Dell Data Guardian

Guia do Utilizador 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 a melhorar a utilização do produto.

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

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

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

Guia do utilizador 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 utilizador do Dell Data Guardian* fornece as informações necessárias para a instalação e utilização do Data Guardian no Windows, Mac, Dispositivo móvel ou portal Web.

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

Descrição geral

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

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

NOTA:
O seu administrador irá informá-lo se a sua empresa utiliza o Data Guardian apenas com armazenamento na nuvem, apenas com documentos do Office ou com ambos. O seu administrador também irá informá-lo em relação a aplicações e tipos de ficheiro adicionais que podem ser protegidos.

Pode utilizar o Data Guardian nas seguintes plataformas:

- Windows
- iOS
- Android
- Mac
- Portal Web do Data Guardian, se for configurado pelo seu administrador

NOTA:
O Data Guardian para Mac pode abrir ficheiros encriptados por outras plataformas. Alguns ficheiros podem ser só de leitura. A maioria das informações do utilizador sobre o Data Guardian para Mac encontra-se no software como ajuda online.

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

Opções de encriptação do Data Guardian

Com base no nível de segurança estabelecido pela sua empresa, o seu administrador define as políticas para proteger os dados inativos e os dados em movimento. O seu administrador informa-o em relação às políticas que se aplicam à sua empresa.

Esta lista apresenta uma descrição geral de algumas opções de encriptação e, para algumas plataformas, a localização das definições das políticas.

Modos e documentos do Office

A política pode ser definida para proteger documentos do Office. O comportamento de encriptação pode variar dependendo da plataforma e do modo. Para Mac, consulte a ajuda online.

Modos	Documentos do Office
As opções de modo para **Windows e Mac**: **Modo opcional** - O utilizador dispõe de algumas opções para determinar os documentos do Office que pretende proteger. • **Windows** e **Mac** - Uma pasta de **Documentos seguros** é adicionada à raiz da sua pasta Documentos. Isto proporciona outra forma de encriptar um ficheiro. **Modo de proteção forçada** - A sua empresa exige um nível de segurança mais elevado. O Data Guardian efetua um varrimento para encriptar os ficheiros. • **Windows** e **Mac** - Outra política pode adicionar uma pasta de **Documentos desprotegidos** à raiz da sua pasta Documentos. Coloque os documentos do Office Protegidos ou os tipos de Proteção Básica de Ficheiros nesta pasta para os desencriptar. • **Mac** - Protege os ficheiros em **/Users**. Estas plataformas não são baseadas em modos: • Dispositivos móveis • Portal Web	**Documentos do Office utilizados em Windows, Mac, dispositivos móveis e portal Web** • .docx • .pptx • .xlsx • .docm • .pptm • .xlsm • .pdf - Se protegidos com o Data Guardian, abrem com o Adobe Acrobat Reader DC ou o Microsoft Word, mas não a partir da rede.

Documentos do Office - Windows

O seu administrador pode definir as políticas do Data Guardian adicionais para controlar ou evitar a perda de dados através destas opções. O comportamento de encriptação pode variar dependendo do modo.

Opções para documentos do Office protegidos no Windows	Descrição
• Guardar - Se um documento do Office estiver protegido, é possível guardar novos conteúdos. (A opção **Guardar Como** é apresentada a cinzento.) • Guardar como protegido	Outras informações para Windows: • Documento do Office **desprotegido** - pode selecionar **Guardar**, **Guardar Como** ou **Guardar como protegido**. • É apresentado um limite vermelho em documentos do Office e e-mails protegidos.

Opções para documentos do Office protegidos no Windows	Descrição
• Se um documento do Office já estiver protegido, a opção **Guardar Como** é apresentada a cinzento.	
Copiar/colar e área de transferência	É possível copiar de um documento do Office protegido e colar noutro documento do Office protegido. Não é possível colar a partir de um documento protegido para um desprotegido.
Imprimir	Com base na política, a impressão de um documento do Office protegido pode ser permitida, incluir uma marca de água ou estar desativada.
Exportar (Windows e Office 2013 e superior, Mobile)	Com base na política, pode ser permitida, ter uma marca de água ou estar desativada. **NOTA:** Se a marca de água estiver definida, é possível exportar documentos do Office. Não é possível exportar PDF.
Captura de ecrã	Com base na política, pode ser permitida ou ser bloqueada.
Processos bloqueados Por exemplo: ferramenta de recorte	Com base na política definida pela empresa, alguns processos são bloqueados quando um documento do Office protegido é aberto.
Marca de água no ecrã	Quando um documento do Office protegido é aberto, o ecrã apresenta uma marca de água com o nome do computador e o nome de utilizador.
Classificação TITUS (Windows com modo opcional)	Se uma política estiver ativada, pode clicar com o botão direito do rato num documento do Office e selecionar a classificação TITUS. Esta constitui outra forma de os utilizadores protegerem um documento do Office.
Classificação de dados (Windows com modo opcional)	Se uma política estiver ativada e configurada para proteger informações sensíveis, tais como números da Segurança Social ou números de cartões de crédito, os documentos do Office com esses dados são encriptados.

Documentos do Office - Mac, dispositivos móveis e portal Web

O comportamento de encriptação pode variar dependendo da plataforma e do modo. O seu administrador informa-o em relação às que se aplicam à sua empresa.

Opção de encriptação	Descrição
Mac - Interface do Dell Data Guardian	**Mac** – Carregar um documento protegido para encriptação. Transferir um documento protegido para desencriptação. Depois de editar um documento protegido, as alterações são guardadas no ficheiro original, na nuvem ou localmente.
Dispositivos móveis - Na aplicação do Data Guardian • Imprimir • Marca de água no ecrã • Marca de água oculta • Exportar	**Dispositivos móveis** – Com base na política: • Os documentos do Office na aplicação do Data Guardian são protegidos. • A impressão de um documento do Office protegido pode ser permitida, ter uma marca de água ou estar desativada.

Opção de encriptação	Descrição
	• Quando um documento do Office protegido é aberto, o ecrã apresenta uma marca de água com o nome do computador e o nome de utilizador.
Portal Web • Marca de água no ecrã	**Portal Web** – É possível carregar documentos protegidos ou desprotegidos, mas qualquer ficheiro carregado é protegido quando clica em Transferir. Quando um documento do Office protegido é aberto, o ecrã apresenta uma marca de água com o nome do computador e o nome de utilizador.

Opções adicionais

O comportamento de encriptação pode variar dependendo da plataforma e do modo. O seu administrador informa-o em relação às que se aplicam à sua empresa.

Opção	Descrição (Modos opcional e Proteção forçada)
Proteção básica de ficheiros - Permite a proteção de aplicações e tipos de ficheiro adicionais. (Windows, Mac, dispositivo móvel e portal Web) • Exemplos: .txt ou .png **NOTA:** De momento, não é apresentado um limite vermelho para estes tipos de ficheiro, mesmo quando estão protegidos.	O seu administrador pode configurar uma política para especificar as aplicações e os tipos de ficheiro a serem encriptados. **Windows, Mac e Mobile** – estes ficheiros são submetidos a varrimento e encriptados. • **Mac** – para extensões de ficheiros definidas pelo administrador, encripta esses tipos de ficheiro na pasta */Users*. **Portal Web** – também com base na política, estes ficheiros podem ser só de leitura ou o utilizador pode editá-los.
Partilhar documentos do Office protegidos com **utilizadores externos**. (Windows, Mac, dispositivo móvel e portal Web) Uma página de rosto apresenta as ligações para o registo e as informações para instalar o Data Guardian.	• Utilizadores externos e **Windows** – Também é possível adicionar uma **restrição de data (embargo)** em PDF e documentos do Office protegidos. • **Portal Web** - É possível carregar ficheiros partilhados para o portal Web. Não é possível partilhar um ficheiro a partir do portal Web, mas pode partilhá-lo após a transferência.
Adulteração de ficheiro ou página de rosto (Windows, Mac, dispositivo móvel e Web)	Para ficheiros do Office, o Data Guardian pode analisar documentos protegidos para detetar algumas formas de adulteração.
Grupos de Acesso (no local) (Windows, Mac, dispositivo móvel e portal Web)	Quando ativado pelo administrador, apenas as pessoas no seu grupo de acesso podem ver os seus ficheiros encriptados. Pode conceder acesso a ficheiros individuais a utilizadores internos e externos, e estes podem solicitar acesso. Com base na política adicional, pode clicar com o botão direito do rato num e-mail do Outlook identificado como [PROTEGIDO] e remover o acesso para utilizadores individuais.
Geofencing (dispositivo móvel)	Apenas os utilizadores numa área específica podem aceder a ficheiros dos respetivos telemóveis.
Encriptação de e-mail do Outlook (Windows)	Com base em política, o botão *Proteger* permite encriptar o conteúdo de um e-mail e dos anexos. Quando enviado para utilizadores externos, uma página de rosto apresenta as ligações para o registo e as informações para instalar o Data Guardian.

Alojado ou on-prem

Se tiver de instalar o Data Guardian sozinho, o seu administrador irá confirmar a opção aplicável à sua empresa.

NOTA:
Para aplicações móveis, se tiver o Workspace ONE instalado, é possível autenticar-se no Data Guardian com início de sessão único.

Dell Security Center Alojado	Dell Management Server No Local
Uma solução Software como serviço (SaaS) alojada destinada à gestão do software Dell Data Security. Se a sua empresa tiver vários inquilinos, o seu administrador fornecerá uma ID de instalação. Quando é apresentada uma página de rosto para um utilizador que ainda não tem acesso a um documento protegido, as informações sobre a ID de instalação estão incluídas na página de rosto. Todas as plataformas – se um inquilino não pagar durante um determinado período de tempo, o inquilino em questão pode ser suspenso.	Um servidor no local abrangido pela rede da empresa destinado à gestão do software Dell Data Security. O seu administrador fornecerá o nome do URL do Dell Server.

Encriptação em nuvem

O comportamento de encriptação pode variar dependendo da plataforma e do modo. O seu administrador informa-o em relação às que se aplicam à sua empresa.

Plataformas	Descrição
Dispositivos móveis	Consulte Utilizar a Proteção da nuvem com dispositivos móveis.
Mac	Consulte a Ajuda online.
Portal Web	Consulte a Ajuda online.
Windows	De momento, a proteção da encriptação em nuvem do Data Guardian encontra-se desativada no Windows, para evitar problemas de compatibilidade com as funções mais recentes dos fornecedores de serviços de nuvem. Para ver ficheiros .xen já protegidos com Encriptação em Nuvem, utilize a aplicação móvel ou o portal Web do Data Guardian, ou o Data Guardian com Mac.

Definições das políticas

Algumas plataformas incluem uma lista parcial das definições das políticas para o seu dispositivo.

Plataforma	Localização das definições das políticas
Mac	Painel *Preferências*
Dispositivos móveis	Ícone **Definições** > **Acerca de**
Portal Web	Ícone **Definições** > **Acerca de**

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

Suporte adicional

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

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

Requisitos

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

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

Dell Server

O Data Guardian para Windows, Mac e Mobile requer o Security Management Server ou o Security Management Server Virtual v9.6 ou posterior. O cliente Web do Data Guardian requer o Security Management Server ou o Security Management Server Virtual v9.8 ou posterior. Neste documento, ambos os servidores estão assinalados como Dell Server, a não ser que seja necessário indicar uma versão específica (por exemplo, um procedimento que seja diferente ao utilizar o Security Management Server Virtual).

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

Data Guardian para Windows

- Durante a implementação, devem ser seguidas as melhores práticas de TI. Estas incluem, entre outras, ambientes de teste controlados para os testes iniciais e a implementação progressiva para os utilizadores.
- A conta de utilizador que realiza a instalação/atualização/desinstalação deve ser um utilizador administrador local ou de domínio, que poderá ser atribuído temporariamente por uma ferramenta de implementação, como o Microsoft SMS ou Dell KACE. Não são suportados utilizadores não administradores com privilégios elevados.
- Realize uma cópia de segurança de todos os dados importantes antes de iniciar a instalação/desinstalação.
- Não realize alterações no computador, incluindo inserir ou remover unidades externas (USB) durante a instalação.
- O Data Guardian é compatível com versões específicas do Microsoft Office 2016 e também do Microsoft Office 365 Empresas e Empresas - Versão Premium. Não é compatível com o Office 365 Empresas - Versão Essentials.
- O Data Guardian para Windows é compatível com o Workspace ONE. O instalador do Data Guardian para o Workspace ONE e a instalação MSI têm uma extensão .msi.
- O Data Guardian v2.4 e posterior para Windows é suportado em ambientes de "air gap", mas com algumas limitações. Neste momento, não são suportados dados de geolocalização em eventos de auditoria e ficheiros de embargo. O web beacon necessita de alguma configuração.
- Certifique-se de que os dispositivos de destino estão ligados a https://yoursecurityservername.domain.com:8443/cloudweb/register https://yoursecurityservername.domain.com:8443/cloudweb
- Antes de implementar o Data Guardian, é preferível que os dispositivos de destino não tenham ainda contas de armazenamento na nuvem configuradas. Se os utilizadores decidirem manter as respetivas contas existentes, devem certificar-se de que quaisquer ficheiros que devam permanecer *sem encriptação* são retirados do cliente de sincronização antes de instalar o Data Guardian.
- Os utilizadores devem estar preparados para reiniciarem os respetivos computadores depois de instalarem o cliente.
- O Data Guardian não interfere no comportamento de clientes de sincronização. Por conseguinte, os administradores e utilizadores devem familiarizar-se com o funcionamento destas aplicações antes de implementarem o Data Guardian. Para obter mais informações, consulte o apoio técnico do Box em https://support.box.com/home, o apoio técnico do Dropbox em https://www.dropbox.com/help ou o apoio técnico do OneDrive em http://windows.microsoft.com/en-us/onedrive/onedrive-help#onedrive=other.

- Os documentos do Office protegidos são suportados pelo Mozy, uma solução complementar do Data Guardian, bem como por outros produtos de armazenamento em nuvem, e-mail e NFS.
- Embora a Dell Encryption não seja necessária, se for utilizada, o cliente de encriptação deve ser v8.12 ou posterior.
- O Data Guardian não é compatível com a ferramenta de restauro do sistema Windows nem com o Windows Insider Preview.
- O Redirecionamento de Pastas da Microsoft não é suportado com o Data Guardian.
- Certifique-se de que verifica periodicamente a página dell.com/support para procurar a documentação e os avisos técnicos mais atuais.

Pré-requisitos

Pré-requisitos .exe

Se ainda não estiver instalado, o programa de instalação instala o Pacote Redistribuível do Microsoft Visual C++ 2017 (x86 e x64).

NOTA:
No Windows 7 e Windows 8.1, os computadores devem estar atualizados com o Windows Update. Para obter mais informações, consulte https://support.microsoft.com/en-us/help/2919355 e https://support.microsoft.com/en-us/help/2999226.

Pré-requisitos .msi

Tem de instalar o Pacote redistribuível do Microsoft Visual Studio C++ 2017 (x86 e x64).

NOTA:
Além disso, ao executar o MSI, tem também de instalar o Visual Studio 2010 Tools para o Office Runtime (x86 e x64).

Pré-requisitos gerais

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

Hardware

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

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

Sistemas operativos

A tabela seguinte apresenta os sistemas operativos suportados.

Sistemas operativos Windows (32 bits e 64 bits)

- Windows 7 SP1: Enterprise, Professional, Ultimate
- Windows 8.1 Atualização 0-1: Enterprise Edition, Pro Edition
- Windows 10: Education, Enterprise, Pro Versão 1703 (Creators Update/Redstone 2) até à Versão 1809 (Atualização de outubro de 2018/Redstone 5)

NOTA:
O cliente tem de dispor de um dos seguintes sistemas operativos ou será bloqueado. Se necessário, uma definição numa chave de registo permite ao administrador ultrapassar o bloqueio.

Para obter suporte para o Redstone 4, tem de atualizar o agente antes de atualizar o sistema operativo. 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 posterior ou com o Enhanced Mitigation Experience Toolkit (EMET) no Redstone 2 e anterior.

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

O Data Guardian não suporta várias versões do Office num computador.

Microsoft Office

O Data Guardian suporta as seguintes versões do Office. No entanto, é preciso 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

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

Hardware para Mac

- Intel Core 2 Duo, Core i3, Core i5, Core i7 ou processador Xeon
- 2 GB de RAM

Hardware para Mac

- 10 GB de espaço livre em disco

Sistemas operativos

Segue-se uma lista dos sistemas operativos suportados.

Sistemas operativos para Mac

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

Fornecedores de armazenamento na nuvem

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

Fornecedores de armazenamento na nuvem

- DropBox
- Box
- Google Drive

  NOTA:
  A *cópia de segurança e a sincronização da Google* não são suportadas.

- OneDrive
- OneDrive for Business

Microsoft Office

O Data Guardian para Mac suporta as seguintes versões do Office.

Microsoft Office

- Office 2013 SP1
- Office 2016
- Office 2019

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

Aplicação Data Guardian for Mobile

Segue-se uma lista dos sistemas operativos suportados pela aplicação Data Guardian for Mobile.

Sistemas operativos para 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 operativos iOS

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

Sistema operativo Chromebook

É necessária a versão M53 ou superior do Chrome OS para executar aplicações Android no Chrome OS. Estes dispositivos estão validados para executar aplicações Android no Chrome OS, mas confirme a sua opção junto do seu representante de vendas:

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

Microsoft Office

A aplicação Data Guardian for Mobile pode abrir os ficheiros criados com as seguintes versões 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 que instala o cliente Web e comunica com a versão v9.8 ou posterior do Dell Server.

Os seguintes ambientes virtuais podem ser utilizados para implementar o cliente Web do Data Guardian.

Ambientes virtuais

- **VMware ESXi 6.7**
  - Necessário CPU de 64 bits x86
  - Computador anfitrião com pelo menos dois núcleos
  - Recomendado um mínimo de 8 GB de RAM
  - Não é necessário um sistema operativo
  - Consulte http://www.vmware.com/resources/compatibility/search.php para obter uma lista completa dos sistemas operativos anfitriões compatíveis
  - O hardware deve cumprir os requisitos mínimos do VMware
  - RAM mínima de 4 GB para recurso de imagem dedicado
  - Consulte http://pubs.vmware.com/vsphere-67/index.jsp para obter mais informações

- **VMware ESXi 5.5**
  - Necessário CPU de 64 bits x86
  - Computador anfitrião com pelo menos dois núcleos
  - Recomendado um mínimo de 8 GB de RAM
  - Não é necessário um sistema operativo
  - Consulte http://www.vmware.com/resources/compatibility/search.php para obter uma lista completa dos sistemas operativos anfitriões compatíveis
  - O hardware deve cumprir os requisitos mínimos do VMware
  - RAM mínima de 4 GB para recurso de imagem dedicado
  - Consulte http://pubs.vmware.com/vsphere-55/index.jsp para obter mais informações

- **Microsoft Hyper-V**
  - Processador de 64 bits com Tradução de Endereços de Segundo Nível (SLAT)
  - Recomendado um mínimo de 8 GB de RAM
  - O hardware deve cumprir os requisitos mínimos do Hyper-V
  - Para obter mais informações, consulte https://docs.microsoft.com/en-us/virtualization/hyper-v-on-windows/reference/hyper-v-requirements.

NOTA:
Estes mínimos representam vinte e cinco ou menos ligações simultâneas a um único portal Web.

Fornecedores de armazenamento na nuvem

Com base nas definições das políticas, o portal Web do Data Guardian pode aceder aos fornecedores de armazenamento na nuvem.

Fornecedores de armazenamento na nuvem
• OneDrive for Business

Microsoft Office

O Data Guardian para Web pode abrir os ficheiros 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 multifator (MFA) da Amazon Cognito não é suportada em nenhuma plataforma do Data Guardian.

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

Web browsers

Pode utilizar o Data Guardian com o Internet Explorer, Mozilla Firefox, Google Chrome e Microsoft Edge.

Para Mac; também é suportado o Safari.

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

Adobe Acrobat

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

NOTA:

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

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

Instalar ou desinstalar o Data Guardian no Windows

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

Esteja preparado para reiniciar o computador após a instalação do Data Guardian.

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

Descrição geral das tarefas de instalação para Windows

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

Instalar o Data Guardian

Tarefa	Descrição	Para obter mais informações
Instalar o Data Guardian	Determinar o seguinte: O utilizador tem de instalar o Data Guardian O administrador já instalou o Data Guardian - continue para o passo seguinte.	Instalações pelo utilizador: consulte Instalar interativamente o Data Guardian no Windows. Reiniciar e continuar para o passo seguinte.
Confirmar o estado de ativação	Confirme na área de notificação se o ícone do Data Guardian tem uma marca de verificação verde  .	Se o ícone apresentar um ponto de exclamação laranja, consulte Possíveis problemas na ativação - Nuvem e Office protegido. **NOTA:** Se ao abrir um documento do Office for apresentada uma página de rosto com informações de instalação ou ativação, o seu administrador poderá ter definido políticas para proteger os documentos do Office. Confirme se o Data Guardian está instalado e ativado.

Opções para Windows

Tarefa	Descrição	Para obter mais informações
Ver o menu área de notificação	Fornece informações úteis sobre ficheiros, pastas e resolução de problemas.	Compreender os itens de menu da área de notificação do Data Guardian

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

Pastas preexistentes com ficheiros não encriptados

Ao implementar o Data Guardian, é preferível que os dispositivos de destino não tenham ainda as contas configuradas as contas do fornecedor de armazenamento na nuvem.

Se um fornecedor de armazenamento na nuvem estiver configurado com pastas sincronizadas com o computador local antes da instalação do Data Guardian:

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

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

Instalar o Data Guardian interativamente no Windows

Apenas um administrador local tem permissão para instalar o Data Guardian. Se forem os utilizadores a instalar o produto, informe-os sobre a localização do suporte de instalação.

Antes de começar

Dependendo do ambiente e do produto Data Guardian, determine qual destas opções é necessária:

Dell Security Center Alojado	Dell Management Server No Local
Se o seu ambiente alojado tiver vários inquilinos, terá de ter uma ID de instalação.	Certifique-se de que sabe o nome do Dell Server.

Instalar o Data Guardian

Esteja preparado para reiniciar o computador após a instalação do Data Guardian.

1. Para transferir o instalador do Data Guardian, aceda à localização especificada pelo seu administrador.
2. Com base no seu sistema operativo, selecione o programa de instalação de 32 bits ou de 64 bits e copie-o para o computador local. Seguem-se alguns exemplos de nomes de programas de instalação:
   - Dell Security Center Alojado – os nomes dos programa de instalação têm uma extensão .exe
   - on-prem - os nomes dos programas de instalação têm:
     - extensão .exe
     - extensão .msi para Workspace ONE e uma instalação MSI
3. Clique duas vezes no ficheiro para iniciar o programa de instalação.
4. Se for apresentado um aviso de segurança, clique em **Executar**.
5. Selecione um idioma e clique em **OK**.
6. Caso apareça uma mensagem a questionar se deseja instalar o Pacote redistribuível do Microsoft Visual C++ 2015 ou o Microsoft .NET Framework 4.5.2 Client Profile, clique em **OK**.
7. No ecrã de boas-vindas, clique em **Seguinte**.

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

9 No ecrã Pasta de destino, clique em **Seguinte** para instalar na localização predefinida de C:\Program Files\Dell\Data Guardian\.

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

10 Selecione um dos seguintes:

Dell Security Center Alojado	Dell Management Server No Local
Uma solução Software como serviço (SaaS) alojada destinada à gestão do software Dell Data Security.	Um servidor no local abrangido pela rede da empresa destinado à gestão do software Dell Data Security.

a Selecione **Dell Security Center Alojado**.

b Opcionalmente, se a sua empresa tiver vários inquilinos, introduza uma ID de instalação.

> **NOTA:**
> Se a sua empresa tiver vários inquilinos e não introduzir uma ID de instalação, o administrador pode adicioná-la ao registo mais tarde.

c Clique em **Continuar**.

d Avance para o passo 11.

a Selecione **Dell Management Server No Local**.

b No campo `Nome do Dell Management Server:`, introduza o nome do Dell Server com o qual este computador vai comunicar, como, por exemplo, servidor.domínio.com. Não é necessário incluir web ou http(s). Esta informação é fornecida pelo seu administrador.

> **NOTA:**
> Não desmarque a caixa de verificação *Ativar verificação de confiança SSL* exceto se tal for instruído pelo administrador.

c Clique em **Seguinte**.

d No ecrã Confirmar informações do Dell Management Server, certifique-se de que o endereço URL do Dell Server está correto. O instalador adiciona www ou http(s) e, de seguida, a porta. Clique em **Seguinte**.

e Avance para o passo 11.

11 Na janela Tipo de gestão, selecione esta opção:

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

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

Uma janela de estado apresenta o progresso da instalação.

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

14 Clique em **Sim** para reiniciar.

A instalação do Data Guardian está concluída.

15 Os utilizadores têm de confirmar a ativação. O ícone da área de notificação do Data Guardian deverá ter uma marca de verificação verde  .

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

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

Possíveis problemas na ativação - Nuvem e Office protegido

Se tiver instalado o Data Guardian, mas o ícone do Data Guardian na área de notificação não apresentar uma marca de verificação verde  , tenha em atenção o seguinte, consoante tenha encriptação na nuvem, Office protegido ou ambos:

Opção do Data Guardian	Possível problema
Documentos protegidos do Office	• O Data Guardian pode converter documentos do Office existentes no modo protegido antes de proceder à ativação. Se for o caso, quando abrir um

Opção do Data Guardian	Possível problema
	documento do Office, é apresentada uma página de rosto com informações sobre o processo de ativação.
Encriptação em nuvem	• O acesso está bloqueado aos websites de sincronização na nuvem • As aplicações de sincronização na nuvem estão bloqueadas para ligação aos respetivos serviços na Internet. • As pastas sincronizadas locais não são atualizadas durante este período de tempo

Proceda da seguinte forma:

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

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

Ativar o Data Guardian

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

1 Inicie a sessão no Windows.

Na área de notificação, é apresentado um ícone de proteção com um ponto de exclamação laranja.

2 Clique no ícone do **Data Guardian** na área de notificação e selecione **Ativação do utilizador**.

3 Introduza o seu endereço de e-mail e palavra-passe do domínio e clique em **Ativar**.

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

Depois de concluída a ativação, uma marca de verificação verde é apresentada no ícone da área de notificação do Data Guardian  .

4 Confirme o seu estado de modo de utilizador. Clique no ícone da área de notificação e selecione **Detalhes**.

5 Na parte superior, confirme

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

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

> **NOTA:**
> Se o modo de utilizador indicar **Não registado**, o Data Guardian não está ativado.

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

Dell Security Center Alojado e inquilino suspenso

Com o Dell Security Center Alojado, se um inquilino não efetuar pagamentos durante um determinado período de tempo, esse inquilino pode ser suspenso. Isto aplica-se a Windows, a Mac, a dispositivos móveis e a portais Web.

Os utilizadores internos e externos do Data Guardian podem deparar-se com o seguinte:

- Todas as plataformas – se tentar instalar o Data Guardian, ativar ou iniciar sessão, é apresentada uma caixa de diálogo a indicar que o inquilino está suspenso.
- Mac – se o seu inquilino for suspenso enquanto o Data Guardian estiver aberto, após fechar o Explorer e todos os ficheiros e, em seguida, tentar abrir um ficheiro protegido, é apresentada uma caixa de diálogo a indicar que o inquilino está suspenso.
- Portal Web:
  - Se já tiver sessão iniciada e carregar um ficheiro encriptado, é apresentada a mensagem Falha ao carregar.
  - Se um ficheiro encriptado ou não encriptado tiver sido carregado e, em seguida, o inquilino for suspenso, é apresentada a mensagem Falha ao transferir.
  - Se terminar sessão e tentar iniciar sessão novamente, é apresentada uma caixa de diálogo a indicar que o inquilino está suspenso.

Contacte o seu administrador.

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

Compreender os itens de menu da Área de notificação do Data Guardian

Ecrã de detalhes

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

- Para obter suporte técnico, pode fornecer informações de estado ou da versão.
- Para procurar por um nome de ficheiro, selecione Copiar no lado direito inferior e cole o conteúdo num ficheiro Word.
- Para ver quem é o proprietário de uma pasta, selecione Pastas e percorra o texto até à coluna PROPRIETÁRIO DA PASTA.

Para aceder ao ecrã Detalhes:

Clique com o botão direito do rato no ícone da área de notificação do **Data Guardian** e, em seguida, clique em **Detalhes**.

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

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

Estado de execução: o estado de ativação do dispositivo. Os valores são: Ativo, A Reativar, Suspenso, A Suspender

Modo de utilizador:

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

- **Não registado** - um utilizador interno ou externo cujo Data Guardian não está ativado

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

URL do servidor: o Dell Server que comunica com este cliente.

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

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

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

Nome: nome do ficheiro

Nuvem: esta funcionalidade foi desativada, pelo que já não tem dados.

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

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

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

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

Pasta: o nome do caminho completo da pasta.

Última modificação: a data de modificação do ficheiro.

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

Leitura de Ficheiro XEN: esta funcionalidade foi desativada.

Browser criado: *Verdadeiro* ou *Falso*.

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

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

Anteriormente, a Encriptação em Nuvem do Data Guardian tinha a área **Pastas** no ecrã Detalhes. Atualmente, a Encriptação em Nuvem foi desativada.

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

Verificar atualizações de política

Se o seu administrador modificar uma política e o notificar de uma atualização de política, aceda à área de notificação do Windows, clique no ícone **Dell Data Guardian** e selecione **Verificar atualizações de política**.

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

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

Localizar ficheiros de registo

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

Para localizar ficheiros de registo:

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

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

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

Atualizar o Data Guardian

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

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

Desinstalar o Data Guardian no Windows

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

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

Desinstalar o Data Guardian

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

Copiar ficheiros para a sua unidade local

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

1 Antes de desinstalar, determine se necessita de aceder a quaisquer ficheiros.
2 Copie os ficheiros em questão para a sua unidade local.

As pastas e ficheiros no website do cliente de sincronização ficarão encriptados, ainda que os transfira. Para os visualizar, é necessário reinstalar o Data Guardian. Em alternativa, pode visualizá-los no portal Web do Data Guardian.

Desinstalar o Data Guardian

1 Utilize 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 **Seguinte** quando o ecrã de boas-vindas for apresentado.
4 Selecione **Remover** e clique em **Seguinte**.
5 É apresentado um aviso a confirmar a desinstalação do Dell Data Guardian. Em caso afirmativo, clique em **Seguinte**.
6 No ecrã Remover o programa, clique em **Remover**.
A janela de estado exibe o andamento.
7 Se for apresentada uma mensagem de erro do cliente de sincronização, clique em **Continuar**.
8 Se uma caixa de diálogo indicar que o utilizador tem um documento do Office aberto, clique em **OK**, feche o documento do Office e inicie novamente a desinstalação.
9 Clique em **Concluir** quando for apresentado o ecrã Concluído.
10 Clique em **Sim** para reiniciar.

A desinstalação do Data Guardian está concluída.

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

Fornecer feedback à Dell

Se o seu administrador tiver ativado o feedback, poderá fornecer feedback à Dell sobre este produto. O formulário de feedback contém duas perguntas sobre o seu grau de satisfação, com uma área de comentários e uma escala de classificação (onde 10 indica o mais alto grau de satisfação).

Para aceder, clique no ícone do Data Guardian na área de notificação e selecione **Enviar feedback**.

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

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

Utilizar o Data Guardian com o Windows

O seu administrador já configurou as políticas para proteger os documentos e indicar-lhe-á qual destas opções se aplicam à sua empresa.

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

Descrição geral das opções

Esta descrição geral resume as opções possíveis para o Data Guardian com base na política definida pelo seu administrador. Estes documentos estão seguros quando os partilha com outras pessoas ou os guarda num suporte de dados amovível.

Opção	Descrição	Para obter mais informações
Documentos do Office e com permissão para macros	Estes incluem .docx, .pptx, .xlsx, .pdf, .docm, .pptm, .xlsm e .pdf.	Consulte Observar as opções do menu Ficheiro para determinar o nível de segurança para documentos do Office. Terá um dos seguintes modos: • Opcional • Proteção forçada
Proteção básica de ficheiros	Estas são aplicações e tipos de ficheiro adicionais que a sua empresa pretende encriptar e o seu administrador configurou.	Consulte Proteger Aplicações e Tipos de Ficheiro Adicionais com a Proteção Básica de Ficheiros.
Opções adicionais	Estas podem aplicar-se a documentos do Office, ficheiros básicos ou ambos.	Consulte Opções adicionais do Data Guardian.
Partilhar um ficheiro com um utilizador externo	Utilizador que tem um endereço de e-mail externo ao domínio (alguém de uma empresa diferente ou um utilizador interno que pretende aceder a ficheiros protegidos a partir de um endereço de e-mail externo ao domínio).	Consulte Utilizar o Data Guardian como utilizador externo.

Trabalhar online com documentos protegidos

Ao criar documentos protegidos, a melhor prática é trabalhar online, pois são geradas chaves para esses documentos. Se recriar uma imagem do seu computador e tiver criado documentos protegidos offline, certifique-se de que notifica o seu administrador.

Propriedades do ficheiro > Separador do Dell Data Guardian

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

Ícones de sobreposição para Windows

Na versão 2.2 ou posterior do Data Guardian, são apresentados ícones de sobreposição em ficheiros protegidos no Explorador de Ficheiros. Se clicar com o botão direito no ficheiro protegido, é apresentado um separador do Dell Data Guardian com mais informações.

Marca de água oculta

Com base na política definida pelo administrador, os documentos do Office protegidos podem ter uma marca de água oculta que identifica o utilizador. Se imprimir ou partilhar o documento, a marca de água mantém-se.

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

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

Utilizar documentos do Office com o modo protegido do Data Guardian

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

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

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

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

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

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

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

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

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

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

    NOTA:
    Com o modo de proteção forçada, a política também define períodos específicos de varrimento do computador para localizar todos os ficheiros do Office desprotegidos e alterar o respetivo modo para Protegido. Para que o Data Guardian possa varrer todos os ficheiros do Office desprotegidos, tem de ter sessão iniciada e ligação à rede.
  - Pasta **Documentos > Desprotegidos** - Se estiver ativada pela política no modo Proteção forçada (mas não no modo opcional), uma pasta Desprotegida é adicionada à raiz da pasta Documentos. Os documentos do Office nesta pasta estão desencriptados. Se eliminar a pasta, a mesma é recriada.

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

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

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

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

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

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

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

Utilizar o modo opcional para proteger documentos do Office

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

Trabalhar com as opções do menu Ficheiro no modo opcional

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

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

Menu Ficheiro	Modo opcional e documentos do Office protegidos
Abra	Os ficheiros abrem como de costume
Guardar	• Opções: Documento já protegido - É guardado como protegido. Desprotegido – É guardado como desprotegido. Para protegê-lo, clique em **Guardar como protegido**. • Documento só de leitura - Uma caixa de diálogo indica que não é possível guardar um documento desprotegido. A janela *Guardar como* abre-se e terá de guardá-lo com um nome de ficheiro diferente.
Guardar como	Tem as opções padrão (mas não o modo protegido)
Guardar como protegido	A única opção no campo Guardar como tipo é Office protegido
Imprimir	**Ativada** No entanto, para documentos protegidos do Office, se um administrador desativar a impressão através da política, continua a ser possível selecionar a opção Imprimir mas é apresentada uma mensagem de alerta indicando que não é possível imprimir o documento protegido. Se o administrador permitir a impressão, outra política poderá colocar uma marca de água com o nome do utilizador, o nome do domínio e a ID do computador em cada página que imprimir.
Partilhar	**Ativado** para documentos protegidos do Office. **Desativado** para documentos desprotegidos.
Exportar (Office 2013 e versões superiores)	Pode ser ativado ou desativado com base nas políticas definidas pelo seu administrador.
Exportar protegido (Office 2013 e versões superiores)	Se a opção do menu Exportar estiver desativada e a Exportação protegida estiver ativada, o documento exporta com uma marca de água (com o nome do utilizador, o nome do domínio e a ID do computador) em cada página. Se exportar um documento em modo protegido para um utilizador externo, este pode abrir e visualizar o documento, mas não o pode exportar ou imprimir.

Trabalhar online com documentos com permissão para macros protegidos

Num documento com permissão para macros protegido, a macro existe mas está bloqueada. No entanto, atualmente, o Data Guardian apenas consegue controlar um documento com permissão para macros após o documento recentemente protegido (.docm, .pptm, .xlsm)

ser fechado e aberto novamente. Além disso, se guardar um documento protegido com uma macro como desprotegido, é necessário fechar e voltar a abrir o documento, para que a macro seja executada.

Classificação TITUS e modo opcional

Se uma política estiver ativada, o seu administrador configura algumas classificações TITUS para encriptar um documento com essa classificação. Pode clicar com o botão direito do rato num documento do Office e selecionar a respetiva classificação TITUS. Esta constitui outra forma de proteger um documento do Office.

Classificação de dados e modo opcional

Se esta política estiver ativada, o administrador pode definir classificações para conteúdos específicos, tais como números de Segurança Social, números de cartões de crédito ou outras informações sensíveis. O seu administrador irá informar que informações foram classificadas. Quando guarda um documento que contém informações baseadas nestas regras de classificação, o documento é encriptado.

Se utilizar etiquetas num documento do Office para ativar a classificação de dados utilizada nos metadados de etiquetas de ficheiros da política, a etiqueta utilizada no documento do Office é sensível a maiúsculas e minúsculas e tem de corresponder à respetiva utilização pelo administrador na política.

NOTA:

Se esta política estiver ativada, um varrimento causará a encriptação de ficheiros que cumpram as regras de classificação. No entanto, ao criar o ficheiro, pode clicar com o botão direito do rato e selecionar **Proteger ficheiro**.

Consulte também Encriptação de E-mails do Outlook com o Data Guardian.

Solução de problemas para o modo opcional

Se a política do Data Guardian desativar a impressão de documentos do Office protegidos, continua a ser possível selecionar a opção Imprimir em **Ficheiro > Informações** ou quando clica com o botão direito do rato num ficheiro do Office protegido no Explorador do Windows. No entanto, se selecionar Imprimir, ocorre o seguinte:

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

Determinar que documentos no modo opcional estão protegidos

Se tiver o modo opcional e pretender confirmar se um documento está protegido ou não, abra o documento e verifique se é apresentado como protegido na barra de título.

NOTA:

Se tiver o modo de proteção forçada, todos os documentos do Office estão protegidos.

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

Utilizar o modo de proteção forçada para proteger documentos do Office

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

- Trabalhar com as opções do menu Ficheiro no modo de proteção forçada

Trabalhar com as opções do menu Ficheiro no modo de proteção forçada

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

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

Menu Ficheiro	Modo de proteção forçada para protegidos e desprotegidos
Abra	Os documentos sem proteção são abertos no modo só de leitura.
Guardar	· O documento está protegido. · Documento só de leitura - Pode editá-lo, mas não é possível guardar o original. Quando clicar em Guardar, a janela Guardar como protegido abre-se e terá de guardá-lo no modo protegido com um novo nome. · Documentos remotos - se abrir um documento que não esteja protegido numa localização remota, tem de guardá-lo na sua unidade local para poder modificar e guardar esse documento. Não é possível guardar na localização remota. **NOTA:** Clicar em Guardar abre uma janela Guardar como e a única opção no campo Guardar como tipo é Office protegido (Documentos, Apresentação ou Livro).
Guardar como	**Desativado**
Guardar como protegido	A única opção no campo Guardar como tipo é Office protegido
Imprimir	**Ativada** No entanto, para documentos do Office protegidos, se um administrador desativar a impressão através da política, continua a ser possível selecionar a opção Imprimir mas é apresentada uma mensagem de alerta indicando que não é possível imprimir o documento protegido. Se o administrador permitir a impressão, outra política poderá colocar uma marca de água com o nome do utilizador, o nome do domínio e a ID do computador em cada página que imprimir.
Partilhar	**Desativado**
Exportar (Office 2013 e versões superiores)	Pode ser ativado ou desativado com base nas políticas definidas pelo seu administrador.
Exportar protegido (Office 2013 e versões superiores)	Se a opção do menu Exportar estiver desativada e a Exportação protegida estiver ativada, o documento exporta com uma marca de água (com o nome do utilizador, o nome do domínio e a ID do computador) em cada página. **NOTA:** Se exportar um documento em modo protegido para um utilizador externo, este pode abrir e visualizar o documento, mas não o pode exportar ou imprimir.

Trabalhar online com documentos com permissão para macros protegidos

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

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

Opções adicionais do Data Guardian

Opções do menu adicionais para documentos do Office protegidos

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

Clique com o botão direito > Proteger

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

Colar

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

- É possível copiar e colar dados protegidos e desprotegidos no documento protegido original ou num ficheiro .pdf protegido. Contudo, não é possível abrir PDF desprotegidos no Adobe Acrobat Reader DC.
- Não é possível copiar ou colar a partir de um documento protegido para um documento desprotegido. Não é apresentado qualquer conteúdo na Área de transferência e uma mensagem empresarial específica indica que não é possível colar no documento desprotegido ou não gerido.

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

Arrastar e largar no modo protegido

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

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

Ao utilizar o Acrobat Reader DC:

- Pode adicionar anotações a um ficheiro .pdf protegido ou preencher um formulário. Quando guardar o ficheiro, é criado um novo ficheiro .pdf protegido que inclui as alterações. Esta é uma funcionalidade do Acrobat Reader DC.
- Para aumentar a segurança, ao abrir um ficheiro .pdf protegido com o Acrobat Reader DC, o acesso à Internet é bloqueado até que o Acrobat Reader DC seja fechado.
- Para aumentar a segurança, se um .pdf protegido estiver aberto, um utilizador não pode utilizar o programa de e-mail a partir dessa instância.

NOTA:
Não é possível abrir um ficheiro .pdf protegido na rede. Pode utilizar o Word para abrir um ficheiro .pdf protegido na rede.

Imprimir para envelopes e etiquetas

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

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

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

Opções adicionais

Processos bloqueados

Com base nas políticas definidas pelo seu administrador, alguns processos, como a Ferramenta de Recorte, podem estar bloqueados. O seu administrador pode fornecer informações sobre esses processos. Além disso, uma caixa de diálogo informa que o processo está bloqueado.

- **Modo de proteção forçada** - Se o seu administrador definir uma política para bloquear o botão *PrtScr*, isto também poderá bloquear a capacidade para utilizar o ecrã tátil ou de os tablets efetuarem capturas de ecrã.
- O Windows com RS5 tem a aplicação Desenho no ecrã (anteriormente a Ferramenta de Recorte). Com o Data Guardian, o seu administrador pode ativar uma política que bloqueia esta aplicação 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*. A opção *Inserir como texto* cola o conteúdo do documento diretamente no corpo do e-mail e o conteúdo deixa de estar protegido.

Pode anexar um documento do Office protegido, um tipo de ficheiro protegido adicional com base na política ou um ficheiro .xen.

Em computadores Windows com Data Guardian, se anexar um documento protegido, o Data Guardian anexa informações para aceder ao ficheiro encriptado dentro do respetivo e-mail.

- Utilizadores internos – a informação é apresentada com uma ligação para a transferência de um cliente.
- Utilizadores externos – a informação é apresentada com uma ligação para o registo e transferência de um cliente.

> **NOTA:**
> Para que as informações anexadas sejam apresentadas, tem de enviar o e-mail através do Microsoft Office Outlook e não através da versão baseada na Web do Outlook.

Encriptação de e-mails do Outlook com o Data Guardian

Com base na política do Data Guardian v2.0.1 e posteriores, os utilizadores internos dispõem de uma opção *Proteger* no canto superior esquerdo do Outlook para encriptar os e-mails e os anexos. O remetente e o destinatário têm de ter o Data Guardian instalado e ativado.

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

Para utilizar:

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

A melhor prática é ter um e-mail aberto de cada vez. Se tiver mais do que um aberto, certifique-se de que clica no e-mail para o destacar antes de clicar no botão Proteger. Se não colocar o cursor do rato sobre o botão Proteger, este deve permanecer a cinzento.

Os dados em movimento estão seguros. Neste lançamento de pré-visualização, a prevenção de perda de dados (DLP) para dados inativos é parcialmente suportada. Os lançamentos futuros irão continuar a melhorar a segurança.

Para minimizar a DLP quando um e-mail encriptado é aberto, algumas ações são desativadas ou bloqueadas:

- *Passos rápidos* do Outlook
- *Mover*, *Mover para a pasta* e outras ações de Pasta
- Setas *Seguinte* e *Anterior*
- *Encaminhar*
- Algumas opções do botão direito do rato

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

- *Copiar/Colar*
- *Imprimir* e *Exportar* dados
- Algumas opções do botão direito do rato
- Pasta Rascunho e *Guardar automaticamente*

Para destinatários de correio do Outlook

Ao abrir um e-mail do Outlook encriptado, é apresentado um aviso a indicar que o documento está protegido e que o utilizador deve clicar duas vezes para abrir o ficheiro. Não é apresentado qualquer conteúdo do e-mail na pré-visualização, apenas uma página de rosto. A página de rosto apresenta o Nome do Dell Server para on-prem ou uma ID de instalação para o inquilino em questão, se o seu Dell Security Center Alojado tiver vários inquilinos. A página de rosto também inclui ligações para transferir o cliente do Data Guardian.

Classificação de e-mails

Relatório local para documentos do Office protegidos e encriptados com classificação de dados (modo opcional)

Para proteger as informações sensíveis em documentos do Office e PDFs, o seu administrador pode definir uma política para efetuar o varrimento e encriptar os ficheiros com base na classificação de dados. As informações sensíveis podem incluir números da Segurança Social, números de cartões de crédito, endereços dos Estados Unidos, ou dados específicos de empresas. O seu administrador irá informá-lo acerca das informações sensíveis que levam à encriptação dos ficheiros.

Para ver um relatório local de ficheiros encriptados devido à classificação de dados e o motivo para essa encriptação:

1 Navegue até **C:\Utilizadores\<NomedeUtilizador>\AppData\Local\Dell\Data Guardian**.
2 Abra o ficheiro **Classification Report.log**.

> **NOTA:**
> Se o ficheiro estiver a ser criado, o registo pode ter várias linhas até que a encriptação esteja concluída.

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

Proteger aplicações e tipos de ficheiro adicionais com a Proteção básica de ficheiros

O seu administrador informá-lo-á se as políticas permitem a encriptação de aplicações e tipos de ficheiro adicionais. Se alguém abrir um ficheiro encriptado com a Proteção básica de ficheiros, mas não tiver o Data Guardian instalado, o conteúdo é ilegível.

Descrição geral da Proteção básica de ficheiros

Aplicações

Seguem-se exemplos de aplicações que o seu administrador pode pretender encriptar:

- Bloco de notas
- Wordpad
- Visio
- MS Paint

> **NOTA:**
> Algumas aplicações são apenas parcialmente suportadas com o Data Guardian. O seu administrador informá-lo-á sobre este assunto.

Tipos de ficheiro

Seguem-se exemplos de tipos de ficheiro adicionais que podem ser configurados: .txt, .rtf, .csv, .odt, .vsdx, .png, .jpg, .jpeg, .jpe, .jfif, .gif, .tif, .tiff, .bmp

Windows, Mac e Mobile

Quando a política de Proteção Básica de Ficheiros estiver configurada, o Data Guardian varre os computadores dos utilizadores e encripta todos os ficheiros locais com estas extensões. Os ficheiros encriptados com a Proteção básica de ficheiros apenas podem ser visualizados e editados com a aplicação associada à extensão de ficheiro.

> **NOTA:**
> Os ficheiros de pastas de sistema específicas não são encriptados, tal como a pasta AppData. O mesmo ocorre com as pastas relacionadas com documentos do Office protegidos, tal como a pasta Documentos seguros.

Ícones de sobreposição para Windows

Na versão 2.2 ou posterior do Data Guardian, são apresentados ícones de sobreposição em ficheiros protegidos no Explorador de Ficheiros. Se clicar com o botão direito no ficheiro protegido, é apresentado um separador do Dell Data Guardian com mais informações.

Excluir alguns ficheiros do varrimento no Windows ou Mac (antes de o varrimento ser ativado)

Se a sua empresa decidir encriptar um tipo de ficheiro adicional, como .txt, pode não desejar ou necessitar que todos os ficheiros com essa extensão sejam varridos e encriptados.

Antes de ativar a Proteção Básica de Ficheiros para essa extensão, o seu administrador pode definir outra política que lhe permite adicionar uma pasta ao seu computador local e os ficheiros nessa pasta não são varridos. O seu administrador pode definir uma política, criar um nome de pasta, fornecer o nome da pasta e sugerir onde pode adicionar a pasta em questão. Podem ser ficheiros necessários para o seu sistema ou ficheiros que não necessitam de proteção.

> **IMPORTANTE:**
> Tem de criar a pasta antes de o administrador ativar a política de Proteção Básica de Ficheiros.

1 Utilize o nome e o caminho da pasta fornecidos pelo seu administrador.
   - Para Mac, aceda a **Painel Preferências > Exclusões da Proteção Básica de Ficheiros**. O nome da pasta a criar e o caminho são apresentados aqui.

2 Adicione ficheiros com a extensão especificada, como .txt, que não necessitam de ser encriptados. Opcionalmente, pode adicionar subpastas com nomes criados pelo utilizador.

> **NOTA:**
> Se tiver ficheiros com essa extensão previamente encriptados, colocá-los na pasta em questão não os irá desencriptar. Permanecem encriptados. Se tiver uma pasta **Documentos Desprotegidos**, que o seu administrador pode criar através de outra política, pode colocar tipos de Proteção Básica de Ficheiros nesta pasta para os desencriptar.

3 Depois de ativar a Proteção Básica de Ficheiros, se tiver ficheiros desprotegidos com essa extensão numa rede ou numa unidade externa, pode copiá-los para a pasta excluída. Permanecem não encriptados. Caso contrário, são encriptados.

Se o seu computador tiver mais do que um utilizador, apenas o utilizador com sessão iniciada atualmente pode colocar ficheiros nessa pasta e fazer com que sejam excluídos do varrimento. Todos os ficheiros que outro utilizador colocar na pasta serão varridos e encriptados.

Remoção de uma extensão de ficheiro em Windows ou Mac

O seu administrador pode decidir remover uma extensão de ficheiro. Se assim for, o seu computador é varrido para desencriptar esses tipos de ficheiros.

- O separador *Propriedades > Dell Data Guardian* do ficheiro encriptado deixa de ser apresentado.
- Se tinha ícones de sobreposição de ficheiros, os mesmos deixaram de ser apresentados.
- A desencriptação dos ficheiros pode demorar vários minutos a ser concluída. Se um ficheiro com essa extensão ainda estiver encriptado, poderá ter sido aberto durante o varrimento ou armazenado num servidor de ficheiros ou noutro local.

Contacte o seu administrador para solicitar a recuperação de quaisquer ficheiros com essa extensão que não desencriptem.

Aplicações do Office

Pode utilizar uma aplicação do Office para abrir um ficheiro encriptado com a Proteção básica de ficheiros, mas o conteúdo é só de leitura.

Portal Web

Em Definições > Políticas, se a Proteção básica de ficheiros estiver definida para Verdadeiro, o administrador adicionou tipos de ficheiros não-Office que o Data Guardian irá encriptar quando forem transferidos do portal Web. O administrador tem de lhe indicar os tipos de ficheiros.

> **NOTA:**
> Se carregar um tipo de ficheiro que ainda não é suportado, o conteúdo é ilegível no portal Web.

Pode carregar ficheiros não-Office quer estejam encriptados ou não encriptados. No entanto, quando transferir o ficheiro não-Office, a extensão do mesmo varia.

Ficheiros não-Office (como .txt ou .png)	Descrição da transferência
Encriptados antes de carregar Por exemplo: ficheiros não-Office já encriptados por Windows ou Mac.	Quando transferidos do portal Web, mantêm a extensão de ficheiro, como .txt ou .png.
Ficheiros não encriptados	Quando transferidos do portal Web, a extensão do ficheiro varia, dependendo de o administrador ter adicionado a extensão a uma política. No entanto, estão encriptados. Exemplos para um ficheiro .txt transferido a partir do portal Web: • **filename.txt** – o administrador adicionou o tipo de ficheiro .txt a uma política.

Ficheiros não-Office (como .txt ou .png)	Descrição da transferência
	• **filename.txt.xen** – o tipo de ficheiro .txt não está incluído na política. O ficheiro está encriptado, mas é acrescentada uma extensão .xen.

Se a política *Editar* estiver ativada no portal Web, os utilizadores podem editar os ficheiros não-Office.

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

Adulteração e documentos do Office protegidos

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

Se um utilizador interno adulterar um documento do Office protegido:

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

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

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

Visualizar pastas e ficheiros do cliente de sincronização na nuvem

Se tiver uma pasta do cliente de sincronização no computador e o Data Guardian a encriptar, os ficheiros em questão são encriptados na nuvem.

Se utilizar o portal Web do Data Guardian para encriptar ficheiros, os ficheiros em questão podem ser encriptados como ficheiros .xen. Não é possível abrir ficheiros .xen encriptados no Windows. Pode visualizá-los num dispositivo móvel com o Data Guardian ou o portal Web.

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

Partilhar documentos do Office protegidos com utilizadores externos

Com o Data Guardian, pode partilhar um documento do Office protegido através de e-mail, suporte de dados amovível, uma partilha de rede ou pode carregá-lo para a nuvem e partilhá-lo:

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

Se anexar o documento e clicar em *Enviar*, uma caixa de diálogo de confirmação é apresentada, lembrando-o de que a chave do documento protegido em questão será partilhada com o utilizador externo.

Melhorar a segurança adicionando restrições de data

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

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

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

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

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

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

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

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

Se definir o campo da *Data de início* para uma data ou hora futura e o utilizador externo abrir o ficheiro antes dessa data e hora, é apresentada uma mensagem a explicar que não é possível abrir o ficheiro antes dessa data e hora devido a restrições de acesso.

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

Instalar e utilizar o Data Guardian com Mac

O Data Guardian para Mac tem Ajuda incorporada para ecrãs específicos que fornece informações sobre:

- Interface do Dell Data Guardian onde os utilizadores podem carregar ficheiros para os encriptar
- Encriptação em nuvem
- Utilizadores externos e restrições de acesso
- Adulteração

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

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

Instalar cliente para Mac

Se o seu administrador o adicionou à lista branca da sua empresa, pode registar-se em: https://yoursecurityservername.domain.com:8443/cloudweb/register.

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

Tem de ser um administrador local.

Para instalar o Data Guardian para Mac:

1 Para o cliente Data Guardian, localize o programa de instalação em **Dell-Data-Guardian-Mac-0.x.x.xxxx.dmg.**
2 Utilize o ficheiro **.pkg** em Dell-Data-Guardian-0.x.x.xxxx.dmg para efetuar a instalação ou atualização.
3 Clique duas vezes no pacote **Dell-Data-Guardian-x.x.x**.
4 Clique em **Continuar**.
5 Na janela Introdução, clique em **Continuar**.
6 Na janela Contrato de licença de software, clique em **Continuar**.
7 Clique em **Aceito** para continuar.
8 Na janela Tipo de configuração, selecione uma das seguintes opções:

Dell Security Center Alojado	Dell Management Server No Local
Uma solução Software como serviço (SaaS) alojada destinada à gestão do software Dell Data Security. a Selecione **Dell Security Center Alojado**. b Clique em **Continuar**. c Avance para o passo 9.	Um servidor no local abrangido pela rede da empresa destinado à gestão do software Dell Data Security. a Selecione **Dell Management Server No Local**. b No campo *Nome do Dell Management Server:*, introduza o nome do Dell Server com o qual este computador vai comunicar, como, por exemplo, servidor.domínio.com. Não é necessário incluir web ou http(s). Esta informação é fornecida pelo seu administrador.

Dell Security Center Alojado	Dell Management Server No Local
	c Clique em **Continuar**. d Avance para o passo 9.

9 Na janela Tipo de instalação, efetue um destes passos:
- Clique em **Instalar** e, em seguida, avance para o passo 10.
- Clique em **Alterar local de instalação**.
  1 Na janela Selecionar destino, selecione todos os utilizadores. Atualmente, esta é a única opção.
  2 Clique em **Continuar**.
  3 Clique em **Instalar** e, em seguida, avance para o passo 10.

10 Na caixa de diálogo, introduza o seu nome e a sua palavra-passe e clique em **Instalar software**.

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

12 Quando for solicitado, mantenha o ficheiro .pkg guardado ou mova-o para o *Lixo*.

13 Proceda da seguinte forma:

Dell Security Center Alojado	Dell Management Server No Local
A janela Credenciais abre-se automaticamente após a instalação. Se a sua empresa tiver vários inquilinos, terá de ter uma ID de instalação. 1 Na janela Credenciais, introduza o e-mail da conta de início de sessão e clique em **Continuar**. 2 Proceda da seguinte forma: • Se a sua empresa tiver vários inquilinos, introduza uma ID de instalação, clique em **Continuar** e avance para o passo 3. **NOTA:** Se for apresentado um erro, verifique as suas credenciais. Se notar um endereço de correio eletrónico incorreto ou uma ID de instalação incorreta, clique em **Reiniciar a inicialização** para introduzir as suas credenciais novamente. • Para inquilinos únicos, avance para o passo 3. 3 Na janela Microsoft, introduza a sua palavra-passe e clique em **Iniciar sessão**. 4 Na janela Azure, introduza a sua palavra-passe. 5 Clique em **Início de sessão**. **NOTA:** Se for apresentado um erro, verifique as suas credenciais. Se notar um endereço de correio eletrónico incorreto, clique em **Reiniciar a inicialização** para introduzir as suas credenciais novamente. 6 É apresentada a interface Dell Data Guardian. Consulte a aplicação Dell Data Guardian.	1 Feche a janela .dmg para abrir o Finder. 2 Consulte Ativação do utilizador final.

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

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

Ativação do utilizador final (on-prem)

Ativação do Dell Management Server No Local

Com a opção on-prem, depois de abrir o Dell Data Guardian pela primeira vez, tem de iniciar sessão para o ativar:

1 No Finder, selecione **Aplicações** e faça duplo clique em **Dell Data Guardian**.

2 Quando a janela Credenciais se abrir, introduza o endereço do Dell Server, (por exemplo, company.server.com). Esta informação é fornecida pelo seu administrador. O número de porta predefinido é 8443. Se a sua empresa alterar a porta predefinida para um número de porta personalizado, o seu administrador irá informá-lo.

> **NOTA:**
> Não desmarque a caixa de verificação Erros SSL exceto se tal for instruído pelo administrador.

3 Introduza o seu endereço de e-mail e a palavra-passe.

4 Clique em **Iniciar sessão** para ativar o Data Guardian.

5 Consulte a *aplicação Dell Data Guardian* abaixo.

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

Aplicação Dell Data Guardian

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

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

Se a autenticação para o Data Guardian for revogada ou expirar, o nome do fornecedor de armazenamento em nuvem também se apresenta a cinzento.

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

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

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

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

Dell Security Center Alojado e inquilino suspenso

Com o Dell Security Center Alojado, se um inquilino não efetuar pagamentos durante um determinado período de tempo, esse inquilino pode ser suspenso. Isto aplica-se a Windows, a Mac, a dispositivos móveis e a portais Web.

Os utilizadores internos e externos do Data Guardian podem deparar-se com o seguinte:

- Todas as plataformas – se tentar instalar o Data Guardian, ativar ou iniciar sessão, é apresentada uma caixa de diálogo a indicar que o inquilino está suspenso.
- Mac – se o seu inquilino for suspenso enquanto o Data Guardian estiver aberto, após fechar o Explorer e todos os ficheiros e, em seguida, tentar abrir um ficheiro protegido, é apresentada uma caixa de diálogo a indicar que o inquilino está suspenso.
- Portal Web:
  - Se já tiver sessão iniciada e carregar um ficheiro encriptado, é apresentada a mensagem Falha ao carregar.
  - Se um ficheiro encriptado ou não encriptado tiver sido carregado e, em seguida, o inquilino for suspenso, é apresentada a mensagem Falha ao transferir.
  - Se terminar sessão e tentar iniciar sessão novamente, é apresentada uma caixa de diálogo a indicar que o inquilino está suspenso.

Contacte o seu administrador.

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

Proteger aplicações e tipos de ficheiro adicionais com a Proteção básica de ficheiros

O seu administrador informá-lo-á se as políticas permitem a encriptação de aplicações e tipos de ficheiro adicionais. Se alguém abrir um ficheiro encriptado com a Proteção básica de ficheiros, mas não tiver o Data Guardian instalado, o conteúdo é ilegível.

Descrição geral da Proteção básica de ficheiros

Aplicações

Seguem-se exemplos de aplicações que o seu administrador pode pretender encriptar:

- Bloco de notas
- Wordpad
- Visio
- MS Paint

> **NOTA:**
> Algumas aplicações são apenas parcialmente suportadas com o Data Guardian. O seu administrador informá-lo-á sobre este assunto.

Tipos de ficheiro

Seguem-se exemplos de tipos de ficheiro adicionais que podem ser configurados: .txt, .rtf, .csv, .odt, .vsdx, .png, .jpg, .jpeg, .jpe, .jfif, .gif, .tif, .tiff, .bmp

Windows, Mac e Mobile

Quando a política de Proteção Básica de Ficheiros estiver configurada, o Data Guardian varre os computadores dos utilizadores e encripta todos os ficheiros locais com estas extensões. Os ficheiros encriptados com a Proteção básica de ficheiros apenas podem ser visualizados e editados com a aplicação associada à extensão de ficheiro.

> **NOTA:**
> Os ficheiros de pastas de sistema específicas não são encriptados, tal como a pasta AppData. O mesmo ocorre com as pastas relacionadas com documentos do Office protegidos, tal como a pasta Documentos seguros.

Ícones de sobreposição para Windows

Na versão 2.2 ou posterior do Data Guardian, são apresentados ícones de sobreposição em ficheiros protegidos no Explorador de Ficheiros. Se clicar com o botão direito no ficheiro protegido, é apresentado um separador do Dell Data Guardian com mais informações.

Excluir alguns ficheiros do varrimento no Windows ou Mac (antes de o varrimento ser ativado)

Se a sua empresa decidir encriptar um tipo de ficheiro adicional, como .txt, pode não desejar ou necessitar que todos os ficheiros com essa extensão sejam varridos e encriptados.

Antes de ativar a Proteção Básica de Ficheiros para essa extensão, o seu administrador pode definir outra política que lhe permite adicionar uma pasta ao seu computador local e os ficheiros nessa pasta não são varridos. O seu administrador pode definir uma política, criar um nome de pasta, fornecer o nome da pasta e sugerir onde pode adicionar a pasta em questão. Podem ser ficheiros necessários para o seu sistema ou ficheiros que não necessitam de proteção.

IMPORTANTE:
Tem de criar a pasta antes de o administrador ativar a política de Proteção Básica de Ficheiros.

1 Utilize o nome e o caminho da pasta fornecidos pelo seu administrador.
   - Para Mac, aceda a **Painel Preferências > Exclusões da Proteção Básica de Ficheiros**. O nome da pasta a criar e o caminho são apresentados aqui.

2 Adicione ficheiros com a extensão especificada, como .txt, que não necessitam de ser encriptados. Opcionalmente, pode adicionar subpastas com nomes criados pelo utilizador.

   NOTA:
   Se tiver ficheiros com essa extensão previamente encriptados, colocá-los na pasta em questão não os irá desencriptar. Permanecem encriptados. Se tiver uma pasta **Documentos Desprotegidos**, que o seu administrador pode criar através de outra política, pode colocar tipos de Proteção Básica de Ficheiros nesta pasta para os desencriptar.

3 Depois de ativar a Proteção Básica de Ficheiros, se tiver ficheiros desprotegidos com essa extensão numa rede ou numa unidade externa, pode copiá-los para a pasta excluída. Permanecem não encriptados. Caso contrário, são encriptados.

Se o seu computador tiver mais do que um utilizador, apenas o utilizador com sessão iniciada atualmente pode colocar ficheiros nessa pasta e fazer com que sejam excluídos do varrimento. Todos os ficheiros que outro utilizador colocar na pasta serão varridos e encriptados.

Remoção de uma extensão de ficheiro em Windows ou Mac

O seu administrador pode decidir remover uma extensão de ficheiro. Se assim for, o seu computador é varrido para desencriptar esses tipos de ficheiros.

- O separador *Propriedades > Dell Data Guardian* do ficheiro encriptado deixa de ser apresentado.
- Se tinha ícones de sobreposição de ficheiros, os mesmos deixaram de ser apresentados.
- A desencriptação dos ficheiros pode demorar vários minutos a ser concluída. Se um ficheiro com essa extensão ainda estiver encriptado, poderá ter sido aberto durante o varrimento ou armazenado num servidor de ficheiros ou noutro local.

Contacte o seu administrador para solicitar a recuperação de quaisquer ficheiros com essa extensão que não desencriptem.

Aplicações do Office

Pode utilizar uma aplicação do Office para abrir um ficheiro encriptado com a Proteção básica de ficheiros, mas o conteúdo é só de leitura.

Portal Web

Em Definições > Políticas, se a Proteção básica de ficheiros estiver definida para Verdadeiro, o administrador adicionou tipos de ficheiros não-Office que o Data Guardian irá encriptar quando forem transferidos do portal Web. O administrador tem de lhe indicar os tipos de ficheiros.

NOTA:

Se carregar um tipo de ficheiro que ainda não é suportado, o conteúdo é ilegível no portal Web.

Pode carregar ficheiros não-Office quer estejam encriptados ou não encriptados. No entanto, quando transferir o ficheiro não-Office, a extensão do mesmo varia.

Ficheiros não-Office (como .txt ou .png)	Descrição da transferência
Encriptados antes de carregar Por exemplo: ficheiros não-Office já encriptados por Windows ou Mac.	Quando transferidos do portal Web, mantêm a extensão de ficheiro, como .txt ou .png.
Ficheiros não encriptados	Quando transferidos do portal Web, a extensão do ficheiro varia, dependendo de o administrador ter adicionado a extensão a uma política. No entanto, estão encriptados. Exemplos para um ficheiro .txt transferido a partir do portal Web: • **filename.txt** – o administrador adicionou o tipo de ficheiro .txt a uma política. • **filename.txt.xen** – o tipo de ficheiro .txt não está incluído na política. O ficheiro está encriptado, mas é acrescentada uma extensão .xen.

Se a política *Editar* estiver ativada no portal Web, os utilizadores podem editar os ficheiros não-Office.

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

Instalar e utilizar o Data Guardian Mobile com iOS ou Android

Esta secção descreve informações básicas acerca da utilização do Data Guardian Mobile com dispositivos iOS ou Android. Quando o seu administrador define uma política para ativar o Data Guardian, os ficheiros são encriptados e protegidos. A aplicação do Data Guardian tem de estar instalada no dispositivo móvel para poder visualizar ou trabalhar em ficheiros encriptados.

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

Pré-requisito

Antes de utilizar a aplicação do Data Guardian, determine quais dos seguintes necessita, com base no seu ambiente:

Dell Security Center Alojado	Dell Management Server No Local
Se o seu ambiente alojado tiver vários inquilinos, terá de ter uma ID de instalação.	Certifique-se de que sabe o nome do Dell Server, por exemplo, server.domain.com. Esta informação é fornecida pelo seu administrador.

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

Introdução ao Data Guardian Mobile

Siga esta sequência ao utilizar o Data Guardian Mobile.

Tarefa	Descrição	Consultar esta seção
Instalar o Data Guardian – Defina uma opção:	Administrador já instalado O utilizador deve instalar	Instalado pelo administrador: toque na aplicação do Data Guardian e inicie a sessão. Instalações pelo utilizador: consulte um dos seguintes: • Instalação num dispositivo iOS • Instalação num dispositivo Android
Determinar as políticas que se aplicam a dispositivos móveis	O seu administrador informa-o em relação às políticas que se aplicam.	Pode ter: • Documentos protegidos do Office • Proteção da nuvem • Opções adicionais

Tarefa	Descrição	Consultar esta seção
Navegar no Gestor de ficheiros	Consulte as opções do Data Guardian.	Navegar no Gestor de ficheiros
Se a política de Proteção da nuvem estiver ativada, aceda à conta do fornecedor de armazenamento na nuvem	No dispositivo, navegue até ao ecrã Gestor de ficheiros do Data Guardian e toque no seu fornecedor de armazenamento na nuvem.	Consulte Aceder à sua conta do fornecedor de armazenamento na nuvem.

Com base nas políticas do Data Guardian, pode:

- Fazer com que os ficheiros do Office protegidos (.docx, .pptx, .xlsx, .pdf) mantenham a respetiva extensão de ficheiro.
- Aplicações e tipos de ficheiro adicionais, como, por exemplo, .txt.
- Os ficheiros não Office na nuvem têm uma extensão .xen.

Em dispositivos móveis com Data Guardian, pode:

- Criar pastas e ficheiros
- Eliminar pastas e ficheiros
- Partilhar um documento com um utilizador externo (se a política estiver ativada para visualização externa)

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

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

Instalação num dispositivo iOS

Pré-requisito: se o seu dispositivo suportar um sensor de impressões digitais Touch ID e pretender utilizá-lo em vez de um PIN, tem de configurar o Touch ID no dispositivo antes de instalar o Data Guardian.

1 No seu dispositivo, toque em **App Store** e procure por **Data Guardian Mobile**.
2 Selecione e instale a aplicação do **Data Guardian**.
3 Toque na caixa de verificação para aceitar o acordo de licença.
4 Selecione uma das seguintes opções:

Dell Security Center Alojado	No Local
Uma solução Software como serviço (SaaS) alojada destinada à gestão do software Dell Data Security.	Um servidor no local abrangido pela rede da empresa destinado à gestão do software Dell Data Security.
a Toque em **Dell Security Center Alojado**. b Introduza o seu e-mail. c Toque em **Enviar**. **NOTA:** Se o seu endereço de e-mail for encontrado em mais do que um inquilino, introduza a sua ID de instalação. d Na janela Microsoft Azure, introduza a palavra-passe.	a Toque em **On-prem**. b No campo Servidor, no ecrã de início de sessão, introduza o nome do Dell Server da sua empresa, apresentado no formato servidor.domínio.com. c Introduza o seu nome de utilizador e a palavra-passe. d Toque em **Iniciar sessão**.

Dell Security Center Alojado	No Local

e Toque em **Iniciar sessão**.

5 Quando solicitado, toque no sensor de impressões digitais ou crie um PIN.

A sua conta está agora ativada e o ecrã Gestor de ficheiros do Data Guardian é apresentado.

Desinstalar a aplicação do Data Guardian

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

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

Instalar ou desinstalar o Data Guardian num dispositivo iOS com Workspace ONE

Se tiver o Workspace ONE instalado, é possível autenticar-se no Data Guardian com início de sessão único. Estes passos são semelhantes para o Dell Security Center Alojado ou o Dell Management Server No Local.

O seu administrador irá enviar a aplicação do Data Guardian para o seu dispositivo.

1 Quando solicitado sobre se pretende instalar a aplicação do **Data Guardian**, toque em **OK**.
2 Inicie a aplicação 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 utilizar o início de sessão único.
5 Introduza a sua palavra-passe.
6 Quando solicitado, crie um PIN.

> **NOTA:**
> Se iniciar sessão no Workspace ONE, só terá de introduzir o seu PIN para o Data Guardian.

A sua conta está agora ativada e o ecrã Gestor de ficheiros do Data Guardian é apresentado.

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

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

Instalação num dispositivo Android

1 No seu dispositivo, aceda ao **Google Play** e procure por **Data Guardian Mobile**.
2 Selecione e instale a aplicação do **Data Guardian**.
3 Toque na caixa de verificação para aceitar o acordo de licença.
4 Selecione uma das seguintes opções:

Dell Security Center Alojado	Dell Management Server No Local
Uma solução Software como serviço (SaaS) alojada destinada à gestão do software Dell Data Security. a Toque em **Alojado**. b Introduza o seu e-mail. c Toque em **Enviar**. **NOTA:** Se o seu endereço de e-mail for encontrado em mais do que um inquilino, introduza a sua ID de instalação. d Na janela Microsoft Azure, introduza a palavra-passe. e Toque em **Iniciar sessão**.	Um servidor no local abrangido pela rede da empresa destinado à gestão do software Dell Data Security. a Toque em **On-prem**. b No campo Servidor, no ecrã de início de sessão, introduza o nome do Dell Server da sua empresa, apresentado no formato servidor.domínio.com. c Introduza o seu nome de utilizador e a palavra-passe. d Toque em **Iniciar sessão**.

5 Quando solicitado, crie um PIN.

A sua conta está agora ativada e o ecrã Gestor de ficheiros do Data Guardian é apresentado.

Desinstalar a aplicação do Data Guardian

1 No esquema das Aplicações Android, toque em **Definições**.
2 Em **Definições**, toque em **Aplicações**.
3 Mantenha o ícone do **Data Guardian** premido.
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 num dispositivo Android com Workspace ONE

Se tiver o Workspace ONE instalado, é possível autenticar-se no Data Guardian com início de sessão único. Estes passos são semelhantes para o Dell Security Center Alojado ou o Dell Management Server No Local.

1 No seu dispositivo, toque em **Hub**.
2 Toque em **Catálogo de Aplicações**.
3 Na aplicação Dell Data Guardian, toque em **Instalar**.
4 Em *Confirmar instalação*, toque em **Instalar**.
5 Em *Google Play Protect*, toque em **Permitir**.
6 Na mensagem de aplicação instalada, toque em **Concluído**.
7 Toque em **Abrir** para iniciar a aplicação do Data Guardian.
8 Na opção de autenticação com o Workspace ONE ou o Data Guardian, toque em **Workspace ONE** para utilizar o início de sessão único.
9 No contrato de licença, toque na caixa de verificação.
10 Toque em **Início de sessão único**.
11 Quando solicitado, crie um PIN.

NOTA: Se iniciar sessão no Workspace ONE, só terá de introduzir o seu PIN para o Data Guardian.

A sua conta está agora ativada e o ecrã Gestor de ficheiros do Data Guardian é apresentado.

Desinstalar a aplicação do Data Guardian

1 No esquema das Aplicações Android, toque em **Definições**.
2 Em **Definições**, toque em **Aplicações**.
3 Mantenha o ícone do **Data Guardian** premido.
4 Arraste o ícone para a opção Desinstalar.
5 Toque em **OK**.

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

Navegar no Gestor de ficheiros

No Gestor de ficheiros do Data Guardian, pode utilizar armazenamento local ou em nuvem. O Gestor de ficheiros abre-se ao abrir o Data Guardian.

Ecrã do Gestor de ficheiros

As pastas predefinidas do ecrã do Gestor de ficheiros incluem:

- Documents
- Transferências
- Fotografias

Ecrã Criar novo

Toque no ícone Adicionar (**+**) e o ecrã *Criar novo* é apresentado com estas opções:

- Documento
- Folha de cálculo
- Apresentação (PowerPoint)
- Fotografia
- Pasta
- Serviço de nuvem

Opções do esquema de navegação

Toque no ícone do esquema de navegação. As opções incluem:

- **Browser**
- **Gestor de ficheiros**
- Ícone **Definições**:
  - Botão **Alterar PIN** (se estiver ativado pela política)
  - **Browser**
  - **Gestor de ficheiros (Definições)** – Utilize estas opções
    - **Intervalo de atualização** - A frequência com que o Data Guardian sincroniza os seus serviços em nuvem. A Dell recomenda *Manual* ou *Diariamente*. Outras opções são *De hora a hora* ou *Semanalmente*.

- **Aviso de transferência de 10 MB** – Ativar ou desativar. Utilize esta opção quando não tem ligação Wi-Fi e o tamanho da transferência é superior a 10 MB.
- **Limpar cache** – Limpa os ficheiros temporários.

– (iOS) - **Touch ID** ou **Face ID**, consoante a versão do iOS e se tem a impressão digital ou o reconhecimento facial pré-configurados. Toque para ativar ou desativar ao utilizar o Data Guardian.
– **Acerca de** – Consulte Políticas e versão do Data Guardian
– Botão **Sair do Data Guardian**
– **Contas de nuvem** – Indica se estão Associadas ou Desassociadas.

- **Browser**
- **Gestor de ficheiros** – Para regressar ao ecrã Gestor de ficheiros.
- **Bloquear o Data Guardian**

Opções adicionais

- Adicionar um ficheiro a Favoritos
  – Para iOS, consulte o esquema de navegação.
  – Para Android, mantenha premido o nome do ficheiro.

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

Determinar políticas para o Data Guardian Mobile

O seu administrador informa-o em relação às políticas que estão definidas para a sua empresa.

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

Visualizar as políticas e a versão do Data Guardian

Algumas políticas do Data Guardian estão listadas em **Acerca de**. Para ver estas políticas ou a versão do Data Guardian:

1 No esquema de navegação do Data Guardian, toque em **Definições > Acerca de**.
2 Toque em **Política**.
Consoante as políticas definidas pelo seu administrador, a lista pode incluir:
- Comprimento do PIN
- Tempo limite por inatividade
- Falha no início de sessão
- Copiar e colar - Permite-lhe copiar de um documento protegido e colar num documento protegido.

Versão
3 Determinar as opções de políticas adicionais.
Estas podem incluir:
- Documentos protegidos do Office
- Proteção da nuvem
- Políticas adicionais

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

Utilizar os documentos do Office protegidos com dispositivos móveis

O seu administrador informa-o em relação às opções que estão ativadas para a sua empresa. Quando tiver o Data Guardian instalado e abrir um documento do Office protegido, uma mensagem indica que o documento está a desencriptar.

Opções do Data Guardian para documentos do Office

Estas opções do Data Guardian são apresentadas.

- **Criar** - Com base na definição da política, o documento é protegido quando o cria. O cabeçalho deste ficheiro apresenta a informação *Documento protegido*.
- **Copiar/colar** - Com um documento do Office protegido, apenas pode copiar para outro documento do Office protegido.
- **Imprimir** - Com base nas definições das políticas adicionais, pode ter uma marca de água ao imprimir.
- **Exportar** – Com base nas definições das políticas adicionais, pode ter uma marca de água ao exportar.

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

- **Guardar**
- **Guardar como**
- **Exportar**
- **Sair**

Opções adicionais do Office com base na política:

- **Editar** - pode editar os ficheiros do Office .docx e .ppt.

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

- **Marca de água oculta** - Com base na política, os documentos do Office protegidos podem ter uma marca de água oculta que identifica o utilizador. Se imprimir ou partilhar o documento, a marca de água mantém-se.
- **Marca de água no ecrã** - Quando abre qualquer documento do Office protegido, é apresentada uma marca de água no ecrã do cliente.

Informações adicionais para documentos do Office

Documentos do Office protegidos quando estiver offline

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

Resolução de problemas de documentos do Office protegidos

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

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

Proteger aplicações e tipos de ficheiro adicionais com a Proteção básica de ficheiros

O seu administrador informá-lo-á se as políticas permitem a encriptação de aplicações e tipos de ficheiro adicionais. Se alguém abrir um ficheiro encriptado com a Proteção básica de ficheiros, mas não tiver o Data Guardian instalado, o conteúdo é ilegível.

Descrição geral da Proteção básica de ficheiros

Aplicações

Seguem-se exemplos de aplicações que o seu administrador pode pretender encriptar:

- Bloco de notas
- Wordpad
- Visio
- MS Paint

> **NOTA:**
> Algumas aplicações são apenas parcialmente suportadas com o Data Guardian. O seu administrador informá-lo-á sobre este assunto.

Tipos de ficheiro

Seguem-se exemplos de tipos de ficheiro adicionais que podem ser configurados: .txt, .rtf, .csv, .odt, .vsdx, .png, .jpg, .jpeg, .jpe, .jfif, .gif, .tif, .tiff, .bmp

Windows, Mac e Mobile

Quando a política de Proteção Básica de Ficheiros estiver configurada, o Data Guardian varre os computadores dos utilizadores e encripta todos os ficheiros locais com estas extensões. Os ficheiros encriptados com a Proteção básica de ficheiros apenas podem ser visualizados e editados com a aplicação associada à extensão de ficheiro.

> **NOTA:**
> Os ficheiros de pastas de sistema específicas não são encriptados, tal como a pasta AppData. O mesmo ocorre com as pastas relacionadas com documentos do Office protegidos, tal como a pasta Documentos seguros.

Ícones de sobreposição para Windows

Na versão 2.2 ou posterior do Data Guardian, são apresentados ícones de sobreposição em ficheiros protegidos no Explorador de Ficheiros. Se clicar com o botão direito no ficheiro protegido, é apresentado um separador do Dell Data Guardian com mais informações.

Excluir alguns ficheiros do varrimento no Windows ou Mac (antes de o varrimento ser ativado)

Se a sua empresa decidir encriptar um tipo de ficheiro adicional, como .txt, pode não desejar ou necessitar que todos os ficheiros com essa extensão sejam varridos e encriptados.

Antes de ativar a Proteção Básica de Ficheiros para essa extensão, o seu administrador pode definir outra política que lhe permite adicionar uma pasta ao seu computador local e os ficheiros nessa pasta não são varridos. O seu administrador pode definir uma política, criar um nome de pasta, fornecer o nome da pasta e sugerir onde pode adicionar a pasta em questão. Podem ser ficheiros necessários para o seu sistema ou ficheiros que não necessitam de proteção.

IMPORTANTE:

Tem de criar a pasta antes de o administrador ativar a política de Proteção Básica de Ficheiros.

1 Utilize o nome e o caminho da pasta fornecidos pelo seu administrador.
   - Para Mac, aceda a **Painel Preferências > Exclusões da Proteção Básica de Ficheiros**. O nome da pasta a criar e o caminho são apresentados aqui.

2 Adicione ficheiros com a extensão especificada, como .txt, que não necessitam de ser encriptados. Opcionalmente, pode adicionar subpastas com nomes criados pelo utilizador.

NOTA:

Se tiver ficheiros com essa extensão previamente encriptados, colocá-los na pasta em questão não os irá desencriptar. Permanecem encriptados. Se tiver uma pasta **Documentos Desprotegidos**, que o seu administrador pode criar através de outra política, pode colocar tipos de Proteção Básica de Ficheiros nesta pasta para os desencriptar.

3 Depois de ativar a Proteção Básica de Ficheiros, se tiver ficheiros desprotegidos com essa extensão numa rede ou numa unidade externa, pode copiá-los para a pasta excluída. Permanecem não encriptados. Caso contrário, são encriptados.

Se o seu computador tiver mais do que um utilizador, apenas o utilizador com sessão iniciada atualmente pode colocar ficheiros nessa pasta e fazer com que sejam excluídos do varrimento. Todos os ficheiros que outro utilizador colocar na pasta serão varridos e encriptados.

Remoção de uma extensão de ficheiro em Windows ou Mac

O seu administrador pode decidir remover uma extensão de ficheiro. Se assim for, o seu computador é varrido para desencriptar esses tipos de ficheiros.

- O separador *Propriedades > Dell Data Guardian* do ficheiro encriptado deixa de ser apresentado.
- Se tinha ícones de sobreposição de ficheiros, os mesmos deixaram de ser apresentados.
- A desencriptação dos ficheiros pode demorar vários minutos a ser concluída. Se um ficheiro com essa extensão ainda estiver encriptado, poderá ter sido aberto durante o varrimento ou armazenado num servidor de ficheiros ou noutro local.

Contacte o seu administrador para solicitar a recuperação de quaisquer ficheiros com essa extensão que não desencriptem.

Aplicações do Office

Pode utilizar uma aplicação do Office para abrir um ficheiro encriptado com a Proteção básica de ficheiros, mas o conteúdo é só de leitura.

Portal Web

Em Definições > Políticas, se a Proteção básica de ficheiros estiver definida para Verdadeiro, o administrador adicionou tipos de ficheiros não-Office que o Data Guardian irá encriptar quando forem transferidos do portal Web. O administrador tem de lhe indicar os tipos de ficheiros.

NOTA:

Se carregar um tipo de ficheiro que ainda não é suportado, o conteúdo é ilegível no portal Web.

Pode carregar ficheiros não-Office quer estejam encriptados ou não encriptados. No entanto, quando transferir o ficheiro não-Office, a extensão do mesmo varia.

Ficheiros não-Office (como .txt ou .png)	Descrição da transferência
Encriptados antes de carregar Por exemplo: ficheiros não-Office já encriptados por Windows ou Mac.	Quando transferidos do portal Web, mantêm a extensão de ficheiro, como .txt ou .png.
Ficheiros não encriptados	Quando transferidos do portal Web, a extensão do ficheiro varia, dependendo de o administrador ter adicionado a extensão a uma política. No entanto, estão encriptados. Exemplos para um ficheiro .txt transferido a partir do portal Web: • **filename.txt** – o administrador adicionou o tipo de ficheiro .txt a uma política. • **filename.txt.xen** – o tipo de ficheiro .txt não está incluído na política. O ficheiro está encriptado, mas é acrescentada uma extensão .xen.

Se a política *Editar* estiver ativada no portal Web, os utilizadores podem editar os ficheiros não-Office.

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

Utilizar a Proteção da nuvem com dispositivos móveis

Se o seu administrador ativar a Proteção da nuvem, precisa de duas aplicações:

- Aplicação do cliente de sincronização na nuvem - Consulte a ajuda online para saber mais sobre o cliente de sincronização na nuvem.
- A aplicação Data Guardian Mobile apresenta o cliente de sincronização na nuvem utilizado na sua empresa e permite-lhe a respetiva transferência.

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

Aceder à sua conta do fornecedor de armazenamento na nuvem

Para aceder à sua conta do fornecedor de armazenamento na nuvem:

1 No ecrã do Gestor de ficheiros, toque no ícone Adicionar (**+**).

2 Toque em **Serviço em nuvem**.

A política do Data Guardian determina que fornecedores de armazenamento em nuvem são apresentados. O seu administrador pode designar um ou mais fornecedores de armazenamento em nuvem específicos para utilizar na empresa e bloquear os restantes.

3 Proceda de acordo com uma das seguintes opções, seguindo as instruções online:

- Crie uma conta com o fornecedor de armazenamento na nuvem.
- Inicie sessão numa conta de fornecedor de armazenamento na nuvem existente.

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

NOTA:

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

Utilizar a Proteção da nuvem

Em dispositivos móveis com Data Guardian, pode:

- Criar pastas
- Carregar e transferir ficheiros

  NOTA:

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

  NOTA:

  Se um utilizador interno partilhar uma pasta consigo através do Data Guardian, deve aceder ao website de armazenamento na nuvem e movê-la para a pasta raiz ou transferir a pasta partilhada, para poder visualizá-la no dispositivo.
- **Ficheiro > Copiar** – Com base na política definida pelo seu administrador, pode copiar um ficheiro de um fornecedor de nuvem para outro.
- Para Android com OneDrive e Dropbox, se não conseguir partilhar um ficheiro a partir de Aplicações e o ficheiro partilhar uma ligação com a aplicação do Data Guardian, partilhe o ficheiro a partir da aplicação de explorador de ficheiros no dispositivo.

Desassociar um fornecedor de armazenamento na nuvem

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

1 Abra o esquema de navegação do Data Guardian e toque em **Definições > Gestor de ficheiros > Serviço em nuvem**. Quando obtiver o acesso a um fornecedor de armazenamento na nuvem, é exibida uma marca de verificação na caixa de diálogo.

2 Proceda da seguinte forma:

Android

a Toque em **Associado**.

b Toque em **Sim**.

iOS

a Toque em **Desassociado**.

Isto remove o acesso e os ficheiros do Data Guardian. No entanto, não remove os ficheiros da nuvem.

Resolução de problemas da Proteção da nuvem

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

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

Utilizar políticas adicionais com dispositivos móveis

O seu administrador informa-o quais destas políticas estão definidas para a sua empresa.

Utilizar um PIN

O seu administrador pode definir uma política que exija um PIN e definir o respetivo comprimento.

Adulteração

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

Proteção adicional através de geofencing

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

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

Considerações de segurança com o Data Guardian e clientes de sincronização

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

Google Drive

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

- Android
- iOS - É exibida uma mensagem.

NOTA:
A *cópia de segurança e a sincronização da Google* não são suportadas.

OneDrive e OneDrive for Business

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

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

Registos históricos

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

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

Dell Security Center Alojado e inquilino suspenso

Com o Dell Security Center Alojado, se um inquilino não efetuar pagamentos durante um determinado período de tempo, esse inquilino pode ser suspenso. Isto aplica-se a Windows, a Mac, a dispositivos móveis e a portais Web.

Os utilizadores internos e externos do Data Guardian podem deparar-se com o seguinte:

- Todas as plataformas – se tentar instalar o Data Guardian, ativar ou iniciar sessão, é apresentada uma caixa de diálogo a indicar que o inquilino está suspenso.
- Mac – se o seu inquilino for suspenso enquanto o Data Guardian estiver aberto, após fechar o Explorer e todos os ficheiros e, em seguida, tentar abrir um ficheiro protegido, é apresentada uma caixa de diálogo a indicar que o inquilino está suspenso.
- Portal Web:
  - Se já tiver sessão iniciada e carregar um ficheiro encriptado, é apresentada a mensagem Falha ao carregar.
  - Se um ficheiro encriptado ou não encriptado tiver sido carregado e, em seguida, o inquilino for suspenso, é apresentada a mensagem Falha ao transferir.
  - Se terminar sessão e tentar iniciar sessão novamente, é apresentada uma caixa de diálogo a indicar que o inquilino está suspenso.

Contacte o seu administrador.

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

Enviar feedback à Dell

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

Para enviar feedback:

1 No esquema de navegação do Data Guardian, toque em **Feedback**.

2 As questões breves permitem-lhe classificar o seu nível de satisfação (10 indica o nível de satisfação mais elevado) e introduzir um comentário.

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

Visualizar ou editar ficheiros protegidos num cliente Web

Se o seu administrador configurar um portal Web do Data Guardian, é possível fazer uma ligação a um URL desse cliente Web e visualizar os ficheiros encriptados sem instalar um cliente Data Guardian. Com base na política, também pode editar um ficheiro.

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

- Documentos do Office protegidos: .docx, .pptx, .xlsx, .docm, .pptm, .xlsm, .pdf.
- Ficheiros .xen - Ficheiros Office ou não Office que o Data Guardian encriptou ao serem carregados para a nuvem.
- Tipos de ficheiros adicionais, tal como ficheiros do Bloco de notas.

Com base na política definida pelo seu administrador, pode aceder a um fornecedor de armazenamento na nuvem.

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

Aceder ao portal Web para Data Guardian

Os passos variam ligeiramente dependendo do navegador que utilizar.

1 Obtenha o URL para aceder ao portal Web junto do seu administrador.
2 Clique no URL.
Se receber um aviso, clique em **Continuar** ou **Prosseguir**.
3 No ecrã Contrato de licença, clique em **Aceito**.
Se receber um aviso, clique em **Continuar** ou **Prosseguir**.
4 Introduza as credenciais do seu domínio.
5 Clique em **Início de sessão**.
6 Se for solicitado para monitorizar a sua localização, selecione uma opção.
7 Para visualizar ou editar ficheiros, consulte a Ajuda online disponível a partir do portal Web do Data Guardian.

> **NOTA:**
> Para Mac, tem de configurar o Safari para permitir janelas de pop-up.

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

Proteger aplicações e tipos de ficheiro adicionais com a Proteção básica de ficheiros

O seu administrador informá-lo-á se as políticas permitem a encriptação de aplicações e tipos de ficheiro adicionais. Se alguém abrir um ficheiro encriptado com a Proteção básica de ficheiros, mas não tiver o Data Guardian instalado, o conteúdo é ilegível.

Descrição geral da Proteção básica de ficheiros

Aplicações

Seguem-se exemplos de aplicações que o seu administrador pode pretender encriptar:

- Bloco de notas
- Wordpad
- Visio
- MS Paint

> **NOTA:**
> Algumas aplicações são apenas parcialmente suportadas com o Data Guardian. O seu administrador informá-lo-á sobre este assunto.

Tipos de ficheiro

Seguem-se exemplos de tipos de ficheiro adicionais que podem ser configurados: .txt, .rtf, .csv, .odt, .vsdx, .png, .jpg, .jpeg, .jpe, .jfif, .gif, .tif, .tiff, .bmp

Windows, Mac e Mobile

Quando a política de Proteção Básica de Ficheiros estiver configurada, o Data Guardian varre os computadores dos utilizadores e encripta todos os ficheiros locais com estas extensões. Os ficheiros encriptados com a Proteção básica de ficheiros apenas podem ser visualizados e editados com a aplicação associada à extensão de ficheiro.

> **NOTA:**
> Os ficheiros de pastas de sistema específicas não são encriptados, tal como a pasta AppData. O mesmo ocorre com as pastas relacionadas com documentos do Office protegidos, tal como a pasta Documentos seguros.

Ícones de sobreposição para Windows

Na versão 2.2 ou posterior do Data Guardian, são apresentados ícones de sobreposição em ficheiros protegidos no Explorador de Ficheiros. Se clicar com o botão direito no ficheiro protegido, é apresentado um separador do Dell Data Guardian com mais informações.

Excluir alguns ficheiros do varrimento no Windows ou Mac (antes de o varrimento ser ativado)

Se a sua empresa decidir encriptar um tipo de ficheiro adicional, como .txt, pode não desejar ou necessitar que todos os ficheiros com essa extensão sejam varridos e encriptados.

Antes de ativar a Proteção Básica de Ficheiros para essa extensão, o seu administrador pode definir outra política que lhe permite adicionar uma pasta ao seu computador local e os ficheiros nessa pasta não são varridos. O seu administrador pode definir uma política, criar um

nome de pasta, fornecer o nome da pasta e sugerir onde pode adicionar a pasta em questão. Podem ser ficheiros necessários para o seu sistema ou ficheiros que não necessitam de proteção.

IMPORTANTE:

Tem de criar a pasta antes de o administrador ativar a política de Proteção Básica de Ficheiros.

1 Utilize o nome e o caminho da pasta fornecidos pelo seu administrador.
   - Para Mac, aceda a **Painel Preferências > Exclusões da Proteção Básica de Ficheiros**. O nome da pasta a criar e o caminho são apresentados aqui.

2 Adicione ficheiros com a extensão especificada, como .txt, que não necessitam de ser encriptados. Opcionalmente, pode adicionar subpastas com nomes criados pelo utilizador.

   NOTA:

   Se tiver ficheiros com essa extensão previamente encriptados, colocá-los na pasta em questão não os irá desencriptar. Permanecem encriptados. Se tiver uma pasta **Documentos Desprotegidos**, que o seu administrador pode criar através de outra política, pode colocar tipos de Proteção Básica de Ficheiros nesta pasta para os desencriptar.

3 Depois de ativar a Proteção Básica de Ficheiros, se tiver ficheiros desprotegidos com essa extensão numa rede ou numa unidade externa, pode copiá-los para a pasta excluída. Permanecem não encriptados. Caso contrário, são encriptados.

Se o seu computador tiver mais do que um utilizador, apenas o utilizador com sessão iniciada atualmente pode colocar ficheiros nessa pasta e fazer com que sejam excluídos do varrimento. Todos os ficheiros que outro utilizador colocar na pasta serão varridos e encriptados.

Remoção de uma extensão de ficheiro em Windows ou Mac

O seu administrador pode decidir remover uma extensão de ficheiro. Se assim for, o seu computador é varrido para desencriptar esses tipos de ficheiros.

- O separador *Propriedades > Dell Data Guardian* do ficheiro encriptado deixa de ser apresentado.
- Se tinha ícones de sobreposição de ficheiros, os mesmos deixaram de ser apresentados.
- A desencriptação dos ficheiros pode demorar vários minutos a ser concluída. Se um ficheiro com essa extensão ainda estiver encriptado, poderá ter sido aberto durante o varrimento ou armazenado num servidor de ficheiros ou noutro local.

Contacte o seu administrador para solicitar a recuperação de quaisquer ficheiros com essa extensão que não desencriptem.

Aplicações do Office

Pode utilizar uma aplicação do Office para abrir um ficheiro encriptado com a Proteção básica de ficheiros, mas o conteúdo é só de leitura.

Portal Web

Em Definições > Políticas, se a Proteção básica de ficheiros estiver definida para Verdadeiro, o administrador adicionou tipos de ficheiros não-Office que o Data Guardian irá encriptar quando forem transferidos do portal Web. O administrador tem de lhe indicar os tipos de ficheiros.

NOTA:

Se carregar um tipo de ficheiro que ainda não é suportado, o conteúdo é ilegível no portal Web.

Pode carregar ficheiros não-Office quer estejam encriptados ou não encriptados. No entanto, quando transferir o ficheiro não-Office, a extensão do mesmo varia.

Ficheiros não-Office (como .txt ou .png)	Descrição da transferência
Encriptados antes de carregar	Quando transferidos do portal Web, mantêm a extensão de ficheiro, como .txt ou .png.

Ficheiros não-Office (como .txt ou .png)	Descrição da transferência
Por exemplo: ficheiros não-Office já encriptados por Windows ou Mac.	
Ficheiros não encriptados	Quando transferidos do portal Web, a extensão do ficheiro varia, dependendo de o administrador ter adicionado a extensão a uma política. No entanto, estão encriptados. Exemplos para um ficheiro .txt transferido a partir do portal Web: • **filename.txt** – o administrador adicionou o tipo de ficheiro .txt a uma política. • **filename.txt.xen** – o tipo de ficheiro .txt não está incluído na política. O ficheiro está encriptado, mas é acrescentada uma extensão .xen.

Se a política *Editar* estiver ativada no portal Web, os utilizadores podem editar os ficheiros não-Office.

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

Utilizar um fornecedor de armazenamento na nuvem

Com base na política, o portal Web pode aceder a um fornecedor de armazenamento na nuvem. Para obter mais informações, consulte a ajuda online do portal Web.

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

Dell Security Center Alojado e inquilino suspenso

Com o Dell Security Center Alojado, se um inquilino não efetuar pagamentos durante um determinado período de tempo, esse inquilino pode ser suspenso. Isto aplica-se a Windows, a Mac, a dispositivos móveis e a portais Web.

Os utilizadores internos e externos do Data Guardian podem deparar-se com o seguinte:

- Todas as plataformas – se tentar instalar o Data Guardian, ativar ou iniciar sessão, é apresentada uma caixa de diálogo a indicar que o inquilino está suspenso.
- Mac – se o seu inquilino for suspenso enquanto o Data Guardian estiver aberto, após fechar o Explorer e todos os ficheiros e, em seguida, tentar abrir um ficheiro protegido, é apresentada uma caixa de diálogo a indicar que o inquilino está suspenso.
- Portal Web:
  - Se já tiver sessão iniciada e carregar um ficheiro encriptado, é apresentada a mensagem Falha ao carregar.
  - Se um ficheiro encriptado ou não encriptado tiver sido carregado e, em seguida, o inquilino for suspenso, é apresentada a mensagem Falha ao transferir.
  - Se terminar sessão e tentar iniciar sessão novamente, é apresentada uma caixa de diálogo a indicar que o inquilino está suspenso.

Contacte o seu administrador.

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

Utilizar o Data Guardian como utilizador externo

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

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

Os utilizadores externos devem cumprir os Requisitos do servidor. Além disso, o domínio ou utilizador não pode constar na lista negra da empresa.

Para um ambiente alojado, os utilizadores externos só podem ativar contra um inquilino.

As opções para os utilizadores externos incluem:

- **Windows** – Transferir e instalar um cliente do Data Guardian. Consultar as Tarefas dos utilizadores internos no Windows e as Tarefas dos utilizadores externos.
- **Mac** – Ver Utilizador externo e Mac.
- **Dispositivos móveis**
- **Portal Web** – Em vez de transferir um cliente do Data Guardian, utilize o portal Web do Data Guardian. Os utilizadores externos podem ver ficheiros .pdf de documento do Office protegido ou ficheiros .xen. Consoante a política, o utilizador externo pode editar o ficheiro. Consulte Utilizador externo e Portal Web.

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

Tarefas de utilizador interno no Windows

Para partilhar ficheiros protegidos com um utilizador externo, pode:

- Utilizar a opção *Acesso a Ficheiro Protegido* com documentos do Office protegidos
- Aprovar ou negar o acesso quando um utilizador externo solicita acesso
- Enviar um documento do Office protegido através de um e-mail do Outlook.

Conceder acesso a um ou mais ficheiros do Office protegidos

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

1 Clique com o botão direito do rato num ficheiro protegido e selecione **Acesso a Ficheiro Protegido**. Pode selecionar um ou vários ficheiros, até um máximo de 50. Abre-se a janela Partilha de acesso ao documento protegido. Os ficheiros podem estar nos seguintes locais:

- Pasta local ou unidade de rede

- Email
- Suporte de dados amovível
- Partilha de rede

2 No campo superior direito *E-mail a partilhar*, introduza o endereço de e-mail do utilizador fora do domínio e clique em **Adicionar**.

3 Repita este passo para adicionar até um máximo de dez endereços de e-mail.

4 Clique em **OK**.

Uma caixa de diálogo indica que a partilha foi concluída com êxito ou que o endereço de e-mail não está autorizado a receber ficheiros protegidos.

5 Como prática recomendada, para utilizadores externos que ainda não estão registados, informe-os de que irão receber um e-mail seu com instruções que lhes permitem registar-se num Dell Server, transferir e ativar o Data Guardian e posteriormente visualizar ficheiros protegidos partilhados.

Aprovar ou negar o acesso quando um utilizador externo solicita acesso

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

1 Se receber um e-mail de um utilizador externo a solicitar o acesso a um documento protegido, pode visualizar o nome do utilizador externo e o ficheiro solicitado.

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

É enviado um e-mail para o utilizador externo. Se aprovar o pedido, a chave para o documento protegido é partilhada.

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

Enviar um ficheiro protegido através de e-mail do Outlook

Quando anexa um ficheiro protegido e clica em *Enviar*, um pedido de confirmação lembra que a chave para o ficheiro protegido será partilhada.

NOTA:

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

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

Tarefas de utilizador externo no Windows

Um utilizador interno pode decidir dar-lhe acesso a ficheiros protegidos. Pode receber o seguinte:

- E-mail com instruções para efetuar o registo
- Ficheiro protegido com uma página de rosto que contém uma ligação para registar um endereço de e-mail válido

NOTA:

A página de rosto apresenta o Nome do Dell Server para on-prem ou uma ID de instalação para o inquilino em questão, se o seu Dell Security Center Alojado tiver vários inquilinos. A página de rosto também inclui ligações para transferir o cliente do Data Guardian.

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

- Registar-se no Data Guardian

- Transferir e instalar o Data Guardian – o utilizador externo tem de ter direitos de administrador no seu computador.

Registar o Data Guardian

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

Para registar o Data Guardian:

1 Proceda da seguinte forma:
   - E-mail – clique em **Aceitar**.
   - Documento protegido que apresenta um aviso na página de rosto – clique na ligação fornecida para registar um endereço de e-mail válido.

2 Siga um conjunto de passos com base no ambiente da sua empresa:

Dell Security Center Alojado

Uma solução Software como serviço (SaaS) alojada destinada à gestão do software Dell Data Security.

a Quando o portal Web do Dell Data Guardian abrir, introduza o seu endereço de e-mail.

b Percorra para baixo e clique em **Aceito**.

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

d Na página de nova conta, introduza um e-mail, um nome próprio, um apelido e uma palavra-passe. A palavra-passe deve ter pelo menos oito carateres e incluir uma letra minúscula, uma letra maiúscula, um caráter especial e um número.

e Clique em **Inscrever-se**.

f Navegue para o endereço de e-mail que utilizou para o registo, obtenha o código de verificação e introduza-o.

> **NOTA:**
> Se não encontrar um e-mail, verifique a pasta spam.

g Clique em **Confirmar conta**. Se a verificação for bem-sucedida, o portal Web abre-se.

h Arraste o ficheiro protegido para o portal Web e clique em **Carregar agora**.

i Receberá um e-mail de boas-vindas após o registo. Este e-mail contém uma ligação para transferir um cliente Windows.

> **NOTA:**
> Se o seu Dell Security Center Alojado tiver vários inquilinos, o e-mail também apresenta uma ID de instalação de que irá necessitar.

Dell Management Server No Local

Um servidor no local abrangido pela rede da empresa destinado à gestão do software Dell Data Security.

> **NOTA:**
> Para uma instalação on-prem, pode instalar o Data Guardian antes de efetuar o registo. Quando ativar, clique na ligação **Registar**.

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

b Clique em **Registar.**

c Na página Registar, introduza e confirme a sua palavra-passe e, em seguida, clique em **Iniciar sessão**.
É apresentada uma caixa de diálogo de confirmação do registo e é enviado um e-mail para o endereço indicado pelo utilizador interno. Se não encontrar o e-mail, verifique a pasta spam.

d No e-mail de Verificação de conta enviado pelo Dell Server, clique na hiperligação.

> **NOTA:**
> Se não encontrar um e-mail, verifique a pasta spam.

e Continue para a página Web.

f Na página de Confirmação, clique em **Continuar para início de sessão**.

g Na página de Início de sessão, clique em **Esqueci-me da palavra-passe**.

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

h Na página Repor palavra-passe, introduza e confirme a sua palavra-passe e, em seguida, clique em **Registo**.
É apresentada uma caixa de diálogo de confirmação do registo e é enviado um e-mail para o endereço indicado pelo utilizador interno.

i Abra o e-mail de ativação de conta e clique na ligação.
O e-mail também contém o nome do Dell Server a utilizar quando instalar o Data Guardian.

j Na página de início de sessão, introduza o endereço de e-mail e a palavra-passe que utilizou para se registar.

k Clique em **Início de sessão**.

Dell Security Center Alojado	Dell Management Server No Local
	A página Transferência do Data Guardian abre-se.

Transferir e instalar o Data Guardian para Windows

Após efetuar o registo, pode clicar numa ligação para transferir um cliente Windows. Dependendo do que tenha sido fornecido inicialmente pelo utilizador interno, as ligações podem estar disponíveis aqui:

- Com um Security Management Server, abre-se uma página de Transferência com opções para o cliente Windows.
- Com um Security Management Server Virtual, ao clicar em Windows acede ao site dell.com/support.
- Se tiver recebido um ficheiro protegido, a página de rosto contém ligações para transferir um cliente.
- Poderá receber um e-mail de boas-vindas com ligações para transferir um cliente.

Estes passos descrevem a instalação do Data Guardian no Windows.

1 Em Windows, clique em **Transferir (32 bits)** ou **Transferir (64 bits)**, de acordo com o sistema operativo do seu computador.
2 Transfira o ficheiro de configuração para um diretório no seu computador.
3 Clique duas vezes no ficheiro de configuração para iniciar o instalador.
4 Selecione um idioma e clique em **OK**.
5 Se aparecer uma mensagem a questionar se deseja instalar o Pacote redistribuível do Microsoft Visual C++ 2010, clique em **OK**.
6 No ecrã de boas-vindas, clique em **Seguinte**.
7 Leia o contrato de licença, aceite os termos e condições e clique em **Seguinte**.
8 No ecrã Pasta de destino, clique em **Seguinte** para instalar na localização predefinida de **C:\Program Files\Dell\Dell Data Guardian\.**
9 No ecrã Tipo de configuração, selecione um dos seguintes:

Dell Security Center Alojado	Dell Management Server No Local
a Selecione Dell Security Center Alojado. b Se a sua empresa tiver vários inquilinos, introduza a ID de instalação que se encontra na página de rosto ou no e-mail de boas-vindas. c Clique em **Seguinte**. d Avance para o passo 10.	a Selecione Dell Management Server No Local. b No campo *Nome do servidor:*, introduza o nome do Dell Server com o qual este computador vai comunicar. Este nome encontra-se no e-mail de ativação que recebeu, no topo da página de transferência. c Clique em **Seguinte**. d No ecrã Confirmar servidor de ativação, certifique-se de que o endereço URL do Dell Server está correto. O instalador adiciona www ou http(s) e, de seguida, a porta. Clique em **Seguinte**. e Avance para o passo 10.

10 Na janela Tipo de gestão, selecione esta opção:
- Uso externo - um utilizador com um endereço de e-mail fora do domínio da empresa.

11 Clique em **Instalar** para dar início à instalação.
Uma janela de estado apresenta o progresso da instalação.
12 Clique em **Concluir** quando for apresentado o ecrã de Instalação concluída.
13 Clique em **Sim** para reiniciar.
A instalação do Data Guardian está concluída.
14 Consulte Ativar o Data Guardian.

NOTA:
Certifique-se de que consulta as notas e as exceções em Utilizar o Data Guardian com o Windows. Por exemplo, não é possível abrir um ficheiro .pdf protegido a partir da rede. Pode utilizar o Word para abrir um ficheiro .pdf protegido na 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, siga os seguintes passos para ativar:

1 Inicie a sessão no Windows.
Na área de notificação, é apresentado um ícone de nuvem com um ponto de exclamação laranja.

2 Quando for apresentada uma caixa de diálogo na área de notificação, clique em **Clique aqui para ativar**.
Se não for apresentada a caixa de diálogo, clique no ícone do **Data Guardian** na área de notificação e selecione **Ativação do utilizador**.

> **NOTA:**
> Para um ambiente alojado, os utilizadores externos só podem ativar contra um inquilino de cada vez. Se já tiver ativado contra um inquilino, tem de desinstalar o Data Guardian e reinstalá-lo com a outra ID de instalação. Opcionalmente, pode utilizar o portal Web para carregar e ver documentos protegidos.

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

> **NOTA:**
> Para instalação on-prem, se tiver instalado o Data Guardian antes de efetuar o registo, quando ativar, clique na ligação **Registar**.

Depois de concluída a ativação, uma marca de verificação verde é apresentada no ícone da área de notificação do Data Guardian  .

4 Confirme o seu estado de modo de utilizador. Clique no ícone área de notificação e selecione **Detalhes**.
Na parte superior, o Modo de utilizador é:

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

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

Solicitar o acesso a um utilizador interno

Em Windows, em Mac e Mobile, se um utilizador externo tiver instalado e ativado o Data Guardian, esse utilizador pode solicitar acesso a um documento do Office protegido ou a um .pdf a um utilizador interno. O utilizador externo tem de efetuar um pedido separado para cada ficheiro.

1 Se abrir um documento do Office protegido e este indicar que é necessário solicitar o acesso, clique em **Sim** ou **Não**.
Uma caixa de diálogo indica que o pedido foi enviado com êxito. O utilizador interno pode aprovar ou negar o acesso e o utilizador externo recebe um e-mail com o resultado. Se o utilizador externo abrir o ficheiro protegido antes de o utilizador interno aprovar o acesso, é apresentada uma mensagem a indicar que o pedido se encontra pendente.

2 Após 48 horas, o utilizador externo pode solicitar o acesso novamente.
Na área de notificação, o utilizador externo pode clicar com o botão direito no ícone do Data Guardian e selecionar a página **Detalhes**. Clique no separador **Segurança**. Quando o tempo para um pedido regressar a *Nenhum*, o utilizador externo pode solicitar o acesso novamente.

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

Utilizador externo e tarefas Mac

Utilizador interno e tarefas Mac

Proceda da seguinte forma:

- Documentos protegidos – Enviar para o utilizador externo por e-mail, partilha de rede ou armazenamento amovível.
- Se a Encriptação em nuvem do Data Guardian estiver ativada – Na interface do Dell Data Guardian, arraste os ficheiros protegidos para a coluna ao lado da coluna do fornecedor de armazenamento na nuvem.

Utilizador externo e tarefas Mac

Registar o Data Guardian

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

Para registar o Data Guardian:

1 Ao abrir um documento protegido que apresenta um aviso na página de rosto, clique na ligação fornecida para registar um endereço de e-mail válido.

> **NOTA:**
> A página de rosto apresenta o Nome do Dell Server para on-prem ou uma ID de instalação para o inquilino em questão, se o seu Dell Security Center Alojado tiver vários inquilinos. A página de rosto também inclui ligações para transferir o cliente do Data Guardian.

2 Execute uma das seguintes ações, consoante o seu ambiente:

Dell Security Center Alojado

Uma solução Software como serviço (SaaS) alojada destinada à gestão do software Dell Data Security.

a Quando o portal Web do Dell Data Guardian abrir, introduza o seu endereço de e-mail.

b Percorra para baixo e clique em **Aceito**.

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

d Na página de nova conta, introduza um e-mail, um nome próprio, um apelido e uma palavra-passe. A palavra-passe deve ter pelo menos oito carateres e incluir uma letra minúscula, uma letra maiúscula, um caráter especial e um número.

e Clique em **Inscrever-se**.

f Navegue para o endereço de e-mail que utilizou para o registo, obtenha o código de verificação e introduza-o.

> **NOTA:**
> Se não encontrar um e-mail, verifique a pasta spam.

g Clique em **Confirmar conta**. Se a verificação for bem-sucedida, o portal Web abre-se.

Dell Management Server No Local

Um servidor no local abrangido pela rede da empresa destinado à gestão do software Dell Data Security.

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

b Clique em **Registar.**

c Na página Registar, introduza e confirme a sua palavra-passe e, em seguida, clique em **Iniciar sessão**.

É apresentada uma caixa de diálogo de confirmação do registo e é enviado um e-mail para o endereço indicado pelo utilizador interno. Se não encontrar o e-mail, verifique a pasta spam.

d Abra o e-mail de verificação de conta e clique na ligação.

O e-mail também contém o nome do Dell Server a utilizar quando instalar o Data Guardian.

e Na página de Confirmação do registo, clique em **Regressar à página de início de sessão**.

Pode clicar numa ligação na página de rosto para transferir e instalar um cliente. Consulte as instruções abaixo.

Dell Security Center Alojado	Dell Management Server No Local
h Carregue o ficheiro protegido para o ver. Receberá um e-mail com ligações para transferir o cliente Mac. Também pode clicar na ligação na página de rosto. Consulte as instruções abaixo.	

Transferir e instalar um cliente do Data Guardian (opcional)

1 Na página do Dell Data Guardian, introduza o endereço de e-mail e a palavra-passe que utilizou para se registar.
2 Clique em **Início de sessão**.
Abre-se a página Transferência do Data Guardian com opções para Windows, iOS, Android e Mac OS X.
3 Sob Mac OS X, clique em **Transferir**.
4 Na página de *Controladores e transferências*, selecione **Apple Mac OS** e clique em **Transferir**.
5 Transfira o ficheiro .dmg para uma pasta no seu computador e execute o .pkg.
6 Para iniciar sessão/ativar, execute uma das seguintes ações:

Dell Security Center Alojado	Dell Management Server No Local
a Utilize o endereço de e-mail utilizado quando se registou. b As informações de início de sessão são as mesmas que utilizou para aceder ao .dmg. c Clique em **Início de sessão**.	a Consulte a Ajuda online integrada para o Data Guardian e introduza o nome do Dell Server listado no e-mail de verificação de conta. b Além disso, introduza o seu endereço de e-mail e a palavra-passe. A informação de início de sessão é a que utilizou para o registo. c Clique em **Início de sessão**.

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

Utilizador externo e dispositivos móveis

Se um utilizador interno partilhar uma ligação através da nuvem para um ficheiro protegido, o ficheiro apresenta uma página de rosto que contém uma ligação para o registo de um endereço de e-mail válido.

NOTA:
A página de rosto apresenta o Nome do Dell Server para on-prem ou uma ID de instalação para o inquilino em questão, se o seu Dell Security Center Alojado tiver vários inquilinos. A página de rosto também inclui ligações para transferir o cliente do Data Guardian.

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

- Registar-se no Data Guardian
- Transferir e instalar o Data Guardian – o utilizador externo tem de ter direitos de administrador no seu computador.

Registar o Data Guardian

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

Para registar o Data Guardian:

1 No aviso na página de rosto, clique na ligação fornecida para registar um endereço de e-mail válido.
2 Siga um conjunto de passos com base no ambiente da sua empresa:

Dell Security Center Alojado

Uma solução Software como serviço (SaaS) alojada destinada à gestão do software Dell Data Security.

a Quando o portal Web do Dell Data Guardian abrir, introduza o seu endereço de e-mail.

b Percorra para baixo e clique em **Aceito**.

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

d Na página de nova conta, introduza um e-mail, um nome próprio, um apelido e uma palavra-passe. A palavra-passe deve ter pelo menos oito carateres e incluir uma letra minúscula, uma letra maiúscula, um caráter especial e um número.

e Clique em **Inscrever-se**.

f Navegue para o endereço de e-mail que utilizou para o registo, obtenha o código de verificação e introduza-o.

> **NOTA:**
> Se não encontrar um e-mail, verifique a pasta spam.

g Clique em **Confirmar conta**. Se a verificação for bem-sucedida, o portal Web abre-se.

h Arraste o ficheiro protegido para o portal Web e clique em **Carregar agora**.

i Receberá um e-mail de boas-vindas após o registo. Este e-mail contém uma ligação para transferir um cliente Windows.

> **NOTA:**
> Se o seu Dell Security Center Alojado tiver vários inquilinos, o e-mail também apresenta uma ID de instalação de que irá necessitar.

Dell Management Server No Local

Um servidor no local abrangido pela rede da empresa destinado à gestão do software Dell Data Security.

> **NOTA:**
> Para uma instalação on-prem, pode instalar o Data Guardian antes de efetuar o registo. Quando ativar, clique na ligação **Registar**.

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

b Clique em **Registar.**

c Na página Registar, introduza e confirme a sua palavra-passe e, em seguida, clique em **Iniciar sessão**.

É apresentada uma caixa de diálogo de confirmação do registo e é enviado um e-mail para o endereço indicado pelo utilizador interno. Se não encontrar o e-mail, verifique a pasta spam.

d No e-mail de Verificação de conta enviado pelo Dell Server, clique na hiperligação.

> **NOTA:**
> Se não encontrar um e-mail, verifique a pasta spam.

e Continue para a página Web.

f Na página de Confirmação, clique em **Continuar para início de sessão**.

g Na página de Início de sessão, clique em **Esqueci-me da palavra-passe**.

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

h Na página Repor palavra-passe, introduza e confirme a sua palavra-passe e, em seguida, clique em **Registo**.

É apresentada uma caixa de diálogo de confirmação do registo e é enviado um e-mail para o endereço indicado pelo utilizador interno.

i Abra o e-mail de ativação de conta e clique na ligação.

O e-mail também contém o nome do Dell Server a utilizar quando instalar o Data Guardian.

j Na página de início de sessão, introduza o endereço de e-mail e a palavra-passe que utilizou para se registar.

k Clique em **Início de sessão**.

A página Transferência do Data Guardian abre-se.

Transferir e instalar o Data Guardian for Mobile

Proceda da seguinte forma:

- Instalar ou desinstalar o Data Guardian num dispositivo Android
- Instalar ou desinstalar o Data Guardian num dispositivo iOS

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

Utilizador externo e Portal Web

Tarefas dos utilizadores internos

Um utilizador interno pode fazer as seguintes ações:

- Enviar o URL da empresa ao utilizador externo para que este possa aceder ao portal Web do Data Guardian.
- Enviar um ficheiro protegido para o utilizador externo. Quando o utilizador abrir o ficheiro, é apresentada uma página de rosto.

O utilizador externo apenas consegue ver ficheiros .pdf de documento do Office protegido ou ficheiros .xen. Poderá conseguir editar ficheiros, consoante a política definida. No entanto, o utilizador externo não tem de transferir o cliente do Data Guardian.

Tarefas do utilizador externo no Portal Web

Para se registar no Portal Web do Data Guardian:

1 Clique no URL do portal Web, recebido de um utilizador interno ou na página de rosto de um ficheiro protegido.

2 No ecrã Contrato de licença, percorra para baixo e clique em **Aceito**.

3 Utilize um dos seguintes procedimentos consoante a natureza da sua empresa, isto é, se está alojada ou se tem instalação On-prem.

Dell Security Center Alojado	**Dell Management Server No Local**
Uma solução Software como serviço (SaaS) alojada destinada à gestão do software Dell Data Security.	Um servidor no local abrangido pela rede da empresa destinado à gestão do software Dell Data Security.
a Introduza um e-mail e uma palavra-passe. b Clique em **Iniciar sessão**. c Introduza um e-mail, um nome próprio, um apelido e uma palavra-passe. A palavra-passe deve ter pelo menos oito carateres e incluir uma letra minúscula, uma letra maiúscula, um caráter especial e um número. d Clique em **Inscrever-se**. e Navegue para o endereço de e-mail que utilizou para o registo, obtenha o código de verificação e introduza-o. f Introduza o código de verificação e clique em **Confirmar conta**. Abre-se o portal Web.	a b Clique em **Ainda não tem uma conta?** c Introduza um endereço de e-mail e clique em **Registar**. **NOTA:** Para os utilizadores internos que pretendam registar-se como externos, este é um endereço de e-mail externo ao domínio. d Na página de Registo, introduza e confirme uma palavra-passe e, em seguida, clique em **Registar**. A página de confirmação indica que foi enviado um e-mail de confirmação 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 na ligação. f No ecrã de Confirmação do registo, clique em **Regressar à página de início de sessão**. g Introduza o endereço de e-mail e a palavra-passe que utilizou para se registar.
Se um utilizador interno não partilhar a chave, pode aceder ao portal web, mas não pode abrir o ficheiro.	

4 É apresentada a página de carregamento do Dell Data Guardian.

5 Clique em **Procurar** para navegar até ao ficheiro e carregá-lo, ou arraste e largue o ficheiro para o portal Web.

6 Clique em **?** para consultar a Ajuda online de cada página.

Para editar ficheiros, um administrador tem de modificar a política para esse utilizador. Se for concedido após o registo, tem de terminar sessão no portal Web e voltar a iniciar sessão.

Opcionalmente, pode transferir um cliente do Data Guardian. A página de rosto também inclui ligações para transferir o cliente do Data Guardian. A página de rosto também apresenta o Nome do Dell Server para on-prem ou uma ID de instalação para o inquilino em questão, se o seu Dell Security Center Alojado tiver vários inquilinos.

Solicitar acesso a um utilizador interno

Se carregar um documento do Office protegido ou um .pdf e for apresentada a caixa de diálogo *Falha ao carregar* indicando que não tem acesso, pode solicitar o acesso ao autor do ficheiro:

1 Na caixa de diálogo *Falha ao carregar*, clique em **Sim**.
2 Aguarde a receção de um e-mail do utilizador interno a indicar se o acesso foi concedido ou negado.

NOTA:
Se não receber um e-mail do utilizador interno, tem de aguardar 48 horas antes de solicitar acesso novamente. Se abrir o ficheiro protegido antes de o utilizador interno aprovar o acesso, é apresentada uma mensagem a indicar que o pedido se encontra pendente.

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

Visualizar um documento do Office protegido

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

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

- Imprimir
- Exportar
- Guardar como
- Partilhar

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

Dell Security Center Alojado e inquilino suspenso

Com o Dell Security Center Alojado, se um inquilino não efetuar pagamentos durante um determinado período de tempo, esse inquilino pode ser suspenso. Isto aplica-se a Windows, a Mac, a dispositivos móveis e a portais Web.

Os utilizadores internos e externos do Data Guardian podem deparar-se com o seguinte:

- Todas as plataformas – se tentar instalar o Data Guardian, ativar ou iniciar sessão, é apresentada uma caixa de diálogo a indicar que o inquilino está suspenso.
- Mac – se o seu inquilino for suspenso enquanto o Data Guardian estiver aberto, após fechar o Explorer e todos os ficheiros e, em seguida, tentar abrir um ficheiro protegido, é apresentada uma caixa de diálogo a indicar que o inquilino está suspenso.
- Portal Web:
  - Se já tiver sessão iniciada e carregar um ficheiro encriptado, é apresentada a mensagem Falha ao carregar.

- Se um ficheiro encriptado ou não encriptado tiver sido carregado e, em seguida, o inquilino for suspenso, é apresentada a mensagem Falha ao transferir.
- Se terminar sessão e tentar iniciar sessão novamente, é apresentada uma caixa de diálogo a indicar que o inquilino está suspenso.

Contacte o seu administrador.

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

Aumente a Segurança com os Grupos de acesso do Data Guardian (No Local)

Os Grupos de acesso do Data Guardian aumentam a segurança ao criar grupos de utilizadores que podem colaborar em dados encriptados. Os utilizadores fora de um grupo não podem aceder nem ver os dados exceto se o proprietário do ficheiro conceder acesso aos mesmos. Os Grupos de acesso podem incluir utilizadores internos e externos. Pode utilizar Grupos de acesso com Windows, Mac, dispositivos móveis e portais Web.

Selecione uma das seguintes opções de acordo com a sua empresa:

- A Empresa Tem o Data Guardian Instalado com o Modo Opcional
- A Empresa Tem o Data Guardian Instalado com o Modo Proteção Forçada
- A Empresa Ainda Não Tem o Data Guardian e o Modo Opcional
- A Empresa Ainda Não Tem o Data Guardian e o Modo Proteção Forçada

Também pode fazer o seguinte:

- Alterar o Proprietário de um Ficheiro Encriptado
- Revogar o Acesso a uma Chave

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

A Empresa Tem o Data Guardian Instalado com o Modo Opcional

Se a sua empresa utilizar grupos de acesso para aumentar a segurança dos dados confidenciais, terá de saber quem está no seu grupo de acesso. Inicialmente, para garantir uma transição sem problemas, a sua empresa poderá fornecer um breve período para processar quaisquer ficheiros partilhados e encriptados existentes. Após a conclusão do período de transição, os utilizadores no seu grupo de acesso podem visualizar quaisquer ficheiros partilhados e encriptados que crie. Pode conceder acesso a pessoas fora do seu grupo de acesso.

Identificar os utilizadores no seu grupo de acesso

O administrador informa-o de quem está em um ou mais dos seus grupos de acesso, dependendo de quem precisa de acesso a ficheiros específicos. Tal pode incluir utilizadores internos e externos. Se trabalha com dados confidenciais com utilizadores específicos, pode solicitar ao administrador que crie um grupo de acesso para esse conteúdo.

Utilizar um período de transição para processar ficheiros partilhados e encriptados

Caso já tenha o Data Guardian instalado e os ficheiros existentes estiverem encriptados, o ideal para a sua empresa é ter um breve período de transição para os ficheiros encriptados que são partilhados. Para facilitar uma transição sem problemas, tenha em atenção o seguinte para ficheiros encriptados partilhados:

- O proprietário ou o autor do ficheiro, quer seja interno ou externo, continua a ter acesso ao ficheiro.
- Os utilizadores internos ou externos dentro do seu grupo de acesso têm acesso à maior parte dos ficheiros partilhados. Com base no tipo de chave associada a determinados ficheiros, pode perder o acesso a alguns destes.
- Utilizadores internos fora do seu grupo de acesso - Os utilizadores devem abrir quaisquer ficheiros partilhados durante o período de transição para obterem acesso à chave. Se não abrirem um ficheiro partilhado e encriptado durante este breve período, perderão o acesso ao ficheiro.
- Utilizadores externos que não estão no seu grupo de acesso - Se já concedeu acesso a um ficheiro encriptado, o utilizador externo continuará a ter acesso durante e após o período de transição.

Se perder o acesso a um ficheiro após o período de transição, pode solicitar o acesso ao proprietário.

Recuperar o acesso a ficheiros encriptados partilhados após o período de transição

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

- Documentos do Office protegidos - É apresentada uma caixa de diálogo aos utilizadores internos e externos que lhes pede para solicitar o acesso e o proprietário do ficheiro pode decidir se concede o acesso.
- Tipos de ficheiro adicionais encriptados através da Proteção Básica de Ficheiros - Não existe qualquer pedido de pós-partilha. O utilizador tem de conhecer o proprietário do ficheiro e clicar com o botão direito do rato no ficheiro encriptado para encontrar a ID da Chave no separador Data Guardian. O utilizador pode enviar essas informações ao proprietário e solicitar o acesso.

Colaborar em novos ficheiros encriptados após o período de transição

Para ficheiros novos que crie ou encripte após o período de transição:

- Utilizadores internos ou externos dentro do seu grupo de acesso - Têm acesso a todos os ficheiros partilhados e encriptados.
  - Qualquer pessoa que for removida do grupo de acesso perde o acesso.
  - Se o proprietário de um ficheiro for removido do grupo, os outros utilizadores mantêm o acesso.
- Utilizadores internos ou externos fora do seu grupo de acesso - Não podem visualizar um ficheiro encriptado.
  - Um utilizador interno dentro do grupo de acesso pode conceder acesso.
  - Se um utilizador externo for o proprietário de um ficheiro encriptado, pode conceder acesso a outra pessoa.
  - Se um utilizador interno ou externo fora do grupo receber um documento Office protegido e tentar abri-lo, é-lhe apresentada uma caixa de diálogo a pedir que solicite o acesso.
  - Se um utilizador interno ou externo fora do grupo receber e tentar abrir um tipo de ficheiro a partir da Proteção Básica de Ficheiros, o utilizador pode clicar com o botão direito do rato no ficheiro encriptado para encontrar a ID da Chave no separador 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 Proteção Forçada

Se a sua empresa utilizar grupos de acesso para aumentar a segurança dos dados confidenciais, terá de saber quem está no seu grupo de acesso. Inicialmente, para garantir uma transição sem problemas, a sua empresa poderá fornecer um breve período para processar quaisquer ficheiros partilhados e encriptados existentes. Após a conclusão do período de transição, os utilizadores no seu grupo de acesso podem visualizar quaisquer ficheiros partilhados e encriptados que crie. Pode conceder acesso a pessoas fora do seu grupo de acesso.

Identificar os utilizadores no seu grupo de acesso

O administrador informa-o de quem está em um ou mais dos seus grupos de acesso, dependendo de quem precisa de acesso a ficheiros específicos. Tal pode incluir utilizadores internos e externos. Se trabalha com dados confidenciais com utilizadores específicos, pode solicitar ao administrador que crie um grupo de acesso para esse conteúdo.

Utilizar um período de transição para processar ficheiros partilhados e encriptados

Caso já tenha o Data Guardian instalado e os ficheiros existentes estiverem encriptados, o ideal para a sua empresa é ter um breve período de transição para os ficheiros encriptados que são partilhados. Para facilitar uma transição sem problemas, tenha em atenção o seguinte para ficheiros encriptados partilhados:

- O proprietário ou o autor do ficheiro, quer seja interno ou externo, continua a ter acesso ao ficheiro.
- Os utilizadores internos ou externos dentro do seu grupo de acesso têm acesso à maior parte dos ficheiros partilhados. Com base no tipo de chave associada a determinados ficheiros, pode perder o acesso a alguns destes.
- Utilizadores internos fora do seu grupo de acesso - Os utilizadores devem abrir quaisquer ficheiros partilhados durante o período de transição para obterem acesso à chave. Se não abrirem um ficheiro partilhado e encriptado durante este breve período, perderão o acesso ao ficheiro.
- Utilizadores externos que não estão no seu grupo de acesso - Se já concedeu acesso a um ficheiro encriptado, o utilizador externo continuará a ter acesso após o período de transição.

Se perder o acesso a um ficheiro após o período de transição, pode solicitar o acesso ao proprietário.

Recuperar o acesso a ficheiros encriptados partilhados após o período de transição

Para Windows e Mac no modo Proteção Forçada, pode fazer o seguinte para recuperar o acesso:

- Documentos do Office protegidos - É apresentada uma caixa de diálogo aos utilizadores internos e externos que lhes pede para solicitar o acesso e o proprietário do ficheiro pode decidir se concede o acesso.
- Tipos de ficheiro adicionais encriptados através da Proteção Básica de Ficheiros - Não existe qualquer pedido de pós-partilha. O utilizador tem de conhecer o proprietário do ficheiro e clicar com o botão direito do rato no ficheiro encriptado para encontrar a ID da Chave no separador Data Guardian. O utilizador pode enviar essas informações ao proprietário e solicitar o acesso.

Colaborar em ficheiros recentemente criados após o período de transição

Para ficheiros novos que crie ou encripte após o período de transição:

- Utilizadores internos ou externos dentro do seu grupo de acesso - Têm acesso a todos os ficheiros partilhados e encriptados.
  - Qualquer pessoa que for removida do grupo de acesso perde o acesso.
  - Se o proprietário de um ficheiro for removido do grupo, os outros utilizadores mantêm o acesso.
- Utilizadores internos ou externos fora do seu grupo de acesso - Não podem visualizar um ficheiro encriptado.
  - Um utilizador interno dentro do grupo de acesso pode conceder acesso.
  - Se um utilizador externo for o proprietário de um ficheiro encriptado, pode conceder acesso a outra pessoa.
  - Se um utilizador interno ou externo fora do grupo receber um ficheiro encriptado e tentar abri-lo, é-lhes apresentada uma caixa de diálogo a pedir que solicitem o acesso.

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

A Empresa Ainda Não Tem o Data Guardian e o Modo Opcional

Se a sua empresa planear utilizar o Data Guardian com grupos de acesso para aumentar a segurança dos dados confidenciais, o ideal é identificar quaisquer ficheiros que partilhe com utilizadores internos ou externos e descobrir se esses utilizadores estão em algum grupo de acesso criado pelo seu administrador. Inicialmente, para garantir uma transição sem problemas, a sua empresa poderá fornecer um breve período para processar quaisquer ficheiros partilhados existentes. Após a conclusão do período de transição, os utilizadores no seu grupo de acesso podem visualizar quaisquer ficheiros partilhados e encriptados que crie. Pode conceder acesso a pessoas fora do seu grupo de acesso para poder colaborar com elas, mas ter maior segurança.

Identificar os utilizadores no seu grupo de acesso

O administrador informa-o de quem está em um ou mais dos seus grupos de acesso, dependendo de quem precisa de acesso a ficheiros específicos. Tal pode incluir utilizadores internos e externos. Se trabalha com dados confidenciais com utilizadores específicos, pode solicitar ao administrador que crie um grupo de acesso para esse conteúdo.

Utilizar um período de transição para processar ficheiros partilhados

Ao instalar o Data Guardian, ocorre um varrimento no Windows ou Mac e os seguintes ficheiros são encriptados se o seu administrador ativou uma política para os mesmos.

- Tipos de ficheiro adicionais, como .txt ou .png, configurados para Proteção Básica de Ficheiros
- Ficheiros de Classificação de Dados (Windows)
- Ficheiros de Classificação TITUS (Windows)

Se já colabora em ficheiros ou os partilha com utilizadores internos ou externos, esses utilizadores podem ou não estar no seu grupo de acesso. A prática recomendada para uma transição sem problemas é ter um breve período de transição para processar quaisquer ficheiros encriptados que tenham sido partilhados com outros utilizadores. Tem de iniciar sessão no seu computador durante este período de transição.

Se pretender continuar a partilhar ou a colaborar nesses ficheiros, tenha em atenção o seguinte:

- Para os ficheiros partilhados listados acima, a primeira pessoa a iniciar sessão e varrer o computador torna-se o proprietário de quaisquer ficheiros partilhados.
- Se outra pessoa se tornar o proprietário do ficheiro e o autor original não estiver no grupo de acesso, o proprietário original deverá solicitar o acesso ao novo proprietário. O proprietário original pode também solicitar que o administrador altere a propriedade.
- Os computadores de utilizadores externos não são varridos, pelo que quaisquer cópias de ficheiros partilhados desprotegidos não são varridas e encriptadas.
- Se a Encriptação em Nuvem do Data Guardian estiver ativada e os utilizadores partilharem pastas ou ficheiros num fornecedor de armazenamento na nuvem, esses ficheiros também serão varridos.

Colaborar em ficheiros recentemente criados após o período de transição

Para ficheiros novos que crie ou encripte após o período de transição:

- Utilizadores internos ou externos dentro do seu grupo de acesso - Têm acesso a todos os ficheiros partilhados e encriptados.
  - Qualquer pessoa que for removida do grupo de acesso perde o acesso.
  - Se o proprietário de um ficheiro for removido do grupo, os outros utilizadores mantêm o acesso.
- Utilizadores internos ou externos fora do seu grupo de acesso - Não podem visualizar um ficheiro encriptado.
  - Um utilizador interno dentro do grupo de acesso pode conceder acesso.
  - Se um utilizador externo for o proprietário de um ficheiro encriptado, pode conceder acesso a outra pessoa.
  - Se um utilizador interno ou externo fora do grupo receber um ficheiro encriptado e tentar abri-lo, é-lhes apresentada uma caixa de diálogo a pedir que solicitem o acesso.

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

A Empresa Ainda Não Tem o Data Guardian e o Modo Proteção Forçada

Se a sua empresa planear utilizar o Data Guardian com grupos de acesso para aumentar a segurança dos dados confidenciais, o ideal é identificar quaisquer ficheiros que partilhe com utilizadores internos ou externos e descobrir se esses utilizadores estão em algum grupo de acesso criado pelo seu administrador. Inicialmente, para garantir uma transição sem problemas, a sua empresa poderá fornecer um breve período para processar quaisquer ficheiros partilhados existentes. Após a conclusão do período de transição, os utilizadores no seu grupo de acesso podem visualizar quaisquer ficheiros partilhados e encriptados que crie. Pode conceder acesso a pessoas fora do seu grupo de acesso para poder colaborar com elas, mas ter maior segurança.

Identificar os utilizadores no seu grupo de acesso

O administrador informa-o de quem está em um ou mais dos seus grupos de acesso, dependendo de quem precisa de acesso a ficheiros específicos. Tal pode incluir utilizadores internos e externos. Se trabalha com dados confidenciais com utilizadores específicos, pode solicitar ao administrador que crie um grupo de acesso para esse conteúdo.

Utilizar um período de transição para processar ficheiros partilhados

Ao instalar o Data Guardian, ocorre um varrimento no Windows ou Mac e os seguintes ficheiros são encriptados se o seu administrador ativou uma política para os mesmos.

- Documentos do Office

- PDF
- Tipos de ficheiro adicionais, como .txt ou .png, configurados para Proteção Básica de Ficheiros

A prática recomendada para uma transição sem problemas é ter um breve período de transição para processar quaisquer ficheiros encriptados que tenham sido partilhados com outros utilizadores. Tem de iniciar sessão no seu computador durante este período de transição.

Se pretender continuar a partilhar ou a colaborar nesses ficheiros, tenha em atenção o seguinte:

- Para os ficheiros partilhados listados acima, a primeira pessoa a iniciar sessão e varrer o computador torna-se o proprietário de quaisquer ficheiros partilhados.
- Se outra pessoa se tornar o proprietário do ficheiro e o autor original não estiver no grupo de acesso, o proprietário original deverá solicitar o acesso ao novo proprietário. O proprietário original pode também solicitar que o administrador altere a propriedade.
- Os computadores de utilizadores externos não são varridos, pelo que quaisquer cópias de ficheiros partilhados desprotegidos não são varridas e encriptadas.
- Se a Encriptação em Nuvem do Data Guardian estiver ativada e os utilizadores partilharem pastas ou ficheiros num fornecedor de armazenamento na nuvem, esses ficheiros também serão varridos.

Colaborar em ficheiros recentemente criados após o período de transição

Para ficheiros novos que crie ou encripte após o período de transição:

- Utilizadores internos ou externos dentro do seu grupo de acesso - Têm acesso a todos os ficheiros partilhados e encriptados.
  - Qualquer pessoa que for removida do grupo de acesso perde o acesso.
  - Se o proprietário de um ficheiro for removido do grupo, os outros utilizadores mantêm o acesso.
- Utilizadores internos ou externos fora do seu grupo de acesso - Não podem visualizar um ficheiro encriptado.
  - Um utilizador interno dentro do grupo de acesso pode conceder acesso.
  - Se um utilizador externo for o proprietário de um ficheiro encriptado, pode conceder acesso a outra pessoa.
  - Se um utilizador interno ou externo fora do grupo receber um ficheiro encriptado e tentar abri-lo, é-lhes apresentada uma caixa de diálogo a pedir que solicitem o acesso.

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

Alterar o Proprietário de um Ficheiro Encriptado

Durante o período de transição dos grupos de acesso, se outro utilizador for designado como proprietário de um documento encriptado e partilhado que criou originalmente, pode solicitar ao administrador que o designe proprietário.

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

Revogar o Acesso a uma Chave

Se conceder acesso a um ficheiro encriptado a um utilizador externo, o utilizador tem a chave para abrir o ficheiro em questão.

Opcionalmente, se já não pretender que o utilizador externo tenha acesso ao ficheiro, pode solicitar ao administrador a revogação da chave. Isto aplica-se apenas a utilizadores externos.

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

Pré-partilhar Ficheiros Protegidos no Windows

É necessário ter o Data Guardian instalado e estar atribuído a um ou mais grupos de acesso.
Se um utilizador interno ou externo não estiver no seu grupo de acesso, pode pré-partilhar um ficheiro protegido.

1 Clique com o botão direito do rato num ficheiro protegido e selecione **Acesso a Ficheiro Protegido**.

Na IU de *Partilha de Acesso a Ficheiro Protegido*, é apresentado o nome do documento em Ficheiro Selecionado.

2 Em *E-mail para Partilha*, clique em **Adicionar** e introduza um endereço de e-mail válido de um utilizador externo ou de um utilizador interno que não se encontre no seu grupo de acesso.

Pode adicionar até dez endereços individuais de cada vez.

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

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

NOTA:
O nome do proprietário do ficheiro é indicado e não pode ser selecionado nem eliminado.

5 Em Grupos Disponíveis, são apresentados os seus grupos de acesso. Selecione um ou mais grupos e utilize as setas para adicionar a *Grupos Partilhados*.

6 Clique em **OK**. É apresentada uma mensagem de êxito.

NOTA:
Os utilizadores externos não podem partilhar o documento protegido com outro utilizador externo.

Se esta for a primeira vez que um utilizador externo recebe um ficheiro protegido do Data Guardian, o utilizador tem de instalar o Data Guardian ou utilizar o portal Web para ver o ficheiro protegido.

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

Pré-partilhar Ficheiros Protegidos no Mac

É necessário ter o Data Guardian instalado e estar atribuído a um ou mais grupos de acesso.
Se um utilizador interno ou externo não estiver no seu grupo de acesso, pode pré-partilhar um ficheiro protegido.

1 Clique com o botão direito do rato num ficheiro protegido e selecione **Acesso a Ficheiro Protegido**.

Na IU de *Partilha de Acesso a Ficheiro Protegido*, é apresentado o nome do documento em Ficheiro Selecionado.

2 Em *E-mail para Partilha*, clique em **Adicionar** e introduza um endereço de e-mail válido de um utilizador externo ou de um utilizador interno que não se encontre no seu grupo de acesso.

Pode adicionar até dez endereços individuais de cada vez.

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

NOTA:
O nome do proprietário do ficheiro é indicado e não pode ser selecionado nem eliminado.

4 Em Grupos Disponíveis, são apresentados os seus grupos de acesso. Selecione um ou mais grupos e utilize as setas para adicionar a *Grupos Partilhados*.

5 Clique em **OK**. É apresentada uma mensagem de êxito.

NOTA:
Os utilizadores externos não podem partilhar o documento protegido com outro utilizador externo.

Se esta for a primeira vez que um utilizador externo recebe um ficheiro protegido do Data Guardian, o utilizador tem de instalar o Data Guardian ou utilizar o portal Web para ver o ficheiro protegido.

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

Pré-partilhar Ficheiros Protegidos em iOS ou Android

Se um utilizador interno ou externo não estiver no seu grupo de acesso, pode pré-partilhar um ficheiro protegido.

1 Toque num ficheiro protegido.

2

NOTA:
No separador *Utilizadores*, o nome do proprietário do ficheiro é apresentado, mas não pode ser selecionado ou eliminado. Se já partilhou o ficheiro com utilizadores internos ou externos, os nomes em questão são apresentados.

3 No separador *Utilizadores*, para adicionar o endereço de e-mail de um utilizador externo ou de um utilizador interno que não se encontre no grupo de acesso, clique no ícone "Mais" (+) no canto inferior direito.

4 Para eliminar um endereço de e-mail, arraste o dedo e toque em **Eliminar**.

5 Toque no separador **Grupos** para ver os seus grupos de acesso.

6 Toque num grupo para partilhar um ficheiro protegido.

NOTA:
Uma marca de verificação indica um grupo com o qual opta por partilhar o ficheiro protegido.

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

É apresentada uma mensagem de êxito. Os utilizadores externos não podem partilhar o documento protegido com outro utilizador externo.

Se esta for a primeira vez que um utilizador externo recebe um ficheiro protegido do Data Guardian, o utilizador tem de instalar o Data Guardian ou utilizar o portal Web para ver o ficheiro protegido.

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

Pré-partilhar Ficheiros Protegidos no Portal Web

Se um utilizador interno ou externo não estiver no seu grupo de acesso, pode pré-partilhar um ficheiro protegido.

1 No portal Web, carregue um documento protegido.

Se o seu administrador o tiver inserido num ou mais grupos de acesso, é apresentado um ícone *Acesso a Ficheiro Protegido* ao lado do ícone Transferir.

2 Clique no ícone **Acesso a Ficheiro Protegido**.

Na IU de *Partilha de Acesso a Ficheiro Protegido*, é apresentado o nome do documento em Ficheiro Selecionado.

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

4 Introduza um endereço de e-mail válido de um utilizador externo ou de um utilizador interno que não se encontre no seu grupo de acesso e clique na marca de verificação para o guardar. Pode adicionar até dez endereços individuais de cada vez.

NOTA:

Para eliminar um endereço de e-mail, clique em **X**. O nome da pessoa que partilha o documento é destacado e não pode ser selecionado nem eliminado.

5 Em Grupos Disponíveis, são apresentados os seus grupos de acesso. Clique em **Selecionar Tudo** ou clique no ícone de seta junto a uma opção para adicionar a *Grupos Partilhados* ou para remover.

6 Clique em **OK**.

NOTA:

Os utilizadores externos não podem partilhar o documento protegido com outro utilizador externo.

Se esta for a primeira vez que um utilizador externo recebe um ficheiro protegido do Data Guardian, o utilizador tem de instalar o portal Web.

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

Pré-partilhar Ficheiros Protegidos Enquanto Utilizador Externo

É necessário ter o Data Guardian instalado e estar atribuído a um ou mais grupos de acesso.
Se for o originador ou proprietário de um ficheiro protegido, pode pré-partilhar o ficheiro com um utilizador interno. Não pode partilhar o documento protegido com outro utilizador externo. Se não for proprietário do ficheiro, não pode partilhá-lo.

- A funcionalidade *E-mail para Partilha* não apresenta os nomes de outros utilizadores com os quais o documento protegido foi partilhado.
- Não são apresentados grupos em Grupos Disponíveis. Só pode partilhar com pessoas individuais.

1 Clique com o botão direito do rato num ficheiro protegido e selecione **Acesso a Ficheiro Protegido**.

Na IU de *Partilha de Acesso a Ficheiro Protegido*, é apresentado o nome do documento em Ficheiro Selecionado.

2 Em *E-mail para Partilha*, clique em **Adicionar** e introduza um endereço de e-mail válido de um utilizador externo ou de um utilizador interno que não se encontre no seu grupo de acesso.

Pode adicionar até dez endereços individuais de cada vez.

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

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

NOTA:

Enquanto proprietário do ficheiro, não pode selecionar ou eliminar o seu nome.

5 Clique em **OK**. É apresentada uma mensagem de êxito.

Se esta for a primeira vez que um utilizador recebe um ficheiro protegido do Data Guardian, o utilizador tem de instalar o Data Guardian ou utilizar o portal Web para ver o ficheiro protegido.

Identifier	GUID-F97CE528-0A49-4763-80D0-0F5937EAE934
Status	In Translation

Modificar quem tem acesso aos e-mails protegidos

Com base na política definida pelo seu administrador, pode clicar com o botão direito do rato num e-mail que protegeu e enviou aos utilizadores no seu Grupo de Acesso. Pode modificar quem tem acesso ao e-mail em questão.

1 No Outlook, clique com o botão direito do rato num e-mail identificado como [PROTEGIDO].

2 Na parte inferior, selecione **Acesso a E-mail Protegido**.

É apresentada uma lista de utilizadores com quem partilhou o acesso.

3 Remova utilizadores individuais se não pretender que continuem a ter acesso ao e-mail protegido.

Identifier	GUID-F553E0C3-FCF3-4782-8FD4-
Status	Translation Validated

Perguntas frequentes

Identifier	GUID-D70F8E30-C205-474A-BC17-DB3867AE07AE
Status	In Translation

Perguntas diversas

Pergunta

Pergunta

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

Resposta

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

Solução

Desinstale e volte a instalar o Data Guardian. Tem de ter direitos de administrador para desinstalar.

Identifier	GUID-36E78894-7902-4034-8BFA-6D63A1743855
Status	Translation Validated

Perguntas mais frequentes sobre documentos do Office e o modo protegido

Pergunta

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

Resposta

Se o seu administrador definir uma política para proteger documentos do Office, é necessário que o utilizador ou o respetivo administrador instale o Data Guardian. Confirme se o ícone do Data Guardian na área de notificação apresenta uma marca de verificação verde, para indicar que se encontra ativado.

Solução

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

Pergunta

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

Resposta

Verifique o seguinte:

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

Solução

Para verificar as Definições de bloqueio de ficheiros:

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