Dell Data Protection | Dell Data Guardian para Mac

Guia do Administrador v1.2

GUID-5B8DE7B7-879F-45A4-88E0-732155904029

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.

GUID-559E7DE2-5F31-4AF0-8A01-987470FAB58C

Guia do Administrador do Dell Data Guardian para Mac

2017 - 04

Rev. A01

Índice

Introdução ao Dell Data Guardian para Mac

Este guia fornece as informações necessárias para administrar o software de cliente em nuvem para Mac.

GUID-DC905DCF-89A3-4894-B120-B1ED63272AA5

Descrição geral

O Dell Data Guardian para Mac protege os dados em sistemas de partilha de ficheiros baseados na nuvem. Os computadores Mac OS X com Data Guardian conseguem ver, modificar e encriptar ficheiros em sistemas de partilha de ficheiros baseados na nuvem para armazenamento seguro.

Ambas as versões Data Guardian para Mac e para Windows conseguem abrir ficheiros encriptados entre si.

O Data Guardian para Mac contém o seguinte:

- Data Guardian:
  - **Cloud Encryption** - protege os dados em sistemas de partilha de ficheiros baseados na nuvem, como ficheiros .xen.
  - **Protected Office Documents** - protege os documentos do Office (.docx, .pptx, .xlsx, .docm, .pptm, .xlsm) na nuvem, apresentando o nome de ficheiro original e a extensão. Se estiverem protegidos, os ficheiros só podem ser abertos com um cliente do Data Guardian. Se for aberto noutro local, é apresentada uma página de rosto a indicar que o documento está protegido e a explicar de que forma um utilizador autorizado pode solicitar o acesso ao ficheiro encriptado.

    Pode definir as políticas apenas da encriptação da nuvem ou de ambos os grupos de políticas. Para obter mais informações, consulte *Admin Help*.

    O Data Guardian para Mac foi concebido para partilhar ficheiros dentro de fornecedor de encriptação de nuvem. No entanto, se as políticas "Documentos do Office protegidos" estiverem ativadas para Mac, perde-se a auditoria e rastreio de todos os ficheiros se estes forem guardados pelo utilizador final no Mac local. Se a sua organização necessitar de auditoria e de rastreio rigorosos, defina a política *de Permitir ativação Mac do Data Guardian* como "Não selecionado" para impedir que o Data Guardian seja ativado em computadores Mac.
- Security Server - um componente do Servidor Dell que gere o Data Guardian para Mac. O Security Server garante que os dados estão seguros na nuvem, seja com quem for que estes sejam partilhados. O Security Server também impede que os dispositivos internos transmitam dados confidenciais.
- Consola de Gestão Remota - proporciona uma administração centralizada de políticas de segurança, integra-se nos diretórios existentes na empresa e cria relatórios.

  Estes componentes Dell interagem na perfeição para permitirem um ambiente seguro sem reduzir a experiência do utilizador.

GUID-B47CD81A-486F-43A5-816B-86A247C276EA

Contacte o Dell ProSupport

Contacte o número 877-459-7304, extensão 4310039 para obter suporte telefónico permanente (24 x 7) para o seu produto Dell Data Protection.

Adicionalmente, o suporte online para os produtos Dell Data Protection encontra-se disponível em dell.com/support. O suporte online inclui controladores, manuais, conselhos técnicos, FAQ e problemas emergentes.

Para número de telefone fora dos Estados Unidos, consulte Dell ProSupport International Phone Numbers (Números de telefone internacionais do Dell ProSupport).

Requisitos do Dell Data Guardian para Mac

Os requisitos de hardware e software do cliente são apresentados neste capítulo. Certifique-se de que os ambientes de implementação cumprem os requisitos antes de continuar as tarefas de implementação.

NOTA:
O IPv6 não é suportado.

GUID-213663B0-B65F-4945-B2F1-5BEF78085BDF

Servidor

O Data Guardian para Mac obriga o cliente a estar ligado a um Dell Enterprise Server ou Dell Enterprise Server - VE, v9.6 ou superior.

GUID-371FFDE5-7A34-4268-AA88-617E73C0F9A4

Hardware para cliente Mac

Segue-se uma lista do hardware suportado para o cliente Mac.

Hardware para Mac

- Intel Core 2 Duo, Core i3, Core i5, Core i7 ou processador Xeon
- 2 GB de RAM
- 10 GB de espaço livre em disco

GUID-3F5F6005-9FEE-46AE-8400-336215F15DB2

Sistemas operativos

Segue-se uma lista dos sistemas operativos suportados.

Sistemas operativos para Mac

- Mac OS X Yosemite 10.10.5
- Mac OS X El Capitan 10.11.6
- macOS Sierra 10.12.3 e 10.12.4

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

GUID-C4B25B4F-15E5-42AF-9493-D09F2473A534

Fornecedores de armazenamento na nuvem

Com base nas definições das políticas, pode ser apresentado o seguinte na interface do Dell Data Guardian. O utilizador não precisa de transferir ou instalar o cliente de sincronização na nuvem.

Fornecedores de armazenamento na nuvem

- DropBox
- Box
- Google Drive
- OneDrive
- OneDrive for Business

Tarefas de instalação do Data Guardian

GUID-168A1BC7-0DED-43F2-9A99-08FC43099963

Pré-requisitos

Antes de executar estas tarefas, confirme o seguinte:

- Instale o Servidor Dell e respetivos componentes. Consulte uma das seguintes opções:
  - *Guia de migração e instalação do Enterprise Server*
  - *Guia de instalação e Guia de início rápido do Virtual Edition*
- Na Consola de Gestão Remota, atribua a Função de administrador Dell adequada.

GUID-D9C4A912-436F-415D-9499-BAE4F1B53233

Políticas

Por predefinição, o Data Guardian encripta os ficheiros dos utilizadores e envia eventos de auditoria para o DDP EE Server/VE Server. 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).

Se pretender que os eventos de auditoria incluam dados de geolocalização, deve ativar a Wi-Fi. Para obter mais informações sobre a geolocalização e eventos de auditoria, consulte *AdminHelp*.

Para alterar o comportamento predefinido para cada fornecedor de armazenamento em nuvem suportado, defina a política *Fornecedor de proteção de armazenamento em nuvem*. Se a sua empresa prefere um fornecedor de armazenamento em nuvem específico, defina esta política como **Bloquear** para outros fornecedores. Para obter mais informações acerca das políticas, consulte *AdminHelp*, que está acessível a partir da Consola de Gestão Remota do Servidor Dell.

NOTA:
A opção Ignorar desta política destina-se ao Windows. Se selecionar Ignorar para Mac, será apresentada ao utilizador final como Permitir.

GUID-EE401419-8E85-45A9-9775-2C16EEE3FDB0

Tarefas do Dell Enterprise Server

GUID-0E37A5B7-8FF3-4F1E-9A8E-AB49D649C05B

Configurar o Security Server para autorizar transferências de clientes na nuvem

DDP Enterprise Server

1 No DDP Enterprise Server, aceda a <Security Server install dir>\webapps\cloudweb\brand\dell\resources\
2 Abra o ficheiro **messages.properties** com um editor de texto.
3 Certifique-se de que as entradas são as seguintes:
Para a instalação **local**:

download.deviceWin.mode=local

download.deviceMac.local.filename=Dell-Data-Guardian-0.x.x.xxxx.dmg

Para a instalação **remota**:

```
download.deviceWin.mode=remote
```

```
download.deviceMac.remote.link=https://[MachineName:IPaddress]:[port]/yourpath/filename.dmg
```

4 Guarde e feche os ficheiros.
5 Aceda a <Security Server install dir> e crie uma pasta chamada Transferências (Security Server\Transferências).
6 Na pasta Download, crie uma pasta CloudWeb (Security Server\Download\CloudWeb).
7 Adicione os programas de instalação do Dell Data Guardian a essa pasta.

Virtual Edition: instalar manualmente uma versão diferente do cliente de nuvem

Não é necessária qualquer ação para permitir que os utilizadores transfiram o programa de instalação do cliente Dell Data Guardian mais recente. O instalador mais recente está pré-instalado no VE Security Server.

Para instalar manualmente uma versão diferente do programa de instalação do Data Guardian no VE Security Server, atualize o ficheiro message.properties.

1 Aceda a:
/opt/dell/server/security-server/webapps/root/cloudweb/brand/dell/resources/
2 Abra o ficheiro **messages.properties** com um editor de texto.
Para a instalação **local**:

```
download.deviceWin.mode=local
```

```
download.deviceMac.local.filename=Dell-Data-Guardian-0.x.x.xxxx.dmg
```

Para a instalação **remota**:

download.deviceWin.mode=remote

```
download.deviceMac.remote.link=https://[MachineName:IPaddress]:[port]/yourpath/filename.dmg
```

3 Guarde e feche os ficheiros.
4 Copie os ficheiros para /opt/dell/server/security-server/transferências/cloudweb.
5 Adicione os programas de instalação do Data Guardian a essa pasta.

GUID-40291F18-814A-40EC-9D60-A185154BA6FC

Permitir/recusar utilizadores na Lista de acesso completo/lista negra

As entradas na lista branca e na lista negra determinam que utilizadores podem registar-se no Servidor Dell para utilizar o Data Guardian.

Lista de acesso total

A lista de acesso total permite que utilizadores ou grupos de utilizadores específicos se registem no Servidor Dell e utilizem o Data Guardian.

Os utilizadores externos devem ser colocados na lista de acesso total para permitir o registo. Consulte os exemplos seguintes para permitir que os utilizadores se registem:

Tipo de utilizador	Introduzir
Todos os endereços de e-mail organization.com	`organization.com`
Um utilizador específico	`jdoe@organization.com`
Todos os utilizadores do Gmail	`gmail.com`

Lista negra

A lista negra previne que utilizadores específicos ou grupos de utilizadores se registem com o Servidor Dell ou utilizem o Data Guardian. Os utilizadores cujos endereços de e-mail forem introduzidos na lista negra recebem uma mensagem a declarar que não podem registar-se no Data Guardian.

NOTA:
Se um utilizador já se encontrar registado, esta lista **não** os impede de utilizar o Data Guardian.

Pode utilizar a lista negra para excluir utilizadores específicos que sejam membros de grupos aprovados na lista de acesso total. Além disso, pode colocar domínios completos na lista negra, evitando assim o registo de qualquer pessoa com um endereço de e-mail nesse domínio. Consulte os seguintes exemplos para impedir um utilizador ou grupo de se registar no Servidor Dell:

Tipo de utilizador	Introduzir
Todos os endereços de e-mail organization.com	`organization.com`
Um utilizador específico e o respetivo endereço de e-mail	`jdoe@organization.com`
Todos os utilizadores do Gmail	`gmail.com`

Para modificar a lista de acesso total/lista negra, siga estas instruções:

1 No painel esquerdo da Remote Management Console, clique em **Gestão > Gestão de utilizadores externos**.

2 Clique em **Add** (Adicionar).

3 Selecione Tipo de acesso ao registo:

Lista negra - bloqueia o registo de um utilizador ou domínio. O utilizador não pode abrir um documento do Office protegido ou ficheiro .xen.

Lista de acesso total - concede acesso ao registo e a todos os ficheiros para um utilizador ou domínio. Se um utilizador ou domínio também estiverem na lista negra, não é concedido qualquer acesso.

4 No campo Introduzir domínio/e-mail, introduza o domínio do utilizador para definir o acesso a todo o domínio ou o endereço de e-mail para definir o acesso apenas a esse utilizador.

5 Clique em **Add** (Adicionar).

Para obter mais informações sobre como utilizar a lista de acesso total/lista negra, consulte *AdminHelp*, acessível a partir da Consola de Gestão Remota no servidor Dell.

Um utilizador externo pode solicitar o acesso a um utilizador interno através da chave de um ficheiro protegido. Se o utilizador interno não estiver disponível, pode utilizar a Consola de Gestão Remota para aprovar ou recusar o acesso.

1 Selecione **Gestão > Gestão de pedidos de chave**.
2 Para obter mais informações, selecione **?** (Ajuda).

GUID-038F598E-1FF3-4FC8-A419-2F628C92F934

Eliminação remota de uma conta de um membro da equipa do Dropbox for Business

Se a sua empresa possuir o Dropbox for Business, pode remover remotamente um membro da equipa da conta da equipa do Dropbox for Business da empresa se, por exemplo, um utilizador deixar a empresa. Os ficheiros e pastas associados à conta do membro da equipa serão removidos de todos os dispositivos utilizados pela conta. Isto revoga o acesso do utilizador a esses ficheiros.

Pré-requisitos

NOTA:
Antes de realizar este procedimento, deve fazer uma cópia de segurança de todos os ficheiros ou pastas a partir da conta dos membros da equipa que possam ser necessários por parte da empresa ou outros membros da equipa do Dropbox for Business.

Apenas um Administrador do Dropbox for Business pode eliminar remotamente uma conta do Dropbox for Business.

O utilizador final deve ter ativado o Dell Data Guardian e efetuado ligação ao Dropbox for Business.

Registo na Remote Management Console

Apenas é necessário o registo de um Administrador do Dropbox for Business.

1 No painel esquerdo da Consola de Gestão Remota, selecione **Gestão** > **Gestão do Dropbox**.
2 Na página do Dropbox for Business, clique em **Registar**.
O navegador abre o site do Dropbox for Business.
3 Se solicitado, inicie sessão no Dropbox com a sua conta de Administrador do Dropbox for Business.
4 Para permitir o acesso ao Dell Data Guardian, clique em **Permitir**.
É apresentada uma página de confirmação para indicar que a autorização do Dropbox foi concedida ao DDP Enterprise Server - VE.
5 Na Consola de Gestão Remota, regresse a **Gestão** > **Gestão do Dropbox** e clique em **Atualizar**.
O nome do administrador é apresentado.

NOTA:
Geralmente, a melhor prática é não cancelar o registo. No entanto, para retirar os privilégios do administrador do Dropbox for Business para remoção de membros da equipa do Dropbox for Business, clique em **Cancelar o registo**.

Eliminação remota de uma conta de um membro da equipa

NOTA:
A opção Eliminação remota apenas está disponível para contas de membros da equipa do Dropbox for Business registados. Se a opção Eliminação remota não for apresentada para uma conta de utilizador, o utilizador não registou uma conta do Dropbox for Business.

1 Na Remote Management Console, selecione **Populações** > **Utilizadores** no painel esquerdo.
2 Procure o utilizador especificado.
3 Aceda à página **Detalhe do utilizador.**
4 Na coluna Comando, clique em **Eliminação remota.**
A eliminação remota é realizada.

NOTA:
Antes de selecionar a Eliminação remota, deve fazer uma cópia de segurança de quaisquer ficheiros ou pastas da conta de membro da equipa de que a empresa ou outros membros da equipa do Dropbox for Business possam necessitar.

5 Na caixa de diálogo de confirmação da Eliminação remota, clique em **Sim**.
A página Detalhe do utilizador indica a data em que é realizada a eliminação remota.

6 Na sua página de Membros da consola de administração do Dropbox for Business, atualize a lista de Membros da equipa.
O utilizador é removido da lista. Pode selecionar o separador **Membros removidos** para ver os utilizadores que foram removidos.

GUID-B495F3E1-6516-4DFC-9107-4AA52FE296AB

Tarefas do cliente

GUID-88098FA1-F419-45AD-A4BA-F5C30D04DDE3

Pré-requisitos

- Certifique-se de que os dispositivos de destino estão ligados a:
  - https://yoursecurityservername.domain.com:8443/cloudweb/register
  - https://yoursecurityservername.domain.com:8443/cloudweb
- Certifique-se de que o utilizador que executar a instalação tem uma conta local de administrador.
- Se efetuar a instalação através de uma linha de comandos, certifique-se de que possui o nome de domínio totalmente qualificado do Dell Security Server que os utilizadores ativarão.

GUID-5A15F45E-2F97-4EB4-90CD-66CD73275BAB

Melhores práticas

Durante a implementação, certifique-se de que segue as melhores práticas de TI. Isto inclui, mas não se limita a:

- Ambientes de testes controlados para testes iniciais
- Implementações escalonadas para utilizadores

GUID-CF4B88F3-DBAF-4834-B15B-8815EEA72B9D

Cliente de instalação

Neste ponto, os utilizadores que foram adicionados à lista branca podem registar-se em: https://yoursecurityservername.domain.com:8443/cloudweb/register.

Depois do registo, o utilizador recebe um e-mail que o direciona para https://yoursecurityservername.domain.com:8443/cloudweb, de forma a iniciar sessão e transferir o cliente adequado.

A instalação do cliente Mac é opcional para administradores, uma vez que os utilizadores finais instalam normalmente o cliente Mac (após o registo) eles próprios a partir de https://yoursecurityservername.domain.com:8443/cloudweb.

No entanto, pode instalar o cliente Mac se a sua organização exigir que o faça. Instale o cliente Data Guardian através da interface do utilizador ou através da linha de comandos, utilizando qualquer tecnologia push disponível na sua organização. O registo e a ativação pelo utilizador final continuam a ser necessários.

Atualização de versões anteriores do Cloud Edition

Se uma empresa tiver uma versão anterior do Cloud Edition e atualizações do Data Guardian, a versão anterior do Cloud Edition é removida.

NOTA:
Se a empresa atualizar do Cloud Edition para o Data Guardian, os utilizadores têm de efetuar novamente a autenticação e a ligação do Data Guardian ao respetivo fornecedor de armazenamento em nuvem. Para obter mais informações sobre autenticação, consulte a Ajuda do Dell Data Guardian.

Opções de instalação

Para instalar/atualizar o cliente, selecione o seguinte:

- Instalação interativa - Este é o método mais fácil de instalar o Data Guardian para Mac. No entanto, utilize este método apenas se planear instalar o cliente num computador de cada vez.

  ou

- Instalação através da linha de comandos - Para este método de instalação avançado, os administradores têm de ter experiência na sintaxe da linha de comandos. Este método pode ser utilizado para uma instalação com script, ficheiros de batch ou qualquer outra tecnologia disponível na sua organização.

Instalação interativa

1. Para o cliente Data Guardian, localize o programa de instalação em **Dell-Data-Guardian--0.x.x.xxxx.dmg.**
2. Utilize o ficheiro **.pkg** dentro de DDPSL-Explorer-0.x.x.xxxx.dmg para efetuar a instalação ou atualização. Pode utilizar uma instalação com script, ficheiros de batch ou qualquer outra tecnologia disponível na sua organização.
3. Clique duas vezes no pacote **Dell-Data-Guardian-x.x.x**.
4. Clique em **Continuar**.
5. Na janela Introdução, clique em **Continuar**.
6. Na janela Contrato de licença de software, clique em **Continuar**.
7. Clique em **Aceito** para continuar.
8. Na janela Tipo de instalação, efetue um destes passos:
   - Clique em **Instalar** e, em seguida, avance para o passo 9.
   - Na janela Selecionar destino, selecione uma das opções abaixo, clique em **Continuar instalação** e, em seguida, avance para o passo 9.
     - Instalar para todos os utilizadores deste computador
     - Instalar apenas para mim
9. Na caixa de diálogo, introduza o seu nome e a sua palavra-passe e clique em **Instalar software**.
10. Na janela Resumo, clique em **Fechar**.
11. Consulte Ativação do utilizador final.

NOTA:
Se a empresa atualizar do Cloud Edition para o Data Guardian, os utilizadores têm de efetuar novamente a autenticação e a ligação do Data Guardian ao respetivo fornecedor de armazenamento em nuvem. Para obter mais informações sobre autenticação, consulte a Ajuda do Dell Data Guardian.

Instalação com linha de comandos

1. Monte o .dmg.
2. Execute a instalação do pacote a partir da linha de comandos através do comando instalador:
   ```
   sudo installer -pkg/Volumes/Dell\ Data\ Guardian"Dell-Data-Guardian\ 0.x.x.xxxx.pkg" -target /
   ```
3. Instrua os utilizadores finais para ativarem o Data Guardian. Consulte Ativação do utilizador final.

Ativação do Data Guardian e experiência de utilizador

GUID-FCD7AF63-06D4-4D0C-8FA3-369265AB00E2

Ativação do utilizador final

Depois de abrir o Dell Data Guardian no Mac pela primeira vez, siga estes passos:

1 No Finder, selecione **Aplicações** e faça duplo clique em **Dell Data Guardian**.
2 Quando abrir a janela do Servidor Dell, introduza o endereço do servidor DDP e, em seguida, clique em **Guardar**.

É aberta a janela Credenciais.

3 Introduza o endereço de e-mail do seu domínio e palavra-passe do domínio.
4 Clique em **Iniciar sessão** para ativar o Dell Data Guardian.

Quando a aplicação Dell Data Guardian for aberta e a ativação for bem-sucedida, o nome do fornecedor de armazenamento em nuvem é ativado no painel esquerdo.

Se uma empresa pretender que todos os utilizadores colaborem através do mesmo fornecedor de armazenamento em nuvem, o administrador pode definir uma política para permitir apenas esse fornecedor e bloquear a apresentação de outros.

Se a ativação não for bem-sucedida ou se a autenticação da aplicação Dell Data Guardian for revogada ou expirar, o nome do fornecedor de armazenamento em nuvem será destacado a cinzento.

5 No painel à esquerda, selecione o fornecedor de armazenamento na nuvem.

É aberta uma janela e ser-lhe-ão solicitadas as suas credenciais.

6 Para obter mais informações sobre autenticação, consulte a Ajuda do Dell Data Guardian.

GUID-9917238E-00E5-4F56-909D-C76F09426D53

Interface de utilizador

A interface do Dell Data Guardian é semelhante à interface *Ver como colunas* do Finder no OS X. Cada coluna representa uma pasta no fornecedor de armazenamento na nuvem selecionado.

NOTA:
A barra de título pode variar consoante o sistema operativo.

Para encriptar e desencriptar ficheiros, precisa utilizar a interface do Dell Data Guardian e não o site do fornecedor de armazenamento na nuvem.

Pode executar as seguintes tarefas na janela do Dell Data Guardian:

- **Ficheiro** > **Nova Pasta** - Para criar novas pastas.

NOTA:
O Google Drive e o OneDrive adicionam automaticamente uma pasta Partilhada. No entanto, a partilha de dados no OneDrive for Business não é suportada.

- Menu Contexto - Selecione uma ou mais pastas ou ficheiros na janela principal. Em seguida, prime a tecla Controlo e clique com o botão do rato (ou clique com o botão direito do rato, se este tiver dois botões) e selecione uma opção no menu:
  - **Transferir**
  - **Mudar o nome** - Quando mudar o nome de um ficheiro da interface do Dell Data Guardian, o Dell Data Guardian sincroniza a alteração com o site do fornecedor de armazenamento em nuvem. Não mude o nome de um ficheiro .xen no website do fornecedor de armazenamento na nuvem. O ficheiro não será sincronizado.
  - **Eliminar**

    NOTA:
    O Google Drive com o Data Guardian não tem a opção Remover (remove para a reciclagem). Tem apenas a opção Eliminar, para ser consistente com outras funcionalidades do Data Guardian.
- **Desassociar** - Para desassociar o Dell Data Guardian de um fornecedor de armazenamento em nuvem, selecione o fornecedor no painel esquerdo, prima a tecla Control (ou clique com o botão direito do rato) e, em seguida, selecione Desassociar no menu.

Informações adicionais sobre ficheiros e pastas:

- Para adicionar ficheiros e pastas às pastas apresentadas na interface de utilizador do Dell Data Guardian, arraste-os do Finder no OS X ou de outras aplicações que suportam a funcionalidade arrastar e largar. Os ficheiros serão encriptados com base na política atual.
- Para desencriptar e abrir ficheiros em aplicações, clique duas vezes no ficheiro na janela do Dell Data Guardian. Se o ficheiro for modificado numa aplicação externa, este será em seguida encriptado e carregado como uma nova revisão para o fornecedor de armazenamento na nuvem.
- Para efetuar uma cópia local não encriptada, arraste um ficheiro ou pasta da janela do Dell Data Guardian para o Finder.
- O *Cloud Encryption* do 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 site do fornecedor de armazenamento em nuvem, edite-o e, em seguida, carregue-o através da interface do Dell Data Guardian.
- Os atributos expandidos não são copiados para a nuvem.

GUID-12385ECF-2D63-4BD1-8719-260F247D161E

Evite a opção Checkout (Dar Saída) no website

O Data Guardian não protege nem encripta ficheiros utilizados com a opção *Abrir e dar saída* no site OneDrive for Business ou no site de qualquer fornecedor de armazenamento em nuvem. Se um ficheiro for aberto e marcado com saída dada, não utilize o comando Abrir na interface do Dell Data Guardian, pois o carregamento automático será bloqueado.

Ao proteger os seus ficheiros com o Data Guardian, utilize a interface do Dell Data Guardian para trabalhar com ficheiros.

Se pretende trabalhar num ficheiro com propriedades especiais a partir do website de um fornecedor de armazenamento na nuvem:

1. Na interface do Dell Data Guardian, prima a tecla Controlo e clique com o botão do rato (ou clique com o botão direito do rato) num ficheiro e selecione **Transferir**.
2. Selecione e edite o ficheiro.
3. Através da interface do Dell Data Guardian, carregue o ficheiro.

GUID-B18E3439-4C04-4F3A-AADA-DD5552F902D6

Preferências da aplicação

Para abrir as Preferências:

1 Inicie o Dell Data Guardian.
2 Na barra de menus Dell Data Guardian, selecione **Preferências**.

NOTA:
Esta informação também está disponível a partir do ícone Ajuda.

Pode modificar estas definições:

- Oculte os ficheiros que começam com "." - Por predefinição, a caixa está marcada, ocultando os ficheiros. Para ver os ficheiros ocultos, desmarque a caixa.

  NOTA:
  Normalmente, os ficheiros precedidos de um ponto separador são ocultos no Finder no OS X.

- **Desassociar fornecedor de armazenamento em nuvem** - Lista os fornecedores de armazenamento em nuvem autenticados pelo Data Guardian. Para remover um fornecedor de armazenamento em nuvem do Data Guardian, selecione o nome do fornecedor e clique no botão menos (-) no canto inferior esquerdo da janela Preferências.

Políticas do servidor - O administrador do Servidor DPP define as seguintes políticas, que controlam a forma como o Data Guardian gere os ficheiros e as pastas:

- **Servidor DDP** - Lista o URL do servidor.
- **Intervalo de consulta** - Lista o intervalo em minutos que o software de cliente consulta atualizações da política.
- **Encriptar** - Política de encriptação principal que permite a encriptação de ficheiros e pastas no site do armazenamento em nuvem.
- **Apenas extensão** ou **Ocultar**

  A definição de política predefinida, Apenas extensão, apresenta o nome do ficheiro no website.

  Se uma empresa precisar de proteção adicional para ficheiros, defina esta política para **Ocultar**, para esconder o nome dos ficheiros no website da nuvem como nomes GUID.

  NOTA:
  Se a política for inicialmente definida para Apenas extensão e os utilizadores tiverem ficheiros no website na nuvem e, em seguida, a política for alterada para Ocultar, os nomes dos ficheiros pré-existentes no website não serão ocultados. Para ocultar nomes de ficheiros pré-existentes, o utilizador tem de transferir e voltar a carregar os ficheiros através da interface do Data Guardian. Caso contrário, se o utilizador editar um ficheiro, este será carregado com um nome de ficheiro oculto.

- **Documentos do Office protegidos** - protege os documentos do Office (.docx, .pptx, .xlsx, .docm, .pptm, .xlsm) na nuvem, mas apresenta a extensão do ficheiro, não uma extensão .xen.

  Se esta política estiver ativada, os documentos do Office (.docx, .pptx, .xlsx, .docm, .pptm, .xlsm) na nuvem apresentam a extensão do ficheiro, não uma extensão .xen. No entanto, não é possível abrir o ficheiro na nuvem nem depois de transferido. Se for aberto, é apresentada apenas uma página de rosto, indicando que o documento está protegido. Se o Data Guardian estiver instalado mas não autenticado, a página de rosto indica esse facto.
- **Eventos de auditoria** - Se estiver ativada, os eventos de auditoria são enviados para o Servidor Dell.
- **Geolocalização** - Se estiver ativada, os eventos de auditoria que são enviados para o Servidor Dell incluem dados de localização geográfica (latitude e longitude).

- **Beacon de retorno** - Se estiver ativada, é enviado um beacon de retorno para cada ficheiro do Office protegido.
- **URL do beacon de retorno** - Se estiver ativada, especifica o URL que vai ser utilizado quando o beacon de retorno é inserido nos ficheiros do Office protegidos.
- **Fornecedores de proteção de armazenamento em nuvem** - O nome do fornecedor é apresentado com base nas definições da política. As opções são **Box**/**Dropbox**/**Google Drive**/**OneDrive** e **OneDrive for Business**.

  Ative ou desative a encriptação dos ficheiros carregados para esse fornecedor de armazenamento na nuvem. É apresentada uma das seguintes opções:

  - **Encriptar** - Os ficheiros enviados para a nuvem são encriptados.
  - **Permitir** - O utilizador pode aceder aos ficheiros em nuvem, mas os ficheiros enviados para o site de um fornecedor de armazenamento em nuvem não são encriptados.
  - **Bloqueado** - O fornecedor de armazenamento em nuvem encontra-se indisponível e, nesse momento, isso significa que o nome do fornecedor de armazenamento em nuvem não é apresentado na janela principal.

GUID-74395D32-C5C3-46A5-A690-CE195AD50CC0

Segurança e outras considerações para clientes Data Guardian e de sincronização na nuvem

GUID-ED3DC4CF-B650-4583-83F3-84FE0288BBC3

Google Drive

O *Cloud Encryption* do Data Guardian encripta as pastas e os ficheiros na nuvem para proteger os dados. Tenha atenção a estas considerações.

- A política de segurança corporativa, definida como Proteger, proíbe o uso do Google Docs com o Data Guardian. Se estiver definido como Permitir, é possível editá-los. 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. Os Google Docs que criar são apresentados nas pastas do fornecedor de armazenamento na nuvem de Google Docs.

  No entanto, se abrir a pasta, uma caixa de diálogo avisa-o de que o Data Guardian não pode encriptar esse documento.

GUID-5454F80B-40A1-4609-BED2-7D3D08391FC4

OneDrive for Business

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

GUID-A6AA7EE4-E62B-44A2-BAC2-902473A21C42

Feedback sobre este produto

Se ativado por uma política, os utilizadores podem fornecer feedback sobre o Dell Data Guardian. O formulário de feedback está disponível a partir da barra de menu > **Fornecer feedback sobre a Proteção de dados da Dell**.

Tarefas de desinstalação do Data Guardian

Esta secção descreve o processo de administrador de desinstalação do Data Guardian. Se um utilizador final tiver uma conta de Administrador local, pode desinstalar o Data Guardian para Mac.

GUID-0AEC84CA-AADA-44B7-A403-5D8C97FFAFD5

Pré-requisitos

Para realizar a desinstalação, tem de ter uma conta de administrador.

GUID-C8A4F2ED-6FE8-4B26-A3FB-60795DD70304

Desinstalar o Data Guardian

Execute um dos seguintes passos para remover o Data Guardian:

Finder

1 Enquanto prime a tecla <opção>, selecione **Ir** na barra de menu.
2 Abra a pasta **~/Biblioteca/Application Support/Dell**.
3 Elimine a pasta **DataGuardian**.
4 A partir de **Ir** na barra de menu, abra a pasta Aplicações e elimine a aplicação **Data Guardian**.

Terminal

Pode ter o Data Guardian em uma ou ambas as seguintes localizações.

1 Utilize um ou ambos os comandos que se seguem:
   - rm -R ~/Applications/Data\ Guardian.app
   - rm -R ~/Library/Application Support/Dell/DataGuardian
2 Elimine a pasta **DataGuardian**.

Glossário

Ativa(do) - A ativação ocorre quando o computador tiver sido registado no Servidor Dell e tiver recebido, pelo menos, um conjunto inicial de políticas.

Servidor Dell - O Servidor Dell é constituído por um conjunto de componentes. Na perspetiva do lado do servidor, o produto, na sua totalidade, é designado coletivamente como Servidor Dell.

Consola de Gestão Remota - A Consola de Gestão Remota é a consola de administração da totalidade da implementação empresarial. A Consola de Gestão Remota é um componente do Dell Enterprise Server.

Servidor de segurança - Um componente do Servidor Dell que gere o Dell Data Guardian. O Security Server garante que os dados estão seguros na nuvem, seja com quem for que estes sejam partilhados. O Security Server também impede que os dispositivos internos transmitam dados confidenciais.

Utilizadores externos - Utilizadores fora do endereço de domínio da organização.