Dell Data Guardian

Guia do usuário para Windows, Mac, Mobile e Web v2.7

Identifier	GUID-5B8DE7B7-879F-45A4-88E0-732155904029
Status	Translated

Notas, avisos e advertências

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

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

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

Identifier	GUID-8935090F-D61D-41F4-ABC8-F4654D88B0FA
Status	Translation Validated

Guia do usuário para Windows, Mac, Mobile e Web

2019 - 06

Rev. A01

Índice

Identifier	**GUID-1E29C798-6A65-41FB-8102-6**
Status	**Translation Validated**

Introdução

O *Guia do usuário do Dell Data Guardian* fornece as informações necessárias para instalar e usar o Data Guardian no Windows, Mac, Mobile ou portal da web.

Identifier	**GUID-6EE59323-7410-43F4-AD47-C5B7B04044E8**
Status	**Translation Validated**

Visão geral

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

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

  NOTA:
  O administrador informará se sua empresa usa o Data Guardian somente com documentos do Office, somente com armazenamento em nuvem, ou ambos. O administrador pode também falar sobre tipos de aplicativos e arquivos adicionais que podem ser protegidos.

O Data Guardian pode ser usado nas seguintes plataformas:

- Windows
- iOS
- Android
- Mac
- Portal da web do Data Guardian, se configurado pelo administrador

NOTA:
O Data Guardian para Mac pode abrir arquivos criptografados por outras plataformas. Alguns arquivos podem ficar disponíveis como somente leitura. A maioria das informações do usuário do Data Guardian para Mac estão dentro do software como ajuda on-line.

Identifier	**GUID-C9552E05-51A1-4C2D-AADE-C078B4639CD4**
Status	**In Translation**

Opções de criptografia para Data Guardian

De acordo com o nível de segurança estabelecido pela empresa, o administrador define políticas para proteger os dados inativos e os dados em movimento. O administrador indicará quais políticas se aplicam à empresa.

Esta lista fornece uma visão geral de algumas opções de criptografia e, em algumas plataformas, a localização das configuração de política.

Modos e documentos do Office

A política pode ser definida para proteger documentos do Office. O comportamento da criptografia pode variar de acordo com a plataforma e o modo. Para Mac, consulte a Ajuda online.

Modos	Documentos do Office
Opções do modo para **Windows e Mac**: Modo Aceitar - Você tem algumas opções para determinar que documentos do Office serão protegidos. • **Windows** e **Mac** - Uma pasta **Documentos seguros** é adicionada à raiz da pasta Documentos. Isso fornece outra forma de criptografar um arquivo. Modo Forçar protegido - Sua empresa precisa de um nível mais alto de segurança. O Data Guardian realiza uma busca por arquivos criptografados. • **Windows** e **Mac** - Outra política pode adicionar uma pasta **Documentos desprotegidos** para a raiz da pasta Documentos. Coloque documentos protegidos do Office ou tipos de Proteção básica de arquivos nesta pasta para descriptografá-los. • **Mac** - Protege arquivos em **\Users**. Estas plataformas não são baseados em modos: • Móvel • Portal Web	**Documentos do Office usados em Windows, Mac, dispositivos móveis e portal Web** • .docx • .pptx • .xlsx • .docm • .pptm • .xlsm • .pdf - Se protegido com o Data Guardian, é aberto com Adobe Acrobat Reader DC ou Microsoft Word, mas não da rede.

Documentos do Office - Windows

O administrador pode definir políticas adicionais do Data Guardian para controlar ou prevenir a perda de dados nessas opções. O comportamento da criptografia pode variar de acordo com o modo.

As opções para documentos protegidos do Office no Windows	Descrição
• Salvar - Se um documento do Office for protegido, você pode salvar conteúdo novo. (**Salvar como** esmaecido.) • Salvar de forma protegida como • Se um documento do Office já for protegido, a opção **Salvar como** fica esmaecida.	Outras informações para o Windows: • Documento **desprotegido** do Office - pode selecionar **Salvar**, **Salvar como** ou **Salvar como protegido**. • Uma borda vermelha é exibida em e-mails e documentos Office protegidos.
Copiar/colar e área de transferência	Você pode copiar ou colar de um documento protegido do Office para outro documento protegido do Office. Você não poderá colar de um documento protegido para um documento desprotegido.

As opções para documentos protegidos do Office no Windows	Descrição
Imprimir	De acordo com a política, a impressão de um documento protegido do Office pode ser permitida, ter uma marca d'água ou ser desabilitada.
Exportar (Windows e Office 2013 e superior, Mobile)	De acordo com a política, pode ser permitida, ter uma marca d'água ou ser desabilitada. **NOTA:** Se marca d'água estiver definida, os documentos do Office podem ser exportados. PDFs não podem ser exportados.
Captura de tela	De acordo com a política, pode ser permitida ou bloqueada.
Processos bloqueados Exemplo: ferramenta de corte	De acordo com a política definida pela empresa, alguns processos são bloqueados quando um documento protegido do Office do Office é aberto.
Marca d'água na tela	Quando um documento protegido do Office é aberto, a tela exibe uma marca d'água com o nome do computador e o nome do usuário.
Classificação TITUS (Windows com modo Aceitar)	Se a política estiver ativada, você pode clicar com o botão direito do mouse em um documento do Office e selecionar uma classificação TITUS. Isso oferece outra forma para os usuários protegerem um documento do Office.
Classificação de dados (Windows com modo Aceitar)	Se uma política for ativada e configurada para proteger informações confidenciais, como números de previdência social ou de cartão de crédito, o Office documentará quais dados serão criptografados.

Documentos do Office - Mac, dispositivos móveis e portal Web

O comportamento da criptografia pode variar de acordo com a plataforma e o modo. O administrador indicará quais se aplicam à empresa.

Opção de criptografia	Descrição
Mac - Interface do Dell Data Guardian	**Mac** - Carregar um documento protegido para criptografar. Baixar um documento protegido para descriptografar. Depois de editar um documento protegido, as alterações são salvas no arquivo original, seja na nuvem ou no local.
Móvel - no aplicativo Data Guardian • Imprimir • Marca d'água na tela • Marca d'água oculta • Exportar	**Dispositivos móveis** - De acordo com a política: • Documentos do Office dentro do aplicativo Data Guardian são protegidos. • A impressão de um documento protegido do Office pode ser permitida, ter uma marca d'água ou ser desabilitada. • Quando um documento protegido do Office é aberto, a tela exibe uma marca d'água com o nome do computador e o nome do usuário.
Portal Web • Marca d'água na tela	**Portal Web** - Você pode carregar documentos protegidos ou desprotegidos, mas qualquer arquivo carregado é protegido ao clicar em Baixar.

Opção de criptografia	Descrição
	Quando um documento protegido do Office é aberto, a tela exibe uma marca d'água com o nome do computador e o nome do usuário.

Opções adicionais

O comportamento da criptografia pode variar de acordo com a plataforma e o modo. O administrador indicará quais se aplicam à empresa.

Opção	Descrição (modos Aceitar e Forçar protegido)
Proteção básica de arquivos - Permite que tipos de aplicativos e arquivos adicionais sejam protegidos. (Windows, Mac, dispositivos móveis e portal da web) • Exemplos: .txt ou .png **NOTA:** Atualmente, nenhuma borda vermelha é exibida para esses tipos de arquivo, mesmo quando eles são protegidos.	O administrador pode configurar uma política para especificar os aplicativos e arquivos a serem criptografados. **Windows, Mac e dispositivos móveis** - Esses arquivos são verificados e criptografados. • **Mac** - para extensões de arquivo definidas pelo administrador, criptografa esses tipos de arquivo na pasta /Users. **Portal Web** - Com base na política, esses arquivos podem ser somente leitura ou o usuário pode editá-los.
Compartilhar documentos protegidos do Office com **usuários externos**. (Windows, Mac, dispositivos móveis e portal da web) A folha de rosto apresenta uma lista de links para registro e informações sobre como instalar o Data Guardian.	• Usuários externos e **Windows** - você pode também adicionar uma **restrição de data (embargo)** em documentos protegidos do Office e PDFs protegidos. • **Portal Web** - você pode fazer upload de arquivos compartilhados no portal Web. Você não pode compartilhar um arquivo de dentro do portal web, mas pode compartilhá-lo depois de baixá-lo.
Arquivo adulterados ou página de capa (Windows, Mac, dispositivos móveis e web)	Em documentos do Office, o Data Guardian pode analisar documentos protegidos e detectar algumas formas de adulteração.
Grupos de acesso (local) (Windows, Mac, dispositivos móveis e portal da web)	Quando ativado pelo administrador, apenas pessoas no seu grupo de acesso poderão visualizar os seus arquivos criptografados. No caso de arquivos privados, você poderá conceder acesso a usuários internos e externos e eles poderão solicitar o acesso. Com base na política adicional, você pode clicar com o botão direito do mouse em um e-mail do Outlook rotulado como [PROTEGIDO] e remover o acesso para usuários individuais.
Cerca geográfica (dispositivos móveis)	Apenas os usuários em uma área específica podem acessar arquivos em seus celulares.
Criptografia em e-mail do Outlook (Windows)	Dependendo da política, um botão *Proteger* permite que você criptografe o conteúdo de um e-mail e seus anexos. Quando enviada a usuários externos, a folha de rosto apresenta uma lista de links para registro e informações sobre como instalar o Data Guardian.

Hospedado ou no local

Se você precisar instalar o Data Guardian por conta própria, seu administrador confirmará qual opção se aplica à sua empresara.

NOTA:

Para aplicativos móveis, se o Workspace ONE estiver instalado, você pode autenticar-se no Data Guardian com logon único.

Hospedado no Dell Security Center	Dell Management Server no local
Uma solução SaaS (Software as a Service, software como serviço) para gerenciamento do software Dell Data Security. Se sua empresa for multitenant, o administrador fornecerá uma ID de instalação. Quando exibida a usuários que ainda não têm acesso a documentos protegidos, a folha de rosto inclui informações sobre a ID da instalação. Todas as plataformas - se um tenant deixar de pagar por determinado período, ele poderá ser suspenso.	Um servidor no local dentro da rede da empresa para gerenciamento do software Dell Data Security. O administrador fornecerá o nome do URL do Dell Server.

Criptografia na nuvem

O comportamento da criptografia pode variar de acordo com a plataforma e o modo. O administrador indicará quais se aplicam à empresa.

Plataformas	Descrição
Móvel	Consulte Usar a proteção em nuvem com dispositivos móveis.
Mac	Consulte a ajuda on-line.
Portal Web	Consulte a ajuda on-line.
Windows	Atualmente, a proteção da criptografia em nuvem do Data Guardian foi desativada no Windows para evitar problemas de compatibilidade com funções mais recente dos provedores de serviço em nuvem. Para exibir arquivos .xen já protegidos com a criptografia em nuvem, use o aplicativo móvel do Data Guardian, portal Web ou Data Guardian para Mac.

Configurações das políticas

Algumas plataformas incluem uma lista parcial de configurações de políticas para o dispositivo.

Plataforma	Localização das configurações de política
Mac	Painel *Preferências*
Móvel	Ícone **Configurações** > **Sobre**
Portal Web	Ícone **Configurações** > **Sobre**

Identifier	**GUID-DEFFD392-F513-445E-A87C-2CE7250245A2**
Status	**Translation Validated**

Suporte adicional

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

Identifier	**GUID-1DE0401E-4073-46BA-95E3-**
Status	**Translation Validated**

Requirements

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

Identifier	**GUID-7C606C28-5532-4F36-AFA3-03126F14A6EF**
Status	**Translation Validated**

Dell Server

O Data Guardian para Windows, Mac e móvel exige o Servidor de gerenciamento de segurança ou o Servidor de gerenciamento de segurança virtual v9.6 ou superior. O cliente Web do Data Guardian exige o Servidor de gerenciamento de segurança ou o Servidor de gerenciamento de segurança virtual v9.8 ou superior. 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 Security Management Server Virtual).

Identifier	**GUID-198D0A89-3C37-4C12-87A4-1F801B60DB21**
Status	**In Translation**

Data Guardian para Windows

- As práticas recomendadas de TI devem ser seguidas durante a implementação. Isso inclui, sem limitações, ambientes de teste controlados para testes iniciais e implantações escalonadas para os usuários.
- A conta de usuário que executa a instalação/upgrade/desinstalação precisa ser a de um usuário Admin local ou de domínio, que pode ser temporariamente atribuída por uma ferramenta de implementação, como o Microsoft SMS ou o Dell KACE. Não há suporte para um usuário que não é administrador mas possui privilégios elevados.
- Faça backup de todos os dados importantes antes de iniciar a instalação/desinstalação.
- Não realize alterações no computador, incluindo a inserção ou a remoção de unidades externas (USB), durante a instalação.
- O Data Guardian é compatível com versões específicas do Microsoft Office 2016 e do Microsoft Office 365 Business e Business Premium. Ele é incompatível com o Office 365 Business Essentials.
- O Data Guardian para Windows é compatível com Workspace ONE. O instalador do Data Guardian para Workspace ONE e a instalação do MSI incluem uma extensão .msi.
- O Data Guardian v2.4 e superiores no Windows é compatível com ambientes Air Gap, mas com algumas limitações. Atualmente, os dados em geolocalização em eventos de auditoria e arquivos de embargo não são compatíveis. O Web beacon requer alguns configurações.
- Certifique-se de que os dispositivos de destino tenham conectividade com https://yoursecurityservername.domain.com:8443/cloudweb/register e https://yoursecurityservername.domain.com:8443/cloudweb.
- Antes de implantar o Data Guardian, será melhor se os dispositivos de destino ainda não tiverem as contas de armazenamento na nuvem configuradas. Se os usuários decidirem manter suas contas existentes, eles deverão garantir que todos os arquivos que precisem ser mantidos *descriptografados* sejam transferidos para fora do cliente de sincronização antes da instalação do Data Guardian.
- Os usuários finais deverão estar preparados para reiniciar seus computadores quando o cliente for instalado.
- O Data Guardian não interfere no comportamento dos clientes de sincronização. Portanto, os administradores e os usuários deverão se familiarizar com o modo como esses aplicativos funcionam antes de implantar o Data Guardian. Para obter mais informações, consulte suporte ao Box em https://support.box.com/home, suporte ao Dropbox em https://www.dropbox.com/help ou suporte ao OneDrive em http://windows.microsoft.com/en-us/onedrive/onedrive-help#onedrive=other.

- Documentos protegidos do Office são compatíveis com Mozy, uma solução complementar do Data Guardian, bem como outros produtos de armazenamento por nuvem, e-mail e NFS.
- Embora o Dell Encryption não seja exigido, se usado, o cliente de criptografia deverá ser v8.12 ou posterior.
- O Data Guardian é incompatível com a ferramenta Windows System Restore ou o Windows Insider Preview.
- O Redirecionamento de Pasta da Microsoft não é suportado no Data Guardian.
- Verifique periodicamente dell.com/support para obter a documentação e recomendações técnicas mais recentes.

Pré-requisitos

Pré-requisitos de .exe

Se ainda não estiver instalado, o instalador instalará o pacote redistribuível do Microsoft Visual C++ 2017 (x86 e x64).

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

Pré-requisitos .msi

É necessário instalar o Microsoft Visual C++ 2017 Redistributed Package (x86 e x64).

NOTA:
Além disso, se você estiver executando um MSI, é preciso instalar também o Visual Studio 2010 Tools for Office Runtime (x86 e x64).

Pré-requisitos gerais

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

Hardware

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

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

Sistemas operacionais

A tabela a seguir detalha os sistemas operacionais suportados.

Sistemas operacionais Windows (32 bits e 64 bits)

- Windows 7 SP1: Enterprise, Professional, Ultimate
- Windows 8.1 Update 0-1: Enterprise Edition, Pro Edition
- Windows 10: Education, Enterprise, Pro Version 1703 (Creators Update/Redstone 2) até a versão 1809 (October 2018 Update/ Redstone 5)

NOTA:
O cliente precisa ter um desses sistemas operacionais, caso contrário ele será bloqueado. Se necessário, uma configuração em uma chave de registro permite que o administrador substitua o bloco.

Para ser compatível com o Redstone 4, é preciso fazer o upgrade do agente antes de fazer o upgrade do sistema operacional. Consulte https://www.dell.com/support/article/us/en/04/sln307922.

NOTA:
O Data Guardian não é compatível com o Windows Defender Exploit Guard (WDEG) da Microsoft no Redstone 3 e superior ou com o Kit de Ferramentas Avançado de Experiência de Mitigação (EMET) no Redstone 2 e inferior.

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

O Data Guardian não é compatível com várias versões do Office em um computador.

Microsoft Office

O Data Guardian é compatível com as seguintes versões do Office. No entanto, você precisa ter apenas uma versão do Office instalada.

Microsoft Office

- Office 2013 SP1
- Office 2016
- Office 2019
- Office 365 ProPlus: versões 1705, 1708 e 1803 (Canal semianual)

Identifier	**GUID-371FFDE5-7A34-4288-AA88-617E73C0F9A4**
Status	**In Translation**

Data Guardian para 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

Hardware Mac

- 10 GB de espaço livre em disco

Sistemas operacionais

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

Sistemas operacionais Mac

- macOS Sierra 10.12.6
- macOS High Sierra 10.13.6
- macOS Mojave 10.14.4 - 10.14.5

Provedores de armazenamento em nuvem

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

Provedores de armazenamento em nuvem

- DropBox
- Box
- Google Drive

  NOTA:
  Google Backup e Sync não suportados.

- OneDrive
- OneDrive for Business

Microsoft Office

O Data Guardian para Mac é compatível com as versões a seguir do Office.

Microsoft Office

- Office 2013 SP1
- Office 2016
- Office 2019

Identifier	GUID-70934847-A1D7-4AD3-8822-A1E474D4ECD6
Status	In Translation

Aplicativo Data Guardian for Mobile

A lista abaixo apresenta os sistemas operacionais suportados no aplicativo Data Guardian for Mobile.

Sistemas operacionais Android

- 5.0 - 5.1.1 Lollipop
- 6.0 - 6.0.1 Marshmallow
- 7.0 - 7.1.2 Nougat
- 8.0 - 8.1 Oreo
- 9.0 Pie

Sistemas operacionais iOS

- iOS 10.x - 10.3
- iOS 11.x - 11.4.1
- iOS 12.x—12.1.4

Sistema operacional Chromebook

O Chrome OS versão M53 ou superior é necessário para executar aplicativos Android no Chrome OS. Esses dispositivos são validados para executar aplicativos Android no Chrome OS, mas confirme sua opção com seu representante de vendas:

- https://www.chromium.org/chromium-os/chrome-os-systems-supporting-android-apps

Microsoft Office

O aplicativo Data Guardian for Mobile abre arquivos criados com as versões a seguir do Office.

Microsoft Office

- Office 2013 SP1
- Office 2016
- Office 2019

Identifier	GUID-E0E57A65-225C-46FB-9E51-60FAC92BA57A
Status	In Translation

Data Guardian para Web

Para ativar o cliente Web do Data Guardian, o administrador configura uma máquina virtual para hospedar o cliente Web e se comunicar com o Dell Server v9.8 ou superior.

Os seguintes ambientes virtualizados podem ser usados para implantar o cliente Web do Data Guardian.

Ambientes virtualizados

- **VMware ESXi 6.7**
  - CPU x86 de 64 bits necessária
  - Computador host com no mínimo dois núcleos
  - Mínimo de 8 GB de RAM recomendado
  - Não é necessário ter um sistema operacional específico
  - Consulte a página http://www.vmware.com/resources/compatibility/search.php para obter uma lista completa dos sistemas operacionais host compatíveis
  - O hardware precisa estar em conformidade com os requisitos mínimos do VMware
  - Mínimo de 4 GB de RAM para recurso dedicado de imagem
  - Consulte http://pubs.vmware.com/vsphere-67/index.jsp para obter mais informações

- **VMware ESXi 5.5**
  - CPU x86 de 64 bits necessária
  - Computador host com no mínimo dois núcleos
  - Mínimo de 8 GB de RAM recomendado
  - Não é necessário ter um sistema operacional específico
  - Consulte a página http://www.vmware.com/resources/compatibility/search.php para obter uma lista completa dos sistemas operacionais host compatíveis
  - O hardware precisa estar em conformidade com os requisitos mínimos do VMware
  - Mínimo de 4 GB de RAM para recurso dedicado de imagem
  - Consulte http://pubs.vmware.com/vsphere-55/index.jsp para obter mais informações

- **Microsoft Hyper-V**
  - Processador de 64 bits com Conversão de Endereços de Segundo Nível (SLAT)
  - Mínimo de 8 GB de RAM recomendado
  - O hardware precisa estar em conformidade com os requisitos mínimos do Hyper-V
  - Consulte https://docs.microsoft.com/en-us/virtualization/hyper-v-on-windows/reference/hyper-v-requirements para obter mais informações.

NOTA:
Esses requisitos mínimos representam vinte e cinco ou menos conexões simultâneas a um único portal Web.

Provedores de armazenamento em nuvem

Com base nas configurações de política, o portal da web do Data Guardian pode acessar esses provedores de armazenamento em nuvem.

Provedores de armazenamento em nuvem
• OneDrive for Business

Microsoft Office

O Data Guardian para Web abre arquivos criados com as seguintes versões do Office.

Microsoft Office
• Office 2013 SP1
• Office 2016
• Office 2019

Identifier	**GUID-F414365D-DE5B-4703-88AB-FCB73F3BD14D**
Status	**Translation Validated**

Outros requisitos

Atualmente, a autenticação de vários fatores (MFA) do Amazon Cognito não é compatível com a plataforma Data Guardian.

Identifier	**GUID-E2815EA1-85AF-4049-B317-DF016FBA39EE**
Status	**Translation Validated**

Navegadores da Web

Você pode usar o Data Guardian com o Internet Explorer, Mozilla Firefox, Google Chrome e Microsoft Edge.

Para Mac, o Safari também é compatível.

Identifier	**GUID-582A5665-D2A2-4B98-A51D-5F14376D98BA**
Status	**Translation Validated**

Adobe Acrobat

Para Windows e Mac, arquivos .pdf protegidos podem ser abertos com o Adobe Acrobat Reader DC.

NOTA:

Os seguintes não são suportados: Adobe Acrobat *Standard* DC, Adobe Acrobat *Pro* DC, CC e Adobe Acrobat DC.

Identifier	GUID-36045ECC-D303-4A63-9ABA
Status	In Translation

Instalar ou desinstalar o Data Guardian no Windows

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

Esteja preparado para reiniciar o computador depois que o Data Guardian for instalado.

Identifier	GUID-D0717325-F700-400C-BC03-5FD8190A81A9
Status	In Translation

Visão geral sobre as tarefas de instalação para o Windows

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

Instalar o Data Guardian

Tarefa	Descrição	Para obter mais informações
Instalar o Data Guardian	Determine se: O usuário precisa instalar o Data Guardian Administrador já instalou o Data Guardian - passe para a próxima etapa.	O usuário instala: Consulte Instalar o Data Guardian de forma interativa no Windows. Reinicialize e vá para a próxima etapa.
Confirmar o estado de ativação	Confirme, na área de notificações, se o ícone do Data Guardian tem uma marca de seleção verde  .	Se o ícone tiver um ponto de exclamação laranja, consulte Possíveis problemas com a ativação - Armazenamento em nuvem e Documentos protegidos do Office. **NOTA:** Se você abrir um documento do Office e for exibida uma página de rosto com informações sobre instalação ou ativação, o administrador poderá ter definido políticas para proteger documentos do Office. Confirme se o Data Guardian está instalado e ativado.

Opções para Windows

Tarefa	Descrição	Para obter mais informações
Consulte o menu da área de notificações	Fornece informações úteis sobre arquivos, pastas e solução de problemas.	Entender itens do menu da área de notificação do Data Guardian

Identifier	GUID-B54EDFCA-AFBB-4BD0-8427-515A3E052962
Status	In Translation

Pastas pré-existentes com arquivos descriptografados

Ao implantar o Data Guardian, será melhor se os dispositivos de destino ainda não tiverem a conta do provedor de armazenamento na nuvem configurada.

Se uma conta do provedor de armazenamento em nuvem estiver configurada com pastas sincronizadas com o computador local antes da instalação do Data Guardian:

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

Identifier	GUID-7BBFA9B6-C19E-44E8-908C-F5AF181462C8
Status	In Translation

Instalar o Data Guardian interativamente no Windows

Você precisa ser um administrador local para instalar o Data Guardian. Se os usuários irão instalar o produto, informe-os sobre a localização da mídia de instalação.

Antes de começar

Dependendo do ambiente e do produto Data Guardian, determine qual destes você precisa:

Hospedado no Dell Security Center	Dell Management Server no local
Se o seu ambiente hospedado for multi-usuário, você precisará de um ID de instalação.	Certifique-se de que conhece o nome do Dell Server.

Instalar o Data Guardian

Esteja preparado para reiniciar o computador depois que o Data Guardian for instalado.

1. Para fazer download do instalador do Data Guardian, acesse o local especificado pelo administrador.
2. Com base no sistema operacional, selecione o instalador de 32 bits ou 64 bits e copie-o para o computador local. Estes são exemplos de nomes de instalador:
   - Hospedado no Dell Security Center - os nomes dos instaladores têm extensão .exe
   - no local - os nomes dos instaladores têm:
     - extensão .exe
     - extensão .msi para Workspace ONE e instalação MSI
3. Clique duas vezes no arquivo para abrir o instalador.
4. Se for mostrado um aviso de segurança, clique em **Executar**.
5. Selecione um idioma e clique em **OK**.
6. Se aparecer uma mensagem perguntando se você quer instalar o Pacote Redistribuível do Microsoft Visual C++ 2015 ou o Microsoft .NET Framework 4.5.2 Client Profile, clique em **OK**.
7. Na página de boas-vindas, clique em **Avançar**.

8 Leia o contrato de licença, aceite os termos e condições e clique em **Avançar**.

9 Na tela Pasta de destino, clique em **Avançar** para fazer a instalação no local padrão de C:\Arquivos de Programas\Dell\Data Guardian \.

Não instale o Data Guardian nas pastas C:\Usuários, C:\Windows, ou na raiz de qualquer unidade.

10 Selecione uma dessas opções:

Hospedado no Dell Security Center	Dell Management Server no local
Uma solução SaaS (Software as a Service, software como serviço) para gerenciamento do software Dell Data Security.	Um servidor no local dentro da rede da empresa para gerenciamento do software Dell Data Security.

a Selecione **Hospedado no Dell Security Center**.

b Opcionalmente, se sua empresa for multi-usuário, digite um ID de instalação.

> **NOTA:**
> Se sua empresa for multi-usuário e você não digitar um ID de instalação, o administrador poderá adicioná-lo ao registro posteriormente.

c Clique em **Continuar**.

d Continue com a etapa 11.

a Selecione **Dell Management Server no local**.

b No campo *Nome do servidor de gerenciamento Dell:*, digite o nome do Dell Server com o qual o computador irá se comunicar, como server.domain.com. Não é necessário incluir www ou http(s). Esse dado é fornecido pelo administrador.

> **NOTA:**
> Não desmarque a caixa de seleção *Ativar verificação da confiabilidade do SSL*, a menos que seu administrador instrua que você o faça.

c Clique em **Avançar**.

d Na tela Confirmar informações do servidor de gerenciamento Dell, verifique se o endereço URL do Dell Server está correto. O instalador acrescenta www ou http(s) e a porta. Clique em **Avançar**.

e Continue com a etapa 11.

11 Na janela Tipo de gerenciamento, selecione a opção:

- Uso interno – Um usuário com endereço de e-mail no domínio da empresa.

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

Uma janela de status mostra o andamento da instalação.

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

14 Clique em **Sim** para reiniciar.

A instalação doData Guardian está concluída.

15 Os usuários devem confirmar a ativação. O ícone da área de notificações do Data Guardian deve ter uma marca de seleção verde  .

> **NOTA:**
>
> Dependendo da forma como o Data Guardian é implantado dentro da empresa, a ativação pode não ser imediata. No entanto, se a ativação não ocorrer, o usuário deverá ativar manualmente.

Identifier	**GUID-AF4BEC71-F3FB-43E9-A588-FA2C2BC7E4BD**
Status	**Translation Validated**

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

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

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

Execute um destes processos:

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

Identifier	**GUID-10DDD78A-61B2-4AE9-9DF4-0527FEE42D0D**
Status	**In Translation**

Ativar o Data Guardian

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

1 Faça login no Windows.

Na área de notificações, é exibido um ícone de blindagem com um ponto de exclamação laranja.

2 Clique no ícone do **Data Guardian** na área de notificações e selecione **Ativação do usuário**.

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

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

Após o término da ativação, uma marca verde é exibida no ícone da área de notificações do Data Guardian  .

4 Confirme seu status de modo de usuário. Clique na área de notificações e selecione **Detalhes**.

5 Na parte superior, confirme o modo de usuário:

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

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

> **NOTA:**
> Se o Modo Usuário listar **Não registrado**, seu Data Guardian ainda não foi ativado.

Identifier	**GUID-8882A835-A7A8-4C7B-8330-3080F871A121**
Status	**Translation Validated**

Dell Security Center Hospedado e Tenant Suspenso

Com o Dell Security Center Hospedado, se um tenant deixar de pagar por determinado período, ele poderá ser suspenso. Isso se aplica a Windows, Mac, dispositivos móveis e portal da web.

Os usuários internos e externos do Data Guardian poderão vivenciar as seguintes situações:

- Todas as plataformas - Se você tentar instalar o Data Guardian, ativar ou fazer login, uma caixa de diálogo será exibida indicando que o tenant está suspenso.
- Mac - Se o tenant for suspenso com o Data Guardian aberto, a caixa de diálogo do tenant suspenso será exibida após você fechar o Explorer e todos os arquivos e, em seguida, tentar abrir um arquivo protegido.
- Portal da Web:
  - Se você já estiver conectado e carregar um arquivo criptografado, uma mensagem indicará Falha no upload.
  - Se um arquivo criptografado ou não criptografado foi carregado e o tenant logo em seguida ficou suspenso, será exibida uma mensagem de Falha no download.
  - Se você se desconectar e tentar fazer login novamente, uma caixa de diálogo será exibida indicando que o tenant está suspenso.

Entre em contato com o administrador.

Identifier	**GUID-43BA606D-3F31-4E67-97B4-039DE9CEBC65**
Status	**In Translation**

Entender itens do menu da Área de notificações do Data Guardian

Tela de detalhes

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

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

Para ter acesso à tela Detalhes:

Clique com o botão direito no ícone da área de notificações do **Data Guardian** e, a seguir, clique em **Detalhes**.

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

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

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

Modo de usuário:

- **Usuário interno** - usuário dentro desse endereço de domínio
- **Usuário externo** - usuário fora desse endereço de domínio

- **Não registrado** - um usuário interno ou externo cujo Data Guardian não está ativado

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

URL do servidor: Dell Server que se comunica com esse cliente.

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

Versão da política: versão da política gerada pelo Dell Server.

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

Nome: nome do arquivo

Nuvem: este recurso foi desabilitado e não tem mais dados.

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

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

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

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

Pasta: nome do caminho completo da pasta.

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

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

Leitura de arquivo Xen: este recurso foi desabilitado.

*Criado pelo n**avegador***: *Verdadeiro* ou *Falso*.

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

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

Anteriormente, a criptografia em nuvem do Data Guardian tinha uma área **Pastas** na tela Detalhes. Atualmente, a criptografia na nuvem foi desativada.

Identifier	**GUID-5726752F-D15C-479E-8E8E-6BBE27B23F90**
Status	**Translation Validated**

Check for Policy Updates

Se o administrador modifica uma política e notifica você sobre uma atualização de política, vá para a área de notificações do Windows, clique no ícone do **Dell Data Guardian** e selecione **Verificar se há atualizações de política**.

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

Identifier	**GUID-62C18A73-A619-46BF-BE3A-76911412C43A**
Status	**Translation Validated**

Localizar arquivos de log

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

Para localizar os arquivos de log:

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

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

Identifier	**GUID-E67381E8-70C7-46BE-A822-9B5C48B0FFC3**
Status	**Translation Validated**

Atualizar o Data Guardian

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

Identifier	**GUID-CC8C1B76-3E85-415F-AAE0-3C20521D70A6**
Status	**In Translation**

Desinstalar o Data Guardian do Windows

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

Identifier	**GUID-FB8AEF07-F76C-4E52-9920-B56A973DB1E6**
Status	**In Translation**

Desinstalar o Data Guardian

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

Copiar arquivos para a unidade local

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

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

As pastas e os arquivos no site do cliente de sincronização permanecerão criptografados, mesmo que você faça download deles. Para vê-los, será preciso reinstalar o Data Guardian. Ou você pode visualizá-los no portal da web do Data Guardian.

Desinstalar o Data Guardian

1 Use o Painel de controle do Windows para desinstalar o programa.
2 Selecione **Dell Data Guardian** e clique em **Alterar** no menu superior.
3 Clique em **Avançar** quando a tela Boas-vindas for mostrada.
4 Selecione **Remover** e clique em **Avançar**.
5 Uma mensagem de aviso é exibida para confirmar a desinstalação do Dell Data Guardian. Caso positivo, clique em **Avançar.**
6 Na tela Remover o programa, clique em **Remover**.
A janela de status mostrará o andamento.
7 Se for exibida uma caixa de diálogo de erro do cliente de sincronização, clique em **Continuar**.
8 Se uma caixa de diálogo indicar que você tem um documento do Office aberto, clique em **OK**, feche o documento do Office e recomece a desinstalação.
9 Clique em **Concluir** quando a tela Concluído for exibida.
10 Clique em **Sim** para reiniciar.

A desinstalação doData Guardian está concluída.

Identifier	**GUID-05F5667F-C3BE-4C5E-B64D-5629C60C049D**
Status	**Translation Validated**

Provide Feedback to Dell

Se seu administrador tiver habilitado o feedback, você poderá fornecer feedback à Dell sobre este produto. O formulário breve de feedback contém duas perguntas sobre o seu nível de satisfação, uma área para comentários e uma escala de classificação (em que 10 indica o mais alto nível de satisfação).

Para acessar oData Guardian, clique no ícone na área de notificações e selecione **Enviar feedback**.

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

Identifier	GUID-E68E0B8D-7519-4C11-A918-
Status	In Translation

Usar o Data Guardian no Windows

O administrador já configurou as políticas para proteger os documentos e indicará quais dessas opções se aplicam à empresa.

Identifier	GUID-162A20CF-D1AD-4701-9A28-1000DB2FE1D4
Status	In Translation

Visão geral das opções

Esta visão geral mostra um resumo dos possíveis opções para o Data Guardian de acordo com a política definida pelo administrador. Esses documentos serão protegidos quando você compartilhá-los com outros usuários ou armazená-los em mídia removível.

Opção	Descrição	Para obter mais informações
Documentos do Office e acionados por macro	Esses incluem: .docx, .pptx, .xlsx, .docm, .pptm, .xlsm e .pdf.	Consulte Observar as opções do menu Arquivo para determinar o nível de segurança para Documentos do Office. Você terá um destes modos: • Aceitar • Forçar protegido
Proteção básica de arquivos	Esses são os tipos de aplicativos e arquivos adicionais que a empresa deseja criptografar e que o administrador configurou.	Consulte Proteger tipos de aplicativos e arquivos adicionais com a proteção básica de arquivos.
Opções adicionais	Esses podem se aplicar a documentos do Office, arquivos básicos ou ambos.	Consulte Opções adicionais para Data Guardian.
Compartilhar um arquivo com um usuário externo	Um usuário tem um endereço de e-mail sem domínio (seja alguém de uma empresa diferente ou usuário interno que deseje acesso aos arquivos protegidos de um endereço de e-mail sem domínio.	Consulte Usar o Data Guardian como usuário externo.

Trabalhar on-line com documentos protegidos

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

Guia Propriedades do arquivo > Dell Data Guardian

Em documentos protegidos do Office, você pode clicar com o botão direito e selecionar **Propriedades**. Uma guia **Dell Data Guardian** é exibida com informações, como a ID de chave do arquivo e o acesso e os dados no embargo.

Ícones de sobreposição para Windows

No Data Guardian 2.2 e superior, os ícones de sobreposição são exibidos em arquivos protegidos no Explorador de arquivos. Ao clicar com o botão direito do mouse em um arquivo protegido, a guia Dell Data Guardian fornece mais informações.

Marca d'água oculta

Com base na política definida pelo administrador, os documentos protegidos do Office podem ter uma marca d'água oculta que identifica o usuário. Se você imprimir ou compartilhar o documento, a marca d'água persistirá.

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

Identifier	**GUID-E88C0771-29BE-4292-AD26-F913747EE0FC**
Status	**Translation Validated**

Usar documentos do Office com o modo protegido do Data Guardian

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

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

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

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

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

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

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

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

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

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

    NOTA:
    Com o modo Force-Protected, a política também ativa horários específicos para verificar seu computador e localizar arquivos desprotegidos do Office, e alterá-los para o modo Protegido. Você precisa estar conectado à rede para que o Data Guardian verifique todos os arquivos do Office desprotegidos.
  - **Documentos >** Pasta **Desprotegidos** - Se ativada pela política no modo Forçar protegido (mas fora do modo Aceitar), uma pasta Desprotegida é adicionada à raiz da pasta Documentos. Os documentos do Office nessa pasta estão criptografadas. Se você apagar a pasta, ela será recriada.

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

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

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

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

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

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

Identifier	**GUID-077EC2B6-61AD-4F13-95D0-CF91EF0143AF**
Status	**In Translation**

Usar modo de aceitação para proteger documentos do Office

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

Trabalhar com opções de menu do Arquivo no modo Aceitar

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

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

Menu Arquivo	Modo Aceitar e documentos protegidos do Office
Abra	Os arquivos abrem normalmente
Salvar	• Opções: Documento já protegido - Salva como protegido. Desprotegido - Salva como desprotegido. Para protegê-lo, clique em **Salvar como protegido**. • Documento somente leitura - Uma caixa de diálogo indica que não é possível salvar um documento desprotegido. A janela Salvar como é exibida e é preciso salvá-lo com outro nome de arquivo.
Salvar como	Tem as opções padrão (mas não o modo protegido)
Salvar de forma protegida como	A única opção no campo Salvar como tipo é Protegido do Office
Imprimir	**Ativado** No entanto, para documentos protegidos do Office, se um administrador desativa Imprimir por meio da política, você ainda pode selecionar Imprimir, mas uma caixa de notificação será exibida indicando que o documento protegido não pode ser impresso. Se o seu administrador permite Imprimir, outra política poderá colocar uma marca d'água contendo nome de usuário, nome de domínio e ID do computador em cada página que você imprimir.
Compartilhar	**Ativado** para documentos protegidos do Office. **Desativado** para documentos desprotegidos.
Exportar (Office 2013 e superior)	Pode estar ativado ou esmaecido com base nas políticas definidas pelo administrador.
Exportação protegida (Office 2013 e superior)	Se a opção de menu Exportar estiver esmaecida e Exportação protegida estiver ativada, o documento exportará com uma marca d'água, contendo nome de usuário, nome de domínio e ID do computador em cada página. Se você exportar um documento no modo protegido para um usuário externo, ele poderá abrir e ver o documento, mas não poderá exportar ou imprimi-lo.

Trabalhar online com documentos protegidos habilitados para macro

Com um documento protegido habilitado para macro, a macro existe, mas está bloqueada. No entanto, atualmente, o Data Guardian só pode controlar um documento habilitado para macro depois que o documento recém-protegido (.docm, .pptm, .xlsm) seja fechado e

reaberto. Além disso, se você salvar um documento protegido com uma macro como desprotegido, precisará fechar e reabrir a documento, para que a macro seja executada.

Classificação TITUS e modo Aceitar

Se uma política estiver ativada, o administrador configura algumas classificações TITUS para criptografar um documento com essa classificação. Você pode clicar com o botão direito do mouse em um documento desprotegido do Office e selecionar essa classificação TITUS. Isso oferece outra forma de proteger um documento do Office.

Classificação de dados e modo Aceitar

Se essa política estiver ativada, seu administrador pode definir as classificações para determinado conteúdo, como número de previdência social, número de cartão de crédito ou outras informações confidenciais. O administrador avisará quais informações foram classificadas como confidenciais. Quando você salva um documento com informações que estão de acordo com essas regras de classificação, o documento é criptografado.

Se você usar tags em um documento do Office para acionar uma classificação de dados usada nos metadados de tag do arquivo da política, a tag que você usar no documento do Office diferenciará entre maiúsculas e minúsculas e deverá corresponder ao uso de maiúsculas e minúsculas feito pelo administrador na política.

NOTA:

Se esta política estiver ativada, uma limpeza fará com que os arquivos atendam às regras de classificação para serem criptografados. No entanto, quando você criar o arquivo, você pode clicar com o botão direito e selecionar **Proteger arquivo**.

Veja também Criptografia de e-mails do Outlook com o Data Guardian.

Solução de problemas para o modo Aceitar

Se a política do Data Guardian desativou a impressão para documentos protegidos do Office, você ainda pode selecionar Imprimir em **Arquivo > Informações** ou ao clicar com o botão direito do mouse em um arquivo protegido do Office no Windows Explorer. Porém, se você selecionar Imprimir, ocorrerá o seguinte:

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

Determinar que documentos do modo Aceitar estão protegidos

Se você tiver o modo Aceitar e quiser confirmar se um documento está protegido ou não, abra o documento e a barra de título o mostrará como protegido.

NOTA:

Se você tiver o modo Forçar protegido, todos os documentos do Office estarão protegidos.

Identifier	GUID-5E368002-F3BB-48A7-9A30-B4591019B21F
Status	In Translation

Usar modo Forçar protegido para proteger documentos do Office

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

Trabalhar com opções de menu do Arquivo no modo Forçar protegido

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

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

Menu Arquivo	Modo Forçar protegido para documentos protegidos e desprotegidos
Abra	Documentos desprotegidos abertos no modo somente leitura.
Salvar	• O documento está protegido. • Documento somente leitura - Você pode editá-lo, mas não poderá salvar o original. Quando você clicar em Salvar, a janela Salvar como protegido será exibida e você precisará salvar o documento no modo protegido com um novo nome. • Documentos remotos - Se você abrir um documento em um local remoto e ele não estiver protegido, precisará salvá-lo na unidade local para modificar e salvar. Você não pode salvar o documento no local remoto. **NOTA:** Clicar em Salvar abre a janela Salvar como, e a única opção no campo Salvar como tipo é Protegido do Office (documentos, apresentação, ou pasta de trabalho).
Salvar como	**Desativado**
Salvar de forma protegida como	A única opção no campo Salvar como tipo é Protegido do Office
Imprimir	**Ativado** No entanto, para documentos protegidos do Office, se um administrador desativa Imprimir por meio da política, você ainda pode selecionar Imprimir, mas uma caixa de notificação será exibida indicando que o documento protegido não pode ser impresso. Se o seu administrador permite Imprimir, outra política poderá colocar uma marca d'água contendo nome de usuário, nome de domínio e ID do computador em cada página que você imprimir.
Compartilhar	**Desativado**
Exportar (Office 2013 e superior)	Pode estar ativado ou esmaecido com base nas políticas definidas pelo administrador.
Exportação protegida (Office 2013 e superior)	Se a opção de menu Exportar estiver esmaecida e Exportação protegida estiver ativada, o documento exportará com uma marca d'água, contendo nome de usuário, nome de domínio e ID do computador em cada página. **NOTA:** Se você exportar um documento no modo protegido para um usuário externo, ele poderá abrir e ver o documento, mas não poderá exportar ou imprimi-lo.
Trabalhar online com documentos protegidos habilitados para macro	

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

Identifier	GUID-669244A9-0658-46A3-A9EB-A5D349D7EDBC
Status	In Translation

Opções adicionais para Data Guardian

Opções de menu adicionais para documentos protegidos do Office

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

Clicar com o botão direito do mouse > Proteger

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

Colar

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

- É possível copiar e colar dados protegidos ou desprotegidos no documento original protegido ou para um PDF protegido. No entanto, nenhum PDF desprotegido pode ser aberto no Adobe Acrobat Reader DC.
- Você não poderá copiar ou colar de um documento protegido para um documento desprotegido. Nada será mostrado na área de transferência, e uma mensagem de texto específica para a empresa informará que não é possível colar no documento desprotegido ou não gerenciado.

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

Arrastar e soltar no modo protegido

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

Abrir e editar um PDF protegido com o Adobe Acrobat Reader DC

Quando usar o Acrobat Reader DC:

- você pode adicionar anotações a um arquivo .pdf protegido ou preencher um formulário. Quando você salvar o arquivo, um novo .pdf protegido, que inclui as alterações, será criado. Esta é a funcionalidade do Acrobat Reader DC.
- Para aumentar a segurança, quando um arquivo .pdf protegido for aberto com o Acrobat Reader DC, o acesso à Internet será bloqueado até que o Acrobat Reader DC seja fechado.
- Para aumentar a segurança, se um pdf protegido estiver aberto, o usuário não conseguirá usar o e-mail.

NOTA:
Você não pode abrir um arquivo .pdf protegido pela rede. Você pode usar o Word para abrir um arquivo .pdf pela rede.

Impressão de envelopes e etiquetas

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

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

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

Opções adicionais

Processos bloqueados

Com base na política definida pelo administrador, alguns processos, como a ferramenta de corte, podem ser bloqueados. O seu administrador pode informá-lo sobre esses processos. Além disso, uma caixa de diálogo informa que o processo está bloqueado.

- **Modo Forçar protegido** - Se o administrador definir uma política para bloquear o botão *PrtScr*, isso também pode bloquear o recurso de usar telas de toque ou tablets para captura de telas.
- O Windows com RS5 tem o aplicativo Captura e Esboço (antiga Ferramenta de corte). Com o Data Guardian, o administrador pode ativar uma política que bloqueia esse aplicativo para melhorar a segurança.

Anexar um documento protegido a um e-mail do Outlook

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

É possível anexar documento protegido do Office, tipos de arquivos adicionais protegidos com base na política ou arquivos .xen.

Para Windows com Data Guardian, se você anexar um documento protegido, o Data Guardian incluirá informações de como acessar o arquivo criptografado que está contido no e-mail.

- Usuários internos - As informações são exibidas com um link para fazer o download de um cliente.
- Usuários externos - As informações são exibidas com um link para registrar e fazer o download de um cliente.

> **NOTA:**
> Para que as informações anexadas sejam exibidas, é necessário enviar o e-mail do Microsoft Office Outlook, e não da versão do Outlook baseada na Web.

Criptografia de e-mails do Outlook com o Data Guardian

Com base na política do Data Guardian v2.0.1 e posterior, os usuários internos têm a opção *Proteger* no lado superior esquerdo do Outlook para criptografar tanto o e-mail quanto os anexos. O emissor e o remetente devem ter o Data Guardian instalado e ativado.

A criptografia de e-mails do Outlook do Data Guardian é compatível com o Office 2013 e versões posteriores, mas não é compatível com web mail.

Para usar:

1 No canto superior esquerdo, clique em **Proteger**.
2 Para um endereço de e-mail externo, clique em **Sim** para confirmar o compartilhamento de chaves ou **Não** se escolher não enviar o e-mail.

A melhor prática é ter um e-mail aberto por vez. Se mais de um estiver aberto, certifique-se de clicar no e-mail para direcionar o foco para a janela dele antes de clicar no botão Proteger. O botão Proteger deve ficar cinza quando você não pairar o cursor sobre ele.

Os dados em movimento estão protegidos. Nesta versão de testes, a prevenção de perda de dados (DLP) para dados em repouso tem suporte parcial. Versões futuras continuarão a melhorar a segurança.

Para minimizar a DLP quando um e-mail criptografado for aberto, algumas ações estão desativadas ou bloqueadas:

- *Etapas rápidas do Outlook*
- *Mover*, *Mover para a pasta* e ações adicionais de pasta
- Setas *Avançar* e *Voltar*
- *Encaminhar*
- Algumas opções de clique com o botão direito

Para minimizar a DLP quando um e-mail criptografado for aberto, estas ações são controladas:

- *Copiar/Colar*
- Impressão e *exportação* de dados
- Algumas opções de clique com o botão direito
- Pasta de rascunhos e *Salvamento automático*

Para de destinatários de e-mail no Outlook

Ao abrir esse um e-mail criptografado do Outlook, um aviso será exibido de que o documento está protegido e que o usuário deverá clicar duas vezes para abrir o arquivo. Nenhum conteúdo do e-mail é exibido na visualização, apenas a folha de rosto. A folha de rosto lista o nome do Dell Server para no local ou uma ID de instalação para o tenant específico se o seu Hospedado no Dell Security Center for multitenant. A folha de rosto também inclui um link para fazer o download do cliente do Data Guardian.

Classificação de e-mail

Relatório local para documentos protegidos do Office criptografados com classificação de dados (Modo Aceitar)

Para proteger documentos do Office e PDFs confidenciais, seu administrador pode definir uma política para verificar e criptografar arquivos de acordo com a classificação de dados. Informações confidenciais podem incluir números da previdência social, números de cartões de crédito, endereços dos Estados Unidos ou dados específicos de empresas. O administrador informará se suas informações confidenciais farão com que seus arquivos sejam criptografados.

Para ver um relatório local sobre os arquivos criptografados devido à classificação de dados e o motivo da criptografia:

1 Acesse **C:\Users\<username>\AppData\Local\Dell\Data Guardian**.

2 Abra o **Classification Report.log**.

> **NOTA:**
> Se um arquivo estiver no processo de criptografia, a entrada pode ter várias linhas até que a criptografia esteja concluída.

Identifier	**GUID-D11E8451-72A7-4179-8693-28D0FAFF9B8B**
Status	**In Translation**

Proteger tipos de aplicativos e arquivos adicionais com a proteção básica de arquivos

O administrador informará se as políticas permitirem que tipos de aplicativos e arquivos adicionais sejam criptografados. Se alguém abrir um arquivo criptografado com a proteção básica de arquivos, mas não tiver o Data Guardian instalado, o conteúdo fica ilegível.

Visão geral da proteção básica de arquivos

Aplicativos

Estes são exemplos de aplicativos que o administrador pode desejar criptografar:

- Notepad
- Wordpad
- Visio
- MS Paint

> **NOTA:**
> Alguns aplicativos têm apenas o suporte parcial do Data Guardian e o administrador informará quais.

Tipos de arquivo

Estes são exemplos de tipos de arquivos adicionais que podem ser
configurados: .txt, .rtf, .csv, .odt, .vsdx, .png, .jpg, .jpeg, .jpe, .jfif, .gif, .tif, .tiff, .bmp

Windows, Mac e dispositivos móveis

Quando a política da proteção básica de arquivos for configurada, o Data Guardian analisa os computadores dos usuários e criptografa todos os arquivos locais com essas extensões. Os arquivos criptografados com a proteção básica de arquivos podem ser visualizados e editados usando o aplicativo associado à extensão de arquivo.

> **NOTA:**
> Arquivos em pastas do sistema específicas não são criptografados, como AppData. Também pastas relacionadas aos documentos protegidos do Office, como a pasta Documentos seguros.

Ícones de sobreposição para Windows

No Data Guardian 2.2 e superior, os ícones de sobreposição são exibidos em arquivos protegidos no Explorador de arquivos. Ao clicar com o botão direito do mouse em um arquivo protegido, a guia Dell Data Guardian fornece mais informações.

Excluir alguns arquivos da varredura no Windows ou Mac (antes de a varredura ser ativada)

Se a sua empresa decidir criptografar um tipo de arquivo adicional, como .txt, talvez você não queira ou precise que todos os arquivos com essa extensão sejam verificados e criptografados.

Antes de ativar a Proteção básica de arquivos para essa extensão, o administrador pode definir outra política que permita adicionar uma pasta ao computador local e os arquivos nessa pasta não sejam verificados. O administrador pode definir uma política, criar um nome de pasta, fornecer o nome da pasta e sugerir onde você pode adicionar essa pasta. Esses arquivos podem ser necessários para o seu sistema ou arquivos que não exigem proteção.

> **IMPORTANTE:**
> Você deve criar a pasta antes de o administrador ativar a política de Proteção básica de arquivos.

1 Use o nome e o caminho da pasta fornecidos pelo administrador.
   - Para Mac, navegue até **o painel Preferências > Exclusões de proteção básica de arquivos**. O nome da pasta a ser criada e o caminho são exibidos aqui.

2 Adicione arquivos com a extensão especificada, como .txt, que não precisam ser criptografados. Como alternativa, você pode adicionar subpastas com nomes criados pelo usuário.

NOTA:
Se você tiver arquivos com essa extensão que foram previamente criptografados, colocá-los nessa pasta não os descriptografará. Eles permanecem criptografados. Se você tiver uma pasta **Documentos desprotegidos**, que o administrador pode criar por meio de outra política, você pode colocar os tipos de Proteção básica de arquivos nesta pasta para descriptografá-los.

3 Depois que a Proteção básica de arquivos estiver ativada, se você tiver arquivos desprotegidos com essa extensão em uma rede ou unidade externa, poderá copiá-los para a pasta excluída. Eles permanecem descriptografados. Do contrário, eles são criptografados.

Se o computador tiver mais de um usuário, somente o usuário conectado no momento poderá colocar arquivos nessa pasta e excluí-los da varredura. Todos os arquivos que outro usuário colocar nessa pasta passarão por varredura e serão criptografados.

Remoção de uma extensão de arquivo no Windows ou Mac

O administrador poderá decidir remover uma extensão de arquivo. Se o fizer, o seu computador passará por uma varredura para descriptografar esses tipos de arquivo.

- A aba *Propriedades > Dell Data Guardian* dos arquivos criptografados não será mais exibida.
- Se você tiver sobreposição de ícones de arquivo, eles não serão mais exibidos.
- A descriptografia poderá levar vários minutos para ser concluída. Se o arquivo com essa extensão ainda estiver criptografado, ele poderá ter sido aberto durante a varredura ou armazenado em um servidor de arquivos ou outra localização.

Entre em contato com o administrador para solicitar a recuperação de arquivos com essa extensão que não foram descriptografados.

Aplicativos do Office

Você pode usar um aplicativo do Office para abrir um arquivo criptografado com a proteção básica de arquivos, mas o conteúdo fica disponível como somente leitura.

Portal da Web

Em Configurações > Políticas, se Proteção básica de arquivos estiver definida como Verdadeiro, o administrador adicionou tipos de arquivos não Office ao baixá-los do portal da Web. O administrador deve informar os tipos de arquivo.

NOTA:
Se você fizer o upload de um tipo de arquivo que ainda não é compatível com suporte, o conteúdo ficará ilegível no portal da Web.

É possível fazer o upload de tipos de arquivos não Office, sejam eles criptografados ou não. No entanto, ao fazer o download do arquivo não Office, a extensão varia.

Arquivos não Office (como .txt ou .png)	Descrição do download
Criptografado antes do upload Exemplo: arquivos não Office já criptografados pelo Windows ou Mac.	Quando baixados do portal da Web, mantêm a extensão do arquivo, como .txt ou .png.
Arquivos não criptografados	Quando baixados do portal da Web, a extensão do arquivo varia com base em o administrador ter adicionado ou não a extensão a uma política. No entanto, são criptografados. Exemplos de arquivos .txt baixados do portal da Web: • **nomedoarquivo.txt** - O administrador adicionou o tipo de arquivo .txt a uma política.

Arquivos não Office (como .txt ou .png)	Descrição do download
	• **nomedoarquivo.txt.xen** - O tipo de arquivo .txt não foi incluído na política. O arquivo é criptografado, mas adiciona uma extensão .xen.

Se a política *Edit* estiver ativada no portal da Web, os usuários poderão editar arquivos não Office.

Identifier	**GUID-801B897D-9A0F-48C0-B46C-A3726B8BD9E4**
Status	**Translation Validated**

Documentos Office protegidos e adulterados

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

Se um usuário interno adulterar um documento protegido do Office:

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

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

Identifier	**GUID-A8209D75-E380-4809-A55A-CF89E3FBE29A**
Status	**In Translation**

Ver pastas e arquivos do cliente de sincronização na nuvem

Se você tiver uma pasta de cliente de sincronização no seu computador e Data Guardian criptografá-la, esses arquivos serão criptografados na nuvem.

Se você usar o portal da web do Data Guardian para criptografar arquivos, eles poderão ser criptografados como arquivos .xen. Não é possível abrir arquivos .xen criptografados no Windows. Você pode visualizá-los em um dispositivo móvel com o Data Guardian ou no portal da web.

Identifier	**GUID-7A2816C4-2882-4B5B-B2C6-A8032B1C4508**
Status	**Translation Validated**

Compartilhar documentos protegidos do Office com usuários externos

Com Data Guardian, você pode compartilhar um documento protegido do Office por e-mail, mídia removível, compartilhamento de rede ou pode carregá-lo para a nuvem e compartilhá-lo:

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

Quando você anexa um documento e clica em Enviar, uma caixa de diálogo de confirmação exibe um lembrete de que a chave para esse documento protegido será compartilhada com o usuário externo.

Melhorar a segurança ao adicionar restrições de data

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

1 Selecione **Arquivo > Info > Restringir data**.

2 No menu suspenso, selecione uma Data de início e uma Data de término e a hora para um usuário externo ver o documento.

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

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

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

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

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

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

Identifier	GUID-FFED5E16-B72A-4858-A64D-
Status	Translation Validated

Instalar e usar o Data Guardian no Mac

O Data Guardian para Mac possui uma Ajuda incorporada para telas com informações sobre:

- A interface do Dell Data Guardian em que os usuários fazem o carregamento de arquivos a serem criptografados
- Criptografia na nuvem
- Usuários externos e restrições de acesso
- Adulteração

Na interface do Dell Data Guardian interface para Mac, clique no ícone de Ajuda.

Identifier	GUID-0DB59561-F614-4FEB-9265-6F2711737741
Status	Translated

Instalar o cliente para Mac

Se o administrador o adicionou à lista branca da sua empresa, é possível se registrar em: https://yoursecurityservername.domain.com:8443/cloudweb/register.

Após se registrar, você receberá um e-mail direcionando-o a https://yoursecurityservername.domain.com:8443/cloudweb para fazer login e o download do cliente adequado.

Você deve ser administrador local.

Para instalar o Data Guardian para Mac:

1. Para o cliente Data Guardian, localize o instalador em **Dell-Data-Guardian-Mac-0.x.x.xxxx.dmg.**
2. Use o arquivo **.pkg** dentro do Dell-Data-Guardian-0.x.x.xxxx.dmg para instalar ou atualizar.
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 Tipo de configuração, selecione um dos seguintes:

Hospedado no Dell Security Center	Dell Management Server no local
Uma solução SaaS (Software as a Service, software como serviço) para gerenciamento do software Dell Data Security. a Selecione **Hospedado no Dell Security Center**. b Clique em **Continuar**. c Continue com a etapa 9.	Um servidor no local dentro da rede da empresa para gerenciamento do software Dell Data Security. a Selecione **Dell Management Server no local**. b No campo *Nome do servidor de gerenciamento Dell:*, digite o nome do Dell Server com o qual o computador irá se comunicar, como server.domain.com. Não é necessário incluir www ou http(s). Esse dado é fornecido pelo administrador.

Hospedado no Dell Security Center	Dell Management Server no local
	c Clique em **Continuar**. d Continue com a etapa 9.

9 Na janela Tipo de instalação, faça um dos seguintes:

- Clique em **Instalar** e, em seguida, vá para a etapa 10.
- Clique em **Alterar local de instalação**.
  1 Na janela Seleção de destino, selecione todos os usuários. Atualmente, essa é a única opção.
  2 Clique em **Continuar**.
  3 Clique em **Instalar** e, em seguida, vá para a etapa 10.

10 Na caixa de diálogo, digite o nome de usuário e a senha, e clique em **Instalar software**.

11 Na janela Resumo, clique em **Fechar**.

12 Quando solicitado, mantenha o arquivo .pkg ou mova-o para a *Lixeira*.

13 Execute um destes processos:

Hospedado no Dell Security Center	Dell Management Server no local
A janela Credenciais será aberta automaticamente após a instalação. Se sua empresa for multiusuário, você precisará de um ID de instalação.	1 Feche a janela .dmg para abrir o Finder. 2 Consulte Ativação do usuário final.

1 Na janela Credenciais, digite a conta de e-mail de login e clique em **Continuar**.

2 Execute um destes processos:

- Se sua empresa for multitenant, digite uma ID de instalação e clique em **Continuar** e prossiga com a etapa 3.

  NOTA:
  Se um erro é exibido, verifique suas credenciais. Se você notar um endereço de e-mail incorreto ou ID de instalação, clique em **Reiniciar inicialização** para inserir novamente suas credenciais.

- Para tenants únicos, prossiga com a etapa 3.

3 Na janela Microsoft, digite a senha e clique em **Entrar**.

4 Na janela Azure, digite a sua senha.

5 Clique em **Fazer login**.

NOTA:
Se um erro é exibido, verifique suas credenciais. Se você notar um endereço de e-mail incorreto, clique em **Reiniciar inicialização** para inserir novamente suas credenciais.

6 A interface do Dell Data Guardian será aberta. Consulte Aplicativo Dell Data Guardian.

NOTA:
Se a empresa fizer a atualização do Cloud Edition para o Data Guardian, você deverá 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 Data Guardian.

Identifier	GUID-839E9A73-4125-4A28-84A6-4F5CC4D734AC
Status	In Translation

Ativação do usuário final (no local)

Ativação do Dell Management Server no local

Em no local, após você abrir o Dell Data Guardian pela primeira vez, você precisa fazer log-in para ativar:

1 No Finder, selecione **Aplicativos**, e clique duas vezes em **Dell Data Guardian**.

2 Quando a janela Credenciais abre, digite o endereço do Dell Server, por exemplo, company.server.com. Esse dado é fornecido pelo administrador. Por padrão, o número da porta é 8443. Se a sua empresa modificar a porta padrão para um número de porta personalizado, o administrador informará você.

> **NOTA:**
> Não selecione a caixa de seleção Erros de SSL, a menos que seu administrador instrua que você o faça.

3 Digite também seu endereço de e-mail e senha.

4 Clique em **Log-in** para ativar o Data Guardian.

5 Consulte o *aplicativo Dell Data Guardian* abaixo.

Para obter mais informações sobre a autenticação, consulte a ajuda on-line do Dell Data Guardian.

Aplicativo Dell Data Guardian

Quando o aplicativo Dell Data Guardian abrir e a ativação for concluída com sucesso, o nome do provedor de armazenamento na nuvem é exibido 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 autenticação do Data Guardian for revogada ou expirar, o nome do provedor de armazenamento na nuvem aparecerá esmaecido.

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

2 Uma janela será aberta solicitando suas credenciais. Insira suas credenciais.

Quando autenticado, o nome de fornecedor do armazenamento em nuvem é ativado.

Identifier	GUID-8882A835-A7A8-4C7B-8330-3080F871A121
Status	Translation Validated

Dell Security Center Hospedado e Tenant Suspenso

Com o Dell Security Center Hospedado, se um tenant deixar de pagar por determinado período, ele poderá ser suspenso. Isso se aplica a Windows, Mac, dispositivos móveis e portal da web.

Os usuários internos e externos do Data Guardian poderão vivenciar as seguintes situações:

- Todas as plataformas - Se você tentar instalar o Data Guardian, ativar ou fazer login, uma caixa de diálogo será exibida indicando que o tenant está suspenso.

- Mac - Se o tenant for suspenso com o Data Guardian aberto, a caixa de diálogo do tenant suspenso será exibida após você fechar o Explorer e todos os arquivos e, em seguida, tentar abrir um arquivo protegido.
- Portal da Web:
  - Se você já estiver conectado e carregar um arquivo criptografado, uma mensagem indicará Falha no upload.
  - Se um arquivo criptografado ou não criptografado foi carregado e o tenant logo em seguida ficou suspenso, será exibida uma mensagem de Falha no download.
  - Se você se desconectar e tentar fazer login novamente, uma caixa de diálogo será exibida indicando que o tenant está suspenso.

Entre em contato com o administrador.

Identifier	**GUID-D11E8451-72A7-4179-8693-28D0FAFF9B8B**
Status	**In Translation**

Proteger tipos de aplicativos e arquivos adicionais com a proteção básica de arquivos

O administrador informará se as políticas permitirem que tipos de aplicativos e arquivos adicionais sejam criptografados. Se alguém abrir um arquivo criptografado com a proteção básica de arquivos, mas não tiver o Data Guardian instalado, o conteúdo fica ilegível.

Visão geral da proteção básica de arquivos

Aplicativos

Estes são exemplos de aplicativos que o administrador pode desejar criptografar:

- Notepad
- Wordpad
- Visio
- MS Paint

> **NOTA:**
> Alguns aplicativos têm apenas o suporte parcial do Data Guardian e o administrador informará quais.

Tipos de arquivo

Estes são exemplos de tipos de arquivos adicionais que podem ser configurados: .txt, .rtf, .csv, .odt, .vsdx, .png, .jpg, .jpeg, .jpe, .jfif, .gif, .tif, .tiff, .bmp

Windows, Mac e dispositivos móveis

Quando a política da proteção básica de arquivos for configurada, o Data Guardian analisa os computadores dos usuários e criptografa todos os arquivos locais com essas extensões. Os arquivos criptografados com a proteção básica de arquivos podem ser visualizados e editados usando o aplicativo associado à extensão de arquivo.

> **NOTA:**
> Arquivos em pastas do sistema específicas não são criptografados, como AppData. Também pastas relacionadas aos documentos protegidos do Office, como a pasta Documentos seguros.

Ícones de sobreposição para Windows

No Data Guardian 2.2 e superior, os ícones de sobreposição são exibidos em arquivos protegidos no Explorador de arquivos. Ao clicar com o botão direito do mouse em um arquivo protegido, a guia Dell Data Guardian fornece mais informações.

Excluir alguns arquivos da varredura no Windows ou Mac (antes de a varredura ser ativada)

Se a sua empresa decidir criptografar um tipo de arquivo adicional, como .txt, talvez você não queira ou precise que todos os arquivos com essa extensão sejam verificados e criptografados.

Antes de ativar a Proteção básica de arquivos para essa extensão, o administrador pode definir outra política que permita adicionar uma pasta ao computador local e os arquivos nessa pasta não sejam verificados. O administrador pode definir uma política, criar um nome de pasta, fornecer o nome da pasta e sugerir onde você pode adicionar essa pasta. Esses arquivos podem ser necessários para o seu sistema ou arquivos que não exigem proteção.

IMPORTANTE:

Você deve criar a pasta antes de o administrador ativar a política de Proteção básica de arquivos.

1 Use o nome e o caminho da pasta fornecidos pelo administrador.
   - Para Mac, navegue até **o painel Preferências > Exclusões de proteção básica de arquivos**. O nome da pasta a ser criada e o caminho são exibidos aqui.

2 Adicione arquivos com a extensão especificada, como .txt, que não precisam ser criptografados. Como alternativa, você pode adicionar subpastas com nomes criados pelo usuário.

   NOTA:

   Se você tiver arquivos com essa extensão que foram previamente criptografados, colocá-los nessa pasta não os descriptografará. Eles permanecem criptografados. Se você tiver uma pasta **Documentos desprotegidos**, que o administrador pode criar por meio de outra política, você pode colocar os tipos de Proteção básica de arquivos nesta pasta para descriptografá-los.

3 Depois que a Proteção básica de arquivos estiver ativada, se você tiver arquivos desprotegidos com essa extensão em uma rede ou unidade externa, poderá copiá-los para a pasta excluída. Eles permanecem descriptografados. Do contrário, eles são criptografados.

Se o computador tiver mais de um usuário, somente o usuário conectado no momento poderá colocar arquivos nessa pasta e excluí-los da varredura. Todos os arquivos que outro usuário colocar nessa pasta passarão por varredura e serão criptografados.

Remoção de uma extensão de arquivo no Windows ou Mac

O administrador poderá decidir remover uma extensão de arquivo. Se o fizer, o seu computador passará por uma varredura para descriptografar esses tipos de arquivo.

- A aba *Propriedades > Dell Data Guardian* dos arquivos criptografados não será mais exibida.
- Se você tiver sobreposição de ícones de arquivo, eles não serão mais exibidos.
- A descriptografia poderá levar vários minutos para ser concluída. Se o arquivo com essa extensão ainda estiver criptografado, ele poderá ter sido aberto durante a varredura ou armazenado em um servidor de arquivos ou outra localização.

Entre em contato com o administrador para solicitar a recuperação de arquivos com essa extensão que não foram descriptografados.

Aplicativos do Office

Você pode usar um aplicativo do Office para abrir um arquivo criptografado com a proteção básica de arquivos, mas o conteúdo fica disponível como somente leitura.

Portal da Web

Em Configurações > Políticas, se Proteção básica de arquivos estiver definida como Verdadeiro, o administrador adicionou tipos de arquivos não Office ao baixá-los do portal da Web. O administrador deve informar os tipos de arquivo.

NOTA:

Se você fizer o upload de um tipo de arquivo que ainda não é compatível com suporte, o conteúdo ficará ilegível no portal da Web.

É possível fazer o upload de tipos de arquivos não Office, sejam eles criptografados ou não. No entanto, ao fazer o download do arquivo não Office, a extensão varia.

Arquivos não Office (como .txt ou .png)	Descrição do download
Criptografado antes do upload Exemplo: arquivos não Office já criptografados pelo Windows ou Mac.	Quando baixados do portal da Web, mantêm a extensão do arquivo, como .txt ou .png.
Arquivos não criptografados	Quando baixados do portal da Web, a extensão do arquivo varia com base em o administrador ter adicionado ou não a extensão a uma política. No entanto, são criptografados. Exemplos de arquivos .txt baixados do portal da Web: • **nomedoarquivo.txt** - O administrador adicionou o tipo de arquivo .txt a uma política. • **nomedoarquivo.txt.xen** - O tipo de arquivo .txt não foi incluído na política. O arquivo é criptografado, mas adiciona uma extensão .xen.

Se a política *Edit* estiver ativada no portal da Web, os usuários poderão editar arquivos não Office.

Identifier	GUID-FC539BCB-1939-4E0A-8A36-
Status	Translation Validated

Instalar e usar o Data Guardian Mobile com iOS ou Android

Esta seção descreve informações básicas sobre como usar o Data Guardian Mobile com dispositivos iOS ou Android. Quando o administrador define uma política para ativar o Data Guardian, os arquivos ficam criptografados e protegidos. É preciso que o aplicativo Data Guardian seja instalado no seu dispositivo móvel para ver arquivos criptografados.

Identifier	GUID-116F412E-15BE-4E29-A886-5A308BA693ED
Status	Translated

Pré-requisito

Antes de usar o aplicativo Data Guardian, determine quais desses você precisa com base no seu ambiente:

Hospedado no Dell Security Center	Dell Management Server no local
Se o seu ambiente hospedado for multi-usuário, você precisará de um ID de instalação.	Certifique-se de que saiba o nome do Dell Server, como por exemplo, server.domain.com. Esse dado é fornecido pelo administrador.

Identifier	GUID-A802F8F9-1B8F-47DD-8525-518A4C004221
Status	Translation Validated

Introdução ao Data Guardian Mobile

Siga esta sequência quando usar o Data Guardian Mobile.

Tarefa	Descrição	Veja esta seção
Instalar o Data Guardian - Determinar uma opção:	O administrador já instalou O usuário precisa instalar	Instalado pelo administrador: toque no aplicativo Data Guardian e faça login. O usuário instala: veja uma destas opções: • Instalar em um dispositivo iOS • Instalar em um dispositivo Android
Determinar quais as políticas se aplicam a dispositivos móveis	O administrador indicará quais as políticas se aplicam.	Você pode ter: • Documentos do Office protegidos • Proteção na nuvem • Opções adicionais

Tarefa	Descrição	Veja esta seção
Navegar no Gerenciador de arquivos	Consulte as opções do Data Guardian.	Navegar no Gerenciador de arquivos
Se a política de proteção em nuvem estiver ativada, acesse sua conta do fornecedor de armazenamento em nuvem	No dispositivo, vá para o Gerenciador de arquivos do aplicativo Data Guardian e toque no seu provedor de armazenamento em nuvem.	Consulte Acessar sua conta do fornecedor de armazenamento em nuvem.

De acordo com as políticas do Data Guardian, você pode:

- Arquivos protegidos do Office (.docx, .pptx, .xlsx, .docm, .pptm, .xlsm, .pdf) mantêm sua extensão de arquivo.
- Tipos de aplicativos e arquivos adicionais, como .txt.
- Os arquivos não Office na nuvem têm a extensão .xen.

Em dispositivos móveis com o Data Guardian, você pode:

- Criar pastas e arquivos
- Apagar pastas e arquivos
- Compartilhar um documento com um usuário externo (se a política estiver ativa para visualizações externas)

Identifier	**GUID-618A6EAF-794D-4077-A675-AC9ACA624CC3**
Status	**In Translation**

Instalar ou desinstalar o Data Guardian em um dispositivo iOS através da App Store

Instalar em um dispositivo iOS

Pré-requisito: se o seu dispositivo for compatível com um scanner de impressão digital Touch ID e você quiser usá-lo em vez de um PIN, configure o dispositivo para Touch ID antes de instalar Data Guardian.

1 No seu dispositivo, toque em **App Store** e procure por **Data Guardian Mobile**.
2 Selecione e instale o aplicativo **Data Guardian**.
3 Toque na caixa de seleção para aceitar o contrato de licença.
4 Selecione uma dessas opções:

Hospedado no Dell Security Center	No local
Uma solução SaaS (Software as a Service, software como serviço) para gerenciamento do software Dell Data Security. a Toque em **Hospedado no Dell Security Center**. b Digite o e-mail. c Toque em **Enviar**. **NOTA:** Se o seu endereço de e-mail for encontrado em mais de um tenant, digite a ID de instalação. d Na janela do Microsoft Azure, digite a senha.	Um servidor no local dentro da rede da empresa para gerenciamento do software Dell Data Security. a Toque em **No local**. b Para o campo Servidor na tela de login, digite o nome do Dell Server da sua empresa, como server.domain.com. c Digite o nome de usuário e a senha. d Toque em **Entrar**.

Hospedado no Dell Security Center	No local

e Toque em **Entrar**.

5 Quando solicitado, toque no sensor de impressão digital ou crie um PIN.

Agora a sua conta está ativada e a tela do Gerenciador de arquivos do Data Guardian é exibida.

Desinstalar o aplicativo Data Guardian

1 Na gaveta Aplicativos iOS, toque e segure o ícone do Data Guardian.
2 Toque em **x**.
3 Toque em **Excluir**.

Identifier	GUID-7247F5B1-D730-4DE6-97BA-7E88AD40B7E4
Status	In Translation

Instalar ou desinstalar o Data Guardian em um dispositivo iOS com Workspace ONE

Se você tiver o Workspace ONE instalado, você pode autenticar-se no Data Guardian com logon único. Estas etapas são as mesmas para Hospedado no Dell Security Center ou Dell Management Server no local.

Seu administrador enviará por push o aplicativo Data Guardian para o seu dispositivo.

1 Quando for perguntado se deseja instalar o aplicativo do **Data Guardian**, toque em **OK**.
2 Execute o aplicativo do **Data Guardian**.
3 No contrato de licença, toque em **Aceitar**.
4 Na opção para selecionar o Workspace ONE ou o Data Guardian, toque em **Workspace ONE** para fazer um logon único
5 Digite uma senha.
6 Quando solicitado, crie um PIN.

> **NOTA:**
> Se fizer login no Workspace ONE, você só precisará digitar seu PIN para o Data Guardian.

Agora a sua conta está ativada e a tela do Gerenciador de arquivos do Data Guardian é exibida.

Identifier	GUID-D045F8A7-9124-4843-BAF6-E0BB27CE1046
Status	In Translation

Instalar ou desinstalar o Data Guardian em um dispositivo Android através do Google Play

Instalar em um dispositivo Android

1 No seu dispositivo, toque em **Google Play** e procure por **Data Guardian Mobile**.
2 Selecione e instale o aplicativo **Data Guardian**.
3 Toque na caixa de seleção para aceitar o contrato de licença.
4 Selecione uma dessas opções:

Hospedado no Dell Security Center	Dell Management Server no local
Uma solução SaaS (Software as a Service, software como serviço) para gerenciamento do software Dell Data Security. a Toque em **Hospedado**. b Digite o e-mail. c Toque em **Enviar**. **NOTA:** Se o seu endereço de e-mail for encontrado em mais de um tenant, digite a ID de instalação. d Na janela do Microsoft Azure, digite a senha. e Toque em **Entrar**.	Um servidor no local dentro da rede da empresa para gerenciamento do software Dell Data Security. a Toque em **No local**. b Para o campo Servidor na tela de login, digite o nome do Dell Server da sua empresa, como server.domain.com. c Digite o nome de usuário e a senha. d Toque em **Entrar**.

5 Quando solicitado, crie um PIN.

Agora a sua conta está ativada e a tela do Gerenciador de arquivos do Data Guardian é exibida.

Desinstalar o aplicativo Data Guardian

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

Identifier	GUID-37A6FDB2-CD4D-4EB3-BDE1-EC151BC08814
Status	In Translation

Instalar ou desinstalar o Data Guardian em um dispositivo Android com Workspace ONE

Se você tiver o Workspace ONE instalado, você pode autenticar-se no Data Guardian com logon único. Estas etapas são as mesmas para Hospedado no Dell Security Center ou Dell Management Server no local.

1 No dispositivo, toque em **Hub**.
2 Toque em **Catálogo do aplicativo**.
3 No aplicativo Dell Data Guardian, toque em **Instalar**.
4 Em *Confirmar instalação*, toque em **Instalar**.
5 Em *Google Play Protect*, toque em **Permitir**.
6 Ao receber a mensagem do aplicativo instalado, toque em **Concluído**.
7 Toque em **Abrir** para executar o aplicativo do Data Guardian.
8 Na opção para autenticar com Workspace ONE ou Data Guardian, toque em **Workspace ONE** para fazer logon único.
9 No contrato de licença, toque na caixa de seleção.
10 Toque em **logon único**.
11 Quando solicitado, crie um PIN.

NOTA: Se fizer login no Workspace ONE, você só precisará digitar seu PIN para o Data Guardian.

Agora a sua conta está ativada e a tela do Gerenciador de arquivos do Data Guardian é exibida.

Desinstalar o aplicativo Data Guardian

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

Identifier	**GUID-5B8DFEFC-DC7C-42AE-A662-627068964BC8**
Status	**In Translation**

Navegue até o Gerenciador de arquivos

No Gerenciador de arquivos do Data Guardian, é possível usar o armazenamento local ou a nuvem. O Gerenciador de arquivos se abre quando você abrir o Data Guardian.

Tela do Gerenciador de arquivos

As pastas padrão para o Gerenciador de arquivos tela incluem:

- Documents
- Downloads
- Fotos

Tela Criar novo

Toque no ícone Adicionar (**+**) e a tela *Criar novo* exibirá estas opções:

- Documento
- Planilha
- Apresentação (PowerPoint)
- Foto
- Pasta
- Serviços de nuvem

Opções de navegação em gaveta

Toque no ícone de navegação em gaveta. As opções incluem:

- **Navegador**
- **Gerenciador de arquivos**
- Ícone de **Configurações:**
  - Botão **Alterar PIN** (se estiver ativado pela política)
  - **Navegador**
  - **Gerenciador de arquivos (Configurações)** - Use estas opções
    - **Intervalo de atualização** - Frequência com que o Data Guardian sincroniza os serviços em nuvem. A Dell recomenda *Manual* ou *Diariamente*. Outras opções são *Por hora* ou *Semanalmente*.
    - **Aviso de download de 10 MB** - habilitar ou desabilitar. Use isso se não estiver em Wi-Fi e o tamanho do download exceder 10 MB.

- **Limpar cache** - Limpa os arquivos temporários.
  - (IOS) - **Touch ID** ou **Face ID** , dependendo da versão do iOS e se você tiver impressão digital ou reconhecimento facial pré-configurados. Toque para ativar ou desativar ao usar o Data Guardian.
  - **Sobre** - Visualizar políticas e versão do Data Guardian
  - Botão **Sair do Data Guardian**
  - **Contas em nuvem** - indica se estão vinculadas ou não vinculadas.
- **Navegador**
- **Gerenciador de arquivos** - Para retornar à tela Gerenciador de arquivos.
- **Bloquear o Data Guardian**

Opções adicionais

- Adicionar um arquivo aos Favoritos
  - No iOS, use a gaveta de navegação.
  - No Android, pressione e mantenha pressionado o nome do arquivo.

Identifier	**GUID-8826272C-679E-40FF-B0A9-D1C9888AF6E5**
Status	**Translation Validated**

Determinar as políticas para o Data Guardian Mobile

O administrador indicará quais políticas estão definidas para a empresa.

Identifier	**GUID-4C1E2DAD-C0CA-4E6F-96D4-0297C01CE8B2**
Status	**Translation Validated**

Visualizar políticas e versão do Data Guardian

Algumas das políticas do Data Guardian estão listadas em **Sobre**. Para visualizar essas políticas ou a versão do Data Guardian:

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

2 Toque em **Política**.

Com base nas políticas definidas pelo seu administrador, a lista pode incluir:

- Tamanho do PIN
- Limite de inatividade
- Falha no Login
- Copiar e colar - Permite que você a copie de um documento protegido para um documento protegido.

Versão

3 Determinar as opções de política adicionais.

Elas podem incluir:

- Documentos protegidos do Office
- Proteção na nuvem
- Políticas adicionais

Identifier	**GUID-3613C9F0-10DE-4A67-9158-1964C8D2D77E**
Status	**Translation Validated**

Usar documentos protegidos do Office com dispositivos móveis

O administrador indicará quais opções estão habilitadas para sua empresa. Quando você tiver o Data Guardian instalado e abrir um documento protegido do Office, uma mensagem mostra que o documento está sendo descriptografado.

Opções do Data Guardian para documentos do Office

Essas opções do Data Guardian são exibidas.

- **Criar** - De acordo com a configuração da política, o documento fica protegido ao ser criado. O cabeçalho desse arquivo exibe *Protected Document*(Documento protegido).
- **Copiar/Colar** - Com um documento protegido do Office, você pode copiar apenas para outro documento protegido do Office.
- **Imprimir** - De acordo com as configurações da política, o documento pode ter uma marca d'água na impressão.
- **Exportar** - De acordo com as configurações da política, o documento pode ter uma marca d'água na exportação.

Quando um documento do Office estiver aberto, toque no ícone do canto superior esquerdo para estas opções:

- **Salvar**
- **Salvar como**
- **Exportar**
- **Sair**

Opções adicionais do Office de acordo com a política:

- **Editar** - Você pode editar arquivos .docx e .ppt do Office.

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

- **Marca d'água oculta** - De acordo com a política, os documentos protegidos do Office podem ter uma marca d'água oculta que identifica o usuário. Se você imprimir ou compartilhar o documento, a marca d'água persistirá.
- **Marca d'água na tela** - Quando qualquer documento protegido do Office é aberto, uma marca d'água é exibida na tela do cliente.

Informações adicionais para documentos do Office

Documentos protegidos do Office quando estiver offline

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

Solução de problemas em documentos protegidos do Office

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

Identifier	GUID-D11E8451-72A7-4179-8693-28D0FAFF9B8B
Status	In Translation

Proteger tipos de aplicativos e arquivos adicionais com a proteção básica de arquivos

O administrador informará se as políticas permitirem que tipos de aplicativos e arquivos adicionais sejam criptografados. Se alguém abrir um arquivo criptografado com a proteção básica de arquivos, mas não tiver o Data Guardian instalado, o conteúdo fica ilegível.

Visão geral da proteção básica de arquivos

Aplicativos

Estes são exemplos de aplicativos que o administrador pode desejar criptografar:

- Notepad
- Wordpad
- Visio
- MS Paint

> **NOTA:**
> Alguns aplicativos têm apenas o suporte parcial do Data Guardian e o administrador informará quais.

Tipos de arquivo

Estes são exemplos de tipos de arquivos adicionais que podem ser configurados: .txt, .rtf, .csv, .odt, .vsdx, .png, .jpg, .jpeg, .jpe, .jfif, .gif, .tif, .tiff, .bmp

Windows, Mac e dispositivos móveis

Quando a política da proteção básica de arquivos for configurada, o Data Guardian analisa os computadores dos usuários e criptografa todos os arquivos locais com essas extensões. Os arquivos criptografados com a proteção básica de arquivos podem ser visualizados e editados usando o aplicativo associado à extensão de arquivo.

> **NOTA:**
> Arquivos em pastas do sistema específicas não são criptografados, como AppData. Também pastas relacionadas aos documentos protegidos do Office, como a pasta Documentos seguros.

Ícones de sobreposição para Windows

No Data Guardian 2.2 e superior, os ícones de sobreposição são exibidos em arquivos protegidos no Explorador de arquivos. Ao clicar com o botão direito do mouse em um arquivo protegido, a guia Dell Data Guardian fornece mais informações.

Excluir alguns arquivos da varredura no Windows ou Mac (antes de a varredura ser ativada)

Se a sua empresa decidir criptografar um tipo de arquivo adicional, como .txt, talvez você não queira ou precise que todos os arquivos com essa extensão sejam verificados e criptografados.

Antes de ativar a Proteção básica de arquivos para essa extensão, o administrador pode definir outra política que permita adicionar uma pasta ao computador local e os arquivos nessa pasta não sejam verificados. O administrador pode definir uma política, criar um nome de pasta, fornecer o nome da pasta e sugerir onde você pode adicionar essa pasta. Esses arquivos podem ser necessários para o seu sistema ou arquivos que não exigem proteção.

IMPORTANTE:

Você deve criar a pasta antes de o administrador ativar a política de Proteção básica de arquivos.

1 Use o nome e o caminho da pasta fornecidos pelo administrador.
   - Para Mac, navegue até **o painel Preferências > Exclusões de proteção básica de arquivos**. O nome da pasta a ser criada e o caminho são exibidos aqui.

2 Adicione arquivos com a extensão especificada, como .txt, que não precisam ser criptografados. Como alternativa, você pode adicionar subpastas com nomes criados pelo usuário.

   NOTA:

   Se você tiver arquivos com essa extensão que foram previamente criptografados, colocá-los nessa pasta não os descriptografará. Eles permanecem criptografados. Se você tiver uma pasta **Documentos desprotegidos**, que o administrador pode criar por meio de outra política, você pode colocar os tipos de Proteção básica de arquivos nesta pasta para descriptografá-los.

3 Depois que a Proteção básica de arquivos estiver ativada, se você tiver arquivos desprotegidos com essa extensão em uma rede ou unidade externa, poderá copiá-los para a pasta excluída. Eles permanecem descriptografados. Do contrário, eles são criptografados.

Se o computador tiver mais de um usuário, somente o usuário conectado no momento poderá colocar arquivos nessa pasta e excluí-los da varredura. Todos os arquivos que outro usuário colocar nessa pasta passarão por varredura e serão criptografados.

Remoção de uma extensão de arquivo no Windows ou Mac

O administrador poderá decidir remover uma extensão de arquivo. Se o fizer, o seu computador passará por uma varredura para descriptografar esses tipos de arquivo.

- A aba *Propriedades > Dell Data Guardian* dos arquivos criptografados não será mais exibida.
- Se você tiver sobreposição de ícones de arquivo, eles não serão mais exibidos.
- A descriptografia poderá levar vários minutos para ser concluída. Se o arquivo com essa extensão ainda estiver criptografado, ele poderá ter sido aberto durante a varredura ou armazenado em um servidor de arquivos ou outra localização.

Entre em contato com o administrador para solicitar a recuperação de arquivos com essa extensão que não foram descriptografados.

Aplicativos do Office

Você pode usar um aplicativo do Office para abrir um arquivo criptografado com a proteção básica de arquivos, mas o conteúdo fica disponível como somente leitura.

Portal da Web

Em Configurações > Políticas, se Proteção básica de arquivos estiver definida como Verdadeiro, o administrador adicionou tipos de arquivos não Office ao baixá-los do portal da Web. O administrador deve informar os tipos de arquivo.

NOTA:

Se você fizer o upload de um tipo de arquivo que ainda não é compatível com suporte, o conteúdo ficará ilegível no portal da Web.

É possível fazer o upload de tipos de arquivos não Office, sejam eles criptografados ou não. No entanto, ao fazer o download do arquivo não Office, a extensão varia.

Arquivos não Office (como .txt ou .png)	Descrição do download
Criptografado antes do upload Exemplo: arquivos não Office já criptografados pelo Windows ou Mac.	Quando baixados do portal da Web, mantêm a extensão do arquivo, como .txt ou .png.
Arquivos não criptografados	Quando baixados do portal da Web, a extensão do arquivo varia com base em o administrador ter adicionado ou não a extensão a uma política. No entanto, são criptografados. Exemplos de arquivos .txt baixados do portal da Web: • **nomedoarquivo.txt** - O administrador adicionou o tipo de arquivo .txt a uma política. • **nomedoarquivo.txt.xen** - O tipo de arquivo .txt não foi incluído na política. O arquivo é criptografado, mas adiciona uma extensão .xen.

Se a política *Edit* estiver ativada no portal da Web, os usuários poderão editar arquivos não Office.

Identifier	**GUID-36644E42-9324-479F-8128-F89D438E8F17**
Status	**Translation Validated**

Usar a proteção em nuvem com dispositivos móveis

Se o administrador ativar a proteção em nuvem, você precisará de dois aplicativos:

- Aplicativo de cliente de sincronização em nuvem - consulte a ajuda on-line para o cliente de sincronização em nuvem em questão.
- O aplicativo Data Guardian Mobile lista o cliente de sincronização de nuvem usado na empresa e permite que você faça download dele.

Se uma pessoa não autorizada acessar sua conta de armazenamento em nuvem e fizer download de um arquivo para um dispositivo móvel que **não** tenha o Data Guardian instalado, a pessoa não poderá abrir ou ver seus arquivos. Se essa pessoa abrir um documento protegido do Office, será exibida somente uma página de rosto indicando que a pessoa não poderá ver o documento sem o Data Guardian. Isso torna seus dados mais seguros.

Acessar sua conta do fornecedor de armazenamento em nuvem

Para acessar uma conta do fornecedor de armazenamento em nuvem:

1. Na tela do Gerenciador de arquivos, toque no ícone Adicionar (+).
2. Toque em **Serviço de nuvem**.
   Uma política do Data Guardian determina quais provedores de armazenamento em nuvem são exibidos. Seu administrador pode designar um ou mais provedores de armazenamento em nuvem específicos para uso dentro da empresa e bloquear os demais.
3. Execute uma das seguintes ações seguindo as instruções on-line:
   - Crie uma conta no provedor de armazenamento em nuvem.
   - Faça login em uma conta existente do provedor de armazenamento em nuvem.

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

NOTA:

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

Usar proteção em nuvem

Em dispositivos móveis com o Data Guardian, você pode:

- Criar pastas
- Fazer upload e download de arquivos

  NOTA:

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

  NOTA:

  Se um usuário interno compartilhar uma pasta com você através do Data Guardian, você deverá ir para o site de armazenamento em nuvem e movê-la para a pasta raiz ou fazer download da pasta compartilhada para vê-la no dispositivo.
- **Arquivo > Copiar** - De acordo com a política definida pelo administrador, é possível copiar um arquivo de um provedor de nuvem para outro.
- No Android com OneDrive e Dropbox, se não for possível compartilhar um arquivo de Aplicativos e o arquivo compartilhar um link com o aplicativo Data Guardian, compartilhe o arquivo a partir do aplicativo Navegador de arquivos do dispositivo.

Desvincular um provedor de armazenamento em nuvem

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

1 Abra a gaveta de navegação do Data Guardian e toque em **Configurações > Gerenciador de arquivos > Serviço de nuvem**. Quando o acesso a um provedor de armazenamento em nuvem for concedido a você, uma marca de seleção será mostrada na caixa de seleção.

2 Execute um destes processos:

Android

a Toque em **Vinculado**.

b Toque em **Sim**.

iOS

a Toque em **Desvinculado**.

Isso remove acesso e os arquivos do Data Guardian. No entanto, isso não remove os arquivos da nuvem.

Solução de problemas da proteção em nuvem

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

Identifier	**GUID-19337C15-12E9-4E8D-B908-29416128B500**
Status	**Translation Validated**

Usar as políticas adicionais em dispositivos móveis

O administrador indicará quais destas políticas foram definidas para a empresa.

Usar um PIN

O administrador pode definir uma política para exigir um PIN e definir seu comprimento.

Adulteração

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

Proteção adicional por Cerca geográfica

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

Identifier	**GUID-21086952-1999-4F9B-A47C-C57073C7C715**
Status	**Translation Validated**

Considerações de segurança com o Data Guardian e clientes de sincronização

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

Google Drive

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

- Android
- iOS - Uma mensagem é mostrada.

NOTA:
Google Backup e Sync não suportados.

OneDrive e OneDrive for Business

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

Identifier	**GUID-46C6144D-AF30-4559-96AC-39DB1738D2D8**
Status	**Translation Validated**

Logs

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

Identifier	**GUID-8882A835-A7A8-4C7B-8330-3080F871A121**
Status	**Translation Validated**

Dell Security Center Hospedado e Tenant Suspenso

Com o Dell Security Center Hospedado, se um tenant deixar de pagar por determinado período, ele poderá ser suspenso. Isso se aplica a Windows, Mac, dispositivos móveis e portal da web.

Os usuários internos e externos do Data Guardian poderão vivenciar as seguintes situações:

- Todas as plataformas - Se você tentar instalar o Data Guardian, ativar ou fazer login, uma caixa de diálogo será exibida indicando que o tenant está suspenso.
- Mac - Se o tenant for suspenso com o Data Guardian aberto, a caixa de diálogo do tenant suspenso será exibida após você fechar o Explorer e todos os arquivos e, em seguida, tentar abrir um arquivo protegido.
- Portal da Web:
  - Se você já estiver conectado e carregar um arquivo criptografado, uma mensagem indicará Falha no upload.
  - Se um arquivo criptografado ou não criptografado foi carregado e o tenant logo em seguida ficou suspenso, será exibida uma mensagem de Falha no download.
  - Se você se desconectar e tentar fazer login novamente, uma caixa de diálogo será exibida indicando que o tenant está suspenso.

Entre em contato com o administrador.

Identifier	**GUID-66FB1CE0-6669-4DDD-80E8-BCBAA27D4E13**
Status	**Translation Validated**

Enviar feedback à Dell

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

Para enviar feedback:

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

Identifier	GUID-BDAC1DD8-21C2-4ED1-B0A
Status	In Translation

Ver ou editar arquivos protegidos em um Web Client

Se o administrador configurar um portal da web do Data Guardian, você pode vincular um URL para esse cliente da web e visualizar os arquivos criptografados sem instalar um cliente do Data Guardian. Com base na política, você também pode editar um arquivo.

Com base na política definida pelo administrador, você pode visualizar o seguinte:

- Documentos do Office protegidos: .docx, .pptx, .xlsx, .docm, .pptm, .xlsm, .pdf.
- arquivos .xen - Arquivos do Office ou de outros programas que o Data Guardian criptografou ao carregar para a nuvem.
- Tipos de arquivos adicionais, como do Bloco de notas.

Com base na política definida pelo administrador, você pode acessar um provedor de serviços em nuvem.

Identifier	GUID-C468D78F-0ADF-45FC-B5A2-44B933EB2497
Status	Translation Validated

Acessar o portal da web para Data Guardian

As etapas podem variar um pouco, dependendo do navegador que você usar.

1 Obtenha o URL para acessar o portal da web com o administrador.
2 Clique no URL.
Se um aviso for exibido, clique em **Continuar** ou **Prosseguir**.
3 Na tela do contrato de licença, clique em **Concordar**.
Se um aviso for exibido, clique em **Continuar** ou **Prosseguir**.
4 Insira suas credenciais de domínio.
5 Clique em **Fazer login**.
6 Se você for solicitado a rastrear seu local, selecione uma opção.
7 Para ver ou editar arquivos, consulte a Ajuda online disponível no portal Web do Data Guardian.

> **NOTA:**
> Para Mac, você precisa configurar o Safari para permitir pop-ups.

Identifier	GUID-D11E8451-72A7-4179-8693-28D0FAFF9B8B
Status	In Translation

Proteger tipos de aplicativos e arquivos adicionais com a proteção básica de arquivos

O administrador informará se as políticas permitirem que tipos de aplicativos e arquivos adicionais sejam criptografados. Se alguém abrir um arquivo criptografado com a proteção básica de arquivos, mas não tiver o Data Guardian instalado, o conteúdo fica ilegível.

Visão geral da proteção básica de arquivos

Aplicativos

Estes são exemplos de aplicativos que o administrador pode desejar criptografar:

- Notepad
- Wordpad
- Visio
- MS Paint

> **NOTA:**
> Alguns aplicativos têm apenas o suporte parcial do Data Guardian e o administrador informará quais.

Tipos de arquivo

Estes são exemplos de tipos de arquivos adicionais que podem ser configurados: .txt, .rtf, .csv, .odt, .vsdx, .png, .jpg, .jpeg, .jpe, .jfif, .gif, .tif, .tiff, .bmp

Windows, Mac e dispositivos móveis

Quando a política da proteção básica de arquivos for configurada, o Data Guardian analisa os computadores dos usuários e criptografa todos os arquivos locais com essas extensões. Os arquivos criptografados com a proteção básica de arquivos podem ser visualizados e editados usando o aplicativo associado à extensão de arquivo.

> **NOTA:**
> Arquivos em pastas do sistema específicas não são criptografados, como AppData. Também pastas relacionadas aos documentos protegidos do Office, como a pasta Documentos seguros.

Ícones de sobreposição para Windows

No Data Guardian 2.2 e superior, os ícones de sobreposição são exibidos em arquivos protegidos no Explorador de arquivos. Ao clicar com o botão direito do mouse em um arquivo protegido, a guia Dell Data Guardian fornece mais informações.

Excluir alguns arquivos da varredura no Windows ou Mac (antes de a varredura ser ativada)

Se a sua empresa decidir criptografar um tipo de arquivo adicional, como .txt, talvez você não queira ou precise que todos os arquivos com essa extensão sejam verificados e criptografados.

Antes de ativar a Proteção básica de arquivos para essa extensão, o administrador pode definir outra política que permita adicionar uma pasta ao computador local e os arquivos nessa pasta não sejam verificados. O administrador pode definir uma política, criar um nome de

pasta, fornecer o nome da pasta e sugerir onde você pode adicionar essa pasta. Esses arquivos podem ser necessários para o seu sistema ou arquivos que não exigem proteção.

IMPORTANTE:

Você deve criar a pasta antes de o administrador ativar a política de Proteção básica de arquivos.

1 Use o nome e o caminho da pasta fornecidos pelo administrador.
   - Para Mac, navegue até **o painel Preferências > Exclusões de proteção básica de arquivos**. O nome da pasta a ser criada e o caminho são exibidos aqui.

2 Adicione arquivos com a extensão especificada, como .txt, que não precisam ser criptografados. Como alternativa, você pode adicionar subpastas com nomes criados pelo usuário.

   NOTA:

   Se você tiver arquivos com essa extensão que foram previamente criptografados, colocá-los nessa pasta não os descriptografará. Eles permanecem criptografados. Se você tiver uma pasta **Documentos desprotegidos**, que o administrador pode criar por meio de outra política, você pode colocar os tipos de Proteção básica de arquivos nesta pasta para descriptografá-los.

3 Depois que a Proteção básica de arquivos estiver ativada, se você tiver arquivos desprotegidos com essa extensão em uma rede ou unidade externa, poderá copiá-los para a pasta excluída. Eles permanecem descriptografados. Do contrário, eles são criptografados.

Se o computador tiver mais de um usuário, somente o usuário conectado no momento poderá colocar arquivos nessa pasta e excluí-los da varredura. Todos os arquivos que outro usuário colocar nessa pasta passarão por varredura e serão criptografados.

Remoção de uma extensão de arquivo no Windows ou Mac

O administrador poderá decidir remover uma extensão de arquivo. Se o fizer, o seu computador passará por uma varredura para descriptografar esses tipos de arquivo.

- A aba *Propriedades > Dell Data Guardian* dos arquivos criptografados não será mais exibida.
- Se você tiver sobreposição de ícones de arquivo, eles não serão mais exibidos.
- A descriptografia poderá levar vários minutos para ser concluída. Se o arquivo com essa extensão ainda estiver criptografado, ele poderá ter sido aberto durante a varredura ou armazenado em um servidor de arquivos ou outra localização.

Entre em contato com o administrador para solicitar a recuperação de arquivos com essa extensão que não foram descriptografados.

Aplicativos do Office

Você pode usar um aplicativo do Office para abrir um arquivo criptografado com a proteção básica de arquivos, mas o conteúdo fica disponível como somente leitura.

Portal da Web

Em Configurações > Políticas, se Proteção básica de arquivos estiver definida como Verdadeiro, o administrador adicionou tipos de arquivos não Office ao baixá-los do portal da Web. O administrador deve informar os tipos de arquivo.

NOTA:

Se você fizer o upload de um tipo de arquivo que ainda não é compatível com suporte, o conteúdo ficará ilegível no portal da Web.

É possível fazer o upload de tipos de arquivos não Office, sejam eles criptografados ou não. No entanto, ao fazer o download do arquivo não Office, a extensão varia.

Arquivos não Office (como .txt ou .png)	Descrição do download
Criptografado antes do upload	Quando baixados do portal da Web, mantêm a extensão do arquivo, como .txt ou .png.

Arquivos não Office (como .txt ou .png)	Descrição do download
Exemplo: arquivos não Office já criptografados pelo Windows ou Mac.	
Arquivos não criptografados	Quando baixados do portal da Web, a extensão do arquivo varia com base em o administrador ter adicionado ou não a extensão a uma política. No entanto, são criptografados. Exemplos de arquivos .txt baixados do portal da Web: • **nomedoarquivo.txt** - O administrador adicionou o tipo de arquivo .txt a uma política. • **nomedoarquivo.txt.xen** - O tipo de arquivo .txt não foi incluído na política. O arquivo é criptografado, mas adiciona uma extensão .xen.

Se a política *Edit* estiver ativada no portal da Web, os usuários poderão editar arquivos não Office.

Identifier	**GUID-932E973E-B2CD-4305-B50F-F85231243FA4**
Status	**In Translation**

Usar um provedor de armazenamento na nuvem

Com base na política, o portal da web pode acessar um provedor de armazenamento em nuvem. Para obter mais informações, consulte a ajuda on-line do portal da web.

Identifier	**GUID-8882A835-A7A8-4C7B-8330-3080F871A121**
Status	**Translation Validated**

Dell Security Center Hospedado e Tenant Suspenso

Com o Dell Security Center Hospedado, se um tenant deixar de pagar por determinado período, ele poderá ser suspenso. Isso se aplica a Windows, Mac, dispositivos móveis e portal da web.

Os usuários internos e externos do Data Guardian poderão vivenciar as seguintes situações:

- Todas as plataformas - Se você tentar instalar o Data Guardian, ativar ou fazer login, uma caixa de diálogo será exibida indicando que o tenant está suspenso.
- Mac - Se o tenant for suspenso com o Data Guardian aberto, a caixa de diálogo do tenant suspenso será exibida após você fechar o Explorer e todos os arquivos e, em seguida, tentar abrir um arquivo protegido.
- Portal da Web:
  - Se você já estiver conectado e carregar um arquivo criptografado, uma mensagem indicará Falha no upload.
  - Se um arquivo criptografado ou não criptografado foi carregado e o tenant logo em seguida ficou suspenso, será exibida uma mensagem de Falha no download.
  - Se você se desconectar e tentar fazer login novamente, uma caixa de diálogo será exibida indicando que o tenant está suspenso.

Entre em contato com o administrador.

Identifier	GUID-FF3D5442-1632-454D-8787-1
Status	Translation Validated

Usar o Data Guardian como usuário externo

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

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

Os usuários externos precisam atender aos requisitos do servidor. Além disso, o domínio ou o usuário não pode estar na lista negra da empresa.

Para um ambiente de host, os usuários externos só podem ativar para um tenant.

As opções para os usuários externos incluem:

- **Windows** - Fazer download e instalar um cliente do Data Guardian. Consultar as Tarefas de usuário interno no Windows e as Tarefas de usuário externo.
- **Mac** - Consulte Usuário externo e Mac.
- **Móvel**
- Portal da Web - Em vez de fazer o download de um cliente do Data Guardian, use o portal Web do Data Guardian. Usuários externos podem visualizar um arquivo .pdf ou . xen de um documento protegido do Office. Com base na política externa, o usuário pode editar o arquivo. Consulte Usuário externo e portal Web.

Identifier	GUID-EBDBAE23-A90F-4603-934B-6B40EE93C248
Status	In Translation

Tarefas do usuário interno no Windows

Para compartilhar arquivos protegidos com um usuário externo, você pode:

- Use a opção *Acesso a arquivos protegidos* com documentos do Office protegidos
- Aprovar ou negar acesso quando um usuário externo solicitar acesso
- Enviar um documento protegido do Office por e-mail no Outlook.

Conceder acesso a um ou mais arquivos protegidos do Office

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

1 Clique com o botão direito do mouse em um arquivo protegido e selecione **Acesso a arquivos protegidos**. Você pode selecionar de um até 50 arquivos. A janela Compartilhamento de acesso a documento protegido é exibida. Os arquivos podem estar nestes locais:
   - Pasta local ou unidade de rede

- E-mail
- Mídia removível
- Compartilhamento de rede

2 No canto superior direito do campo *E-mail para compartilhar*, digite o endereço de e-mail do usuário sem domínio e clique em **Adicionar**.

3 Repita essa etapa para adicionar até dez endereços de email.

4 Clique em **OK**.

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

5 Como prática recomendável, informe aos usuários externos que ainda não estiverem registrados de que eles receberão um e-mail seu com instruções para permitir que eles se registrem em um Dell Server, façam download e ativem o Dell Data Guardian e, a seguir, vejam os arquivos protegidos compartilhados.

Aprovar ou negar acesso quando um usuário externo solicitar acesso

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

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

2 Selecione **Aprovar** ou **Negar**.

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

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

Enviar um arquivo protegido por e-mail do Outlook

Ao anexar um arquivo protegido e clicar em *Enviar*, um prompt de confirmação avisa que a chave para o arquivo protegido será compartilhada.

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

Identifier	**GUID-967BF32F-F6F1-4C5A-BA0B-34CA9F73A438**
Status	**In Translation**

Tarefas do usuário externo no Windows

Um usuário interno pode decidir fornecer acesso a arquivos protegidos. Você poderá receber o seguinte:

- E-mail com instruções para se registrar
- Arquivo protegido com uma página de rosto com um link para registrar um endereço de e-mail válido

NOTA:
A folha de rosto lista o nome do Dell Server para no local ou uma ID de instalação para o tenant específico se o seu Hospedado no Dell Security Center for multitenant. A folha de rosto também inclui um link para fazer o download do cliente do Data Guardian.

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

- Registrar-se no Data Guardian
- Fazer o download do Data Guardian e instalá-lo - o usuário externo precisa ter direitos de administrador no computador.

Registrar-se no Data Guardian

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

Para se registrar no Data Guardian:

1 Execute um destes processos:
   - E-mail - clique em **Aceitar**.
   - Documento protegido que exibe um aviso na folha de rosto - Clique no link fornecido para registrar um endereço de e-mail válido.

2 Siga um conjunto de etapas baseadas no ambiente da sua empresa:

Hospedado no Dell Security Center	Dell Management Server no local
Uma solução SaaS (Software as a Service, software como serviço) para gerenciamento do software Dell Data Security.	Um servidor no local dentro da rede da empresa para gerenciamento do software Dell Data Security.
a Quando o portal da web do Dell Data Guardian abrir, digite o seu endereço de e-mail. b Role para baixo e clique em **Concordar**. c Na janela Dell Security Center, role para baixo para *Precisa de uma conta?* e clique em **Inscrever-se**. d Na página da nova conta, digite um e-mail, um nome, um sobrenome e uma senha. A senha precisa ter pelo menos oito caracteres e incluir uma letra minúscula, uma letra maiúscula, um caractere especial e um número. e Clique em **Inscrever-se**. f Acesse o e-mail que você usou para se registrar, recupere o código de verificação e digite-o. **NOTA:** Se você não receber um e-mail, verifique a caixa de spam. g Clique em **Confirmar conta**. Se você for verificado, o portal da web é exibido. h Arraste o arquivo protegido para o portal da Web e clique em **Fazer upload agora**. i Você receberá um e-mail de boas-vindas após o registro. O e-mail contém um link para fazer o download de um cliente Windows.	**NOTA:** Para no local, você pode instalar o Data Guardian antes de fazer o registro. Ao ativar, clique no link **Registro**. a Quando a janela do Dell Data Guardian abrir, digite o seu endereço de e-mail. b Clique em **Inscrever**. c Na página Registrar, digite e confirme sua senha e clique em **Inscrever-se**. A caixa de diálogo Confirmação de registro é exibida e um email é enviado ao endereço informado pelo usuário interno. Se você não receber o e-mail, verifique a caixa de spam. d No email de Verificação da conta do Dell Server, clique no hiperlink. **NOTA:** Se você não receber um e-mail, verifique a caixa de spam. e Continue para a página da Web. f Na página de confirmação, clique em **Continuar para fazer login**. g Na página de login, clique em **Esqueci a senha**. **NOTA:** O Dell Server atribuiu uma senha aleatória, que você deverá redefinir. h Na página Redefinição da senha, digite e confirme sua senha e clique em **Registrar**. A caixa de diálogo Confirmação de registro é exibida e um email é enviado ao endereço informado pelo usuário interno. i Abra o email de ativação da conta e clique no link. O email também informa o nome do Dell Server a ser usado durante a instalação do Data Guardian. j Na página Login, digite o endereço de email e a senha usados para se registrar. k Clique em **Fazer login**. A página Download do Data Guardian é exibida.
NOTA: Se o Hospedado no Dell Security Center for multitenant, o e-mail listará também a ID da instalação necessária.	

Fazer o download do Data Guardian para Windows e instalá-lo

Após fazer o registro, você pode clicar no link para fazer o download de um cliente Windows. Dependendo do que o usuário interno forneceu inicialmente, os links podem estar disponíveis aqui:

- Para o Servidor de gerenciamento de segurança, uma página de download é aberta com opções relacionadas ao cliente Windows.
- Para o Servidor de gerenciamento de segurança virtual, clicar no Windows levará você para o site dell.com/support (em inglês).
- Se você recebeu um arquivo protegido, a página de rosto terá links para o download de um cliente.
- Você receberá um e-mail de boas-vindas com links para o download de um cliente.

As etapas a seguir descrevem como instalar o Data Guardian no Windows.

1 No Windows, clique em **Download (32 bits)** ou **Download (64 bits)**, dependendo do sistema operacional do computador.
2 Faça download do arquivo de instalação para um diretório no seu computador.
3 Clique duas vezes no arquivo de instalação para abrir o instalador.
4 Selecione um idioma e clique em **OK**.
5 Se você for solicitado a instalar o Pacote redistribuível do Microsoft Visual C++ 2010, clique em **OK**.
6 Na página de boas-vindas, clique em **Avançar**.
7 Leia o contrato de licença, aceite os termos e condições e clique em **Avançar**.
8 Na tela Pasta de destino, clique em **Avançar** para fazer a instalação no local padrão de **C:\Arquivos de Programas\Dell\Dell Data Guardian\.**
9 Na tela Tipo de configuração, selecione um destes:

Hospedado no Dell Security Center	Dell Management Server no local
a Selecione Hospedado no Dell Security Center. b Se sua empresa for multitenant, digite a ID de instalação encontrada na folha de rosto ou no e-mail de boas-vindas. c Clique em **Avançar**. d Continue com a etapa 10.	a Selecione Dell Management Server no local. b No campo *Nome do servidor*, digite o nome do Dell Server com o qual o computador irá se comunicar. Esse nome está no email de ativação recebido ou no topo da página de download. c Clique em **Avançar**. d Na tela Confirmar servidor de ativação, certifique-se de que o endereço de URL do Dell Server está correto. O instalador acrescenta www ou http(s) e a porta. Clique em **Avançar**. e Continue com a etapa 10.

10 Na janela Tipo de gerenciamento, selecione a opção:
   - Uso externo - Um usuário com endereço de e-mail fora do domínio da empresa.
11 Clique em **Instalar** para iniciar a instalação.
   Uma janela de status mostra o andamento da instalação.
12 Clique em **Concluir** quando a tela Instalação concluída for exibida.
13 Clique em **Sim** para reiniciar.
   A instalação doData Guardian está concluída.
14 Consulte Ativar o Data Guardian.

NOTA:
Consulte as notas e exceções no Usar o Data Guardian com o Windows, por exemplo, você não pode abrir um arquivo .pdf da rede. Você pode usar o Word para abrir um arquivo .pdf pela rede.

Identifier	GUID-92B941BF-52D2-4302-AFA1-3D348E260E03
Status	In Translation

Ativar o Data Guardian

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

1 Faça login no Windows.

A área de notificações mostra um ícone de nuvem com um ponto de exclamação laranja.

2 Quando uma caixa de diálogo for exibida na área de notificações, clique em **Clique aqui para ativar**.

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

> **NOTA:**
> Para um ambiente de host, os usuários externos só podem ativar para um tenant por vez. Se você já tiver ativado em um tenant, você precisa desinstalar o Data Guardian e reinstalá-lo com a outra ID de instalação. Se preferir, você pode usar o portal da web para carregar e ver documentos protegidos.

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

> **NOTA:**
> Para no local, se você instalou o Data Guardian antes de fazer o registro, quando ativar, clique no link **Registro**.

Após o término da ativação, uma marca verde é exibida no ícone da área de notificações do Data Guardian  .

4 Confirme seu status de modo de usuário. Clique no ícone área de notificações e selecione **Detalhes**.

Na parte superior, o modo de usuário é:

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

Identifier	GUID-55AD51F6-9437-4B64-9A9F-E598A3BBDC74
Status	Translation Validated

Solicitar acesso a um usuário interno

Com Windows, Mac e dispositivos móveis, se um usuário externo tiver instalado e ativado o Data Guardian, poderá solicitar a um usuário interno acesso a um documento protegido do Office ou .pdf. O usuário externo precisará fazer uma solicitação separada para cada arquivo.

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

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

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

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

Identifier	**GUID-1DB6F793-018B-4F14-AA95-63980FCDD713**
Status	**Translation Validated**

Usuário externo e Tarefas Mac

Tarefas de usuário interno para Mac

Execute um destes processos:

- Documentos protegidos - envie para o usuário externo por e-mail, compartilhamento de rede ou armazenamento removível.
- Se a criptografia na nuvem do Data Guardian estiver ativada - na interface do Dell Data Guardian, arraste os arquivos protegidos para a coluna ao lado do fornecedor de armazenamento na coluna do provedor de armazenamento em nuvem.

Tarefas de usuário externo para Mac

Registrar-se no Data Guardian

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

Para se registrar no Data Guardian:

1 Quando você abrir um documento protegido que exibe um aviso na folha de rosto, clique no link fornecido para registrar um endereço de e-mail válido.

> **NOTA:**
> A folha de rosto lista o nome do Dell Server para no local ou uma ID de instalação para o tenant específico se o seu Hospedado no Dell Security Center for multitenant. A folha de rosto também inclui links para fazer o download do cliente do Data Guardian.

2 Execute um destes procedimentos, dependendo do seu ambiente:

Hospedado no Dell Security Center

Uma solução SaaS (Software as a Service, software como serviço) para gerenciamento do software Dell Data Security.

a Quando o portal da web do Dell Data Guardian abrir, digite o seu endereço de e-mail.

b Role para baixo e clique em **Concordar**.

c Na janela Dell Security Center, role para baixo para *Precisa de uma conta?* e clique em **Inscrever-se**.

d Na página da nova conta, digite um e-mail, um nome, um sobrenome e uma senha. A senha precisa ter pelo menos oito caracteres e incluir uma letra minúscula, uma letra maiúscula, um caractere especial e um número.

e Clique em **Inscrever-se**.

f Acesse o e-mail que você usou para se registrar, recupere o código de verificação e digite-o.

> **NOTA:**
> Se você não receber um e-mail, verifique a caixa de spam.

g Clique em **Confirmar conta**. Se você for verificado, o portal da web é exibido.

Dell Management Server no local

Um servidor no local dentro da rede da empresa para gerenciamento do software Dell Data Security.

a Quando a janela do Dell Data Guardian abrir, digite o seu endereço de e-mail.

b Clique em **Inscrever**.

c Na página Registrar, digite e confirme sua senha e clique em **Inscrever-se**.

A caixa de diálogo Confirmação de registro é exibida e um email é enviado ao endereço informado pelo usuário interno. Se você não receber o e-mail, verifique a caixa de spam.

d Abra o e-mail de ativação da conta e clique no link.

O email também informa o nome do Dell Server a ser usado durante a instalação do Data Guardian.

e Na página de confirmação do registro, clique em **Retornar para o login**.

Você pode clicar em um link da página de rosto para fazer o download e instalar um cliente. Veja a seguir.

Hospedado no Dell Security Center	Dell Management Server no local
h Carregue o arquivo protegido para vê-lo. Você receberá um e-mail com links para o download do cliente de Mac. Ou você pode clicar no link da página de rosto. Veja a seguir.	

Fazer download e instalar um cliente do Data Guardian (opcional)

1 Na página do Data Guardian, digite o endereço de e-mail e a senha usados para se registrar.
2 Clique em **Fazer login**.
É exibida uma página de download do Data Guardian com opções para Windows, iOS, Android e Mac OS X.
3 Em Mac OS X, clique em **Download**.
4 Na página *Drivers & downloads*, selecione **Apple Mac OS** e clique em **Download**.
5 Faça o download do .dmg em um diretório do seu computador e execute o .pkg.
6 Para fazer login/ativar, faça um destes procedimentos:

Hospedado no Dell Security Center	Dell Management Server no local
a Use o endereço de e-mail usado no registro. b As informações de login são as mesmas que você usou para fazer login no .dmg. c Clique em **Fazer login**.	a Veja a ajuda on-line incorporada do Data Guardian e digite um nome de Dell Server listado no e-mail de verificação de conta. b Também digite seu endereço de e-mail e sua senha. As informações de login são as que você usou para se registrar. c Clique em **Fazer login**.

Identifier	**GUID-B2D2A78A-86B7-4D46-A530-C531CE3B706A**
Status	**Translation Validated**

Usuário externo e dispositivo móvel

Se um usuário interno compartilhar um link na nuvem para um arquivo protegido, o arquivo exibirá uma folha de rosto contendo um link para registrar um endereço de e-mail válido.

NOTA:
A folha de rosto lista o nome do Dell Server para no local ou uma ID de instalação para o tenant específico se o seu Hospedado no Dell Security Center for multitenant. A folha de rosto também inclui um link para fazer o download do cliente do Data Guardian.

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

- Registrar-se no Data Guardian
- Fazer o download do Data Guardian e instalá-lo - o usuário externo precisa ter direitos de administrador no computador.

Registrar-se no Data Guardian

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

Para se registrar no Data Guardian:

1 Na advertência da folha de rosto, clique no link fornecido para registrar um endereço de e-mail válido.
2 Siga um conjunto de etapas baseadas no ambiente da sua empresa:

Hospedado no Dell Security Center

Uma solução SaaS (Software as a Service, software como serviço) para gerenciamento do software Dell Data Security.

a Quando o portal da web do Dell Data Guardian abrir, digite o seu endereço de e-mail.

b Role para baixo e clique em **Concordar**.

c Na janela Dell Security Center, role para baixo para *Precisa de uma conta?* e clique em **Inscrever-se**.

d Na página da nova conta, digite um e-mail, um nome, um sobrenome e uma senha. A senha precisa ter pelo menos oito caracteres e incluir uma letra minúscula, uma letra maiúscula, um caractere especial e um número.

e Clique em **Inscrever-se**.

f Acesse o e-mail que você usou para se registrar, recupere o código de verificação e digite-o.

> **NOTA:**
> Se você não receber um e-mail, verifique a caixa de spam.

g Clique em **Confirmar conta**. Se você for verificado, o portal da web é exibido.

h Arraste o arquivo protegido para o portal da Web e clique em **Fazer upload agora**.

i Você receberá um e-mail de boas-vindas após o registro. O e-mail contém um link para fazer o download de um cliente Windows.

> **NOTA:**
> Se o Hospedado no Dell Security Center for multitenant, o e-mail listará também a ID da instalação necessária.

Dell Management Server no local

Um servidor no local dentro da rede da empresa para gerenciamento do software Dell Data Security.

> **NOTA:**
> Para no local, você pode instalar o Data Guardian antes de fazer o registro. Ao ativar, clique no link **Registro**.

a Quando a janela do Dell Data Guardian abrir, digite o seu endereço de e-mail.

b Clique em **Inscrever**.

c Na página Registrar, digite e confirme sua senha e clique em **Inscrever-se**.

A caixa de diálogo Confirmação de registro é exibida e um email é enviado ao endereço informado pelo usuário interno. Se você não receber o e-mail, verifique a caixa de spam.

d No email de Verificação da conta do Dell Server, clique no hiperlink.

> **NOTA:**
> Se você não receber um e-mail, verifique a caixa de spam.

e Continue para a página da Web.

f Na página de confirmação, clique em **Continuar para fazer login**.

g Na página de login, clique em **Esqueci a senha**.

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

h Na página Redefinição da senha, digite e confirme sua senha e clique em **Registrar**.

A caixa de diálogo Confirmação de registro é exibida e um email é enviado ao endereço informado pelo usuário interno.

i Abra o email de ativação da conta e clique no link.

O email também informa o nome do Dell Server a ser usado durante a instalação do Data Guardian.

j Na página Login, digite o endereço de email e a senha usados para se registrar.

k Clique em **Fazer login**.

A página Download do Data Guardian é exibida.

Fazer download e instalar o Data Guardian for Mobile

Execute um destes processos:

- Instalar ou desinstalar o Data Guardian em um dispositivo Android
- Instalar ou desinstalar o Data Guardian em um dispositivo iOS

Identifier	**GUID-FE0A7159-E0F3-4E21-9FE6-008C831F7D44**
Status	**Translation Validated**

Usuário externo e portal Web

Tarefas do usuário interno

Um usuário interno pode fazer um destes procedimentos:

- Enviar ao usuário externo o URL da empresa para acessar o portal da web do Data Guardian.
- Enviar um arquivo protegido para o usuário externo. Quando o usuário abre o arquivo, uma folha de rosto é exibida.

O usuário externo pode apenas visualizar arquivos .pdf e arquivos .xen de documento protegido do Office ou editar os arquivos com base na política. No entanto, o usuário externo não precisa fazer download de um cliente do Data Guardian.

Tarefas de usuário externo para o portal Web

Para registrar-se no portal Web do Data Guardian:

1 Clique no URL do portal da web recebido de um usuário interno ou na página de rosto de um arquivo protegido.

2 Na tela do contrato de licença, role para baixo e clique em **Concordar**.

3 Execute um destes procedimentos, dependendo se sua empresa é hospedada ou No local.

Hospedado no Dell Security Center	**Dell Management Server no local**
Uma solução SaaS (Software as a Service, software como serviço) para gerenciamento do software Dell Data Security.	Um servidor no local dentro da rede da empresa para gerenciamento do software Dell Data Security.
a Digite um e-mail e uma senha. b Clique em **Entrar**. c Digite um e-mail, um nome, um sobrenome e uma senha. A senha precisa ter pelo menos oito caracteres e incluir uma letra minúscula, uma letra maiúscula, um caractere especial e um número. d Clique em **Inscrever-se**. e Acesse o e-mail que você usou para se registrar, recupere o código de verificação e digite-o. f Digite um código verificação e clique em **Confirmar conta**. O portal da web é exibido.	a b Clique em **Ainda não tem uma conta?** c Digite um endereço de e-mail e clique em **Registrar**. **NOTA:** Para os usuários internos que desejarem se cadastrar como externos, esse é um endereço de e-mail sem domínio. d Na página Registrar, digite e confirme uma senha e, em seguida, clique em **Registrar**. A página de confirmação indica que um e-mail de confirmação foi enviado para o endereço de e-mail fornecido. e Para concluir a ativação da conta, abra o e-mail com o assunto *Verificação de conta* e clique no link. f Na tela de confirmação do registro, clique em **Retornar para o login**. g Digite o endereço de e-mail e senha utilizados no registro.
Se um usuário interno não compartilhar a chave, você pode acessar o portal da web, mas não abrir o arquivo.	

4 A página de upload do Dell Data Guardian é aberta.

5 Clique em **Procurar** para ir para o arquivo e carregá-lo ou arraste e solte o arquivo no portal da web.

6 Clique em **?** Para ver a Ajuda online para cada página.

Para editar arquivos, o administrador deve modificar uma política para o usuário. Se for concedido após o registro, você deve sair do portal Web e fazer o login novamente.

Opcionalmente, você pode fazer o download de um cliente do Data Guardian. A folha de rosto também inclui links para fazer o download do cliente do Data Guardian. A folha de rosto lista também o nome do Dell Server para no local ou uma ID de instalação para o tenant específico se o seu Hospedado no Dell Security Center for multitenant.

Solicitar acesso a um usuário interno

Se, ao carregar um documento protegido do Office ou .pdf, uma caixa de diálogo de *Falha no upload* indicar que você não tem acesso, é possível solicitar acesso do autor do arquivo:

1 Na caixa de diálogo *Falha no upload*, clique em **Sim**.
2 Aguarde um e-mail do usuário interno informando se o acesso foi concedido ou negado.

NOTA:
Se você não receber um e-mail do usuário interno, será necessário aguardar 48 horas antes de solicitar acesso novamente. Se você abrir o arquivo protegido antes que o usuário interno aprove o acesso, será mostrada uma mensagem informando que a solicitação está pendente.

Identifier	**GUID-01B874EC-88D4-4264-803C-472B65D1180F**
Status	**Translation Validated**

View a Protected Office Document

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

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

- Imprimir
- Exportar
- Salvar como
- Compartilhar

Identifier	**GUID-8882A835-A7A8-4C7B-8330-3080F871A121**
Status	**Translation Validated**

Dell Security Center Hospedado e Tenant Suspenso

Com o Dell Security Center Hospedado, se um tenant deixar de pagar por determinado período, ele poderá ser suspenso. Isso se aplica a Windows, Mac, dispositivos móveis e portal da web.

Os usuários internos e externos do Data Guardian poderão vivenciar as seguintes situações:

- Todas as plataformas - Se você tentar instalar o Data Guardian, ativar ou fazer login, uma caixa de diálogo será exibida indicando que o tenant está suspenso.
- Mac - Se o tenant for suspenso com o Data Guardian aberto, a caixa de diálogo do tenant suspenso será exibida após você fechar o Explorer e todos os arquivos e, em seguida, tentar abrir um arquivo protegido.
- Portal da Web:

- Se você já estiver conectado e carregar um arquivo criptografado, uma mensagem indicará Falha no upload.
- Se um arquivo criptografado ou não criptografado foi carregado e o tenant logo em seguida ficou suspenso, será exibida uma mensagem de Falha no download.
- Se você se desconectar e tentar fazer login novamente, uma caixa de diálogo será exibida indicando que o tenant está suspenso.

Entre em contato com o administrador.

Identifier	GUID-EF1D5890-EB47-482E-AF29-
Status	In Translation

Aumentar a segurança com os Grupos de acesso do Data Guardian (local)

Os Grupos de acesso do Data Guardian aumentam a segurança, criando grupos de usuários que podem colaborar em dados criptografados. Os usuários fora de um grupo não podem acessar ou visualizar os dados, a menos que o proprietário do arquivo conceda acesso. Os Grupos de acesso poderão incluir usuários internos e externos. Você pode usar os Grupos de acesso com Windows, Mac, dispositivos móveis e portais da Web.

Selecionar uma dessas opções com base na sua empresa:

- A empresa tem o Data Guardian instalado com o modo Aceitar
- A empresa tem o Data Guardian instalado com o modo Forçar protegido
- A empresa ainda não tem o Data Guardian e o modo Aceitar
- A empresa ainda não tem o Data Guardian e o modo Forçar protegido

Você também pode fazer o seguinte:

- Alterar o proprietário de um arquivo criptografado
- Revogar acesso a uma chave

Identifier	GUID-F71ADE66-5107-4796-B57E-FC00340C788C
Status	In Translation

A empresa tem o Data Guardian instalado com o modo Aceitar

Se a sua empresa usa grupos de acesso para aumentar a segurança de dados confidenciais, você precisa saber quem está no seu grupo de acesso. Inicialmente, a fim de garantir uma transição uniforme, sua empresa poderá estabelecer um breve período para processar os arquivos criptografados e compartilhados existentes. Depois que o período de transição estiver concluído, aqueles no seu grupo de acesso poderão visualizar os arquivos criptografados e compartilhados criados por você. Você poderá conceder acesso a pessoas fora do seu grupo de acesso.

Identifique-os no seu grupo de acesso

O administrador informará a você quem está em um ou mais dos seus grupos de acesso, dependendo de quem precisar de acesso a arquivos específicos. Isso poderá incluir usuários internos e externos. Se você trabalha com dados confidenciais e usuários específicos, você poderá solicitar que o administrador crie um grupo de acesso para esse conteúdo.

Usar o período de transição para processar arquivos criptografados e compartilhados

Se você já tem o Data Guardian instalado e os arquivos existentes estão criptografados, o melhor para a sua empresa é ter um breve período de transição para os arquivos criptografados que estão compartilhados. Para facilitar uma transição tranquila, esteja ciente do seguinte para arquivos criptografados compartilhados:

- O proprietário ou autor do arquivo, interno ou externo, continua a ter acesso ao arquivo.
- Usuários internos ou externos dentro do seu grupo de acesso terão acesso à maioria dos arquivos compartilhados. Com base no tipo de chave associada a alguns arquivos, você pode perder o acesso a alguns.
- Usuários internos fora do seu grupo de acesso - Os usuários deverão abrir os arquivos compartilhados durante o período de transição para obter acesso à chave. Se eles não abrirem o arquivo criptografado e compartilhado durante esse breve período, perderão o acesso ao arquivo.
- Usuários externos fora do seu grupo de acesso - Se você já concedeu acesso a um arquivo criptografado, o usuário externo continuará com acesso durante e após o período de transição.

Se você perder o acesso a um arquivo após o período de transição, poderá solicitar o acesso do proprietário.

Recuperar o acesso a arquivos criptografados compartilhados após o período de transição

Para Windows e Mac no modo Aceitar, você pode fazer o seguinte para recuperar o acesso:

- Arquivos protegidos do Office - uma caixa de diálogo solicitará o acesso para usuários internos e externos e o proprietário do arquivo poderá decidir se concederá ou não o acesso.
- Tipos de arquivos adicionais criptografados por meio da Proteção básica de arquivos - Não existe solicitação de pós-compartilhamento. O usuário precisa conhecer o proprietário do arquivo e clicar com o botão direito no arquivo criptografado para encontrar o ID de chave na guia Data Guardian. O usuário pode enviar essas informações ao proprietário e solicitar acesso.

Colaborar em novos arquivos criptografados após o período de transição

Para arquivos novos criados e criptografados por você após o período de transição:

- Usuários internos ou externos dentro do seu grupo de acesso - Terão acesso a todos os arquivos criptografados e compartilhados.
  - Qualquer pessoa que for removida do grupo de acesso, perderá acesso.
  - Se o proprietário de um arquivo for removido do grupo, os outros usuários ainda terão acesso.
- Usuários internos ou externos fora do seu grupo de acesso - Não poderão visualizar um arquivo criptografado.
  - Um usuário interno dentro do grupo de acesso poderá conceder acesso.
  - Se um usuário externo for o proprietário de um arquivo criptografado, ele poderá conceder acesso a outra pessoa.
  - Se um usuário interno ou externo fora do grupo receber um documento do Office e tentar abri-lo, uma caixa de diálogo pedirá que ele solicite acesso.
  - Se um usuário interno ou externo fora do grupo receber e tentar abrir um tipo de arquivo da Proteção básica de arquivos, o usuário poderá clicar com o botão direito do mouse no arquivo criptografado para encontrar o ID de chave na guia Data Guardian e, em seguida, enviar essas informações ao proprietário.

Identifier	GUID-18DE070B-862D-4CAF-8CDE-DA86552E6C57
Status	In Translation

A empresa tem o Data Guardian instalado com o modo Forçar protegido

Se a sua empresa usa grupos de acesso para aumentar a segurança de dados confidenciais, você precisa saber quem está no seu grupo de acesso. Inicialmente, a fim de garantir uma transição uniforme, sua empresa poderá estabelecer um breve período para processar os arquivos criptografados e compartilhados existentes. Depois que o período de transição estiver concluído, aqueles no seu grupo de acesso poderão visualizar os arquivos criptografados e compartilhados criados por você. Você poderá conceder acesso a pessoas fora do seu grupo de acesso.

Identifique-os no seu grupo de acesso

O administrador informará a você quem está em um ou mais dos seus grupos de acesso, dependendo de quem precisar de acesso a arquivos específicos. Isso poderá incluir usuários internos e externos. Se você trabalha com dados confidenciais e usuários específicos, você poderá solicitar que o administrador crie um grupo de acesso para esse conteúdo.

Usar o período de transição para processar arquivos criptografados e compartilhados

Se você já tem o Data Guardian instalado e os arquivos existentes estão criptografados, o melhor para a sua empresa é ter um breve período de transição para os arquivos criptografados que estão compartilhados. Para facilitar uma transição tranquila, esteja ciente do seguinte para arquivos criptografados compartilhados:

- O proprietário ou autor do arquivo, interno ou externo, continua a ter acesso ao arquivo.
- Usuários internos ou externos dentro do seu grupo de acesso terão acesso à maioria dos arquivos compartilhados. Com base no tipo de chave associada a alguns arquivos, você pode perder o acesso a alguns.
- Usuários internos fora do seu grupo de acesso - Os usuários deverão abrir os arquivos compartilhados durante o período de transição para obter acesso à chave. Se eles não abrirem o arquivo criptografado e compartilhado durante esse breve período, perderão o acesso ao arquivo.
- Usuários externos fora do seu grupo de acesso - Se você já concedeu acesso a um arquivo criptografado, o usuário externo continuará com acesso após o período de transição.

Se você perder o acesso a um arquivo após o período de transição, poderá solicitar o acesso do proprietário.

Recuperar o acesso a arquivos criptografados compartilhados após o período de transição

Para Windows e Mac no modo Forçar protegido, você pode fazer o seguinte para recuperar o acesso:

- Arquivos protegidos do Office - uma caixa de diálogo solicitará o acesso para usuários internos e externos e o proprietário do arquivo poderá decidir se concederá ou não o acesso.
- Tipos de arquivos adicionais criptografados por meio da Proteção básica de arquivos - Não existe solicitação de pós-compartilhamento. O usuário precisa conhecer o proprietário do arquivo e clicar com o botão direito no arquivo criptografado para encontrar o ID de chave na guia Data Guardian. O usuário pode enviar essas informações ao proprietário e solicitar acesso.

Colaborar em arquivos recém-criados após o período de transição

Para arquivos novos criados e criptografados por você após o período de transição:

- Usuários internos ou externos dentro do seu grupo de acesso - Terão acesso a todos os arquivos criptografados e compartilhados.
  - Qualquer pessoa que for removida do grupo de acesso, perderá acesso.
  - Se o proprietário de um arquivo for removido do grupo, os outros usuários ainda terão acesso.
- Usuários internos ou externos fora do seu grupo de acesso - Não poderão visualizar um arquivo criptografado.
  - Um usuário interno dentro do grupo de acesso poderá conceder acesso.
  - Se um usuário externo for o proprietário de um arquivo criptografado, ele poderá conceder acesso a outra pessoa.
  - Se um usuário interno ou externo fora do grupo receber um arquivo criptografado e tentar abri-lo, uma caixa de diálogo pedirá que ele solicite acesso.

Identifier	**GUID-BDD3EF46-A9A1-48C2-BB76-B9D874BC37E4**
Status	**In Translation**

A empresa ainda não tem o Data Guardian e o modo Aceitar

Se sua empresa planeja usar o Data Guardian com grupos de acesso para aumentar a segurança dos dados confidenciais, o melhor a fazer é identificar os arquivos que você compartilha com os usuários internos e externos e descobrir se estes usuários estarão em algum grupo de acesso que o administrador criará para você. Inicialmente, a fim de garantir uma transição uniforme, sua empresa poderá estabelecer um breve período para processar os arquivos compartilhados existentes. Depois que o período de transição estiver concluído, aqueles no seu grupo de acesso poderão visualizar os arquivos criptografados e compartilhados criados por você. Você pode conceder acesso a pessoas fora do seu grupo de acesso para que você possa colaborar com elas e ter maior segurança.

Identifique-os no seu grupo de acesso

O administrador informará a você quem está em um ou mais dos seus grupos de acesso, dependendo de quem precisar de acesso a arquivos específicos. Isso poderá incluir usuários internos e externos. Se você trabalha com dados confidenciais e usuários específicos, você poderá solicitar que o administrador crie um grupo de acesso para esse conteúdo.

Usar o período de transição para processar os arquivos compartilhados

Quando o Data Guardian for instalado, uma varredura será feita no Windows ou Mac e criptografará os arquivos a seguir, se o administrador tiver ativado a política para eles.

- Tipos de arquivos adicionais, como, por exemplo, .txt ou .png, configurados para proteção básica de arquivos
- Arquivos para classificação de dados (Windows)
- Arquivos para classificação TITUS (Windows)

Se você já colabora em arquivos ou os compartilha com usuários internos ou externos, estes usuários poderão ou não fazer parte do seu grupo de acesso. O melhor a fazer para uma transição uniforme é ter um breve período de transição para processar os arquivos criptografados que são compartilhados com outros usuários. Você deverá fazer login no seu computador durante o período de transição.

Lembre-se do seguinte se quiser continuar compartilhando e colaborando nestes arquivos:

- No caso de arquivos compartilhados listados acima, a primeira pessoa a fazer login e ter a varredura feita em seu computador, se tornará o proprietário dos arquivos compartilhados.
- Se outra pessoa se tornar o proprietário do arquivo e o autor original não estiver no seu grupo de acesso, o proprietário original precisará solicitar o acesso ao novo proprietário. O proprietário original também poderá solicitar que o administrador altere a propriedade.
- Computadores de usuários externos não passarão por varredura, portanto, as cópias de arquivos compartilhados desprotegidos não serão verificadas e criptografadas.
- Se o Cloud Encryption do Data Guardianestiver ativado e os usuários compartilharem pastas ou arquivos em um provedor de serviços de armazenamento em nuvem, esses arquivos também serão verificados.

Colaborar em arquivos recém-criados após o período de transição

Para arquivos novos criados e criptografados por você após o período de transição:

- Usuários internos ou externos dentro do seu grupo de acesso - Terão acesso a todos os arquivos criptografados e compartilhados.
  - Qualquer pessoa que for removida do grupo de acesso, perderá acesso.
  - Se o proprietário de um arquivo for removido do grupo, os outros usuários ainda terão acesso.
- Usuários internos ou externos fora do seu grupo de acesso - Não poderão visualizar um arquivo criptografado.
  - Um usuário interno dentro do grupo de acesso poderá conceder acesso.
  - Se um usuário externo for o proprietário de um arquivo criptografado, ele poderá conceder acesso a outra pessoa.
  - Se um usuário interno ou externo fora do grupo receber um arquivo criptografado e tentar abri-lo, uma caixa de diálogo pedirá que ele solicite acesso.

Identifier	**GUID-16B7D77E-57D2-47D9-B2CC-39DB65B223E2**
Status	**In Translation**

A empresa ainda não tem o Data Guardian e o modo Forçar protegido

Se sua empresa planeja usar o Data Guardian com grupos de acesso para aumentar a segurança dos dados confidenciais, o melhor a fazer é identificar os arquivos que você compartilha com os usuários internos e externos e descobrir se estes usuários estarão em algum grupo de acesso que o administrador criará para você. Inicialmente, a fim de garantir uma transição uniforme, sua empresa poderá estabelecer um breve período para processar os arquivos compartilhados existentes. Depois que o período de transição estiver concluído, aqueles no seu grupo de acesso poderão visualizar os arquivos criptografados e compartilhados criados por você. Você pode conceder acesso a pessoas fora do seu grupo de acesso para que você possa colaborar com elas e ter maior segurança.

Identifique-os no seu grupo de acesso

O administrador informará a você quem está em um ou mais dos seus grupos de acesso, dependendo de quem precisar de acesso a arquivos específicos. Isso poderá incluir usuários internos e externos. Se você trabalha com dados confidenciais e usuários específicos, você poderá solicitar que o administrador crie um grupo de acesso para esse conteúdo.

Usar o período de transição para processar os arquivos compartilhados

Quando o Data Guardian for instalado, uma varredura será feita no Windows ou Mac e criptografará os arquivos a seguir, se o administrador tiver ativado a política para eles.

- Documentos do Office
- PDFs
- Tipos de arquivos adicionais, como, por exemplo, .txt ou .png, configurados para proteção básica de arquivos

O melhor a fazer para uma transição uniforme é ter um breve período de transição para processar os arquivos criptografados que são compartilhados com outros usuários. Você deverá fazer login no seu computador durante o período de transição.

Lembre-se do seguinte se quiser continuar compartilhando e colaborando nestes arquivos:

- No caso de arquivos compartilhados listados acima, a primeira pessoa a fazer login e ter a varredura feita em seu computador, se tornará o proprietário dos arquivos compartilhados.
- Se outra pessoa se tornar o proprietário do arquivo e o autor original não estiver no seu grupo de acesso, o proprietário original precisará solicitar o acesso ao novo proprietário. O proprietário original também poderá solicitar que o administrador altere a propriedade.
- Computadores de usuários externos não passarão por varredura, portanto, as cópias de arquivos compartilhados desprotegidos não serão verificadas e criptografadas.
- Se o Cloud Encryption do Data Guardian estiver ativado e os usuários compartilharem pastas ou arquivos em um provedor de serviços de armazenamento em nuvem, esses arquivos também serão verificados.

Colaborar em arquivos recém-criados após o período de transição

Para arquivos novos criados e criptografados por você após o período de transição:

- Usuários internos ou externos dentro do seu grupo de acesso - Terão acesso a todos os arquivos criptografados e compartilhados.
  - Qualquer pessoa que for removida do grupo de acesso, perderá acesso.
  - Se o proprietário de um arquivo for removido do grupo, os outros usuários ainda terão acesso.
- Usuários internos ou externos fora do seu grupo de acesso - Não poderão visualizar um arquivo criptografado.
  - Um usuário interno dentro do grupo de acesso poderá conceder acesso.
  - Se um usuário externo for o proprietário de um arquivo criptografado, ele poderá conceder acesso a outra pessoa.
  - Se um usuário interno ou externo fora do grupo receber um arquivo criptografado e tentar abri-lo, uma caixa de diálogo pedirá que ele solicite acesso.

Identifier	**GUID-2627974A-3D0D-4075-81BC-86DFD31CF90B**
Status	**Translated**

Alterar o proprietário de um arquivo criptografado

Durante o período de transição para grupos de acesso, se um outro usuário for designado como proprietário de um documento criptografado e compartilhado cujo autor original era você, você poderá solicitar que o administrador designe você como proprietário.

Identifier	**GUID-0ED28BBC-3A7C-48F3-A1AE-A5039C39C392**
Status	**In Translation**

Revogar acesso a uma chave

Se você conceder acesso a um arquivo criptografado para um usuário externo, o usuário terá a chave para abrir esse arquivo.

Como alternativa, se você não quiser mais que o usuário externo tenha acesso ao arquivo, poderá solicitar que o administrador revogue a chave. Isso se aplica somente a usuários externos.

Identifier	GUID-8B76A529-19A6-4107-983B-707F5AB1D09C
Status	In Translation

Pré-compartilhar arquivos protegidos no Windows

Você precisa ter o Data Guardian instalado e ser atribuído a um ou mais grupos de acesso.
Se um usuário interno ou externo não estiver em seu grupo de acesso, você poderá pré-compartilhar um arquivo protegido.

1 Clique com o botão direito do mouse em um arquivo protegido e selecione **Acesso a arquivos protegidos**.

Na UI de *Compartilhamento de acesso de arquivos protegidos*, o nome do documento é exibido no Arquivo selecionado.

2 Em *E-mail para compartilhar*, clique em **Adicionar** e insira um endereço de e-mail válido de um usuário externo ou interno que não esteja em seu grupo de acesso.

Você pode adicionar até dez endereços individuais por vez.

3 Para modificar um endereço de e-mail, clique **em Modificar**.

4 Para excluir um endereço de e-mail, selecione uma entrada e clique em **Excluir**.

NOTA:
O nome do proprietário do arquivo é indicado e não pode ser selecionado ou excluído.

5 Em Grupos disponíveis, seus grupos de acesso são exibidos. Selecione um ou mais grupos e use as setas para adicionar aos *Grupos compartilhados*.

6 Clique em **OK**. Uma mensagem de êxito será exibida.

NOTA:
Os usuários externos não podem compartilhar o documento protegido com outro usuário externo.

Se esta for a primeira vez que um usuário externo recebe um arquivo protegido do Data Guardian, o usuário precisa instalar o Data Guardian ou usar o portal da web para visualizar o arquivo protegido.

Identifier	GUID-C67795A0-FA20-4E32-9A2B-89654D67DFB2
Status	In Translation

Pré-compartilhar arquivos protegidos no Mac

Você precisa ter o Data Guardian instalado e ser atribuído a um ou mais grupos de acesso.
Se um usuário interno ou externo não estiver em seu grupo de acesso, você poderá pré-compartilhar um arquivo protegido.

1 Clique com o botão direito do mouse em um arquivo protegido e selecione **Acesso a arquivos protegidos**.

Na UI de *Compartilhamento de acesso de arquivos protegidos*, o nome do documento é exibido no Arquivo selecionado.

2 Em *E-mail para compartilhar*, clique em **Adicionar** e insira um endereço de e-mail válido de um usuário externo ou interno que não esteja em seu grupo de acesso.

Você pode adicionar até dez endereços individuais por vez.

3 Para excluir um endereço de e-mail, selecione uma entrada e clique em **Excluir**.

NOTA:
O nome do proprietário do arquivo é indicado e não pode ser selecionado ou excluído.

4 Em Grupos disponíveis, seus grupos de acesso são exibidos. Selecione um ou mais grupos e use as setas para adicionar aos *Grupos compartilhados*.

5 Clique em **OK**. Uma mensagem de êxito será exibida.

NOTA:
Os usuários externos não podem compartilhar o documento protegido com outro usuário externo.

Se esta for a primeira vez que um usuário externo recebe um arquivo protegido do Data Guardian, o usuário precisa instalar o Data Guardian ou usar o portal da web para visualizar o arquivo protegido.

Identifier	GUID-FAF997A4-8E8E-4DCB-BA76-575F951F0799
Status	In Translation

Pré-compartilhar arquivos protegidos no iOS ou Android

Se um usuário interno ou externo não estiver em seu grupo de acesso, você poderá pré-compartilhar um arquivo protegido.

1 Toque em um arquivo protegido.

2

NOTA:
Na guia Usuários, o nome do proprietário do arquivo é exibido, mas não pode ser selecionado nem excluído. Se você já tiver compartilhado o arquivo com usuários internos ou externos, esses nomes serão exibidos.

3 Na guia *Usuários*, para adicionar o endereço de e-mail de um usuário externo ou interno que não esteja no seu grupo de acesso, clique no ícone de mais (+) no canto inferior direito.

4 Para excluir um endereço de e-mail, deslize e toque em **Excluir**.

5 Toque na guia **Grupos** para visualizar seus grupos de acesso.

6 Toque em um grupo para compartilhar um arquivo protegido.

NOTA:
Uma marca de seleção indica um grupo com quem você optou por compartilhar o arquivo protegido.

7 No canto superior direito, toque em **Compartilhar**.

Uma mensagem de êxito será exibida. Os usuários externos não podem compartilhar o documento protegido com outro usuário externo.

Se esta for a primeira vez que um usuário externo recebe um arquivo protegido do Data Guardian, o usuário precisa instalar o Data Guardian ou usar o portal da web para visualizar o arquivo protegido.

Identifier	GUID-455BE40E-83D4-4C42-890C-18067EE3CFD5
Status	In Translation

Pré-compartilhar arquivos protegidos no Portal da web

Se um usuário interno ou externo não estiver em seu grupo de acesso, você poderá pré-compartilhar um arquivo protegido.

1 No portal da Web, faça upload de um documento protegido.

Se o administrador tiver colocado você em um ou mais grupos de acesso, o ícone de Acesso ao arquivo protegido é mostrado ao lado do ícone de Download.

2 Clique no ícone de **Acesso ao arquivo protegido**.

Na UI de *Compartilhamento de acesso de arquivos protegidos*, o nome do documento é exibido no Arquivo selecionado.

3 Em *E-mail para compartilhar*, clique em **Adicionar novo**.

4 Insira um endereço de e-mail válido de um usuário externo ou interno que não esteja no seu grupo de acesso e clique na marca de seleção para salvá-lo. Você pode adicionar até dez endereços individuais por vez.

> **NOTA:**
> Para excluir um endereço de e-mail, clique no **X**. O nome da pessoa que está compartilhando o documento fica destacado e não pode ser selecionado ou excluído.

5 Em Grupos disponíveis, seus grupos de acesso são exibidos. Clique em **Selecionar Tudo** ou clique no ícone de seta ao lado de uma opção para adicionar a *Grupos Compartilhados* ou para remover.

6 Clique em **OK**.

> **NOTA:**
> Os usuários externos não podem compartilhar o documento protegido com outro usuário externo.

Se essa for a primeira vez que um usuário externo recebe um arquivo protegido do Data Guardian, o usuário deve instalar o portal da web.

Identifier	**GUID-5BE95524-98D7-476C-9790-CA2298568418**
Status	**In Translation**

Pré-compartilhar arquivos protegidos como um usuário externo

Você precisa ter o Data Guardian instalado e ser atribuído a um ou mais grupos de acesso.
Se você for o originador ou proprietário de um arquivo protegido, poderá pré-compartilhar o arquivo com um usuário interno. Você não pode compartilhar o documento protegido com outro usuário. Se você não for proprietário do arquivo, não poderá compartilhá-lo.

- O *E-mail para compartilhamento* não lista os nomes de outros usuários com os quais a documentação protegida foi compartilhada.
- Nenhum grupo é exibido em Grupos disponíveis. Você só pode compartilhar com indivíduos.

1 Clique com o botão direito do mouse em um arquivo protegido e selecione **Acesso a arquivos protegidos**.
Na UI de *Compartilhamento de acesso de arquivos protegidos*, o nome do documento é exibido no Arquivo selecionado.

2 Em *E-mail para compartilhar*, clique em **Adicionar** e insira um endereço de e-mail válido de um usuário externo ou interno que não esteja em seu grupo de acesso.
Você pode adicionar até dez endereços individuais por vez.

3 Para modificar um endereço de e-mail, clique **em Modificar**.

4 Para excluir um endereço de e-mail, selecione uma entrada e clique em **Excluir**.

> **NOTA:**
> Como proprietário do arquivo, não é possível selecionar nem excluir seu nome.

5 Clique em **OK**. Uma mensagem de êxito será exibida.

Se esta for a primeira vez que um usuário recebe um arquivo protegido do Data Guardian, o usuário precisa instalar o Data Guardian ou usar o portal da web para visualizar o arquivo protegido.

Identifier	GUID-F97CE528-0A49-4763-80D0-0F5937EAE934
Status	In Translation

Modificar quem tem acesso a e-mails protegidos

Com base na política definida pelo administrador, você pode clicar com o botão direito do mouse em um e-mail que você protegeu e enviou aos usuários do seu Grupo de acesso. Você pode modificar quem tem acesso a esse e-mail.

1 No Outlook, clique com o botão direito do mouse em um e-mail rotulado como [PROTEGIDO].

2 Na parte inferior, selecione **Acesso a e-mails protegidos**.

Uma lista exibe os usuários com quem você compartilhou o acesso.

3 Remova usuários individuais se você não quiser mais que eles tenham acesso ao e-mail protegido.

Identifier	GUID-F553E0C3-FCF3-4782-8FD4-
Status	Translation Validated

Frequently Asked Questions

Identifier	GUID-D70F8E30-C205-474A-BC17-DB3867AE07AE
Status	In Translation

Miscellaneous FAQs

Pergunta

Pergunta

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

Resposta

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

Solução

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

Identifier	GUID-36E78894-7902-4034-8BFA-6D63A1743855
Status	Translation Validated

Perguntas frequentes sobre documentos do Office e modo protegido

Pergunta

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

Resposta

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

Solução

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

Pergunta

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

Resposta

Verifique o seguinte:

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

Solução

Para verificar as Configurações do Bloqueio avançado de arquivo:

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