de sincronização utilizado.

**Partilhar uma pasta no cliente de sincronização para partilhar ficheiros .xen**

1 No Explorador do Windows, aceda ao seu cliente de sincronização, crie uma pasta e carregue um ficheiro para partilhar com um utilizador externo. Consulte Visualizar pastas e ficheiros no computador local e na nuvem.

Os documentos do Office protegidos podem estar na Unidade virtual DDG VDisk, na pasta do Data Guardian ou no ambiente de trabalho.

**NOTA:**
Com ficheiros do Office protegidos, não é possível selecionar uma pasta.

Abre-se a página *Partilha de acesso ao documento protegido* com uma coluna que apresenta os ficheiros selecionados.

2 No website do cliente de sincronização, confirme se a pasta e o ficheiro foram criados e encriptados.
Quando o utilizador adiciona um ficheiro .xen a uma nova pasta na Unidade virtual DDG VDisk, o Data Guardian adiciona um documento, *Como aceder a ficheiros protegidos.html*, à pasta no website. Este ficheiro é utilizado apenas na partilha da pasta com um utilizador externo.

3 No website do cliente de sincronização, clique com o botão direito do rato na pasta que criou e clique em **Partilhar**.
É aberta uma janela que lhe permitirá introduzir a conta de e-mail de um utilizador externo. Os passos variam consoante o cliente de sincronização utilizado. Para obter ligações a informações acerca do seu cliente de sincronização, consulte Trabalhar com o cliente de sincronização na nuvem na unidade virtual do DDG VDisk.

4 Conceder acesso a ficheiros individuais dentro da pasta que pretende partilhar.

#### Conceder acesso a um ou mais ficheiros do Office protegidos

É necessário conceder acesso a todos os ficheiros que partilhar com utilizadores externos.

1 Clique com o botão direito do rato num ficheiro seguro e selecione **Conceder acesso ao ficheiro protegido**. Pode selecionar um ou vários ficheiros, até um máximo de 50.
2 No campo *E-mail a partilhar*, introduza o endereço de e-mail do utilizador fora do domínio e clique em **Adicionar**.
3 Repita este passo para adicionar até um máximo de dez endereços de e-mail.
4 Clique em **OK**.
Uma caixa de diálogo indica que a partilha foi concluída com êxito ou que o endereço de e-mail não está autorizado a receber ficheiros protegidos.
5 Como uma prática recomendada, informe o utilizador externo de que irá receber um e-mail com instruções que lhes permitem registar-se num servidor Dell, transferir e ativar o Dell Data Protection | Data Guardian e posteriormente visualizar ficheiros protegidos partilhados.

#### Aprovar ou negar o acesso quando um utilizador externo solicita acesso

Um utilizador externo que tenha o Data Guardian instalado pode solicitar o acesso a um documento protegido, se não tiver a chave para esse documento.

1 Se receber um e-mail de um utilizador externo a solicitar o acesso a um documento protegido, pode visualizar o nome do utilizador externo e o ficheiro solicitado.
2 Selecione **Aprovar** ou **Negar**.
É enviado um e-mail para o utilizador externo. Se aprovar o pedido, a chave para o documento protegido é partilhada.

Caso não esteja disponível, o seu administrador também tem a opção de aprovar ou negar o acesso.

# Tarefas do utilizador externo

Para poder abrir e visualizar um documento do Data Guardian, o utilizador externo deve:

- Registar-se no Data Guardian

- Instalar o Data Guardian - o utilizador externo tem de ter direitos de administrador no seu computador
- Se o utilizador interno partilhar uma pasta através de um cliente de sincronização, o utilizador externo tem de possuir uma conta do cliente de sincronização. Consulte Instalar um cliente de sincronização na nuvem e, em seguida, Trabalhar com o cliente de sincronização na nuvem na unidade virtual do DDG VDisk.

**Registar o Data Guardian**

Na primeira vez que um utilizador interno partilha um ficheiro, o utilizador externo tem de efetuar o registo.

Para registar o Data Guardian:

1 No e-mail de Verificação de conta enviado pelo Dell Enterprise Server, clique na hiperligação.
2 Continue para a página Web.
3 Na página de Confirmação, clique em **Continuar para início de sessão**.
4 Na página de Início de sessão, clique em **Esqueci-me da palavra-passe**.

> **NOTA:**
> O servidor Dell atribuiu uma palavra-passe aleatória, que terá de repor.

5 Na página Repor palavra-passe, introduza e confirme a sua palavra-passe e, em seguida, clique em **Registo**.
É apresentada uma caixa de diálogo de confirmação do registo e é enviado um e-mail para o endereço indicado pelo utilizador interno.
6 Abra o e-mail de ativação de conta e clique na ligação.
O e-mail também contém o nome do servidor a utilizar quando instalar o Data Guardian.
7 Na página de início de sessão, introduza o endereço de e-mail e a palavra-passe que utilizou para se registar.
8 Clique em **Início de sessão**.
A página Transferência do Data Guardian abre-se.
9 Transferir e instalar o Data Guardian.
Abre-se a página Transferência com opções para Windows, iOS, Android e Mac OS X. Com o Enterprise Server, a página Transferência abre-se. Com o Dell Enterprise Server - VE, ao clicar em Windows acede ao site dell.com/support.

Estes passos descrevem a instalação do Data Guardian no Windows. Consulte também Tarefas do utilizador - Office protegido sem encriptação na nuvem.

> **NOTA:**
> A página de transferência também contém o nome do servidor que precisará nestes passos.

10 Em Windows, clique em **Transferir (32 bits)** ou **Transferir (64 bits)**, de acordo com o sistema operativo do seu computador.
11 Transfira o ficheiro de configuração para um diretório no seu computador.
12 Clique duas vezes no ficheiro de configuração para iniciar o instalador.
13 Selecione um idioma e clique em **OK**.
14 Se aparecer uma mensagem a questionar se deseja instalar o Pacote redistribuível do Microsoft Visual C++ 2010, clique em **OK**.
15 No ecrã de boas-vindas, clique em **Seguinte**.
16 Leia o contrato de licença, aceite os termos e condições e clique em **Seguinte**.
17 No ecrã Pasta de destino, clique em **Seguinte** para instalar na localização predefinida de **C:\Program Files\Dell\Dell Data Protection \Dell Data Guardian\.**
18 No campo *Nome do servidor:*, introduza o nome do servidor com o qual este computador vai comunicar. Este nome encontra-se no e-mail de ativação que recebeu, no topo da página de transferência.
19 Clique em **Seguinte**.
20 No ecrã Confirmar servidor de ativação, certifique-se de que o endereço URL do servidor está correto. O instalador adiciona www ou http(s) e, de seguida, a porta. Clique em **Seguinte**.
21 Na janela Tipo de gestão, selecione esta opção:
- Uso externo - um utilizador com um endereço de e-mail fora do domínio da empresa.

22 Clique em **Instalar** para dar início à instalação.

Uma janela de estado apresenta o progresso da instalação.

23 Clique em **Concluir** quando for apresentado o ecrã de Instalação concluída.

24 Clique em **Sim** para reiniciar.

A instalação do Data Guardian está concluída.

25 Consulte Ativar o Data Guardian.

# Ativar o Data Guardian

Depois de instalar o Data Guardian e reiniciar o computador, siga os seguintes passos para ativar:

1 Inicie a sessão no Windows.

No tabuleiro do sistema, é apresentado um ícone de nuvem com um ponto de exclamação laranja.

2 Quando for apresentada uma caixa de diálogo no tabuleiro do sistema, clique em **Clique aqui para ativar**.

Se não for apresentada a caixa de diálogo, clique no ícone do **Data Guardian** no tabuleiro do sistema e selecione **Ativação do utilizador**.

3 Introduza o endereço de e-mail e palavra-passe que utilizou para se registar e clique em **Ativar**.

Depois de concluída a ativação, uma marca de verificação verde é apresentada no ícone do tabuleiro do sistema do Data Guardian  .

4 Confirme o seu estado de modo de utilizador. Clique na ligação no tabuleiro de sistema e selecione **Detalhes**.

Na parte superior, o Modo de utilizador é:

**Externo**: um utilizador com um endereço de e-mail fora do domínio.

Se já tiver instalado e iniciado sessão num cliente de sincronização, a Unidade virtual DDG VDisk é apresentada no Explorador do Windows.

# Solicitar o acesso a um utilizador interno

Com o Windows e Mobile, se um utilizador externo tiver instalado e ativado o Data Guardian, o utilizador pode solicitar o acesso a um ficheiro a um utilizador interno. O utilizador externo tem de efetuar um pedido separado para cada ficheiro.

1 Se abrir um ficheiro do Office protegido e este indicar que é necessário solicitar o acesso, clique em **Sim** ou **Não**.

Uma caixa de diálogo indica que o pedido foi enviado com êxito. O utilizador interno pode aprovar ou negar o acesso e o utilizador externo recebe um e-mail com o resultado. Se o utilizador externo abrir o ficheiro protegido antes de o utilizador interno aprovar o acesso, é apresentada uma mensagem a indicar que o pedido se encontra pendente.

2 Após 48 horas, o utilizador externo pode solicitar o acesso novamente.

No tabuleiro do sistema, o utilizador externo pode clicar com o botão direito no ícone do Data Guardian e selecionar a página **Detalhes**. Clique no separador **Segurança**. Quando o tempo para um pedido regressar a *Nenhum*, o utilizador externo pode solicitar o acesso novamente.

# Visualizar um documento do Office protegido

Se uma empresa ativar uma política para proteger documentos do Office e um utilizador interno enviar um ficheiro protegido para um utilizador externo, o utilizador externo tem de estar ligado ao servidor Dell quando abrir o documento pela primeira vez. Depois, poderá abrir e visualizar o documento offline durante um período de tempo especificado, por exemplo, uma semana. O utilizador externo terá então de se ligar ao servidor e voltar a abrir o documento protegido.

Por motivos de segurança, um utilizador externo não pode realizar as seguintes ações com um documento do Office protegido.

- Imprimir
- Exportar

- Guardar como
- Partilhar

# Desinstalar um cliente de sincronização ou o Data Guardian

Se o seu administrador tiver instalado o Data Guardian, apenas o administrador poderá desinstalar o produto. Um utilizador externo que tenha sido convidado a partilhar uma pasta e tenha direitos de administrador num computador externo também poderá desinstalar o Data Guardian desse computador externo.

## Desinstalar um cliente de sincronização na nuvem

Se desinstalar o seu cliente de sincronização na nuvem, mas mantiver o Data Guardian no seu computador, continua a poder visualizar os seus ficheiros como texto desencriptado na Unidade virtual DDG VDisk.

No entanto, se reinstalar o mesmo cliente de sincronização na nuvem, necessitará de uma nova chave para os abrir na Unidade virtual DDG VDisk e terá de transferir os seus ficheiros do website do cliente de sincronização.

## Desinstalar o Data Guardian

Apenas um administrador local do computador tem permissão para desinstalar o Data Guardian.

**Copiar ficheiros para a sua unidade local**

Se desinstalar o Data Guardian do seu computador ou dispositivo, os ficheiros no website do cliente de sincronização têm de se manter seguros, para permanecerem encriptados.

1 Antes de desinstalar, determine se necessita de aceder a quaisquer ficheiros.
2 Copie esses ficheiros da Unidade virtual DDG VDisk para a sua unidade local.

Estes ficheiros, copiados a partir da Unidade virtual DDG VDisk, são apresentados como texto desencriptado. As pastas e ficheiros no website do cliente de sincronização ficarão encriptados, ainda que os transfira. Para os visualizar, é necessário reinstalar o Data Guardian.

**Desinstalar o Data Guardian**

1 Utilize 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 **Seguinte** quando o ecrã de boas-vindas for apresentado.
4 Selecione **Remover** e clique em **Seguinte**.
5 É apresentado um aviso para confirmar se pretende desinstalar o Dell Data Protection | Data Guardian. Em caso afirmativo, clique em **Seguinte**.
6 No ecrã Remover o programa, clique em **Remover**.
A janela de estado exibe o andamento.
7 Se for apresentada uma mensagem de erro do cliente de sincronização, clique em **Continuar**.
8 Clique em **Concluir** quando for apresentado o ecrã Concluído.
9 Clique em **Sim** para reiniciar.

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

# 8

# Perguntas frequentes

## Perguntas diversas

**Pergunta**

Movi a pasta de sincronização do fornecedor de serviços na nuvem para Ficheiros de programa e agora não consigo desencriptar os ficheiros que estão a ser transferidos para a minha pasta de sincronização a partir da nuvem.

***Resposta***

Por predefinição, a pasta Ficheiros de programa ou outras pastas excluídas são desprotegidas, com base na política. O Data Guardian não irá desencriptar quaisquer ficheiros transferidos para esta pasta ou respetivas subpastas.

***Solução***

Desassocie ou desinstale o cliente de sincronização e mova novamente a pasta de sincronização para a respetiva localização predefinida ou para uma localização alternativa gerida.

**NOTA:**
Para obter uma lista de localizações geridas ou não geridas, contacte o seu administrador.

**Pergunta**

Tenho alguns ficheiros .xen arquivados e copiei-os para o meu ambiente de trabalho. Alguns deles ficaram desencriptados, mas outros não.

***Resposta***

Durante a sincronização, o Data Guardian foi projetado para desencriptar diretamente para a unidade virtual ou desencriptar quando estiver a transferir através de um browser. Para ficheiros copiados a partir de outra localização, utilize o Explorador do Windows e mova o ficheiro .xen para a unidade virtual para ser desencriptado.

***Solução***

Mova os ficheiros .xen para a unidade virtual para poder carregá-los na nuvem. Em seguida, estes serão desencriptados localmente.

**Pergunta**

Mudei o nome do meu computador. Agora, não recebo nenhuma atualização de políticas e não estou a encriptar na nuvem.

***Resposta***

Atualmente, o Servidor apenas reconhece o endpoint face ao qual foi realizada a ativação original. Se alterar o nome do endpoint, o Servidor não irá reconhecer o local para envio da política e o Data Guardian não funcionará como esperado.

***Solução***

1 Pare de sincronizar ficheiros com o computador local.

**NOTA:**
Se não parar a sincronização antes da desinstalação, dados valiosos podem ficar desprotegidos na nuvem ou poderão ser eliminados.

2 Desinstale e volte a instalar o Data Guardian. Deve ter direitos de Administrador para desinstalar.

**Pergunta**

Em dispositivos Windows suspensos, quando tento transferir ficheiros para a nuvem, nada acontece. Ao fechar as janelas que já estavam abertas, recebo a seguinte mensagem de erro: Acesso negado.

***Resposta***

A mensagem de erro não é do Data Guardian. Pode aceder aos ficheiros localmente, mas não irá receber futuras atualizações aos ficheiros.

# Perguntas mais frequentes sobre documentos do Office e o modo protegido

**Pergunta**

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

***Resposta***

Se o seu administrador definir uma política para proteger documentos do Office, é necessário que o utilizador ou o respetivo administrador instale o Data Guardian. Confirme se o ícone do Data Guardian no tabuleiro do sistema apresenta uma marca de verificação verde, para indicar que se encontra ativado.

***Solução***

Determine se necessita de instalar ou ativar o Data Guardian. Consulte Instalar o Data Guardian ou Possíveis problemas na ativação.

**Pergunta**

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

***Resposta***

Verifique o seguinte:

- Definições de bloqueio de ficheiros - Se o seu administrador definir políticas para proteger documentos do Office, não utilize esta definição em **Ficheiro > Opções**.

***Solução***

Para verificar as Definições de bloqueio de ficheiros:

1 Num documento do Office, selecione **Ficheiro > Opções**.
2 Selecione **Centro de fidedignidade** na lista.
3 No lado direito, clique em **Definições do centro de fidedignidade**.
4 Selecione **Definições de bloqueio de ficheiros** na lista.
5 Para *Documentos e modelos Word/Excel/PowerPoint 2007 e posteriores*, certifique-se de que a caixa de verificação *Abrir* não está marcada.
6 Clique em **OK**.