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 você a usar melhor o seu produto.

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

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

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

Guia do administrador do Dell Data Guardian para Mac

2017 - 04

Rev. A01

Índice

Introdução do Dell Data Guardian para Mac

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

GUID-DC905DCF-89A3-4B94-B120-B1ED63272AA5

Visão geral

O Dell Data Guardian para Mac protege os dados em sistemas de compartilhamento de arquivos baseados em nuvem. Computadores Mac OS X que usam o Data Guardian podem ver, modificar e criptografar arquivos em sistemas de compartilhamento de arquivos baseados em nuvem para o armazenamento seguro.

O Data Guardian para Mac e Windows pode abrir arquivos criptografados pelo outro.

O Data Guardian para Mac consiste no seguinte:

- Data Guardian:
  - **Criptografia em nuvem** - Protege os dados em sistemas de compartilhamento de arquivos baseados em nuvem como arquivos .xen.
  - **Documentos protegidos do Office** - protege documentos do Office (.docx, .pptx, .xlsx, .docm, .pptm, .xlsm) na nuvem, exibindo a extensão e o nome do arquivo original. Se protegidos, os arquivos só podem ser abertos com um cliente Data Guardian. Se aberto em outro lugar, uma folha de rosto é exibida, indicando que o documento está protegido e explica como um usuário autorizado pode solicitar o acesso aos arquivos criptografados.

    É possível definir políticas apenas para Criptografia em nuvem ou ambos os grupos de políticas. Para obter mais informações, consulte *Admin Help*.

    O Data Guardian para Mac é projetado para compartilhar arquivos dentro de provedores de criptografia em nuvem. No entanto, se políticas de "Documentos protegidos do Office" forem ativadas para Macs e se o arquivo for salvo pelo usuário final no Mac local, a auditoria e a rastreabilidade de todos os arquivos serão perdidas. Caso sua organização precise de uma rigorosa auditoria e rastreabilidade de arquivos, defina a política *Permitir ativação do Data Guardian no Mac* como "Not Selected" (Não selecionado) para impedir que o Data Guardian seja ativado em Macs.
- Security Server - Um componente do Dell Server que gerencia o Data Guardian para Mac. O Security Server garante que os dados estão seguros na nuvem, independentemente da pessoa com quem eles são compartilhados. O Security Server também protege dispositivos internos de passarem adiante dados confidenciais.
- Remote Management Console - Fornece administração centralizada da política de segurança, integra-se a diretórios existentes da empresa e cria relatórios.

  Esses componentes Dell interoperam diretamente para fornecer um ambiente seguro sem desprezar a experiência do usuário.

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

Entre em contato com o Dell ProSupport

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

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

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

Requisitos do Dell Data Guardian para Mac

Os requisitos de hardware e software de cliente são apresentados neste capítulo. Verifique se os ambientes de implementação atendem aos requisitos antes de continuar com as tarefas de implementação.

NOTA:
IPv6 não é compatível.

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

Servidor

O Data Guardian para Mac necessita que o cliente esteja conectado a um Dell Enterprise Server ou ao Dell Enterprise Server - VE, v9.6 ou superior.

GUID-371FFDE5-7A34-4288-AA88-617E73C0F9A4

Hardware para cliente Mac

A seguir, consta uma lista com hardwares suportados para o cliente Mac.

Hardware Mac

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

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

Sistemas operacionais

A seguir, consta uma lista com os sistemas operacionais suportados.

Sistemas operacionais 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 operacionais Android

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

Sistemas operacionais iOS

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

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

Provedores de armazenamento em nuvem

Com base nas configurações das políticas, as seguintes opções podem ser mostradas na interface do Dell Data Guardian. O usuário não precisa fazer download nem instalar o cliente de sincronização de nuvem.

Provedores de armazenamento em 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 realizar essas tarefas, confirme o seguinte:

- Instale o Dell Server e seus componentes. Veja uma dessas opções:
  - *Enterprise Server Installation and Migration Guide (Guia de Instalação e Migração do Enterprise Server)*
  - *Guia de Instalação e de Início Rápido do Virtual Edition*
- No Remote Management Console, atribua uma função de administrador Dell apropriada.

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

Políticas

Por padrão, o Data Guardian criptografa os arquivos dos usuários e envia eventos de auditoria ao DDP EE Server/VE Server. Para a finalidade deste documento, ambos os servidores são citados como Dell Server, a menos que uma versão específica precise ser citada (por exemplo, um procedimento é diferente ao ser usado o Dell Enterprise Server - VE).

Se quiser que os eventos de auditoria incluam dados de localização geográfica, é preciso ativar o Wi-Fi. Para obter mais informações sobre localização geográfica e eventos de auditoria, consulte *AdminHelp*.

Para alterar o comportamento padrão de cada provedor de armazenamento em nuvem suportado, configure a política de *Provedores de proteção de armazenamento na nuvem*. Caso sua empresa prefira um provedor de armazenamento em nuvem específico, defina essa política como **Bloquear** para outros provedores. Para obter mais informações sobre políticas, consulte a *AdminHelp*, que pode ser acessada no Remote Management Console do Dell Server.

NOTA:
A opção Desviar dessa política é para Windows. Se a opção Desviar for selecionada para Mac, ela será mostrada para o usuário 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 permitir downloads de cliente de nuvem

DDP Enterprise Server

1 No DDP Enterprise Server, vá até <diretório de instalação do Security Server>\webapps\cloudweb\brand\dell\resources\
2 Abra o arquivo **messages.properties** com um editor de texto.
3 Verifique se 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://[NomeDaMáquina:EndereçoIP]:[porta]/caminho/
nome_do_arquivo.dmg
```

4 Salve e feche os arquivos.
5 Vá para <diretório de instalação do Security Server> e crie uma pasta com o nome Download (Security Server\Download).
6 Na pasta Download, crie uma pasta CloudWeb (Security Server\Download\CloudWeb).
7 Adicione os instaladores do Dell Data Guardian a essa pasta.

Virtual Edition: instale manualmente outra versão do cliente de nuvem

Nenhuma ação é necessária para permitir que os usuários façam download do instalador mais recente do Dell Data Guardian. O instalador mais recente é pré-instalado no VE Security Server.

Para instalar manualmente outra versão do instalador do Data Guardian no VE Security Server, atualize o arquivo message.properties.

1 Vá para:
/opt/dell/server/security-server/webapps/root/cloudweb/brand/dell/resources/
2 Abra o arquivo **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://[NomeDaMáquina:EndereçoIP]:[porta]/caminho/
nome_do_arquivo.dmg
```

3 Salve e feche os arquivos.
4 Copie os arquivos para /opt/dell/server/security-server/download/cloudweb.
5 Adicione os instaladores do Data Guardian a essa pasta.

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

Permitir/negar usuários da lista de acesso completo/lista negra

As entradas da lista de acesso completo e da lista negra determinam quais usuários podem se registrar no Dell Server para usar o Data Guardian.

Lista de acesso completo

A lista de acesso completo permite que determinados usuários ou grupos de usuários se registrem no Dell Server e usem o Data Guardian.

Usuários externos precisam ser colocados na lista de acesso completo para permitir o registro. Veja os exemplos a seguir para permitir que os usuários se inscrevam:

Tipo de usuário	Incluir
Todos os endereços de e-mail em organização.com	`organization.com`
Um usuário específico	`jdoe@organization.com`
Todos os usuários do Gmail	`gmail.com`

Lista negra

A lista negra impede que usuários ou grupos específicos se registrem no Dell Server e usem o Data Guardian. Os usuários cujos endereços de e-mail forem inseridos na lista negra receberão uma mensagem informando-os que não podem se registrar no Data Guardian.

NOTA:
Se um usuário já estiver registrado, essa lista **não** o impede de utilizar o Data Guardian.

Você pode usar a lista negra para excluir usuários específicos que são membros de grupos aprovados na lista de acesso completo. Além disso, é possível colocar domínios inteiros na lista negra, o que impedirá que qualquer pessoa com um endereço de e-mail nesse domínio se registre. Veja os exemplos a seguir para impedir que um usuário ou grupo se registre no Dell Server:

Tipo de usuário	Incluir
Todos os endereços de e-mail em organização.com	`organization.com`
Um usuário específico e seu endereço de e-mail	`jdoe@organization.com`
Todos os usuários do Gmail	`gmail.com`

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

1 No painel esquerdo do Remote Management Console, clique em **Gerenciamento > Gerenciamento de usuário externo**.

2 Clique em **Adicionar**.

3 Selecione o tipo de acesso de registro:

Lista negra - Bloqueia o registro para um usuário ou domínio. O usuário não pode abrir um documento protegido do Office ou arquivo .xen.

Lista de acesso total - Concede o acesso a registros e a todos os arquivos para um usuário ou domínio. Se um usuário ou domínio também constar na lista negra, nenhum acesso é concedido.

4 No campo Enter Domain/Email (Inserir domínio/e-mail), digite o domínio do usuário para configurar o acesso para todo o domínio ou o endereço de e-mail para configurar o acesso somente para esse usuário.

5 Clique em **Adicionar**.

Para obter mais informações sobre como usar a lista de acesso completo/lista negra, consulte *AdminHelp*, que pode ser acessado a partir do Remote Management Console do Dell Server.

Um usuário externo pode solicitar acesso à chave para um arquivo protegido a um usuário interno. Se o usuário interno não estiver disponível, é possível usar o Remote Management Console para aprovar ou negar o acesso.

1 Selecione **Gerenciamento > Gerenciamento de solicitação de chave**.

2 Para obter mais informações, selecione **?** (Ajuda).

GUID-036F598E-1FF3-4FC8-A419-2F628C92F934

Remoção remota da conta de um membro da equipe do Dropbox for Business

Se sua empresa tem o Dropbox for Business, você pode remover remotamente um membro da equipe que faz parte da conta corporativa da equipe no Dropbox for Business se, por exemplo, um usuário deixar a empresa. Os arquivos e as pastas associados à conta do membro da equipe serão removidos de todos os dispositivos usados pela conta. Isso revoga o acesso do usuário a esses arquivos.

Pré-requisitos

NOTA:
Antes de executar esse procedimento, você precisa fazer backup de todos os arquivos ou pastas da conta do membro da equipe, os quais podem ser necessários pela empresa ou por outros membros da equipe do Dropbox for Business.

Apenas um administrador do Dropbox for Business pode remover remotamente uma conta do Dropbox for Business.

O usuário final precisa ter ativado o Dell Data Guardian e estar conectado ao Dropbox for Business.

Inscrever-se no Remote Management Console

Apenas um administrador do Dropbox for Business precisa se inscrever.

1 No painel esquerdo do Remote Management Console, selecione **Gerenciamento** > **Gerenciamento do Dropbox**.
2 Na página Dropbox for Business, clique em **Registrar-se**.
O navegador é aberto no site do Dropbox for Business.
3 Se solicitado, faça login no Dropbox com sua conta de administrador do Dropbox for Business.
4 Para permitir o acesso ao Dell Data Guardian, clique em **Permitir**.
Uma página de confirmação é mostrada para indicar que a autorização do Dropbox está concedida ao DDP Enterprise Server - VE.
5 No Remote Management Console, retorne para **Gerenciamento** > **Gerenciamento do Dropbox** e clique em **Atualizar**.
O nome do administrador é mostrado.

NOTA:
Normalmente, a prática recomendada é não remover a inscrição. Entretanto, para cancelar os privilégios do Administrador do Dropbox for Business para a remoção de membros da equipe do Dropbox for Business, clique em **Desfazer o registro**.

Remoção remota da conta de um membro da equipe

NOTA:
A opção de Remoção remota está disponível apenas para contas de membros de equipe inscritas no Dropbox for Business. Se a opção de Remoção remota não for mostrada para uma conta de usuário, o usuário não inscreveu uma conta do Dropbox for Business.

1 No Remote Management Console, selecione **Populações** > **Usuários** no painel esquerdo.
2 Procure pelo usuário especificado.
3 Acesse a página **Detalhes do usuário**.
4 Na coluna Comando, clique em **Remoção remota**.
A remoção remota é realizada.

NOTA:
Antes de selecionar Remoção remota, você precisa fazer backup de todos os arquivos ou pastas da conta do membro da equipe, os quais podem ser necessários pela empresa ou por outros membros da equipe do Dropbox for Business.

5 Na confirmação para a Remoção remota, clique em **Sim**.
A página Detalhes do usuário mostra a data em que a remoção remota foi realizada.

6 Na página Membros do Console do administrador do Dropbox for Business, atualize a lista de membros da equipe.
O usuário é removido da lista. Você pode selecionar a guia **Membros removidos** para ver os usuários que foram removidos.

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

Tarefas de cliente

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

Pré-requisitos

- Verifique se os dispositivos de destino têm conectividade com:
  - https://nome_do_seu_securityserver.domínio.com:8443/cloudweb/register
  - https://nome_do_seu_securityserver.domínio.com:8443/cloudweb
- Confirme que o usuário que está executando a instalação tem uma conta de Administrador local para a instalação.
- Se estiver instalando por linha de comando, verifique se você tem o nome de domínio totalmente qualificado do Dell Security Server no qual os usuários serão ativados.

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

Práticas recomendadas

Durante a implementação, siga as práticas recomendadas de TI. Isso inclui, sem limitações:

- Ambientes de teste controlados para testes iniciais
- Implementações escalonadas para os usuários

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

Instalar o cliente

Neste momento, os usuários que foram adicionados à lista branca podem se inscrever em: https://nome_do_seu_securityserver.domínio.com:8443/cloudweb/register.

Após se inscrever, o usuário receberá um e-mail direcionando-o a https://nome_do_seu_securityserver.domínio.com:8443/cloudweb para fazer login e o download do cliente adequado.

A instalação do cliente Mac é opcional para os administradores, pois os usuários finais normalmente instalarão o cliente Mac sozinhos (após o registro) a partir do site https://yoursecurityservername.domain.com:8443/cloudweb.

Entretanto, você pode instalar o cliente Mac caso sua organização exija. Instale o cliente Data Guardian por meio da interface do usuário ou pela linha de comando usando qualquer tecnologia push disponível para a sua organização. A inscrição e a ativação pelo usuário final ainda são necessárias.

Atualização de versões anteriores do Cloud Edition

Se uma empresa tiver uma versão anterior do Cloud Edition e fizer a atualização para o Data Guardian, a versão anterior do Cloud Edition é removida.

NOTA:
Se a empresa fizer a atualização do Cloud Edition para o Data Guardian, os usuários precisam autenticar e vincular novamente o Data Guardian ao provedor de armazenamento em nuvem deles. Para obter mais informações sobre a autenticação, consulte a ajuda on-line do Dell Data Guardian.

Opções de instalação

Para instalar/fazer upgrade do cliente, selecione uma das opções a seguir:

- Interactive Installation (Instalação interativa) - Esse é o método mais fácil para instalar o Data Guardian para Mac. Entretanto, use este método apenas se você planeja instalar o cliente em um computador de cada vez.

  ou

- Command Line Installation (Instalação por linha de comando) - Para esse método avançado de instalação, os administradores devem ter experiência em sintaxe de linha de comando. Este método pode ser usado para uma instalação com scripts, arquivos de lotes ou qualquer outra tecnologia push disponível para sua organização.

Interactive Installation (Instalação interativa)

1. Para o cliente Data Guardian, localize o instalador em **Dell-Data-Guardian--0.x.x.xxxx.dmg.**
2. Use o arquivo **.pkg** dentro do DDPSL-Explorer-0.x.x.xxxx.dmg para instalar ou atualizar. Você pode usar uma instalação com scripts, arquivos de lotes ou qualquer outra tecnologia push disponível para 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 **Concordo** para continuar.
8. Na janela Installation Type (Tipo de instalação), faça um dos seguintes:
   - Clique em **Instalar** (Instalar) e, em seguida, vá para a etapa 9.
   - Na janela Seleção de destino, selecione uma opção abaixo, clique em **Continuar a instalação** e, em seguida, vá para a etapa 9.
     - Instalar para todos os usuários deste computador
     - Instalar apenas para mim
9. Na caixa de diálogo, digite o nome de usuário e a senha, e clique em **Instalar software**.
10. Na janela Resumo, clique em **Fechar**.
11. Consulte Ativação do usuário final.

NOTA:
Se a empresa fizer a atualização do Cloud Edition para o Data Guardian, os usuários precisam autenticar e vincular novamente o Data Guardian ao provedor de armazenamento em nuvem deles. Para obter mais informações sobre a autenticação, consulte a ajuda on-line do Dell Data Guardian.

Instalação por linha de comando

1. Monte o arquivo .dmg.
2. Execute a instalação do pacote por linha de comando usando o comando installer:

   ```
   sudo installer -pkg/Volumes/Dell\ Data\ Guardian"Dell-Data-Guardian\ 0.x.x.xxxx.pkg" -target /
   ```

3. Instrua os usuários finais a ativar o Data Guardian. Consulte Ativação do usuário final.

Ativação e experiência do usuário do Data Guardian

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

Ativação do usuário final

Depois de abrir o Dell Data Guardian no Mac pela primeira vez, siga estas etapas:

1 No Finder, selecione **Aplicativos**, e clique duas vezes em **Dell Data Guardian**.
2 Quando a janela Dell Server se abrir, digite o endereço do DDP Server e clique em **Salvar**.

   A janela Credenciais será aberta.

3 Digite o seu endereço de e-mail de domínio e a sua senha de domínio.
4 Clique em **Login** para ativar o Dell Data Guardian.

   Quando o aplicativo Dell Data Guardian abrir e a ativação for concluída com sucesso, o nome do provedor de armazenamento em nuvem é ativado no painel esquerdo.

   Se uma empresa desejar que todos os usuários colaborem usando o mesmo provedor na nuvem, o administrador pode configurar uma política para permitir apenas tal provedor e bloquear que outros sejam exibidos.

   Se a ativação não for bem-sucedida ou se a autenticação do aplicativo Dell Data Guardian for revogada ou vencer, o nome do provedor de armazenamento em nuvem aparecerá esmaecido.

5 No painel esquerdo, selecione o provedor de armazenamento em nuvem.

   Uma janela será aberta solicitando suas credenciais.
6 Para obter mais informações sobre a autenticação, consulte a ajuda on-line do Dell Data Guardian.

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

Interface do usuário

A interface do Dell Data Guardian é semelhante à interface *View as Columns* (Exibir como colunas) do OS X Finder. Cada coluna representa uma pasta no provedor de armazenamento em nuvem selecionado.

NOTA:
A barra de título pode variar dependendo do sistema operacional.

Para criptografar e descriptografar arquivos, é preciso usar a interface do Dell Data Guardian, e não o site do provedor de armazenamento em nuvem.

É possível realizar estas tarefas na janela do Dell Data Guardian:

- **Arquivo** > **Nova pasta** - Para criar novas pastas.

NOTA:
O Google Drive e o OneDrive adicionam automaticamente uma pasta compartilhada. Entretanto, o compartilhamento de dados no OneDrive for Business não é suportado.

- Menu contextual - selecione uma ou mais pastas ou arquivos na janela principal. Depois, clique em Controle (ou clique com o botão direito) e selecione uma opção do menu:
  - **Fazer download**
  - **Renomear** - Se você renomear um arquivo na interface do Dell Data Guardian, o Dell Data Guardian sincronizará a alteração no site do provedor de armazenamento em nuvem. Não renomeie um arquivo .xen através do site do provedor de armazenamento em nuvem. O arquivo não será sincronizado.
  - **Apagar**

    NOTA:
    O Google Drive com o Data Guardian não tem a opção Remove (Remover) (remove para a lixeira). Ele tem apenas a opção Delete (Apagar), para ser consistente com outra funcionalidade do Data Guardian.
- **Desvincular** - Para desvincular o Dell Data Guardian de um provedor de armazenamento em nuvem, selecione o provedor no painel esquerdo, clique com o botão direito (ou Control) e, em seguida, selecione Desvincular no menu.

Informações adicionais nos arquivos e pastas:

- Para adicionar arquivos e pastas a pastas exibidas na interface do usuário no Dell Data Guardian, arraste-os do OS X Finder ou de outros aplicativos que suportam o recurso "arrastar e soltar". Os arquivos serão criptografados de acordo com a política atual.
- Para descriptografar e abrir arquivos nos aplicativos, clique duas vezes no arquivo na janela do Dell Data Guardian. Se o arquivo for modificado em um aplicativo externo, o arquivo modificado será então criptografado e transferido por upload como uma nova revisão no provedor de armazenamento em nuvem.
- Para fazer uma cópia local descriptografada, arraste um arquivo ou uma pasta da janela do Dell Data Guardian para o Finder.
- A *Criptografia em nuvem* do Data Guardian não permite a edição de arquivos sem extensões. Esses arquivos são tratados como arquivos somente leitura. Para editar um arquivo sem extensão, obtenha-o por download do site do provedor de armazenamento em nuvem, edite-o e transfira-o por upload através da interface do Dell Data Guardian.
- Os atributos estendidos não serão copiados para a nuvem.

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

Evitar a opção Check-out no site

O Data Guardian não protege nem criptografa arquivos usados com a opção *Open & Check Out* (Abrir e fazer check-out) no site do OneDrive for Business ou no site de qualquer provedor de armazenamento em nuvem. Se houver um arquivo aberto e com check-out, não use o comando Open (Abrir) da interface do Dell Data Guardian, pois o upload automático será bloqueado.

Ao proteger arquivos com o Data Guardian, use a interface do Dell Data Guardian para trabalhar com os arquivos.

Se você quiser trabalhar em um arquivo com propriedades especiais a partir do site de um provedor de armazenamento em nuvem:

1 Na interface do Dell Data Guardian, clique em um arquivo com o botão direito (ou Control) e selecione **Fazer download**.
2 Selecione e edite o arquivo.
3 Na interface do Dell Data Guardian, faça o upload do arquivo.

GUID-B1BB3439-4C04-4F3A-AADA-DD5562F902D6

Preferências do aplicativo

Para abrir as Preferências:

1 Abra o Dell Data Guardian.
2 Na barra de menu Dell Data Guardian, selecione **Preferences** (Preferências).

NOTA:
Estas informações estão também disponíveis a partir do ícone Ajuda.

Você pode modificar estas configurações:

- Hide files that start with "." (Ocultar arquivos que começam com ".") - Por padrão, a caixa está marcada, ocultando os arquivos. Para ver os arquivos ocultos, desmarque a caixa de seleção.

  NOTA:
  Geralmente, os arquivos prefixados com um separador de ponto são ocultos no Finder do OS X.

- **Unlink cloud storage provider** (Desvincular provedor de armazenamento na nuvem) - Lista os provedores de armazenamento na nuvem autenticados pelo Data Guardian. Para remover um provedor de armazenamento em nuvem do Data Guardian, selecione o nome do provedor e clique no botão com sinal de menos (-) no canto inferior esquerdo da janela Preferences (Preferências).

Server Policies (Políticas de servidor) - O administrador do DDP Server define as seguintes políticas que controlam como o Data Guardian gerencia arquivos e pastas:

- **Servidor DDP** - Lista a URL do servidor.
- **Intervalo de pesquisa** - Lista o intervalo em minutos que o software cliente leva para pesquisar atualizações de política.
- **Criptografar** - Política de criptografia mestre que permite a criptografia de pastas e arquivos no site de armazenamento em nuvem.
- **Apenas a extensão** ou **Obscurecer**

  Apenas a extensão (configuração padrão da política) mostra o nome do arquivo no site.

  Se uma empresa exigir proteção adicional para os arquivos, defina essa política como **Obscurecer** para ocultar os nomes de arquivos no site de nuvem como nomes GUID.

  NOTA:
  Caso os usuários tenham arquivos no site de nuvem, se a política for definida primeiro como Apenas a extensão e então alterada para Obscurecer, os nomes dos arquivos preexistentes no site não serão obscurecidos. Para obscurecer nomes de arquivos preexistentes, o usuário precisa fazer o download e, em seguida, o upload dos arquivos por meio da interface do Data Guardian. Ou, se o usuário editar um arquivo, o upload será feito com um nome de arquivo obscurecido.

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

  Se essa política estiver ativada, os documentos do Office (.docx, .pptx, .xlsx, .docm, .pptm, .xlsm) na nuvem exibem a extensão do arquivo, e não uma extensão .xen. No entanto, não é possível abrir o arquivo na nuvem nem depois de fazer o seu download. Se for aberto, apenas a página de rosto será exibida, informando que o documento está protegido. Se você instalar o Data Guardian, mas não o autenticar, a página de rosto indicará isso.
- **Eventos de auditoria** - se ativado, envia eventos de auditoria para o servidor da Dell.
- **Geolocalização** - se ativado, eventos de auditoria que são enviados para o servidor Dell incluem dados de geolocalização (latitude e longitude).
- **Sinalizador de retorno de chamadas** - se ativado, envia um sinal de retorno de chamada para cada arquivo protegido do Office.
- **URL do sinalizador de retorno de chamadas** - se ativada, especifica a URL a ser usada quando o sinalizador de retorno de chamadas é inserido em arquivos protegidos do Office.
- **Provedores de proteção de armazenamento na nuvem** - Um nome de provedor é exibido com base nas configurações de política. As opções são **Box**, **Dropbox**, **Google Drive**, **OneDrive** e **OneDrive for Business**.

  Ative ou desative a criptografia de arquivos transferidos por upload para esse provedor de armazenamento em nuvem. Uma das seguintes opções é mostrada:

  - **Criptografar** - Arquivos enviados para a nuvem são criptografados.

- **Permitir** - O usuário pode acessar arquivos na nuvem, mas os arquivos enviados para um provedor de armazenamento na nuvem não são criptografados.
- **Bloqueado** - O provedor de armazenamento na nuvem está indisponível e, no momento, significa que o nome desse provedor não é exibido na janela principal.

GUID-74395D32-C5C3-46A5-A090-CE195AD50CC0

Segurança e outras considerações para clientes Data Guardian e Cloud Sync

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

Google Drive

A *Criptografia em nuvem* do Data Guardian criptografa pastas e arquivos na nuvem para proteger os dados. Esteja ciente dessas considerações.

- Se a política de segurança corporativa for definida como Protect (Proteger), isso proibirá o uso do Google Docs com o Data Guardian. Se ela for definida como Allow (Permitir), a edição é possível. Para obter mais informações, entre em contato com o administrador de TI.

  O Google Drive contém um aplicativo Google Docs que permite aos usuários colaborar em documentos em tempo real. Entretanto, a colaboração ocorre em um servidor do Google e os arquivos não são criptografados. Os Google Docs que você criar serão mostrados nas pastas do provedor de armazenamento em nuvem do Google Docs.

  Entretanto, se abrir a pasta, uma caixa de diálogo alertará você de que o Data Guardian não pode criptografar o documento.

GUID-5454F808-40A1-4609-BED2-7D3D06391FC4

OneDrive for Business

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

GUID-A6AA7EB4-E62B-44A2-BAC2-902473A21C42

Feedback sobre este produto

Se ativado por política, os usuários podem fornecer um feedback sobre o Dell Data Guardian. O formulário de feedback está disponível na barra de menu > **Provide Dell Data Protection Feedback** (Fornecer feedback do Dell Data Protection).

Tarefas de desinstalação do Data Guardian

Esta seção descreve o processo do administrador para desinstalar o Data Guardian. Se um usuário final tiver uma conta de administrador local, ele mesmo poderá desinstalar o Data Guardian para Mac.

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

Pré-requisitos

Você precisa ter uma conta de Administrador local para fazer a desinstalação.

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

Desinstalar o Data Guardian

Siga um dos procedimentos abaixo para remover o Data Guardian:

Finder

1 Enquanto pressiona a tecla <opção>, selecione **Ir** na barra de menu.
2 Abra a pasta **~/Library/Application Support/Dell**.
3 Remova a pasta **DataGuardian**.
4 Na opção **Ir** na barra de menu, abra a pasta Aplicativos e remova o aplicativo **Data Guardian**.

Terminal

Você pode ter o Data Guardian em um ou nos dois locais a seguir.

1 Use um ou os dois comandos a seguir:
   - rm -R ~/Applications/Data\ Guardian.app
   - rm -R ~/Library/Application Support/Dell/DataGuardian
2 Remova a pasta **DataGuardian**.

Glossário

Ativado: a ativação ocorre quando o computador é registrado no Dell Server e recebe pelo menos um conjunto inicial de políticas.

Dell Server: o Dell Server é composto por um conjunto de componentes. Quando se refere ao lado do servidor do produto como um todo, é conhecido coletivamente como Dell Server.

Remote Management Console: é o console administrativo para a implantação em toda a empresa. O Remote Management Console é um componente do Dell Enterprise Server.

Security Server: um componente do Dell Server que gerencia o Dell Data Guardian. O Security Server garante que os dados estão seguros na nuvem, independentemente da pessoa com quem eles são compartilhados. O Security Server também protege dispositivos internos de passarem adiante dados confidenciais.

Usuários externos - os usuários fora do endereço de domínio da organização.