# HP ProtectTools
## Manual do utilizador

Bluetooth é uma marca comercial, propriedade do titular e utilizada pela Hewlett-Packard Company sob licença. Java é uma marca comercial da Sun Microsystems, Inc. Microsoft e Windows são marcas registadas da Microsoft Corporation. O logótipo SD é uma marca comercial do seu proprietário.

As informações aqui contidas estão sujeitas a alterações sem aviso prévio. As únicas garantias que cobrem os produtos e serviços da HP são estabelecidas exclusivamente na documentação de garantia que os acompanha. Neste documento, nenhuma declaração deverá ser interpretada como a constituição de garantia adicional. A HP não se responsabiliza por erros técnicos e editoriais ou por omissões neste documento.

Primeira edição: Outubro de 2009

Número de publicação do documento: 572661-131

# Índice

# 1 Introdução à segurança

O software HP ProtectTools Security Manager fornece funcionalidades de segurança que o ajudam a proteger-se contra o acesso não autorizado ao computador, redes e dados críticos. O software HP ProtectTools Security Manager é administrado através da funcionalidade Administrative Console.

O administrador local pode efectuar as seguintes tarefas através da consola:

- Activar ou desactivar as funcionalidades de segurança
- Registar impressões digitais dos utilizadores deste computador
- Configurar um smart card
- Especificar as credenciais necessárias para autenticação
- Gerir os utilizadores do computador
- Ajustar parâmetros específicos do dispositivo
- Configurar as aplicações do software Security Manager instaladas
- Adicionar aplicações do software Security Manager adicionais

Os módulos de software disponíveis para o computador podem variar consoante o modelo.

Os módulos de software do HP ProtectTools podem ser pré-instalados, pré-carregados ou estar disponíveis para transferência no Web site da HP. Para obter mais informações, visite http://www.hp.com.

**NOTA:** As instruções existentes neste guia são escritas partindo do princípio que já instalou os módulos de software do HP ProtectTools aplicáveis.

# Funcionalidades do HP ProtectTools

A tabela seguinte enuncia pormenorizadamente as funcionalidades chave dos módulos de software do HP ProtectTools.

| Módulo | Funcionalidades chave |
|---|---|
| Credential Manager for HP ProtectTools | • O Password Manager actua como um cofre pessoal de palavras-passe, simplificando o processo de início de sessão através da funcionalidade Single Sign On, que memoriza e aplica automaticamente as credenciais do utilizador.<br>• A funcionalidade Single Sign On (Início de sessão simples) também proporciona protecção adicional, ao requerer combinações de diferentes tecnologias de segurança, tais como um Java™ Card e leitores biométricos, para autenticação do utilizador.<br>• O armazenamento das palavras-passe é protegido por encriptação do software e pode ser melhorado com o uso de autenticação do dispositivo de segurança, como Java Cards ou biométrica.<br>**NOTA:** A funcionalidade Credential Manager encontra-se na opção do Password Manager do HP ProtectTools Security Manager |
| Drive Encryption para o HP ProtectTools (somente em alguns modelos) | • O Drive Encryption proporciona uma encriptação completa de todo o volume do disco rígido.<br>• O Drive Encryption requer autenticação antes do arranque, de forma a desencriptar e permitir o acesso aos dados. |
| Privacy Manager para o HP ProtectTools (somente em alguns modelos) | • O software Privacy Manager utiliza técnicas de início de sessão avançadas para verificar a fonte, integridade e segurança das comunicações quando usar correio electrónico, documentos Microsoft® Office ou mensagens instantâneas (IM). |
| File Sanitizer para o HP ProtectTools | • O File Sanitizer permite-lhe destruir activos digitais (informações confidenciais, incluindo ficheiros de aplicações, conteúdo histórico ou relacionado com a Web ou outros dados confidenciais) de maneira segura e periodicamente limpar a unidade do disco rígido. |
| Device Access Manager para o HP ProtectTools (somente em alguns modelos) | • O Device Access Manager permite aos gestores de TI controlar o acesso a dispositivos com base em perfis de utilizador.<br>• O Device Access Manager impede os utilizadores não autorizados de removerem dados através de suportes de armazenamento externos e de introduzirem vírus no sistema a partir de suportes externos.<br>• O administrador pode desactivar o acesso a dispositivos graváveis para indivíduos ou grupos de utilizadores específicos. |

# Atingir objectivos de segurança chave

Os módulos HP ProtectTools podem funcionar em conjunto para fornecer soluções para vários problemas de segurança, incluindo os seguintes objectivos de segurança chave:

- Proteger contra furto direccionado
- Restringir o acesso a dados sensíveis
- Impedir o acesso não autorizado a partir de localizações internas ou externas
- Criar políticas para palavras-passe fortes
- Conformidade com os regulamentos de segurança em vigor

## Proteção contra roubo seleccionado

Um exemplo de roubo seleccionado seria o roubo de um computador com dados confidenciais e informações do cliente num ponto de controlo de segurança do aeroporto. As seguintes funcionalidades ajudam a proteger contra roubo seleccionado:

- A funcionalidade de autenticação de pré-arranque, se estiver activada, ajuda a impedir o acesso ao sistema operativo. Consulte os seguintes procedimentos:
  - Security Manager
  - Drive Encryption

## Restringir o acesso a dados confidenciais

Suponha que um auditor de contratos está a trabalhar no exterior e teve acesso ao computador para rever dados financeiros confidenciais; não quer que o auditor imprima os ficheiros ou os guarde num dispositivo passível de ser escrito, como um CD. A funcionalidade seguinte ajuda a restringir o acesso aos dados:

- O software Device Access Manager for HP ProtectTools permite aos gestores de TI restringir o acesso a dispositivos passíveis de serem escritos para que não seja possível imprimir ou copiar informações confidenciais da unidade de disco rígido para suportes amovíveis.

## Impedir o acesso não autorizado a partir de localizações internas ou externas

O acesso não autorizado a um PC empresarial não protegido constitui um risco muito claro para os recursos da rede da empresa, como o acesso a informações dos serviços financeiros, aos registos de um executivo ou de uma equipa de pesquisa e desenvolvimento, e a informação privada, tais como registos de pacientes ou registos financeiros pessoais. As seguintes funcionalidades ajudam a impedir o acesso não autorizado:

- A funcionalidade de autenticação de pré-arranque, se estiver activada, ajuda a impedir o acesso ao sistema operativo. Consulte os seguintes procedimentos:
  - Password Manager
  - Drive Encryption
- O software Password Manager ajuda a assegurar que um utilizador não autorizado não obtenha as palavras-passe ou acesso a aplicações protegidas por palavras-passe.

- O software Device Access Manager for HP ProtectTools permite aos gestores de TI restringir o acesso a dispositivos passíveis de serem escritos para que não seja possível copiar informações confidenciais da unidade de disco rígido.
- O DriveLock ajuda a assegurar que não é possível aceder aos dados mesmo que a unidade de disco rígido seja removida e instalada num sistema sem segurança.

## Criar fortes políticas de palavras-passe

O Security Manager disponibiliza um repositório protegido para palavras-passe e a conveniente funcionalidade Single Sign On (Início de sessão único) se entrar em vigor um mandato que exige o uso de uma forte política de palavras-passe para dúzias de aplicações à base da Web e bases de dados.

# Elementos de segurança adicionais

## Atribuir funções de segurança

Uma prática importante da gestão da segurança informática (principalmente em grandes organizações) é a divisão de responsabilidades e direitos entre vários tipos de administradores e utilizadores.

**NOTA:** Numa organização pequena ou em caso de utilização individual, todas estas funções podem ser mantidas pela mesma pessoa.

No HP ProtectTools, as obrigações e privilégios de segurança podem ser divididos nas seguintes funções:

- Responsável pela segurança—Define o nível de segurança da empresa ou rede e determina as funcionalidades de segurança a implementar, como Java™ Cards, leitores biométricos ou tokens USB.

  **NOTA:** Muitas das funcionalidades do ProtectTools podem ser personalizadas pelo responsável pela segurança em cooperação com a HP. Para obter mais informações, consulte o Web site da HP em http://www.hp.com.

- Administrador de TI—Aplica e gere as funcionalidades de segurança definidas pelo responsável pela segurança. Também pode activar e desactivar algumas funcionalidades. Por exemplo, se o responsável pela segurança tiver decidido implementar Java Cards, o administrador de TI pode activar o modo de segurança do BIOS por Java Card.

- Utilizador—Utiliza as funcionalidades de segurança. Por exemplo, se o responsável pela segurança e o administrador de TI tiverem activado Java Cards para o sistema, o utilizador pode definir o PIN do Java Card e utilizá-lo para autenticação.

**CUIDADO:** Os administradores são encorajados a cumprir as “melhores práticas” no que diz respeito a restringir privilégios do utilizador final bem como de acesso dos utilizadores.

Não devem ser concedidos privilégios administrativos a utilizadores não autorizados.

## Gerir as palavras-passe do HP ProtectTools

A maior parte das funcionalidades do HP ProtectTools Security Manager são protegidas por palavra-passe. A tabela seguinte lista as palavras-passe frequentemente utilizadas, o módulo de segurança onde a palavra-passe é definida e a função da palavra-passe.

As palavras-passe definidas e utilizadas apenas pelos administradores de TI também estão indicadas nesta tabela. Todas as outras palavras-passe podem ser definidas por utilizadores normais ou administradores.

| Palavra-passe do HP ProtectTools | Definir neste módulo do HP ProtectTools | Função |
|---|---|---|
| palavra-passe de início de sessão do Security Manager | Security Manager | Esta palavra-passe oferece 2 opções:<br>• Pode ser utilizada como um início de sessão do Security Manager para aceder a este software após iniciar a sessão no Windows.<br>• Pode ser utilizada para permitir acesso ao Windows e Security Manager simultaneamente. |

| Palavra-passe do HP ProtectTools | Definir neste módulo do HP ProtectTools | Função |
|---|---|---|
| palavra-passe do ficheiro de recuperação do Security Manager | Security Manager, pelo administrador de TI | Protege o acesso ao ficheiro de recuperação do Security Manager. |
| PIN do Java™ Card | Java Card Security | Protege o acesso ao conteúdo do Java Card e autentica os utilizadores do Java Card. Quando utilizado para autenticação na ligação, o PIN do Java Card também protege o acesso ao utilitário Computer Setup e ao conteúdo do computador.<br><br>Autentica os utilizadores do Drive Encryption, se o token de Java Card estiver seleccionado. |
| palavra-passe de início de sessão do Windows | Painel de controlo do Windows® | Pode ser utilizada no início de sessão manual ou guardada no Java Card. |

### Criar uma palavra-passe segura

Quando criar palavras-passe, tem de respeitar quaisquer especificações definidas pelo programa. No entanto, tome em consideração as seguintes directrizes gerais para o ajudar a criar palavras-passe fortes e a reduzir as hipóteses da sua palavra-passe ficar comprometida:

- Utilize palavras-passe com mais de 6 caracteres, de preferência mais de 8.
- Misture letras maiúsculas e minúsculas na palavra-passe.
- Sempre que possível, misture caracteres alfanuméricos e inclua caracteres especiais e sinais de pontuação.
- Substitua letras por caracteres especiais ou números. Por exemplo, pode utilizar o número 1 para substituir as letras I ou L.
- Combine palavras de 2 ou mais idiomas.
- Divida uma palavra ou frase com números ou caracteres especiais pelo meio; por exemplo, “Maria2-2Cat45.”
- Não utilize uma palavra-passe que possa aparecer num dicionário.
- Não utilize o seu nome nem outras informações pessoais na palavra-passe, como a data de nascimento, diminutivos ou apelidos, mesmo que os escreva de trás para a frente.
- Altere as palavras-passe regularmente. Poderá alterar apenas alguns caracteres incrementais.
- Se anotar a sua palavra-passe, não a guarde num local visível perto do computador.
- Não guarde a palavra-passe num ficheiro, tal como uma mensagem de correio electrónico, no computador.
- Não partilhe contas nem diga a sua palavra-passe a ninguém.

## Efectuar cópia de segurança e restaurar as credenciais do HP ProtectTools

Pode utilizar o Drive Encryption for HP ProtectTools para seleccionar e efectuar uma cópia de segurança das credenciais do HP ProtectTools.

# 2 Informação básicas

**NOTA:** A administração do software HP ProtectTools exige privilégios administrativos.

O Assistente de Configuração do software HP ProtectTools guia-o através da configuração das funcionalidades mais utilizadas do Security Manager. Mas existem inúmeras funcionalidades adicionais disponíveis através da HP ProtectTools Administrative Console. Utilize o menu Iniciar do Windows® para aceder à consola, que lhe permite configurar as mesmas definições que se encontram no assistente, bem como funcionalidades de segurança adicionais. Estas definições aplicam-se ao computador e todos os utilizadores que partilham o computador.

1. Pode desactivar a visualização posterior do assistente seleccionando uma das opções na página Boas-vindas.
2. O Assistente de Configuração do software HP ProtectTools inicia automaticamente para o guiar através dos passos básicos de configuração do programa uma semana após a configuração do computador ou quando um utilizador com direitos administrativos passar um dedo pelo leitor de impressões digitais pela primeira vez. Um tutorial de vídeo acerca da configuração do computador começa automaticamente.
3. Siga as instruções apresentadas no ecrã até concluir a configuração.

O assistente inicia-se automaticamente mais duas vezes se não o concluir. Após isto, pode aceder ao assistente através do balão de notificação apresentado perto da área de notificação da barra de tarefas (excepto caso o tenha desactivado conforme descrito no passo 2 acima) até completar a configuração.

Inicie o ProtectTools Security Manager através do menu Iniciar ou clique no botão direito do rato sobre o ícone do Security Manager na área de notificação, situado na extrema direita da barra de tarefas para utilizar as aplicações do software HP ProtectTools Security Manager. A HP ProtectTools Administrative Console e as suas aplicações são disponibilizadas a todos os utilizadores que partilharem este computador.

# Abrir a HP ProtectTools Administrative Console

No caso de tarefas administrativas, como definição de políticas do sistema ou configurar o software, abra a consola da seguinte maneira:

- Clique em **Iniciar**, **Todos os Programas**, **HP** e depois em **HP ProtectTools Administrative Console**.

  – ou –

  Clique em **Administração** no painel esquerdo do Security Manager.

No caso de tarefas do utilizador, como registar impressões digitais ou utilizar o Security Manager, abra a consola da seguinte maneira:

- Clique em **Iniciar**, **Todos os Programas**, **HP** e depois em **HP ProtectTools Security Manager**.

  – ou –

  Clique duas vezes no ícone do **HP ProtectTools Security Manager** da área de notificação, no lado direito da barra de tarefas.

# Activar as funcionalidades de segurança

O Assistente de Configuração permite-lhe verificar a sua identidade.

1. Leia o ecrã de “Boas vindas”, e em seguida clique em **Seguinte**.
2. Verifique a sua identidade, digitando a sua palavra-passe do Windows se ainda não tiver registado as suas impressões digitais ou digitalizando a sua impressão digital com o leitor de impressões digitais. Clique em **Seguinte**.

   Ser-lhe-á pedido que crie uma palavra-passe do Windows se não tiver nenhuma. É necessária uma palavra-passe do Windows para proteger a sua conta do Windows de acesso por pessoas não autorizadas e para utilizar as funcionalidades do software HP ProtectTools Security Manager.

O Assistente de Configuração guia-o através do processo de activação das funcionalidades de segurança que se aplicam a todos os utilizadores do computador:

- A funcionalidade Windows Logon Security protege a(s) sua(s) conta(s) do Windows exigindo a utilização de credenciais específicas para fins de acesso.
- A funcionalidade Drive Encryption protege os seus dados encriptando a(s) sua(s) unidade(s) de disco rígido, impossibilitando a leitura das informações por pessoas sem a devida autorização.
- A funcionalidade Pre-Boot Security protege o computador proibindo o acesso por pessoas não autorizadas antes do arranque do Windows.

Seleccione a caixa de verificação correspondente para activar uma funcionalidade de segurança. O seu computador estará mais seguro quantas mais funcionalidades seleccionar.

**NOTA:** A funcionalidade Pre-Boot Security não estará disponível se a sua BIOS não a suportar.

# Registar as suas impressões digitais

Você será guiado através do processo de configuração ou "registo" das suas impressões digitais se seleccionar "Impressão digital" e o seu computador tiver um leitor de impressões digitais integrado ou ligado:

1. É apresentado um contorno de duas mãos. Os dedos que já tenham sido registados são assinalados a verde. Clique num dedo no contorno.

   **NOTA:** Clique no dedo correspondente para apagar uma impressão digital registada anteriormente.

2. Depois de seleccionar um dedo para registar, ser-lhe-á pedido que digitalize essa impressão digital até ser devidamente registada. Um dedo registado é assinalado a verde no contorno.

3. Tem de registar pelo menos dois dedos; use de preferência os dedos indicador ou do meio. Repita os passos 1 a 3 para outro dedo.

4. Clique em **Seguinte**.

**NOTA:** As informações das impressões digitais só são memorizadas quando clicar em **Seguinte** quando registar as impressões digitais através do processo das Informações Básicas. As alterações efectuadas **não** são memorizadas se deixar o computador inactivo durante algum tempo ou fechar o painel.

# Configurar um smart card

Se seleccionar a opção "Smart card" e um leitor de smart cards estiver integrado ou ligado ao computador, o Assistente de Configuração do software HP ProtectTools irá solicitar a configuração de um PIN (número de identificação pessoal) do smart card.

Para configurar um PIN do smart card:

1. Introduza e confirme um PIN na página “Configurar smart card”.

   Também pode alterar o seu PIN. Forneça o seu PIN antigo e escolha posteriormente um novo.

2. Clique em **Seguinte** para continuar.

# Utilizar a Administrative Console

A HP ProtectTools Administrative Console é o local central para administrar as funcionalidades e aplicações do software HP ProtectTools Security Manager.

A consola é constituída pelos seguintes componentes:

- **Ferramentas**—Apresenta as seguintes categorias para configurar a segurança no computador:
  - **Início**—Permite seleccionar as tarefas de segurança a realizar.
  - **Sistema**—Permite configurar funcionalidades de segurança e autenticação de utilizadores e dispositivos.
  - **Aplicações**—Apresenta as definições gerais do software HP ProtectTools Security Manager e das aplicações do Security Manager.
  - **Dados**—Disponibiliza um menu expansível de ligações às aplicações do Security Manager que protegem os seus dados.
- **Ferramentas de gestão**—Fornece informações acerca de ferramentas adicionais. O painel abaixo apresenta as seguintes escolhas:
  - **HP ProtectTools Setup Wizard** (Assistente de Configuração do HP ProtectTools)— Guia-o através da configuração do software HP ProtectTools Security Manager.
  - **Ajuda**—Apresenta o ficheiro da Ajuda, que fornece informações acerca do Security Manager e das suas aplicações pré-instaladas. A Ajuda de quaisquer aplicações que possa adicionar é disponibilizada nessas mesmas aplicações.
  - **Acerca**—Apresenta informações acerca do software HP ProtectTools Security Manager, como o número da versão e aviso de direitos de autor.
- **Área principal**—Exibe ecrãs específicos da aplicação.

Clique em **Iniciar**, **Todos os Programas**, **HP** e depois em **HP ProtectTools Administrative Console** para abrir a HP ProtectTools Administrative Console.

# 3 Configurar o seu sistema

Pode aceder ao grupo Sistema através do painel do menu Ferramentas no lado esquerdo do ecrã da HP ProtectTools Administrative Console. Pode utilizar as aplicações deste grupo para gerir as políticas e definições do computador, os seus utilizadores e os seus dispositivos.

As seguintes aplicações encontram-se incluídas no grupo Sistema:

- **Segurança**—Gerir funcionalidades, autenticação e definições que regem o modo como os utilizadores interagem com este computador.
- **Utilizadores**—Configurar, gerir e registar os utilizadores deste computador.
- **Dispositivos**—Gerir definições dos dispositivos de segurança integrados ou ligados ao computador.

# Configurar a autenticação do computador

Na aplicação Autenticação pode seleccionar que funcionalidades de segurança devem ser implementadas neste computador, definir políticas que regem o acesso ao computador e configurar as definições avançadas adicionais. Pode especificar as credenciais necessárias para autenticar cada classe de utilizador ao iniciar a sessão no Windows ou em sites da Web e programas durante uma sessão do utilizador.

Para configurar a autenticação no computador:

1. Clique em **Autenticação** no menu do painel Segurança.
2. Clique no separador **Política de início de sessão**, efectue as alterações e clique em **Aplicar** para configurar a autenticação do início de sessão.
3. Clique no separador **Política de sessão**, efectue as alterações e clique em **Aplicar** para configurar a autenticação de sessão.

## Política de início de sessão

Para definir as políticas que regem as credenciais necessárias para autenticar um utilizador ao iniciar a sessão no Windows:

1. Clique em **Segurança** e em **Autenticação** no menu Ferramentas.
2. Clique numa categoria de utilizador no separador **Política de início de sessão**.
3. Especifique a(s) credencial(is) necessária(s) para a categoria de utilizador seleccionada. Tem de especificar pelo menos uma credencial.
4. Escolha se QUALQUER UMA (apenas uma) das credenciais especificas é necessária, ou se TODAS as credenciais especificadas são necessárias para autenticar um utilizador. Também pode impedir o acesso ao computador por parte de qualquer utilizador.
5. Clique em **Aplicar**.

## Política de sessão

Para definir as políticas que regem as credenciais necessárias para aceder às aplicações do software HP ProtectTools durante uma sessão do Windows:

1. Clique em **Segurança** e em **Autenticação** no menu Ferramentas.
2. Clique numa categoria de utilizador no separador **Política de sessão**.
3. Especifique a(s) credencial(is) necessária(s) para a categoria de utilizador seleccionada.
4. Escolha se QUALQUER UMA (apenas uma) das credenciais especificas é necessária, ou se TODAS as credenciais especificadas são necessárias para autenticar um utilizador. Também pode definir que não é necessária qualquer forma de autenticação para aceder ao software HP ProtectTools.
5. Clique em **Aplicar**.

# Definições

Pode permitir uma ou mais das seguintes definições de segurança:

- **Permitir início de sessão num único passo**—Permite aos utilizadores deste computador passar para o início de sessão do Windows se a autenticação for efectuada ao nível da BIOS ou do disco encriptado.
- **Permitir autenticação HP SpareKey para o início de sessão do Windows**—Permite aos utilizadores deste computador usar a funcionalidade HP SpareKey para iniciar a sessão no Windows não obstante qualquer outra política de autenticação exigida pelo Security Manager.

Para editar as definições:

1. Clique para activar ou desactivar uma definição específica.
2. Clique em **Aplicar** para guardar as alterações efectuadas.

# Gerir Utilizadores

Pode monitorizar e gerir os utilizadores do software HP ProtectTools através da aplicação Utilizadores.

Todos os utilizadores do HP ProtectTools são listados e verificados segundo as políticas definidas através do Security Manager e se registaram ou não as credenciais apropriadas que lhes permitem cumprir essas políticas.

Clique em **Adicionar** para adicionar utilizadores adicionais.

Clique num utilizador e depois em **Eliminar** para o eliminar.

Clique no utilizador e depois em **Registar** para registar impressões digitais ou configurar credenciais adicionais para o utilizador.

Seleccione o utilizador e depois clique em **Ver políticas** para consultar as políticas de um utilizador específico.

# Especificar definições do dispositivo

Através da aplicação Dispositivo pode especificar as definições disponíveis para quaisquer dispositivos de segurança integrados ou ligados que sejam reconhecidos pelo software HP ProtectTools Security Manager.

## Impressões digitais

Existem três separadores na página Impressões digitais: Registo, Sensibilidade e Avançado.

**Registo**

Pode escolher o número mínimo e máximo de impressões digitais que um utilizador está autorizado a inscrever.

Também pode limpar todos os dados do leitor de impressões digitais.

⚠ **AVISO!** Serão eliminados todos os dados de impressões digitais de todos os utilizadores, incluindo os administradores. Se a política de início de sessão exigir apenas impressões digitais, todos os utilizadores poderão ser impedidos de iniciarem a sessão no computador.

**Sensibilidade**

Mova o cursor de deslocamento para ajustar o grau de sensibilidade utilizado pelo leitor de impressões digitais ao digitalizar as suas impressões digitais.

Pode ser necessária uma definição de sensibilidade mais baixa se a sua impressão digital não for reconhecida de uma maneira consistente. Uma definição mais elevada aumenta a sensibilidade para detectar variações nas digitalizações das impressões digitais, e consequentemente diminui a possibilidade de uma falsa aceitação. A definição Média-Elevada disponibiliza um bom equilíbrio de segurança e conveniência.

**Avançado**

Pode configurar o leitor de impressões digitais para conservar energia quando o computador é utilizado com alimentação da bateria.

## Smart card

Pode configurar o computador para bloquear automaticamente após a remoção de um smart card. Mas o computador só será bloqueado se utilizar o smart card como uma credencial de autenticação ao iniciar a sessão no Windows. O computador não será bloqueado se remover um smart card que não era utilizado para iniciar a sessão no Windows.

- Seleccione a caixa de verificação para activar ou desactivar o bloqueio do computador ao remover um smart card.

# 4 Configurar as aplicações

Pode aceder ao grupo Aplicações através do painel do menu Aplicações de Segurança no lado esquerdo da HP ProtectTools Administrative Console. Pode utilizar a opção Definições para personalizar o comportamento das aplicações do software HP ProtectTools Security Manager actualmente instaladas.

Para editar as suas definições da aplicação:

1. Clique em **Definições** no grupo **Aplicações** no menu Ferramentas.
2. Clique para activar ou desactivar uma definição específica.
3. Clique em **Aplicar** para guardar as alterações efectuadas.

# Separador Geral

As seguintes definições são disponibilizadas no separador Geral:

- **Não iniciar automaticamente o Assistente de Configuração para administradores**—Seleccione esta opção para impedir a abertura automática do assistente no início de sessão.
- **Não iniciar automaticamente o Assistente de Introdução para administradores**—Seleccione esta opção para impedir a abertura automática da configuração do utilizador no início de sessão.

# Separador Aplicações

As definições aqui apresentadas podem ser alteradas com a introdução de novas aplicações no Security Manager. Por predefinição, as definições mínimas apresentadas são as seguintes:

- **Security Manager**—Activa a aplicação Security Manager para todos os utilizadores do computador.
- **Activar o botão Descobrir mais**—Permite a todos os utilizadores deste computador adicionar aplicações ao software HP ProtectTools Security Manager clicando no botão **[+] Descobrir mais**.

Clique no botão **Restaurar predefinições** para restaurar todas as predefinições de fábrica.

# 5 Adicionar ferramentas de gestão

Aplicações adicionais podem estar disponíveis para adicionar novas ferramentas de gestão ao Security Manager. Esta funcionalidade pode ser desactivada pelo administrador deste computador através da aplicação Definições.

Clique em **[+] Ferramentas de gestão** para adicionar ferramentas de gestão adicionais.

Pode aceder ao site DigitalPersona para verificar se existem novas aplicações ou pode configurar uma programação para actualizações automáticas.

# 6 HP ProtectTools Security Manager

O software HP ProtectTools Security Manager permite-lhe aumentar de maneira significativa a segurança do seu computador.

Pode utilizar aplicações do Security Manager pré-carregadas bem como aplicações adicionais disponíveis para transferência imediata através da Web:

- Gerir o seu início de sessão e palavras-passe
- Altere facilmente a sua palavra-passe do sistema operativo Windows®
- Definir preferências do programa
- Utilizar impressões digitais para maior segurança e conveniência
- Configurar um smart card para autenticação
- Efectuar cópias de segurança e restaurar os seus dados do programa
- Adicionar mais aplicações

# Procedimentos de configuração

## Informação básicas

O Assistente de Configuração do HP ProtectTools surge automaticamente como a página predefinida no software HP ProtectTools Security Manager até concluir a configuração.

Para configurar o Security Manager, siga estes passos:

**NOTA:** Efectue apenas os passos 1, 5 e 6 se não tiver disponível um leitor de impressões digitais ou um smart card.

1. Clique em **Seguinte** na página “Boas-vindas”.
2. A página seguinte lista os métodos de autenticação disponíveis neste computador. Clique em **Seguinte** para continuar.
3. Digite a sua palavra-passe do Windows na página “Verifique a sua identidade” e clique depois em **Seguinte**.
4. Consulte um ou mais dos seguintes tópicos dependendo da configuração do seu computador.
   - Consulte Registar as suas impressões digitais na página 24 se estiver disponível um leitor de impressões digitais.
   - Consulte Configurar um smart card na página 25 se estiver disponível um smart card.
5. Ser-lhe-á pedido que introduza a sua palavra-passe do Windows se não estiver disponível um leitor de impressões digitais ou um smart card. Tem de usar esta palavra-passe no futuro sempre que for necessária autenticação.
6. Clique em **Concluir** na última página do assistente.

   O painel do Security Manager surge no ecrã.

## Registar credenciais

Pode utilizar a página “A Minha Identidade” para registar os seus vários métodos de autenticação, ou credenciais. Após os ter registado, poderá utilizá-los para iniciar sessão no Security Manager.

### Registar as suas impressões digitais

O Assistente de Configuração do software HP ProtectTools Setup Wizard guia-o através da configuração ou “registo” das suas impressões digitais se o computador tiver um leitor de impressões digitais integrado ou ligado.

1. Leia o ecrã de “Boas vindas”, e em seguida clique em **Seguinte**.
2. Verifique a sua identidade, digitando a sua palavra-passe do Windows se ainda não tiver registado as suas impressões digitais ou digitalizando a sua impressão digital com o leitor de impressões digitais. Clique em **Seguinte**.

   Ser-lhe-á pedido que crie uma palavra-passe do Windows se não tiver nenhuma. É necessária uma palavra-passe do Windows para proteger a sua conta do Windows de acesso por pessoas não autorizadas e para utilizar as funcionalidades do software HP ProtectTools Security Manager.
3. É apresentado um contorno de duas mãos. Os dedos que já tenham sido registados são assinalados a verde. Clique num dedo no contorno.

**NOTA:** Clique no dedo correspondente para apagar uma impressão digital registada anteriormente.

4. Depois de seleccionar um dedo para registar, ser-lhe-á pedido que digitalize essa impressão digital até ser devidamente registada. Um dedo registado é assinalado a verde no contorno.
5. Tem de registar pelo menos dois dedos; use de preferência os dedos indicador ou do meio. Repita os passos 3 e 4 para outro dedo.
6. Clique em **Seguinte**.

**NOTA:** As informações das impressões digitais só são memorizadas quando clicar em **Seguinte** quando registar as impressões digitais através do processo das Informações Básicas. As alterações efectuadas **não** são memorizadas se deixar o computador inactivo durante algum tempo ou fechar o painel.

### Alterar a palavra-passe do Windows

Alterar a sua palavra-passe do Windows é mais simples e rápido com o Security Manager do que através do Painel de Controlo do Windows.

Para alterar a sua palavra-passe do Windows, execute os passos seguintes:

1. Clique em **A Minha Identidade** no painel do Security Manager e, em seguida, em **Credenciais** e depois em **Palavra-passe**.
2. Digite a sua actual palavra-passe na caixa de texto **Actual palavra-passe do Windows**.
3. Digite uma nova palavra-passe na caixa de texto **Nova palavra-passe do Windows** e depois digite-a novamente na caixa de texto **Confirmar nova palavra-passe**.
4. Clique em **Alterar** para mudar imediatamente a sua actual palavra-passe para a nova que introduziu.

### Configurar um smart card

O Security Manager solicita a configuração de um PIN (número de identificação pessoal) do smart card se um leitor de smart cards estiver integrado ou ligado ao computador.

- Para configurar um PIN do smart card—Digite e confirme um PIN na página "Configurar smart card".
- Para alterar o PIN—Digite primeiro o PIN antigo e escolha depois um novo.

## Utilizar o painel do Security Manager

O painel do Security Manager é o local central para um fácil acesso às funcionalidades, aplicações e definições do Security Manager.

O painel é constituído pelos seguintes componentes:

- **Cartão de identificação**—Apresenta o nome de utilizador do Windows e uma imagem seleccionada que identifica a conta de utilizador na qual foi iniciada uma sessão.
- **Aplicações de segurança**—Apresenta um menu expansível de ligações para configuração das seguintes categorias de segurança:
  - **A Minha Identidade**
  - **Os Meus Dados**
  - **O Meu Computador**
- **Descobrir mais**—Abre uma página onde poderá encontrar aplicações adicionais para melhorar a segurança da sua identidade, dados e comunicações.
- **Área principal**—Exibe ecrãs específicos da aplicação.
- **Administração**—Abre a HP ProtectTools Administrative Console.
- **Botão Ajuda**—Apresenta informações acerca do ecrã actual.
- **Avançado**—Permite aceder às seguintes opções:
  - **Preferências**—Permite personalizar as definições do Security Manager.
  - **Cópia de segurança e Restauro**—Permite efectuar cópias de segurança e restaurar dados.
  - **Acerca**—Apresenta informações da versão acerca do Security Manager.

Clique em **Iniciar**, **Todos os Programas**, **HP** e depois em **HP ProtectTools Security Manager** para abrir o painel do Security Manager.

## Abrir o HP ProtectTools Security Manager

Pode abrir o HP ProtectTools Security Manager de qualquer uma das seguintes maneiras:

- Clique em **Iniciar**, **Todos os Programas**, **HP** e depois em **HP ProtectTools Security Manager**.
- Faça duplo clique no ícone do **HP ProtectTools** na área de notificação, na extremidade direita da barra de tarefas.
- Clique no botão direito do rato sobre o ícone do **HP ProtectTools** e em **Abrir HP ProtectTools Security Manager**.
- Clique no acessório **Cartão de identificação do Security Manager** na Barra lateral do Windows.
- Prima a combinação de teclas de atalho ctrl+alt+h para abrir o menu Quick Links (Ligações rápidas) do Security Manager.

# Tarefas gerais

As aplicações incluídas neste grupo ajudam-no a gerir vários aspectos da sua identidade digital.

- **Security Manager**—Cria e gere os Quick Links, que permitem abrir e iniciar a sessão em sites e programas por meio de autenticação com a sua palavra-passe do Windows, impressão digital ou um smart card.
- **Credenciais**—Disponibiliza um meio para alterar facilmente a sua palavra-passe do Windows, registar as suas impressões digitais ou configurar um smart card.

Clique no botão [+] **Descobrir mais** no canto inferior esquerdo do painel para adicionar mais aplicações. O administrador pode desactivar este botão.

## Password Manager

A utilização do Password Manager torna o início de sessão no Windows, sites e aplicações mais fácil e seguro. Pode utilizar esta aplicação para criar palavras-passe mais fortes que não tenha de anotar ou memorizar, e iniciar a sessão posteriormente mais fácil e rapidamente através de uma impressão digital, smart card ou a sua palavra-passe do Windows.

O Password Manager disponibiliza as seguintes opções:

- Adicione, edite ou elimine inícios de sessão através do separador Gerir.
- Use a funcionalidade Quick Links para iniciar o browser predefinido e iniciar a sessão em qualquer site ou programa, após a configuração.
- Use a funcionalidade Arrastar e Largar para organizar os Quick Links em categorias.
- Veja rapidamente se qualquer uma das suas palavras-passe constitui um risco de segurança e gere automaticamente uma palavra-passe forte e complexa para utilizar em novos sites.

Muitas funcionalidades do Password Manager são igualmente disponibilizadas a partir do ícone do Password Manager exibido quando uma página da Web ou um ecrã de início de sessão do programa tem o enfoque. Clique no ícone para apresentar um menu de contexto, onde poderá escolher uma entre as seguintes opções.

### No caso de páginas da Web ou programas onde ainda não foi criado um início de sessão

As seguintes opções são apresentadas no menu de contexto:

- **Adicionar [somedomain.com] ao Password Manager**—Permite adicionar um início de sessão para o actual ecrã do início de sessão.
- **Abrir Password Manager**—Inicia o Password Manager.
- **Definições do ícone**—Permite especificar as condições nas quais é apresentado o ícone do Password Manager.
- **Ajuda**—Apresenta a Ajuda do software Password Manager.

## No caso de páginas da Web ou programas onde já foi criado um início de sessão

As seguintes opções são apresentadas no menu de contexto:

- **Preencher dados do início de sessão**—Coloque os seus dados do início de sessão nos campos do início de sessão e submete posteriormente a página (se tiver especificado a submissão quando criou ou editou pela última vez o início de sessão).
- **Editar início de sessão**—Permite editar os seus dados de início de sessão deste site.
- **Adicionar um nova conta**—Permite adicionar uma conta a um início de sessão.
- **Abrir Password Manager**—Inicia a aplicação do Password Manager.
- **Ajuda**—Apresenta a Ajuda do software Password Manager.

**NOTA:** O administrador deste computador pode configurar o Security Manager para exigir mais do que uma credencial ao verificar a sua identidade.

## Adicionar inícios de sessão

Pode adicionar facilmente um início de sessão a um site ou um programa introduzindo as informações do início de sessão uma vez. O Password Manager introduz automaticamente as informações por si doravante. Pode utilizar estes inícios de sessão depois de navegar até ao site ou programa ou clicar num início de sessão a partir do menu **Inícios de sessão** para o Password Manager abrir o site ou programa e iniciar a sua sessão.

Para adicionar um início de sessão:

1. Abra o ecrã do início de sessão de um site ou programa.
2. Clique na seta no ícone do **Password Manager** e depois num dos seguintes, dependendo de se o ecrã do início de sessão ser para um site ou um programa:
   - Clique em **Adicionar [domain name] ao Password Manager** no caso de um site.
   - Clique em **Adicionar este ecrã de início de sessão ao Password Manager** no caso de um programa.
3. Introduza os seus dados do início de sessão. Os campos do início de sessão no ecrã, e os seus campos correspondentes na caixa de diálogo, são identificados através de uma margem laranja a negrito. Clique em **Adicionar início de sessão** no separador **Gerir Password Manager** para visualizar também esta caixa de diálogo. Algumas opções dependem dos dispositivos de segurança ligados ao computador; por exemplo, usando as teclas de atalho ctrl+alt+H, digitalizando a sua impressão digital ou introduzindo um smart card.
   - Clique nas setas situadas à direita do campo do início de sessão para o preencher com uma das escolhas pré-formatadas.
   - Clique em **Escolher outros campos** para adicionar campos adicionais do ecrã ao seu início de sessão.
   - Desmarque a caixa de verificação **Submeter dados do início de sessão** para preencher os campos do início de sessão mas não os submeter.
   - Clique em **Mostrar palavra-passe** para visualizar a palavra-passe deste início de sessão.
4. Clique em **OK**.

Você é notificado da criação do início de sessão através da remoção do sinal mais do Password Manager.

O ícone do Password Manager é apresentado sempre que aceder a esse site ou abrir esse programa, indicando que pode utilizar a(s) sua(s) credencial(is) registada(s) para iniciar a sessão.

## Editar inícios de sessão

Para editar um início de sessão, siga estes passos:

1. Abra o ecrã do início de sessão de um site ou programa.
2. Clique na seta no ícone do **Password Manager** para apresentar uma caixa de diálogo onde possa editar as suas informações do início de sessão e depois clique em **Editar início de sessão**. Os campos do início de sessão no ecrã, e os seus campos correspondentes na caixa de diálogo, são identificados através de uma margem laranja a negrito.

   Também pode visualizar esta caixa de diálogo clicando em **Editar para o início de sessão desejado** no separador **Gerir Password Manager**.
3. Edite as suas informações de início de sessão.
   - Clique nas setas situadas à direita do campo do início de sessão para o preencher com uma das escolhas pré-formatadas.
   - Clique em **Escolher outros campos** para adicionar campos adicionais do ecrã ao seu início de sessão.
   - Desmarque a caixa de verificação **Submeter dados do início de sessão** para preencher os campos do início de sessão mas não os submeter.
   - Clique em **Mostrar palavra-passe** para visualizar a palavra-passe deste início de sessão.
4. Clique em **OK**.

## Utilizar o menu dos inícios de sessão

O Password Manager disponibiliza uma maneira rápida e fácil de iniciar os sites e programas para os quais criou inícios de sessão. Clique duas vezes num inícios de sessão de um programa ou site no menu **Inícios de sessão** ou no separador **Gerir** no **Password Manager** para abrir o ecrã do início de sessão e preencha então os seus dados do início de sessão.

Quando cria um início de sessão, este é automaticamente adicionado ao menu Inícios de sessão do Password Manager.

Para visualizar o menu Inícios de sessão:

1. Prima a combinação de teclas de atalho do **Password Manager**. A predefinição é ctrl+alt+h. Clique em **Password Manager** e depois em **Definições** para alterar a combinação das teclas de atalho.
2. Digitalize a sua impressão digital (em computadores com um leitor de impressões digitais integrado ou ligado).

## Organizar inícios de sessão em categorias

Use as categorias para manter os seus inícios de sessão ordenados criando uma ou mais categorias. Arraste e largue os seus inícios de sessão nas categorias desejadas.

Para adicionar uma categoria:

1. Clique em **Password Manager** no painel do Security Manager.
2. Clique no separador **Gerir** e depois em **Adicionar categoria**.
3. Introduza um nome para a categoria.
4. Clique em **OK**.

Para adicionar um início de sessão a uma categoria:

1. Coloque o ponteiro do rato por cima do início de sessão desejado.
2. Prima ininterruptamente o botão esquerdo do rato.
3. Arraste o início de sessão para a lista das categorias. As categorias serão assinaladas à medida que passa o rato por cima delas.
4. Solte o botão do rato quando a categoria desejada for assinalada.

Os seus inícios de sessão não são movidos para a categoria seleccionada, apenas copiados. Pode adicionar o mesmo início de sessão a mais do que uma categoria e pode visualizar todos os seus inícios de sessão clicando na opção **Todos**.

## Gerir os seus inícios de sessão

O Password Manager facilita a gestão, a partir de uma localização central, das informações do início de sessão para nomes de utilizador, palavra-passe e múltiplas contas de início de sessão.

Os seus inícios de sessão são listados no separador Gerir. Se forem criados múltiplos inícios de sessão para o mesmo site, cada início de sessão é listado então debaixo do nome do site e ordenados na lista do início de sessão.

Para gerir os seus inícios de sessão:

A partir do painel do Security Manager, clique em **Password Manager** e depois no separador **Gerir**.

- **Adicionar um início de sessão**—Clique em **Adicionar início de sessão** e cumpra as instruções no ecrã.
- **Editar um início de sessão**—Clique num início de sessão e em **Editar** e altere depois os dados do início de sessão.
- **Eliminar um início de sessão**—Clique num início de sessão e depois em **Eliminar**.

Para adicionar um início de sessão adicional para um site ou programa:

1. Abra o ecrã do início de sessão para o site ou programa.
2. Clique no ícone do **Password manager** para visualizar o seu menu de atalho.
3. Clique em **Adicionar início de sessão adicional** e siga as instruções apresentadas no ecrã.

## Avaliar a intensidade da palavra-passe

O uso de palavras-passe fortes para o início de sessão nos seus sites e programas é um aspecto importante da protecção da sua identidade.

O Password Manager facilita a monitorização e melhoria da sua segurança através de uma análise instantânea e automatizada da força de cada uma das palavras-passe utilizadas para iniciar a sessão nos sites e programas.

### definições do ícone do Password Manager

O Password Manager tenta identificar ecrãs de início de sessão de sites e programas. O Password Manager solicita a adição de um início de sessão ao ecrã apresentando o ícone do Password Manager com um sinal "+" quando detecta um ecrã de início de sessão para o qual não criou um início de sessão.

Clique na seta do ícone e depois em **Definições do ícone** para personalizar o modo como o **Password Manager** manuseia possíveis sites de início de sessão.

- **Solicitar a adição de inícios de sessão para ecrãs de início de sessão**—Clique nesta opção para o Password Manager solicitar a adição de um início de sessão quando visualizar um ecrã de início de sessão para o qual ainda não tenha configurado o início de sessão.
- **Excluir este ecrã**—Seleccione a caixa de verificação para o Password Manager não lhe pedir novamente para adicionar um início de sessão a este ecrã de início de sessão.

Clique em **Password Manager** e depois em **Definições** no painel do Security Manager para aceder a definições adicionais do Password Manager.

### Definições

Pode especificar definições para personalizar o HP ProtectTools Security Manager:

1. **Solicitar a adição de inícios de sessão para ecrãs de início de sessão**—O ícone do Password Manager com um sinal mais é apresentado sempre que for detectado um ecrã de início de sessão de um site ou programa, indicando que pode adicionar um início de sessão para este ecrã no cofre das palavras-passe. Na caixa de diálogo **Definições do ícone** desmarque a caixa de verificação ao lado de **Solicitar para adicionar inícios de sessão para ecrãs de início de sessão** para desactivar esta funcionalidade.
2. **Abrir Password Manager with ctrl+alt+H**—A combinação predefinição de teclas de atalho que abre o menu Quick Links do Password Manager é ctrl+alt+H. Clique nesta opção e introduza uma nova combinação de teclas de atalho para alterar as teclas de atalho utilizadas. As combinações podem incluir uma ou mais das seguintes teclas: ctrl, alt ou shift e qualquer tecla alfabética ou numérica.
3. Clique em **Aplicar** para guardar as suas alterações.

## Credenciais

As suas credenciais do Security Manager são utilizadas para assegurar que você é de facto você. O administrador local deste computador pode configurar que credenciais podem ser utilizadas para provar a sua identidade ao iniciar a sessão na sua conta do Windows, sites ou programas.

As credenciais disponíveis podem variar dependendo dos dispositivos de segurança integrados ou ligados a este computador. Cada credencial suportada terá uma entrada no grupo **A Minha Identidade, Credenciais**.

As credenciais disponíveis, requisitos e estado actual são listados e podem incluir o seguinte:

- Impressões digitais
- Palavra-passe
- Smart card

Clique na ligação e cumpra as instruções apresentadas no ecrã para registar ou alterar uma credencial.

## O cartão de identificação pessoal

O seu cartão de identificação identifica-o de maneira única como o proprietário desta conta do Windows, apresentando o seu nome e uma imagem da sua escolha. É apresentado de maneira proeminente no canto superior esquerdo das páginas do Security Manager e como um acessório da Barra lateral do Windows.

Pode obter acesso rápido ao Security Manager clicando no cartão de identificação na Barra lateral do Windows, entre muitas outras maneiras.

Pode alterar a imagem e a maneira como é apresentado o seu nome. Por predefinição, o seu nome de utilizador completo do Windows e imagem seleccionada durante a configuração do Windows são apresentados.

Para alterar o nome apresentado:

1. Clique em **Cartão de identificação** no canto superior esquerdo no painel do Security Manager.
2. Clique na caixa que apresenta o nome introduzido para a sua conta no Windows. O sistema apresenta o seu nome de utilizador do Windows para esta conta.
3. Se quiser alterar este nome, digite o novo nome e depois clique no botão **Guardar**.

Para alterar a imagem apresentada:

1. Clique em **A Minha Identidade** e depois em **Cartão de identificação** no canto superior esquerdo no painel do Security Manager.
2. Clique no botão **Seleccionar imagem**, clique numa imagem e depois no botão **Guardar**.

## Definir preferências

Pode personalizar definições do HP ProtectTools Security Manager: Clique em **Avançado** e depois em **Preferências** no painel do Security Manager. As definições disponíveis são apresentadas em dois separadores: Geral e Impressão digital.

**Geral**

As seguintes definições são disponibilizadas no separador Geral:

**Aspecto—Mostrar ícone na barra de tarefas**

Seleccione a caixa de verificação para activar a apresentação do ícone na barra de tarefas.

Desmarque a caixa de verificação para desactivar a apresentação do ícone na barra de tarefas.

**Impressão digital**

As seguintes definições estão disponíveis no separador Impressão digital:

**Quick Actions (Acções rápidas)**—Use a opção Quick Actions (Acções rápidas) para seleccionar a tarefa do Security Manager a ser efectuada quando premir uma tecla designada enquanto digitaliza a sua impressão digital.

Para atribuir uma Acções rápidas a uma das teclas listadas:

- Clique numa opção **(Tecla)+Impressão digital** e depois numa das tarefas disponíveis no menu.

**Feedback da digitalização da impressão digital**—Apresentado apenas quando está disponível um leitor de impressões digitais. Use esta definição para ajustar o feedback que ocorre quando digitaliza a sua impressão digital.

- **Activar feedback do som**—O Security Manager fornece feedback áudio após a digitalização de uma impressão digital, reproduzindo sons diferentes para eventos específicos do programa. Pode atribuir novos sons a estes eventos através do separador Sons no Painel de Controlo do Windows ou desmarcar esta opção para desactivar o feedback do som.
- **Mostrar feedback da qualidade da digitalização**—Por predefinição, o Security Manager apresenta uma imagem de uma impressão digital com um ponto de interrogação sempre que a qualidade da digitalização de uma impresão digital for insuficiente para concluir a sua autenticação. Desmarque esta opção para desactivar a visualização desta imagem.

## Cópia de segurança e restauro dos dados

Recomendamos a realização de uma cópia de segurança dos seus dados do Security Manager regularmente. A frequência da cópia de segurança depende da frequência das alterações dos dados. Por exemplo, se adicionar novos inícios de sessão diariamente, deverá efectuar cópias de segurança diárias dos seus dados.

Também pode utilizar as cópias de segurança para efectuar a migração de um computador para outro, isto é denominado importação e exportação.

**NOTA:** Esta funcionalidade só efectua a cópia de segurança dos dados.

O HP ProtectTools Security Manager deve ser instalado em qualquer computador que vá receber os dados da cópia de segurança para poder restaurar os dados a partir do ficheiro da cópia de segurança.

Para efectuar a cópia de segurança dos seus dados:

1. No painel da esquerda, clique em **Avançado** e, em seguida, clique em **Cópia de segurança e Restauro**.
2. Clique em **Fazer cópia de segurança dos dados**.
3. Seleccione os módulos que quer incluir na cópia de segurança. Na maioria dos casos, você quererá seleccioná-los a todos.
4. Introduza um nome para o ficheiro de armazenamento. Por predefinição, o ficheiro será guardado na sua pasta Documentos. Clique em **Procurar** para especificar uma localização diferente.
5. Introduza uma palavra-passe para proteger o ficheiro.
6. Verifique a sua identidade.
7. Clique em **Concluir**.

Para restaurar os seus dados:

1. No painel da esquerda, clique em **Avançado** e, em seguida, clique em **Cópia de segurança e Restauro**.
2. Clique em **Restaurar dados**.
3. Seleccione o ficheiro de armazenamento criado anteriormente. Pode introduzir o caminho no campo fornecido ou clicar em **Editar**.
4. Introduza a palavra-passe utilizada para proteger o ficheiro.

5. Seleccione os módulos cujos os dados quer restaurar. Na maioria dos casos, seriam todos os módulos listados.

6. Clique em **Concluir**.

## Adicionar aplicações

Podem estar disponíveis aplicações adicionais que fornecem novas funcionalidades para este programa.

Clique em **[+] Descobrir mais** para procurar aplicações adicionais no painel do Security Manager.

**NOTA:** Se não existir nenhuma ligação **[+] Descobrir mais** na parte inferior esquerda do painel, ela foi desactivada pelo administrador deste computador.

## Estado das aplicações de segurança

A página Estado das aplicações do Security Manager apresenta o estado geral das suas aplicações de segurança instaladas. Apresenta as aplicações que são configuradas e o estado de configuração de cada uma. O resumo é apresentado automaticamente quando abre o painel do Security Manager ou quando clicar em **Aplicações de segurança**.

# 7 Drive Encryption for HP ProtectTools (somente em alguns modelos)

△ **CUIDADO:** Se decidir desinstalar o módulo Drive Encryption, primeiro tem de desencriptar todos os discos que estejam encriptados. Se não o fizer, não lhe será possível aceder aos dados existentes em discos encriptados, a menos que se tenha registado no serviço de recuperação do Drive Encryption. A reinstalação do módulo Drive Encryption não lhe dará acesso aos discos encriptados.

O Drive Encryption for HP ProtectTools disponibiliza uma protecção de dados completa através da encriptação da unidade de disco rígido do computador. Quando o Drive Encryption está activado, deve iniciar sessão no ecrã de início de sessão do Drive Encryption, que é apresentado antes do sistema operativo Windows® ser iniciado.

O Assistente de Configuração do HP ProtectTools permite aos administradores do Windows para activar o Drive Encryption, efectuar cópia de segurança de chave de encriptação, adicionar e remover utilizadores e desactivar o Drive Encryption. Consulte a Ajuda do software HP ProtectTools Security Manager para mais informações.

Pode efectuar as seguintes tarefas com o Drive Encryption:

- Gestão de encriptação
  - Encriptar e desencriptar unidades individuais

    **NOTA:** Só é possível encriptar unidades de disco rígido internas.
- Recuperação
  - Criar cópias de segurança de chaves
  - Efectuar uma recuperação

# Procedimentos de configuração

## Abrir o Drive Encryption

1. Clique em **Iniciar**, **Todos os Programas**, **HP** e depois em **HP ProtectTools Administrative Console**.
2. No painel da esquerda, clique em **Drive Encryption**.

# Tarefas gerais

## Activar o Drive Encryption

Use o Assistente de Configuração do HP ProtectTools para activar o Drive Encryption.

**NOTA:** Este assistente é também utilizado para adicionar e remover utilizadores.

– ou –

1. Clique em **Iniciar**, **Todos os Programas**, **HP** e depois em **HP ProtectTools Administrative Console**.
2. No painel da esquerda, clique em **Segurança** e, em seguida, clique em **Funcionalidades**.
3. Seleccione a caixa de verificação **Drive Encryption** e, em seguida, clique em **Seguinte**.
4. Seleccione a caixa de verificação da unidade de disco rígido que quer encriptar em **Unidades a serem encriptadas**.
5. Introduza o dispositivo de armazenamento na ranhura apropriada.

   **NOTA:** Tem de utilizar um dispositivo de armazenamento USB com o formato FAT32 para guardar a chave de encriptação.
6. Seleccione a caixa de verificação do dispositivo de armazenamento onde vai guardar a chave de encriptação em **Dispositivo de armazenamento externo no qual guardar a chave de encriptação**.
7. Clique em **Aplicar**.

   A encriptação da unidade começa.

Consulte a Ajuda do software HP ProtectTools Security Manager para mais informações.

## Desactivar o Drive Encryption

Use o Assistente de Configuração do HP ProtectTools para desactivar o Drive Encryption. Consulte a Ajuda do software HP ProtectTools Security Manager para mais informações.

– ou –

1. Clique em **Iniciar**, **Todos os Programas**, **HP** e depois em **HP ProtectTools Administrative Console**.
2. No painel da esquerda, clique em **Segurança** e, em seguida, clique em **Funcionalidades**.
3. Desmarque a caixa de verificação do **Drive Encryption** e depois clique em **Aplicar**.

   A desencriptação da unidade começa.

## Iniciar sessão depois de activar o Drive Encryption

Quando ligar o computador depois do Drive Encryption ser activado e a sua conta de utilizador er sido registada, deve iniciar sessão no ecrã de início de sessão do Drive Encryption.

**NOTA:** Inicia a sessão no computador imediatamente depois de ligar o computador, e não no ecrã de início de sessão do Drive Encryption se o administrador do Windows activar a funcionalidade Pre-boot Security no HP ProtectTools Security Manager.

1. Clique no seu nome de utilizador e digite depois a sua palavra-passe do Windows ou PIN do Java™ Card ou passe um dedo registado.
2. Clique em **OK**.

**NOTA:** Se utilizar uma chave de recuperação para iniciar sessão no ecrã de início de sessão do Drive Encryption, também lhe será solicitado que seleccione o seu nome de utilizador e digite a sua palavra-passe do Windows no ecrã de início de sessão do Windows.

## Proteja os seus dados encriptando a sua unidade de disco rígido

Use o Assistente de Configuração do HP ProtectTools para proteger os seus dados encriptando a sua unidade de disco rígido:

1. No Security Manager, clique em **Informações Básicas** e no ícone da **Configuração do Security Manager**. Começa uma demonstração que descreve as funcionalidades do Security Manager. (Também pode iniciar o Security Manager na página “Drive Encryption”.)
2. No painel esquerdo, clique em **Drive Encryption** e depois em **Gestão da Encriptação**.
3. Clique em **Alterar Encriptação**.
4. Seleccione a unidade ou unidades a serem encriptadas.

**NOTA:** Recomendamos fortemente que encripte a unidade de disco rígido.

## Visualizar o estado de encriptação

Os utilizadores podem visualizar o estado de encriptação do HP ProtectTools Security Manager.

**NOTA:** Efectue as alterações do estado de encriptação da unidade com a HP ProtectTools Administrative Console.

1. Abra o **HP ProtectTools Security Manager**.
2. Clique em **Estado de Encriptação** em **Os Meus Dados**.

   Se o Drive Encryption estiver activo, o estado da unidade apresenta um dos seguintes códigos do estado:

   - Activa
   - Inactiva
   - Não encriptada
   - Encriptada
   - Encriptar
   - Desencriptar

   Uma barra de progresso apresenta a percentagem concluída e o tempo restante para concluir a encriptação ou desencriptação se a unidade de disco rígido estiver a ser encriptada ou desencriptada.

# Tarefas avançadas

## Gerir o Drive Encryption (tarefa de administrador)

A página “Gestão de Encriptação” permite aos administradores visualizar e alterar o estado do Drive Encryption (activo ou inactivo), assim como visualizar o estado de encriptação de todas as unidades de disco rígido do computador.

- Se o estado for Inactivo, o Drive Encryption ainda não foi activado no HP ProtectTools Security Manager pelo administrador do Windows e não está a proteger a unidade de disco rígido. Use o Assistente de Configuração do HP ProtectTools Security Manager para activar o Drive Encryption.
- Se o estado for Activo, o Drive Encryption foi activado e configurado. A unidade está num dos seguintes estados:
  - Não encriptada
  - Encriptada
  - Encriptar
  - Desencriptar

### Encriptar e desencriptar unidades individuais

Para encriptar uma ou mais unidades de disco rígido no computador ou desencriptar uma unidade que já foi encriptada, utilize a funcionalidade Alterar Encriptação.

1. Abra a **HP ProtectTools Administrative Console**, clique em **Drive Encryption** e depois em **Gestão da Encriptação**.
2. Clique em **Alterar Encriptação**.
3. Na caixa de diálogo Alterar Encriptação, seleccione ou limpe a caixa de verificação junto a cada unidade de disco rígido que pretende encriptar ou desencriptar e, em seguida, clique em **OK**.

**NOTA:** Quando a unidade está a ser encriptada ou desencriptada, a barra de progresso apresenta o tempo que ainda falta para concluir o processo durante a sessão actual. Se o computador for encerrado ou entrar no modo de Suspensão ou Hibernação durante o processo de encriptação e for reiniciado em seguida, o mostrador do Tempo Restante é reposto para o início, mas a encriptação recomeça a partir do ponto onde tinha terminado. O mostrador do tempo restante e do progresso mudará mais rapidamente, para reflectir a evolução anterior.

## Cópia de segurança e recuperação (tarefa de administrador)

A página “Recuperação” permite que os administradores efectuem cópias de segurança das chaves de segurança e as recuperem.

**Cópia de segurança de chave de encriptação da unidade local**—Permite-lhe efectuar uma cópia de segurança das chaves de encriptação para suportes amovíveis quando activar o Drive Encryption.

### Criar cópias de segurança de chaves

Pode efectuar uma cópia de segurança da chave de encriptação de uma unidade encriptada num dispositivo de armazenamento amovível.

△ **CUIDADO:** Certifique-se de que guarda o dispositivo de armazenamento com a cópia de segurança de chave num lugar seguro, porque se se esquecer da palavra-passe ou perder o Java Card, este dispositivo é a única forma de aceder à sua unidade de disco rígido.

1. Abra a **HP ProtectTools Administrative Console**, clique em **Drive Encryption** e depois em **Recuperação**.
2. Clique em **Cópia de Segurança das Chaves**.
3. Na página “Seleccionar Disco da Cópia de Segurança”, seleccione a caixa de verificação do dispositivo onde pretende criar a cópia de segurança da chave de encriptação e clique em **Seguinte**.
4. Leia as informações na próxima página que é apresentada e clique em **Seguinte**. A chave de encriptação fica guardada no dispositivo de armazenamento seleccionado.
5. Clique em **Concluir** quando a caixa de diálogo de confirmação abrir.

## Efectuar uma recuperação

Para efectuar uma recuperação caso se esqueça da sua palavra-passe, cumpra estes passos:

1. Ligue o computador.
2. Insira o dispositivo de armazenamento amovível que contém a sua chave de cópia de segurança.
3. Quando aparecer a caixa de diálogo de início de sessão no Drive Encryption for HP ProtectTools, clique em **Cancelar**.
4. Clique em **Opções** no canto inferior esquerdo do ecrã e clique em **Recuperação**.
5. Seleccione o ficheiro que contém a sua chave de cópia de segurança ou clique em **Procurar** para o procurar e clique em **Seguinte**.
6. Quando a caixa de diálogo de confirmação se abrir, clique em **OK**.

   O seu computador inicia.

**NOTA:** Recomenda-se vivamente que reponha a sua palavra-passe depois de efectuar uma recuperação.

# 8 Privacy Manager para o HP ProtectTools (somente em alguns modelos)

O software Privacy Manager for HP ProtectTools permite-lhe utilizar métodos avançados de início de sessão de segurança (autenticação) para verificar a fonte, integridade e segurança das comunicações quando usar correio electrónico, documentos do Microsoft® Office ou mensagens instantâneas (IM).

O Privacy Manager uniformiza a infra-estrutura de segurança disponibilizada pelo HP ProtectTools Security Manager, que inclui os seguintes métodos de início de sessão de segurança:

- Autenticação da impressão digital
- Palavras-passe do Windows®
- HP ProtectTools Java™ Card

Pode utilizar qualquer um dos anteriores métodos de início de sessão de segurança no Privacy Manager.

O Privacy Manager necessita do seguinte:

- HP ProtectTools Security Manager 5.00 ou posterior
- Sistema operativo Windows® 7, Windows Vista® ou Windows XP
- Microsoft Outlook 2007 ou Microsoft Outlook 2003
- Conta de correio electrónico válida

**NOTA:** Tem de solicitar e instalar um Certificado do Privacy Manager (um certificado digital) através do Privacy Manager para poder aceder às funcionalidades de segurança. Consulte Solicitar e instalar um Certificado do Privacy Manager na página 43 para obter mais informações sobre como solicitar um Certificado do Privacy Manager.

# Procedimentos de configuração

## Abrir Privacy Manager

Para abrir o Privacy Manager:

1. Clique em **Iniciar**, **Todos os Programas**, **HP** e depois em **HP ProtectTools Security Manager**.
2. Clique em **Privacy Manager**.

– ou –

Clique com o botão direito do rato no ícone do **HP ProtectTools** na área de notificação, na extremidade direita da barra de tarefas, e, em seguida, clique em **Privacy Manager** e em **Configuração**.

– ou –

Clique na seta para baixo ao lado de **Enviar em Segurança** (**Privacy** no Outlook 2003), e em seguida clique em **Assinar e Enviar**.

– ou –

Na barra de ferramentas de um documento do Microsoft Office, clique na seta para baixo ao lado de **Assinar e Encriptar** e depois em **Certificados** ou **Contactos Fidedignos**.

## Gerir Certificados do Privacy Manager

Os Certificados do Privacy Manager protegem dados e mensagens através de uma tecnologia criptográfica denominada infra-estrutura de chaves públicas (PKI). O PKI exige que os utilizadores obtenham chaves criptográficas e um Certificado do Privacy Manager emitido por uma autoridade de certificação (CA). O Privacy Manager exige que efectue a autenticação sempre que assinar uma mensagem de correio electrónico ou um documento do Microsoft Office com uma chave criptográfica ao contrário da maioria do software de encriptação de dados e autenticação que só exige a realização periódica da autenticação. O Privacy Manager torna seguro o processo de memorização e envio das suas informações importantes.

Pode efectuar as seguintes tarefas:

- Solicitar e instalar um Certificado do Privacy Manager
- Ver os detalhes do Certificado do Privacy Manager
- Renovar Certificados do Privacy Manager
- Defina um Certificado do Privacy Manager a ser utilizado pelo Privacy Manager quando se encontram disponíveis múltiplos certificados
- Eliminar e revogar um Certificado do Privacy Manager (avançado)

## Solicitar e instalar um Certificado do Privacy Manager

Tem de solicitar e instalar um Certificado do Privacy Manager (através do Privacy Manager) com um endereço de correio electrónico válido para poder utilizar as funcionalidades do Privacy Manager. Tem de configurar o endereço do correio electrónico como uma conta através do Microsoft Outlook no mesmo computador a partir do qual está a solicitar o Certificado do Privacy Manager.

## Solicitar um Certificado do Privacy Manager

1. Abra o Privacy Manager e clique em **Certificados**.
2. Clique em **Solicitar um certificado do Privacy Manager**.
3. Leia o texto na páginas de “Boas vindas”, e em seguida clique em **Seguinte**.
4. Leia o Contrato de licença na página “Contrato de licença”.
5. Certifique-se de que selecciona a caixa de verificação ao lado de **Marcar aqui para aceitar os termos deste Contrato de licença** e depois clique em **Seguinte**.
6. Introduza as informações necessárias na página “Os Detalhes do Certificado” e clique depois em **Seguinte**.
7. Na página “Pedido de Certificado Aceite” clique em **Concluir**.
8. Clique em **OK** para fechar o certificado.

Irá receber uma mensagem de correio electrónico no Microsoft Outlook com o seu Certificado do Privacy Manager anexado.

## Obter um Certificado Empresarial do Privacy Manager pré-atribuído

1. No Outlook, abra a mensagem de correio electrónico recebida a indicar que lhe foi pré-atribuído um Certificado Empresarial.
2. Clique em **Obter**.
3. Irá receber uma mensagem de correio electrónico no Microsoft Outlook com o seu Certificado do Privacy Manager anexado.
4. Consulte Instalar um Certificado do Privacy Manager na página 44 para instalar o certificado.

## Instalar um Certificado do Privacy Manager

1. Quando receber a mensagem de correio electrónico com o seu Certificado do Privacy Manager anexado, abra a mensagem de correio electrónico e clique no botão **Configurar**, no canto inferior direito da mensagem no Outlook 2007, ou no canto superior esquerdo no Outlook 2003.
2. Efectue a autenticação com o seu método seleccionado de início de sessão de segurança.
3. Clique em **Seguinte** na página “Certificado Instalado”.
4. Introduza um local e nome do ficheiro da cópia de segurança na página “Cópia de segurança do Certificado” ou clique em **Procurar** para procurar uma localização.

△ **CUIDADO:** Certifique-se de que guarda o ficheiro numa localização diferente da unidade do disco rígido e coloque-o num local seguro. Este ficheiro deve ser apenas para sua utilização, e é necessário caso tenha de restaurar o Certificado do Privacy Manager e chaves associadas.

5. Introduza e confirme uma palavra-passe e, em seguida, clique em **Seguinte**.
6. Efectue a autenticação com o seu método seleccionado de início de sessão de segurança.
7. Se optar por iniciar o processo de convite de Contacto Fidedigno, cumpra as instruções apresentadas no ecrã começando pelo passo 2 do tópico Adicionar Contactos Fidedignos utilizando os contactos do Microsoft Outlook na página 48.

– ou –

Se clicar em **Cancelar**, consulte as informações Adicionar um Contacto Fidedigno na página 47 sobre como adicionar um Contacto Fidedigno posteriormente.

## Visualizar os detalhes do Certificado do Privacy Manager

1. Abra o Privacy Manager e clique em **Certificados**.
2. Clique num Certificado do Privacy Manager.
3. Clique em **Detalhes do Certificado**.
4. Clique em **OK** quando concluir a visualização dos detalhes.

## Renovar um Certificado do Privacy Manager

Você será notificado de que tem de renovar o Certificado do Privacy Manager quando estiver prestes a expirar:

1. Abra o Privacy Manager e clique em **Certificados**.
2. Clique em **Renovar Certificado**.
3. Cumpra as instruções no ecrã para comprar um novo Certificado do Privacy Manager.

**NOTA:** O processo de renovação do Certificado do Privacy Manager não substitui o seu antigo Certificado do Privacy Manager. Terá de comprar um novo Certificado do Privacy Manager e instalá-lo através dos mesmo procedimentos tal como em Solicitar e instalar um Certificado do Privacy Manager na página 43.

## Definir um Certificado do Privacy Manager predefinido

Apenas os Certificados do Privacy Manager estão visíveis através do Privacy Manager, mesmo que estejam instalados certificados adicionais de outras autoridades de certificação no seu computador.

Para eliminar um certificado do Privacy Manager:

1. Abra o Privacy Manager e clique em **Certificados**.
2. Clique no Certificado do Privacy Manager que queira utilizar como a predefinição e depois em **Definir predefinição**.
3. Clique em **OK**.

**NOTA:** Não tem de utilizar o seu Certificado do Privacy Manager predefinido. Pode seleccionar qualquer um dos seus Certificados do Privacy Manager a utilizar através das várias funcionalidades do Privacy Manager.

## Eliminar um Certificado do Privacy Manager

Se eliminar um Certificado do Privacy Manager, não poderá abrir quaisquer ficheiros ou ver quaisquer dados que tenha encriptado com esse certificado. Se eliminar acidentalmente um Certificado do Privacy Manager, pode-o restaurar utilizando o ficheiro da cópia de segurança que criou quando instalou o certificado. Consulte Restaurar um Certificado do Privacy Manager na página 46 para obter mais informações.

Para eliminar um certificado do Privacy Manager:

1. Abra o Privacy Manager e clique em **Certificados**.
2. Clique no Certificado do Privacy Manager que quer eliminar e depois em **Avançado**.
3. Clique em **Eliminar**.
4. Clique em **OK** quando a caixa de diálogo de confirmação abrir.
5. Clique em **Fechar** e depois em **Aplicar**.

## Restaurar um Certificado do Privacy Manager

Tem de criar uma cópia de segurança do certificado ao instalar o seu Certificado do Privacy Manager. Também pode criar uma cópia de segurança através da página “Migração”. Pode utilizar esta cópia de segurança ao efectuar a migração para outro computador ou restaurar um certificado para o mesmo computador.

1. Abra o Privacy Manager e clique em **Migração**.
2. Clique em **Restaurar**.
3. Na página “Ficheiro de Migração”, clique em **Procurar** para procurar o ficheiro .dppsm que criou durante o processo da cópia de segurança e depois em **Seguinte**.
4. Introduza a palavra-passe utilizada quando criou a cópia de segurança, e clique depois em **Seguinte**.
5. Clique em **Concluir**.
6. Clique em **OK**.

Consulte Instalar um Certificado do Privacy Manager na página 44 ou Efectuar cópia de segurança dos Certificados do Privacy Manager e Contactos Fidedignos na página 61 para obter mais informações.

## Revogar o seu Certificado do Privacy Manager

Se achar que a segurança do seu Certificado do Privacy Manager foi colocada em perigo, pode revogar o seu próprio certificado:

**NOTA:** Um Certificado do Privacy Manager revogado não é eliminado. Pode ainda utilizar o certificado para ver os ficheiros que estejam encriptados.

1. Abra o Privacy Manager e clique em **Certificados**.
2. Clique em **Avançado**.
3. Clique no Certificado do Privacy Manager que quer revogar e depois em **Revogar**.
4. Clique em **OK** quando a caixa de diálogo de confirmação abrir.
5. Efectue a autenticação com o seu método seleccionado de início de sessão de segurança.
6. Siga as instruções no ecrã.

# Gerir Contactos Fidedignos

Os Contactos Fidedignos são os utilizadores com os quais trocou Certificados do Privacy Manager, permitindo-lhe comunicar em segurança uns com os outros.

O Trusted Contacts Manager permite realizar as seguintes tarefas:

- Ver detalhes do Contacto Fidedigno
- Eliminar Contactos Fidedignos
- Verificar estado de revogação dos Contactos Fidedignos (avançado)

## Adicionar Contactos Fidedignos

Adicionar Contactos Fidedignos é um processo com 3 passos:

1. Envia um convite por mensagem de correio electrónico para um destinatário Contacto Fidedigno.
2. O destinatário Contacto Fidedigno responde à mensagem do correio electrónico.
3. Você recebe uma resposta à mensagem de correio electrónico do destinatário Contacto Fidedigno e clique em **Aceitar**.

Pode enviar convites por mensagem de correio electrónico de Contacto Fidedigno a destinatários individuais ou pode enviar o convite para todos os contactos no seu livro de endereços do Microsoft Outlook.

Consulte as secções seguintes para adicionar Contactos Fidedignos.

**NOTA:** Para responder ao seu convite para ser tornar um Contacto Fidedigno, os destinatários Contactos Fidedignos devem ter o Privacy Manager instalado nos seus computadores ou ter o cliente alternativo instalado. Aceda ao site DigitalPersona em http://DigitalPersona.com/PrivacyManager para obter informações sobre como instalar o cliente alternativo.

### Adicionar um Contacto Fidedigno

1. Abra o Privacy Manager e clique em **Trusted Contacts Manager** e depois em **Convidar Contactos**.

   – ou –

   No Microsoft Outlook, clique na seta para baixo ao lado de **Enviar em Segurança** na barra de tarefas e depois em **Convidar Contactos**.

2. Clique no Certificado do Privacy Manager que quer utilizar e depois em **OK** se a caixa do diálogo Seleccionar Certificado surgir no ecrã.
3. Quando a caixa de diálogo Convite de Contacto Fidedigno, leia o texto e clique em **OK**.

   Uma mensagem de correio electrónico é gerada automaticamente.

4. Introduza uma ou mais endereços de correio electrónico dos destinatários que quer adicionar como Contactos Fidedignos.
5. Edite o texto e assine o seu nome (opcional).
6. Clique em **Enviar**.

**NOTA:** Se ainda tiver obtido um Certificado do Privacy Manager, é informado através de uma mensagem de que deve ter um Certificado do Privacy Manager para enviar um pedido de Contacto Fidedigno. Clique em **OK** para iniciar o Assistente do Pedido do Certificado. Consulte Solicitar e instalar um Certificado do Privacy Manager na página 43 para obter mais informações.

7. Efectue a autenticação com o seu método seleccionado de início de sessão de segurança.

**NOTA:** Quando o destinatário Contacto Fidedigno recebe a mensagem de correio electrónico, tem de o abrir e clicar em **Aceitar** no canto inferior direito do mensagem de correio electrónico, e depois em **OK** quando a caixa de diálogo de confirmação surgir no ecrã.

8. Quando receber um e-mail de resposta de um destinatário que aceitou o convite de Contacto Fidedigno, clique em **Aceitar** no canto inferior direito do e-mail.

   Uma caixa de diálogo surge no ecrã, a confirmar que o destinatário foi adicionado com sucesso à lista de Contactos Fidedignos.

9. Clique em **OK**.

### Adicionar Contactos Fidedignos utilizando os contactos do Microsoft Outlook

1. Abra o Privacy Manager e clique em **Trusted Contacts Manager** e depois em **Convidar Contactos**.

   – ou –

   No Microsoft Outlook, clique na seta para baixo ao lado de **Enviar em Segurança** na barra de tarefas e depois em **Convidar todos os meus Contactos do Outlook**.

2. Seleccione os endereços de correio electrónico que quer adicionar como Contactos Fidedignos quando a página “Convite de Contacto Fidedigno” surgir no ecrã e clique em **Seguinte**.

3. Clique em **Concluir** quando a página “Enviar Convite” abrir.

   Uma mensagem de correio electrónico é gerada automaticamente a listar os endereços de correio electrónico do Microsoft Outlook.

4. Edite o texto e assine o seu nome (opcional).

5. Clique em **Enviar**.

**NOTA:** Se ainda tiver obtido um Certificado do Privacy Manager, é informado através de uma mensagem de que deve ter um Certificado do Privacy Manager para enviar um pedido de Contacto Fidedigno. Clique em **OK** para iniciar o Assistente do Pedido do Certificado. Consulte Solicitar e instalar um Certificado do Privacy Manager na página 43 para obter mais informações.

6. Efectue a autenticação com o seu método seleccionado de início de sessão de segurança.

**NOTA:** Quando o destinatário Contacto Fidedigno recebe a mensagem de correio electrónico, tem de o abrir e clicar em **Aceitar** no canto inferior direito do mensagem de correio electrónico, e depois em **OK** quando a caixa de diálogo de confirmação surgir no ecrã.

7. Quando receber um e-mail de resposta de um destinatário que aceitou o convite de Contacto Fidedigno, clique em **Aceitar** no canto inferior direito do e-mail.

   Uma caixa de diálogo surge no ecrã, a confirmar que o destinatário foi adicionado com sucesso à lista de Contactos Fidedignos.

8. Clique em **OK**.

## Visualizar detalhes do Contacto Fidedigno

1. Abra o Privacy Manager e clique em **Contactos Fidedignos**.
2. Clique num Contacto Fidedigno.
3. Clique em **Detalhes do Contacto**.
4. Clique em **OK** quando concluir a visualização dos detalhes.

## Eliminar um Contacto Fidedigno

1. Abra o Privacy Manager e clique em **Contactos Fidedignos**.
2. Clique no Contacto Fidedigno que quer eliminar.
3. Clique em **Eliminar contacto**.
4. Clique em **OK** quando a caixa de diálogo de confirmação abrir.

## Verificar estado de revogação de um Contacto Fidedigno

Para verificar se um Contacto Fidedigno revogou o seu Certificado do Privacy Manager:

1. Abra o Privacy Manager e clique em **Contactos Fidedignos**.
2. Clique num Contacto Fidedigno.
3. Clique no botão **Avançado**.

   A caixa de diálogo Gestão avançada do Contacto Fidedigno surge no ecrã.
4. Clique em **Verificar revogação**.
5. Clique em **Fechar**.

# Tarefas gerais

Pode utilizar o Privacy Manager com os seguintes produtos da Microsoft:

- Microsoft Outlook
- Microsoft Office
- Windows Live Messenger

## Utilizar o Privacy Manager no Microsoft Outlook

Quando o Privacy Manager está instalado, é apresentado um botão Privacidade na barra de tarefas do Microsoft Outlook e um botão Enviar em segurança na barra de tarefas de cada mensagem de correio electrónico do Microsoft Outlook. Quando clica na seta para baixo ao lado do botão **Privacidade** ou **Enviar em segurança**, pode escolher uma das seguintes opções:

- Assinar e Enviar (apenas o botão Enviar em segurança)—Esta opção adiciona uma assinatura digital à mensagem de correio electrónico e envia-a após a autenticação com o seu método seleccionado de início de sessão de segurança.
- Selar para Contactos Fidedignos e Enviar (apenas o botão Enviar em segurança)—Esta opção adiciona uma assinatura digital e encripta a mensagem de correio electrónico e envia-a após a autenticação com o seu método seleccionado de início de sessão de segurança.
- Convidar Contactos—Esta opção permite-lhe enviar um convite de Contacto Fidedigno. Consulte Adicionar um Contacto Fidedigno na página 47 para obter mais informações.
- Convidar Contactos do Outlook—Esta opção permite enviar um convite de Contacto Fidedigno para todos os contactos no seu livro de endereços do Microsoft Outlook. Consulte Adicionar Contactos Fidedignos utilizando os contactos do Microsoft Outlook na página 48 para obter mais informações.
- Abrir o software Privacy Manager—As opções Certificados, Contactos Fidedignos e Definições permitem abrir o software Privacy Manager para adicionar, ver ou alterar as actuais definições. Consulte Configurar o Privacy Manager for Microsoft Outlook na página 50 para obter mais informações.

## Configurar o Privacy Manager for Microsoft Outlook

1. Abra o Privacy Manager, clique em **Definições** e depois no separador **E-mail**.

   – ou –

   Na barra de ferramentas principal do Microsoft Outlook, clique na seta para baixo ao lado da opção **Enviar em Segurança** (**Privacidade** no Outlook 2003) e clique depois em **Definições**.

   – ou –

   Na barra de ferramentas de uma mensagem de correio electrónico do Microsoft, clique na seta para baixo ao lado da opção **Enviar em segurança** e depois em **Definições**.

2. Seleccione as acções que quer efectuar quando enviar uma mensagem de correio electrónico segura e depois clique em **OK**.

### Assinar e enviar uma mensagem de correio electrónico

1. No Microsoft Outlook, clique em **Novo** ou **Responder**.
2. Digite a sua mensagem de correio electrónico.
3. Clique na seta para baixo ao lado da opção **Enviar em segurança** (**Privacidade** no Outlook 2003) e depois em **Assinar e Enviar**.
4. Efectue a autenticação com o seu método seleccionado de início de sessão de segurança.

### Selar e enviar uma mensagem de correio electrónico

As mensagens de correio electrónico seladas que sejam assinadas e seladas (encriptadas) digitalmente só podem ser visualizadas pelas pessoas que escolher da sua lista de Contactos Fidedignos.

Para selar e enviar uma mensagem de correio electrónico para um Contacto Fidedigno:

1. No Microsoft Outlook, clique em **Novo** ou **Responder**.
2. Digite a sua mensagem de correio electrónico.
3. Clique na seta para baixo ao lado da opção **Enviar em segurança** (**Privacidade** no Outlook 2003) e depois em **Selar para Contactos Fidedignos e Enviar**.
4. Efectue a autenticação com o seu método seleccionado de início de sessão de segurança.

### Visualizar uma mensagem de correio electrónico selada

Quando abre uma mensagem de correio electrónico selada, a etiqueta de segurança é exibida no cabeçalho do correio electrónico. A etiqueta de segurança disponibiliza a seguinte informação:

- Que credenciais foram utilizadas para verificar a identidade da pessoa que assinou a mensagem de correio electrónico
- O produto que foi utilizado para verificar as credenciais da pessoa que assinou a mensagem de correio electrónico

## Utilizar o Privacy Manager num documento de Microsoft Office 2007

**NOTA:** O Privacy Manager só pode ser utilizado com documentos do Microsoft Office 2007.

Depois de instalar o seu Certificado do Privacy Manager, é apresentado um botão Assinar e Encriptar no lado direito da barra de ferramentas de todos os documentos do Microsoft Word, Microsoft Excel e Microsoft PowerPoint. Quando clica na seta para baixo ao lado do botão **Assinar e Encriptar**, pode escolher uma das seguintes opções:

- Assinar Documento—Esta opção adiciona a sua assinatura digital ao documento.
- Adicionar linha de assinatura antes de assinar (apenas no Microsoft Word e Microsoft Excel)—Por predefinição, é adicionada uma linha de assinatura quando assina ou encripta um documento do Microsoft Word ou Microsoft Excel. Clique em **Adicionar linha de assinatura** para remover a marca de verificação para desactivar esta opção.
- Encriptar Documento—Esta opção adiciona a sua assinatura digital ao documento e encripta-o.

- Remover Encriptação—Esta opção remove a encriptação do documento.
- Abrir o software Privacy Manager—As opções Certificados, Contactos Fidedignos e Definições permitem abrir o software Privacy Manager para adicionar, ver ou alterar as actuais definições. Consulte Gerir Certificados do Privacy Manager na página 43, Gerir Contactos Fidedignos na página 47 ou Configurar o Privacy Manager for Microsoft Office na página 52 para obter mais informações.

## Configurar o Privacy Manager for Microsoft Office

1. Abra o Privacy Manager, clique em **Definições** e depois no separador **Documentos**.

   – ou –

   Na barra de ferramentas de um documento do Microsoft Office, clique na seta para baixo ao lado de **Assinar e Encriptar** e depois em **Definições**.

2. Seleccione as acções que pretende configurar e, em seguida, clique em **OK**.

## Assinar um documento do Microsoft Office

1. Crie e guarde um documento do Microsoft Word, Microsoft Excel ou Microsoft PowerPoint.
2. Clique na seta para baixo ao lado da opção **Assinar e Encriptar** e depois em **Assinar Documento**.
3. Efectue a autenticação com o seu método seleccionado de início de sessão de segurança.
4. Quando a caixa de diálogo de confirmação surgir no ecrã, leia o texto e clique em **OK**.

Se decidir editar o documento posteriormente, cumpra estes passos:

1. Clique no botão **Office** no canto superior esquerdo do ecrã.
2. Clique em **Preparar** e depois em **Marcar como Final**.
3. Clique em **OK** quando a caixa de diálogo de confirmação abrir e continue a trabalhar.
4. Assine o documento novamente depois de concluir a edição.

## Adicionar uma linha de assinatura ao assinar um documento do Microsoft Word ou Microsoft Excel

O Privacy Manager permite-lhe adicionar uma linha de assinatura quando assina um documento do Microsoft Word ou Microsoft Excel:

1. Crie e guarde um documento do Microsoft Word ou Microsoft Excel.
2. Clique no menu **Início**.
3. Clique na seta para baixo ao lado da opção **Assinar e Encriptar** e depois em **Adicionar linha de assinatura antes de assinar**.

**NOTA:** Quando selecciona esta opção, surge uma marca de verificação ao lado da opção Adicionar linha de assinatura antes de assinar. Por predefinição, esta opção está activada.

4. Clique na seta para baixo ao lado da opção **Assinar e Encriptar** e depois em **Assinar Documento**.

5. Efectue a autenticação com o seu método seleccionado de início de sessão de segurança.

### Adicionar assinaturas sugeridas a um documento do Microsoft Word ou Microsoft Excel

Pode adicionar mais do que uma linha de assinatura ao documento nomeando assinaturas sugeridas. Uma assinatura sugerida é um utilizador designado pelo proprietário de um documento do Microsoft Word ou Microsoft Excel para adicionar uma linha de assinatura ao documento. As assinaturas sugeridas podem ser você ou outra pessoa que queira que assine o seu documento. Por exemplo, se preparar um documento que precisa de ser assinado por todos os membros do seu departamento, pode incluir linhas de assinatura para esses utilizadores no fundo da página final do documento com instruções para assinar até uma data específica.

Para adicionar uma assinatura sugerida a um documento do Microsoft Word ou Microsoft Excel:

1. Crie e guarde um documento do Microsoft Word ou Microsoft Excel.

2. Clique no menu **Introduzir**.

3. No grupo **Texto** na barra de ferramentas, clique na seta ao lado da opção **Linha de assinatura** e depois em **Fornecedor da assinatura do Privacy Manager**.

   É apresentada a caixa de diálogo Configuração da Assinatura.

4. Introduza o nome da assinatura sugerida na caixa debaixo da opção **Assinatura sugerida**.

5. Introduza uma mensagem para esta assinatura sugerida na caixa debaixo da opção **Instruções para a assinatura**.

   **NOTA:** Esta mensagem surgirá em vez de um título, e é eliminada ou substituída pelo título do utilizador quando o documento for assinado.

6. Seleccione a caixa de verificação **Mostrar data da assinatura na linha de assinatura** para apresentar a data.

7. Seleccione a caixa de verificação **Mostrar título da assinatura na linha de assinatura** para apresentar o título.

   **NOTA:** Como o proprietário do documento atribui assinaturas sugeridas para o seu documento, se as caixas de verificação **Mostrar data de assinatura na linha de assinatura** e/ou **Mostrar título da assinatura na linha de assinatura'** não forem seleccionadas, a assinatura sugerida não poderá apresentar a data e/ou título na linha de assinatura mesmo que as definições do documento da assinatura sugerida estiverem configuradas para o fazer.'

8. Clique em **OK**.

### Adicionar uma linha de assinatura da assinatura sugerida

Quando as assinaturas sugeridas abrem o documento, irão ver o seu nome entre parêntesis, o que indica que a sua assinatura é necessária.

Para assinar o documento:

1. Clique duas vezes na linha de assinatura apropriada.

2. Efectue a autenticação com o seu método seleccionado de início de sessão de segurança.

A linha de assinatura será apresentada de acordo com as definições especificadas pelo proprietário do documento.

## Encriptar um documento do Microsoft Office

Pode encriptar um documento do Microsoft Office document para si e para os seus Contactos Fidedignos. Quando encripta um documento e o fecha, você e os Contacto(s) Fidedigno(s) que seleccionar na lista têm de o autenticar antes de o abrir.

Para encriptar um documento do Microsoft Office:

1. Crie e guarde um documento do Microsoft Word, Microsoft Excel ou Microsoft PowerPoint.
2. Clique no menu **Início**.
3. Clique na seta para baixo ao lado da opção **Assinar e Encriptar** e depois em **Encriptar Documento**.

   Surge a caixa de diálogo Seleccionar Contactos Fidedignos.
4. Clique no nome de um Contacto Fidedigno que poderá abrir o documento e ver o seu conteúdo.

**NOTA:** Prima ininterruptamente a tecla ctrl e clique nos nomes individuais para seleccionar múltiplos nomes de Contactos Fidedignos.

5. Clique em **OK**.

Se decidir editar o documento posteriormente, cumpra os passos Remover a encriptação de um documento do Microsoft Office na página 54. Pode editar o documento quando remover a encriptação. Cumpra os passos indicados nesta secção para encriptar o documento novamente.

## Remover a encriptação de um documento do Microsoft Office

Quando remover encriptação de um documento do Microsoft Office, você e os seus Contactos Fidedignos já não têm de efectuar a autenticação para abrir e ver o conteúdo do documento.

Para remover a encriptação de um documento do Microsoft Office:

1. Abra um documento encriptado do Microsoft Word, Microsoft Excel ou Microsoft PowerPoint.
2. Efectue a autenticação com o seu método seleccionado de início de sessão de segurança.
3. Clique no menu **Início**.
4. Clique na seta para baixo ao lado da opção **Assinar e Encriptar** e depois em **Remover Encriptação**.

## Enviar um documento do Microsoft Office encriptado

Pode anexar um documento do Microsoft Office encriptado a uma mensagem de correio electrónico sem assinar ou encriptar a mensagem de correio electrónico propriamente dita. Para fazer isto, crie e envie uma mensagem de correio electrónico com um documento assinado ou encriptado tal como faria com uma mensagem de correio electrónico normal com um anexo.

Mas, para uma melhor segurança, recomendamos que encripte a mensagem de correio electrónico ao anexar um documento do Microsoft Office assinado ou encriptado.

Para enviar uma mensagem de correio electrónico selada com um documento do Microsoft Office assinado e/ou encriptado, cumpra os seguintes passos:

1. No Microsoft Outlook, clique em **Novo** ou **Responder**.
2. Digite a sua mensagem de correio electrónico.
3. Anexe o documento do Microsoft Office.
4. Consulte Selar e enviar uma mensagem de correio electrónico na página 51 para obter mais instruções.

### Visualizar um documento do Microsoft Office assinado

**NOTA:** Não tem de ter um Certificado do Privacy Manager para ver um documento do Microsoft Office assinado.

Um ícone da Assinatura Digital surge na barra do estado no fundo da janela do documento quando abrir um documento do Microsoft Office assinado.

1. Clique no ícone das **Assinaturas Digitais** para alternar a visualização da caixa de diálogo das Assinaturas que apresenta o nome de todos os utilizadores que assinaram o documento e a data em que o fizeram.
2. Clique no botão direito do rato sobre um nome na caixa de diálogo das Assinaturas e seleccione a opção Detalhes da Assinatura para ver detalhes adicionais acerca de cada uma das assinaturas.

### Visualizar um documento do Microsoft Office encriptado

Para ver um documento do Microsoft Office encriptado de outro computador, tem de instalar o Privacy Manager nesse computador. Para além disso, tem de restaurar o Certificado do Privacy Manager utilizado para encriptar o ficheiro.

Um Contacto Fidedigno que queira ver um documento do Microsoft Office encriptado tem de ter um Certificado do Privacy Manager, e este último deve estar instalado no seu computador. Além disso, o Contacto Fidedigno deve ser seleccionado pelo proprietário do documento do Microsoft Office encriptado.

## Utilizar o Privacy Manager no Windows Live Messenger

O Privacy Manager adiciona as seguintes funcionalidades de comunicações seguras ao Windows Live Messenger:

- **Conversação segura**—As mensagens são transmitidas utilizando o protocolo SSL/TLS (Secure Sockets Layer/Transport Layer Security) em detrimento do protocolo XML, a mesma tecnologia que assegura a segurança das transacções comerciais electrónicas.
- **Identificação do destinatário**—Pode verificar a presença e identidade de uma pessoa antes de enviar uma mensagem.
- **Mensagens assinadas**—Pode assinar electronicamente as suas mensagens. Neste caso, se a mensagem for utilizada indevidamente, será assinalada como inválida quando for recebida pelo destinatário.
- **Funcionalidade Ocultar/Mostrar**—Pode ocultar qualquer uma ou todas as mensagens na janela do Privacy Manager Chat. Também pode enviar uma mensagem com o conteúdo oculto. É necessária a autenticação para apresentar a mensagem.

- **Histórico de conversação segura**—Os registos das suas sessões de conversação são encriptados antes de serem memorizados e exigem autenticação para serem visualizados.
- **Bloqueio/Desbloqueio automático**—Pode bloquear e desbloquear a janela do Privacy Manager Chat ou configurá-lo para se bloquear automaticamente após um período de inactividade especificado.

## Iniciar uma sessão do Privacy Manager Chat

**NOTA:** Para utilizar o Privacy Manager Chat, ambas as partes devem ter instalado o Privacy Manager bem como um Certificado do Privacy Manager. Consulte Solicitar e instalar um Certificado do Privacy Manager na página 43 para obter mais detalhes acerca da instalação de um Certificado do Privacy Manager.

1. Para iniciar o Privacy Manager Chat no Windows Live Messenger, realize um dos seguintes procedimentos:

   a. Clique no botão direito do rato sobre um contacto online no Live Messenger e seleccione depois a opção **Iniciar uma actividade**.

   b. Clique em **Iniciar Conversação**.

   – ou –

   a. Faça duplo clique sobre um contacto online no Live Messenger, e em seguida seleccione o menu **Ver uma lista de actividades**.

   b. Clique em **Acção** e, em seguida, em **Iniciar Conversação**.

   – ou –

   a. Clique no botão direito do rato sobre o ícone ProtectTools na área de notificação, clique em **Privacy Manager for HP ProtectTools** e seleccione depois **Iniciar Conversação**.

   b. No Live Messenger, clique em **Acções: Iniciar uma actividade** e seleccione depois **Privacy Manager Chat**.

   **NOTA:** Cada utilizador deve estar online no Live Messenger e os utilizadores devem ser apresentados na janela online do seu Live Messenger. Clique para seleccionar um utilizador online.

   O Privacy Manager envia um convite para o contacto para iniciar o Privacy Manager Chat. A janela do Privacy Manager Chat abre quando o contacto convidado aceitar o convite. Se o contacto convidado não tiver o Privacy Manager instalado, ser-lhe-á pedido que o transfira.

2. Clique em **Iniciar** para iniciar uma conversação segura.

## Configurar o Privacy Manager for Windows Live Messenger

1. Clique no botão **Definições** no Privacy Manager Chat.

   – ou –

   No Privacy Manager, clique em **Definições** e depois no separador **Conversação**.

   – ou –

   Clique no botão **Definições** no Privacy Manager Live Messenger History Viewer.

2. Seleccione um número na caixa**Bloquear sessão após _ minutos de inactividade** para especificar o período de tempo de espera antes do Privacy Manager Chat bloquear a sua sessão.

3. Clique em **Procurar** para procurar uma pasta e depois em **OK** para especificar uma pasta do histórico para as suas sessões de conversação.

4. Para encriptar e memorizar automaticamente as suas sessões quando as fechar, seleccione a caixa de verificação **Guardar automaticamente o histórico de conversação segura**.

5. Clique em **OK**.

## Conversar na janela do Privacy Manager Chat

Uma janela do Privacy Manager Chat abre no Windows Live Messenger depois de iniciar o Privacy Manager Chat. O uso do Privacy Manager Chat é semelhante à utilização básica do Windows Live Messenger, excepto que as seguintes funcionalidades adicionais estão disponíveis na janela do Privacy Manager Chat:

- **Guardar**–Clique neste botão para guardar a sessão de chat na pasta especificada nas definições de configuração. Também pode configurar o Privacy Manager Chat para guardar automaticamente cada sessão quando for encerrado.
- **Ocultar tudo** e **Mostrar tudo**–Clique no botão apropriado para expandir ou reduzir as mensagens apresentadas na janela Comunicações Seguras. Também pode ocultar ou apresentar mensagens individuais clicando no cabeçalho da mensagem.
- **Estás aí?**–Clique neste botão para solicitar a autenticação do seu contacto.
- **Bloquear**–Clique aqui para fechar a janela do Privacy Manager Chat eregressar à janela Chat Entry. Clique em **Retomar sessão** para apresentar a janela Secure Communications novamente, e autentique com o método de segurança do início da sessão escolhido.
- **Enviar**–Clique neste botão para enviar uma mensagem encriptada ao seu contacto.
- **Enviar assinado**–Seleccione esta caixa de verificação para assinar e encriptar electronicamente as suas mensagens. Neste caso, se a mensagem for utilizada indevidamente, será assinalada como inválida quando for recebida pelo destinatário. Tem de efectuar a autenticação sempre enviar uma mensagem assinada.
- **Enviar oculto**–Seleccione esta caixa de verificação para encriptar e enviar uma mensagem que apresenta apenas o cabeçalho. Para o contacto ler o conteúdo da mensagem tem de a autenticar.

## Visualizar histórico da conversação

O Privacy Manager Chat: Live Messenger History Viewer apresenta os ficheiros da sessão do Privacy Manager Chat. Clique em **Guardar** na janela do Privacy Manager Chat para guardar as sessões ou configure a opção para guardar automaticamente no separador Chat no Privacy Manager. No Viewer,

cada sessão apresenta o (encriptado) Nome do Contacto, e a data e a hora de início e fim da sessão. As sessões são apresentadas, por predefinição, para todas as contas de correio electrónico configuradas. Pode usar o menu **Apresentar histórico de** para seleccionar apenas contas específicas a consultar.

O visualizador permite efectuar as seguintes tarefas:

- Revelar todas as sessões na página 58
- Revelar sessões de uma conta específica na página 58
- Ver a identificação de uma sessão na página 59
- Ver uma sessão na página 59
- Procurar texto específico nas sessões na página 59
- Eliminar uma sessão na página 59
- Adicionar ou remover colunas na página 60
- Sessões apresentadas com filtro na página 60

Para iniciar o Live Messenger History Viewer:

▲ Na área de notificação, na extrema direita da barra de tarefas, clique no botão direito do rato sobre o ícone do **HP ProtectTools** e em **Privacy Manager: for HP ProtectTools** e depois em **Live Messenger History Viewer**.

– ou –

▲ Numa sessão de Conversação, clique em **Visualizador do Histórico** ou **Histórico**.

### Revelar todas as sessões

A opção Revelar todas as sessões apresenta o Nome de Ecrã do Contacto desencriptado da(s) sessão (ões) actualmente seleccionada(s) e todas as sessões na mesma conta.

Para revelar todas as suas sessões memorizadas do históricoda conversação:

1. No Live Messenger History Viewer, clique no botão direito do rato sobre qualquer sessão e seleccione depois a opção **Revelar todas as sessões**.
2. Efectue a autenticação com o seu método seleccionado de início de sessão de segurança.

   Os Nomes de Ecrã do Contacto são desencriptados.
3. Clique duas vezes sobre qualquer sessão para ver o seu conteúdo.

### Revelar sessões de uma conta específica

A opção Revelar uma sessão apresenta o Nome de Ecrã do Contacto desencriptado da sessão actualmente seleccionada.

Para revelar uma sessão específica do histórico de conversação:

1. No Live Messenger History Viewer, clique no botão direito do rato sobre qualquer sessão e seleccione depois a opção **Revelar sessão**.
2. Efectue a autenticação com o seu método seleccionado de início de sessão de segurança.

   O Nome de Ecrã do Contacto é desencriptado.
3. Clique duas vezes sobre a sessão revelada para ver o seu conteúdo.

**NOTA:** As sessões adicionais encriptadas com o mesmo certificado apresentam um ícone desbloqueado, indicando que as pode ver clicando duas vezes em qualquer uma dessas sessões sem autenticação adicional. As sessões encriptadas com um certificado diferente apresentam um ícone bloqueado, que indica que é necessário efetuar outra autenticação para essas sessões antes de visualizar os Nomes de Ecrã do Contacto ou conteúdo.

### Ver a identificação de uma sessão

Para ver uma identificação de uma sessão:

- No Live Messenger History Viewer, clique no botão direito do rato sobre qualquer sessão e seleccione depois a opção **Ver identificação da sessão**.

### Ver uma sessão

Visualizar uma sessão abre o ficheiro com vista à visualização. Se a sessão não tiver sido revelada (apresentando o Nome de Ecrã do Contacto desencriptada) anteriormente, é revelada simultaneamente.

Para ver uma sessão do histórico do Live Messenger:

1. No Live Messenger History Viewer, clique no botão direito do rato sobre qualquer sessão e seleccione depois a opção **Ver**.
2. Se solicitado, efectue a autenticação com o seu método seleccionado de início de sessão de segurança.

   O conteúdo da sessão é desencriptado.

### Procurar texto específico nas sessões

Só pode procurar texto em sessões reveladas (desencriptadas) apresentadas na janela do visualizador. Estas são as sessões nas quais o Nome de Ecrã do Contacto é apresentado em texto normal.

Para procurar texto em sessões do histórico da conversação:

1. Clique no botão **Procurar** no Live Messenger History Viewer.
2. Introduza o texto a procurar, configure quaisquer parâmetros de procura desejados e clique em **OK**.

   As sessões que tiverem o texto são assinaladas na janela do visualizador.

### Eliminar uma sessão

1. Seleccione uma sessão do histórico da conversação.
2. Clique em **Eliminar**.

### Adicionar ou remover colunas

Por predefinição, as 3 colunas mais utilizadas são apresentadas no Live Messenger History Viewer. Pode adicionar colunas adicionais à visualização ou pode remover colunas da visualização.

Para adicionar colunas à visualização:

1. Clique no botão direito do rato sobre qualquer cabeçalho da coluna e seleccione a opção **Adicionar/Remover colunas**.
2. Seleccione um cabeçalho da coluna no painel esquerdo e clique depois em **Adicionar** para o mover para o painel direito.

Para remover colunas à visualização:

1. Clique no botão direito do rato sobre qualquer cabeçalho da coluna e seleccione a opção **Adicionar/Remover colunas**.
2. Seleccione um cabeçalho da coluna no painel direito e clique depois em **Remover** para o mover para o painel esquerdo.

### Sessões apresentadas com filtro

É apresentada uma lista das sessões de todas as suas contas no Live Messenger History Viewer. Também pode filtrar as sessões apresentadas para o seguinte:

- Contas específicas. Para obter informações detalhadas, consulte Apresentar sessões de uma conta específica na página 60.
- Intervalo de datas. Para obter informações detalhadas, consulte Apresentar sessões de um intervalo de datas na página 60.
- Pastas diferentes. Para obter informações detalhadas, consulte Apresentar sessões que são guardadas numa pasta que não a pasta predefinida na página 60.

### Apresentar sessões de uma conta específica

▲ No Live Messenger History Viewer, seleccione uma conta do menu **Apresentar histórico de**.

### Apresentar sessões de um intervalo de datas

1. Clique no ícone do **Filtro avançado** no Live Messenger History Viewer.

   Abre-se uma caixa de diálogo Filtro avançado.
2. Seleccione a caixa de verificação **Apresentar apenas sessões de um intervalo de datas especificado**.
3. Introduza o dia, mês e/ou ano nas caixas de verificação **Desde** e **Até** ou clique na seta ao lado do calendário para seleccionar as datas.
4. Clique em **OK**.

### Apresentar sessões que são guardadas numa pasta que não a pasta predefinida

1. Clique no ícone do **Filtro avançado** no Live Messenger History Viewer.
2. Seleccione a caixa de verificação **Utilizar uma pasta alternativa de ficheiros do histórico**.

3. Introduza a localização da pasta ou clique em **Procurar** para procurar uma pasta.
4. Clique em **OK**.

# Tarefas avançadas

## Migrar certificados do Privacy Manager e Contactos de confiança para um computador diferente

Pode efectuar a migração em segurança dos seus Certificados do Privacy Manager e dos Contactos Fidedignos para outro computador ou efectuar uma cópia de segurança para guardar para uso futuro. Para tal, efectue uma cópia de segurança dos dados como um ficheiro protegido pela palavra-passe para uma localização na rede ou qualquer dispositivo de armazenamento amovível e restaure depois o ficheiro para o novo computador.

### Efectuar cópia de segurança dos Certificados do Privacy Manager e Contactos Fidedignos

Para efectuar uma cópia de segurança dos seus Certificados do Privacy Manager e Contactos Fidedignos para um ficheiro protegido por palavra-passe, cumpra estes passos:

1. Abra o Privacy Manager e clique em **Migração**.
2. Clique em **Cópia de Segurança**.
3. Seleccione as categorias de dados a serem incluídas no ficheiro de migração na página “Seleccionar Dados” e clique depois em **Seguinte**.
4. Introduza um nome de ficheiro na página “Ficheiro de Migração” ou clique em **Procurar** para procurar uma localização e depois em **Seguinte**.
5. Introduza e confirme uma palavra-passe e, em seguida, clique em **Seguinte**.

**NOTA:** Armazene esta palavra-passe num local seguro, porque precisará dela ao restaurar o ficheiro de migração.

6. Efectue a autenticação com o seu método seleccionado de início de sessão de segurança.
7. Na página “Ficheiro de Migração Guardado” clique em **Concluir**.

### Restaurar os Certificados do Privacy Manager e Contactos Fidedignos

Para restaurar os seus Certificados do Privacy Manager e Contactos Fidedignos num computador diferente como parte do processo de migração ou no mesmo computador, cumpra estes passos:

1. Abra o Privacy Manager e clique em **Migração**.
2. Clique em **Restaurar**.
3. Na página “Ficheiro de Migração” clique em **Procurar** para procurar um ficheiro e depois em **Seguinte**.
4. Introduza a palavra-passe utilizada quando criou o ficheiro da cópia de segurança, e clique depois em **Seguinte**.
5. Na página “Ficheiro de Migração” clique em **Concluir**.

## Administração central do Privacy Manager

A instalação do Privacy Manager pode fazer parte de uma instalação centralizada, que tenha sido personalizada pelo administrador. Uma ou mais das seguintes funcionalidades pode estar activada ou desactivada:

- **Política de utilização do certificado**—Pode ser restringido a utilizar certificados do Privacy Manager emitidos pela Comodo, ou pode ser autorizado a utilizar certificados digitais emitidos por outras autoridades de certificação.
- **Política de encriptação**—As capacidades de encriptação podem ser activadas ou desactivadas individualmente no Microsoft Office ou Outlook e no Windows Live Messenger.

# 9 File Sanitizer para o HP ProtectTools

O File Sanitizer é uma ferramenta que lhe permite fragmentar activos em segurança (informações pessoais ou ficheiros, dados históricos ou relacionados com a Web ou outros componentes dos dados) no seu computador e limpe periodicamente a sua unidade do disco rígido.

**NOTA:** Esta versão do File Sanitizer suporta apenas a unidade do disco rígido do sistema.

# Fragmentar

A fragmentação é diferente de uma eliminação padrão do Windows® (também denominada como uma eliminação simples no File Sanitizer) no sentido em que a fragmentação de um activo com o File Sanitizer invoca um algoritmo que obscurece os dados, o que torna praticamente impossível recuperar o activo original. Uma eliminação simples do Windows pode deixar o ficheiro (ou activo) intacto na unidade do disco rígido ou num estado no qual os métodos forênsicos podem ser utilizados para recuperar o ficheiro (ou activo).

Uma lista de activos predefinidos e um método de fragmentação são automaticamente seleccionados para fragmentação quando escolhe um perfil de fragmentação (Segurança elevada, Segurança média ou Baixa segurança). Também pode personalizar um perfil de fragmentação, que permite especificar o número de ciclos de fragmentação, os activos a incluir para fragmentação, os activos a confirmar antes da fragmentação e os activos a excluir da fragmentação. Para obter mais informações, consulte Seleccionar ou criar um perfil de fragmentação na página 67.

Pode configurar um calendário automático de fragmentação, e também pode fragmentar manualmente os activos sempre que quiser. Para obter mais informações, consulte Definir um calendário de fragmentação na página 66, Fragmentar um activo manualmente na página 71 ou Fragmentar todos os itens seleccionados manualmente na página 71.

**NOTA:** Um ficheiro .dll é fragmentado e removido do sistema apenas se tiver sido movido para a Reciclagem.

# Limpeza do espaço livre

A eliminação de um activo no Windows não remove completamente o conteúdo do activo da unidade do disco rígido. O Windows só elimina a referência para o activo. O conteúdo do activo permanece na unidade do disco rígido até ser substituído por outro activo nessa mesma área na unidade do disco rígido com novas informações.

A limpeza do espaço livre permite escrever em segurança dados aleatórios sobre activos eliminados, impedindo os utilizadores de visualizar o conteúdo original do activo eliminado.

**NOTA:** A limpeza do espaço livre destina-se aos activos que eliminar com a Reciclagem do Windows ou quando eliminar manualmente um activo. A limpeza do espaço livre não disponibiliza segurança adicional a activos fragmentados.

Pode definir um calendário automático de limpeza do espaço livre ou pode activar manualmente a limpeza do espaço livre utilizando o ícone do **HP ProtectTools** na área de notificação na extrema direita da barra de tarefas. Para obter mais informações, consulte Definição de um calendário de limpeza do espaço livre na página 67 ou Activar a limpeza do espaço livre manualmente na página 72.

# Procedimentos de configuração

## Abrir File Sanitizer

Para abrir o File Sanitizer:

1. Clique em **Iniciar**, **Todos os Programas**, **HP** e depois em **HP ProtectTools Security Manager**.
2. Clique em **File Sanitizer**.

– ou –

▲ Clique duas vezes no ícone do **File Sanitizer** situado no ambiente de trabalho.

– ou –

▲ Clique com o botão direito do rato no ícone do **HP ProtectTools** na área de notificação, na extremidade mais à direita da barra de tarefas, e, em seguida, clique em **File Sanitizer** e depois em **Abrir File Sanitizer**.

## Definir um calendário de fragmentação

**NOTA:** Para obter informações acerca da selecção de um perfil de fragmentação predefinido ou criar um perfil de fragmentação, consulte Seleccionar ou criar um perfil de fragmentação na página 67.

**NOTA:** Para obter informações sobre como fragmentar activos manualmente, consulte Fragmentar um activo manualmente na página 71.

1. Abra o File Sanitizer e clique em **Fragmentar**.
2. Seleccione uma opção de fragmentação:
   - **Encerramento do Windows**—Escolha esta opção para fragmentar todos os activos seleccionados quando encerrar o Windows.

     **NOTA:** Quando selecciona esta opção, surge uma caixa de diálogo ao encerrar a perguntar se quer continuar a fragmentar os activos seleccionados ou se quer ignorar o procedimento. Clique em **Sim** para passar o procedimento de fragmentação ou em **Não** para continuar a fragmentar.

   - **Abertura do browser da Web**—Escolha esta opção para fragmentar todos os activos relacionados com a Web, como histórico de URLs do browser, quando abrir um browser da Web.
   - **Saída do browser da Web**—Escolha esta opção para fragmentar todos os activos relacionados com a Web, como histórico de URLs do browser, quando fechar um browser da Web.
   - **Sequência de teclas**—Escolha esta opção para iniciar a fragmentação com uma sequência de teclas.
   - **Scheduler**—Seleccione a caixa de verificação **Activar Scheduler**, introduza a sua palavra-passe do Windows e em seguida um dia e hora para fragmentar os activos seleccionados.

   **NOTA:** Um ficheiro .dll é fragmentado e removido do sistema apenas se tiver sido movido para a Reciclagem.

3. Clique em **Apply** (Aplicar) e, em seguida, clique em **OK**.

## Definição de um calendário de limpeza do espaço livre

**NOTA:** A limpeza do espaço livre destina-se aos activos que eliminar com a Reciclagem do Windows ou para activos eliminados manualmente. A limpeza do espaço livre não disponibiliza segurança adicional a activos fragmentados.

Para definir um calendário de limpeza do espaço livre:

1. Abra o File Sanitizer e clique em **Limpeza do espaço livre**.
2. Seleccione a caixa de verificação **Activar Scheduler**, introduza a sua palavra-passe do Windows e depois um dia e hora aos quais iniciar a limpeza da sua unidade do disco rígido.
3. Clique em **Apply** (Aplicar) e, em seguida, clique em **OK**.

**NOTA:** A operação de limpeza do espaço livre pode demorar muito tempo. Embora a limpeza do espaço livre seja efectuada no fundo, o desempenho do computador pode ser mais lento por causa do aumento da utilização do processador.

## Seleccionar ou criar um perfil de fragmentação

Pode especificar um método de eliminação e seleccionar os activos para fragmentar seleccionando um perfil predefinido ou criando o seu próprio perfil.

### Seleccionar um perfil de fragmentação predefinido

Um método de eliminação e uma lista de activos predefinidos são automaticamente seleccionados para fragmentação quando escolhe um perfil de fragmentação predefinido (Segurança elevada, Segurança média ou Baixa segurança). Pode clicar no botão **Ver Detalhes** para ver a lista predefinida dos activos seleccionados para fragmentação.

Para seleccionar um perfil de fragmentação predefinido:

1. Abra o File Sanitizer e clique em **Definições**.
2. Clique num perfil de fragmentação predefinido.
3. Clique em **Ver Detalhes** para ver a lista de activos seleccionados para fragmentação.
4. Em **Fragmentar o seguinte**, seleccione a caixa de verificação ao lado de cada activo que quer confirmar antes de fragmentar.
5. Clique em **Aplicar** e, em seguida, em **OK**.

## Personalizar um perfil de fragmentação

Quando cria um perfil de fragmentação, especifica o número de ciclos de fragmentação, os activos a incluir para fragmentação, os activos a confirmar antes da fragmentação e os activos a excluir da fragmentação:

1. Abra o File Sanitizer e clique em **Definições**, **Definições de segurança avançadas** e depois em **Ver Detalhes**.
2. Especifique o número de ciclos de fragmentação.

**NOTA:** O número seleccionado de ciclos de fragmentação é efectuado para cada activo. Por exemplo, se escolher 3 ciclos de fragmentação, um algoritmo que obscurece os dados é executado 3 vezes separadamente. Se escolher os ciclos de fragmentação de segurança elevada, a fragmentação pode demorar um período de tempo significativo; mas quando mais elevado for o número de ciclos de fragmentação especificado, menos provável será que consiga recuperar os dados.

3. Seleccione os activos que quer fragmentar:
   a. Em **Opções de Fragmentação Disponíveis**, clique num activo e depois em **Adicionar**.
   b. Clique em **Adicionar Opção Personalizada** para adicionar um acitov personalizado, e depois procure ou digite o caminho até ao nome ou pasta do ficheiro. Clique em **Abrir** e depois em **OK**. Em **Opções de Fragmentação Disponíveis**, clique no activo personalizado e depois em **Adicionar**.

**NOTA:** Clique num activo e depois em **Eliminar** para o remover das opções de fragmentação disponíveis.

4. Em **Fragmentar o seguinte**, seleccione a caixa de verificação ao lado de cada activo que quer confirmar antes de fragmentar.

**NOTA:** Clique num activo e depois em **Remover** para o remover da lista de fragmentação.

5. Em **Não fragmentar o seguinte**, clique em **Adicionar** e depois procure ou digite o caminho até ao nome ou pasta do ficheiro para proteger ficheiros ou pastas da fragmentação automática. Clique em **Abrir** e depois em **OK**.

**NOTA:** Clique num activo e depois em **Eliminar** para o remover da lista de exclusões.

6. Clique em **Aplicar** e depois em **OK** quando concluir a configuração do perfil de fragmentação.

## Personalizar um perfil de eliminação simples

O perfil de eliminação simples efectua uma eliminação de activos padrão sem fragmentação. Quando personalizar um perfil de eliminação simples, especifica que activos incluir para uma eliminação simples, os activos a confirmar antes de executar uma eliminação simples e os activos a excluir de uma eliminação simples.

**NOTA:** A limpeza do espaço livre pode ser efectuada ocasionalmente nos activos que tenham sido eliminados manualmente ou atravésda Reciclagem do Windows se usar a opção de eliminação simples.

Para personalizar um perfil de eliminação simples:

1. Abra o File Sanitizer e clique em **Definições**, **Definição de Eliminação Simples** e depois em **Ver Detalhes**.
2. Seleccione os activos que quer eliminar:
   a. Em **Opções de Eliminação Disponíveis**, clique num activo e depois em **Adicionar**.
   b. Clique em **Adicionar Opção Personalizado** para adicionar um activo personalizado, introduza um nome do ficheiro ou da pasta e clique em **OK**. Clique no activo personalizado e depois em **Adicionar**.

**NOTA:** Clique num activo e depois em **Eliminar** para o eliminar das opções de eliminação disponíveis.

3. Em **Eliminar o seguinte**, seleccione a caixa de verificação ao lado de cada activo que quer confirmar antes de eliminar.

**NOTA:** Clique num activo e depois em **Remover** para o remover da lista de eliminação.

4. Em **Não fragmentar os seguintes**, clique em **Adicionar** para seleccionar os activos específicos que pretende excluir da fragmentação.

**NOTA:** Clique num activo e depois em **Eliminar** para o remover da lista de exclusões.

5. Clique em **Aplicar** e depois em **OK** quando concluir a configuração do perfil de eliminação simples.

# Tarefas gerais

Pode utilizar o File Sanitizer para efectuar as seguintes tarefas:

- Use uma sequência de teclas para iniciar a fragmentação—Esta funcionalidade permite criar uma sequência de teclas (por exemplo, ctrl+alt+s) para iniciar a fragmentação. Para obter informações detalhadas, consulte Utilizar uma sequência de teclas para iniciar a fragmentação na página 70.
- Use o ícone do File Sanitizer para iniciar a fragmentação—É semelhante à funcionalidade arrastar e largar do Windows. Para obter informações detalhadas, consulte Utilizar o ícone do File Sanitizer na página 71.
- Fragmentar manualmente um activo específico ou todos os activos seleccionados—Estas funcionalidades permitem fragmentar manualmente sem ser necessário esperar pela invocação do calendário de fragmentação regular. Para obter informações detalhadas, consulte Fragmentar um activo manualmente na página 71 ou Fragmentar todos os itens seleccionados manualmente na página 71.
- Active manualmente a limpeza do espaço livre—Esta funcionalidade permite activar manualmente a limpeza do espaço livre. Para obter informações detalhadas, consulte Activar a limpeza do espaço livre manualmente na página 72.
- Abortar uma operação de fragmentação ou limpeza do espaço livre—Esta funcionalidade permite interromper a operação de fragmentação ou limpeza do espaço livre. Para obter informações detalhadas, consulte Abortar uma operação de fragmentação ou limpeza do espaço livre na página 72.
- Ver os ficheiros de registo—Esta funcionalidade permite ver os ficheiros do registo de fragmentação e limpeza do espaço livre, que contêm quaisquer erros ou falhas da última operação de fragmentação ou limpeza do espaço livre. Para obter informações detalhadas, consulte Visualizar os ficheiros do registo na página 72.

**NOTA:** A operação de fragmentação ou limpeza do espaço livre pode demorar um período de tempo significativo. Embora a fragmentação e a limpeza do espaço livre seja efectuada no fundo, o desempenho do computador pode ser mais lento por causa do aumento da utilização do processador.

## Utilizar uma sequência de teclas para iniciar a fragmentação

Para especificar uma sequência de teclas, siga estes passos:

1. Abra o File Sanitizer e clique em **Fragmentar**.
2. Seleccione a caixa de verificação **Sequência de teclas**.
3. Introduza um carácter na caixa disponível.
4. Seleccione a caixa **CTRL** ou a caixa **ALT** e depois seleccione a caixa **SHIFT**.

   Por exemplo, para iniciar a fragmentação automática com a tecla s e as teclas ctrl+shift, introduza s na caixa e seleccione depois as opções **CTRL** e **SHIFT**.

**NOTA:** Certifique-se de que selecciona uma sequência de teclas diferente das outras sequências de teclas configuradas.

Para iniciar a fragmentação com uma sequência de teclas:

1. Prima a tecla shift e a tecla ctrl ou a tecla alt (ou a combinação que especificou) enquanto prime o carácter seleccionado.
2. Clique em **Sim** se a caixa de diálogo de confirmação surgir no ecrã.

## Utilizar o ícone do File Sanitizer

△ **CUIDADO:** Não é possível recuperar os activos fragmentados. Considere cuidadosamente os itens que seleccionar para fragmentação manual.

1. Navegue até ao documento ou pasta que quer fragmentar.
2. Arraste o activo ao ícone do File Sanitizer no ambiente de trabalho.
3. Clique em **OK** quando a caixa de diálogo de confirmação abrir.

## Fragmentar um activo manualmente

△ **CUIDADO:** Não é possível recuperar os activos fragmentados. Considere cuidadosamente os itens que seleccionar para fragmentação manual.

1. Clique com o botão direito do rato no ícone do **HP ProtectTools** na área de notificação, na extremidade mais à direita da barra de tarefas, e, em seguida, clique em **File Sanitizer** e depois em **Fragmentar Um**.
2. Navegue até ao activo e clique em **OK** quando a caixa de diálogo Procurar.

**NOTA:** O activo seleccionado pode ser um ficheiro único ou pasta.

3. Clique em **OK** quando a caixa de diálogo de confirmação abrir.

– ou –

1. Clique no botão direito do rato sobre o ícone do **File Sanitizer** no ambiente e depois em **Fragmentar Um**.
2. Navegue até ao activo e clique em **OK** quando a caixa de diálogo Procurar.
3. Clique em **OK** quando a caixa de diálogo de confirmação abrir.

– ou –

1. Abra o File Sanitizer e clique em **Fragmentar**.
2. Clique no botão **Procurar**.
3. Navegue até ao activo e clique em **OK** quando a caixa de diálogo Procurar.
4. Clique em **OK** quando a caixa de diálogo de confirmação abrir.

## Fragmentar todos os itens seleccionados manualmente

1. Clique com o botão direito do rato no ícone do **HP ProtectTools** na área de notificação, na extremidade mais à direita da barra de tarefas, e, em seguida, clique em **File Sanitizer** e depois em **Fragmentar Agora**.
2. Clique em **OK** quando a caixa de diálogo de confirmação abrir.

– ou –

1. Clique no botão direito do rato sobre o ícone do **File Sanitizer** no ambiente e depois em **Fragmentar Agora**.
2. Clique em **OK** quando a caixa de diálogo de confirmação abrir.

– ou –

1. Abra o File Sanitizer e clique em **Fragmentar**.
2. Clique no botão **Fragmentar Agora**.
3. Clique em **OK** quando a caixa de diálogo de confirmação abrir.

## Activar a limpeza do espaço livre manualmente

1. Clique com o botão direito do rato no ícone do **HP ProtectTools** na área de notificação, na extremidade mais à direita da barra de tarefas, e, em seguida, clique em **File Sanitizer** e depois em **Limpar Agora**.
2. Clique em **OK** quando a caixa de diálogo de confirmação abrir.

– ou –

1. Abra o File Sanitizer e clique em **Limpeza do espaço livre**.
2. Clique em **Limpar Agora**.
3. Clique em **OK** quando a caixa de diálogo de confirmação abrir.

## Abortar uma operação de fragmentação ou limpeza do espaço livre

É apresentada uma mensagem em cima do ícone do HP ProtectTools Security Manager na área de notificação quando uma operação de fragmentação ou limpeza do espaço livre estiver em curso. A mensagem disponibiliza detalhes acerca do processo de fragmentação ou limpeza do espaço livre (percentagem concluída) bem como a opção para abortar a operação.

Para abortar a operação:

▲ Clique na mensagem, e depois clique em **Parar** para cancelar a operação.

## Visualizar os ficheiros do registo

Os ficheiros do registo de quaisquer erros ou falhas são gerados sempre que efectuar uma operação de fragmentação ou limpeza do espaço livre. Os ficheiros do registo são sempre actualizados segundo a mais recente operação de fragmentação ou limpeza do espaço livre.

**NOTA:** Os ficheiros que são fragmentados ou limpos com sucesso não surgem nos ficheiros do registo.

É criado um ficheiro do registo para operações de fragmentação e é criado outro ficheiro do registo para as operações de limpeza do espaço livre. Ambos os ficheiros do registo encontram-se na unidade do disco rígido em:

- C:\Program Files\Hewlett-Packard\File Sanitizer*[Nome de utilizador]*_ShredderLog.txt
- C:\Program Files\Hewlett-Packard\File Sanitizer*[Nome de utilizador]*_DiskBleachLog.txt

# 10 Device Access Manager para o HP ProtectTools (somente em alguns modelos)

Os administradores do sistema operativo Windows® utilizam o Device Access Manager for HP ProtectTools para controlar o acesso aos dispositivos num sistema e proteger contra o acesso não autorizado:

- Os perfis do dispositivo são criados para cada utilizador para definir os dispositivos aos quais estejam autorizados a aceder ou não.
- Os utilizadores são também organizados em grupos, como o grupo predefinido do Administrador do Dispositivo ou é possível definir os grupos através da opção Gestão do Computador na secção Ferramentas Administrativas do Painel de Controlo.
- O acesso aos dispositivos pode ser permitido ou negado, com base na pertença ao grupo.
- No caso de classes de dispositivo, como as unidades de CD-ROM e unidades de DVD, o acesso de leitura e de escrita pode ser permitido ou negado separadamente.

Os utilizadores limitados também podem conceder autorização para ler e modificar a política de controlo ao acesso ao dispositivo.

# Procedimentos de configuração

## Abrir Device Access Manager

Para abrir o Device Access Manager, siga estes passos:

1. Clique em **Iniciar**, **Todos os Programas**, **HP** e depois em **HP ProtectTools Administrative Console**.
2. No painel da esquerda, clique em **Device Access Manager**.

## Configurar o acesso ao dispositivo

O Device Access Manager for HP ProtectTools disponibiliza três visualizações:

- A vista Configuração Simples é utilizada para permitir ou recusar o acesso às classes dos dispositivos para membros do grupo Administradores do Dispositivo.
- A vista Configuração da Classe do Dispositivo é utilizada para permitir ou recusar acesso aos tipos de dispositivos ou dispositivos específicos para utilizadores ou grupos específicos.
- A vista Definições de Acesso ao Utilizador é utilizada para especificar que utilizadores podem ver ou modificar as informações da Configuração Simples e Configuração da Classe do Dispositivo.

### Grupo de administradores do dispositivo

Quando o Device Access Manager é instalado, é criado um grupo Administradores do Dispositivo.

O administrador do sistema pode implementar uma política simples de controlo do acesso ao dispositivo recusando o acesso a um conjunto de classes do dispositivo excepto caso o utilizador seja classificado como sendo fidedigno (no que diz respeito ao acesso do dispositivo). A maneira recomendada para efectuar a distinção entre utilizadores de “dispositivo fidedigno” e utilizadores de “dispositivo não fidedigno” destina-se a tornar todos os utilizadores de “dispositivo fidedigno” membros do grupo Administradores do Dispositivo. A concessão de membros do grupo Administradores do Dispositivo acesso a dispositivos através das vistas Configuração Simples ou Configuração da Classe do Dispositivo irá assim assegurar que os utilizadores do "dispositivo fidedignos" terão acesso completo ao conjunto especificado de classes do dispositivo.

**NOTA:** A adição de um utilizador ao grupo Administradores do Dispositivo não permite automaticamente o utilizador a aceder aos dispositivos. Mas a vista Configuração Simples pode ser utilizada para conceder acesso ao conjunto necessário de classes do dispositivo para utilizadores do “dispositivo fidedigno”.

Para adicionar os utilizadores ao grupo Administradores do Dispositivo, cumpra estes passos:

- Use o encaixe MMC “Utilizadores locais e Grupos” padrão para o Windows 7, Vista ou XP Professional.
- No caso de versões domésticas do Windows 7, Vista® ou XP, digite, a partir de uma conta privilegiada, a seguinte janela de pedido do comando:

```
c:\> net grupo local “Administradores do Dispositivo” nome de utilizar /
ADICIONAR
```

## Configuração simples

Os administradores e utilizadores autorizados podem utilizar a vista Configuração simples para modificar o acesso às seguintes classes de dispositivos para todos os Utilizadores que não sejam Administradores:

**NOTA:** Para utilizar esta vista para ler as informações de acesso ao dispositivo, deve conceder acesso de "leitura" ao utilizador ou grupo na vista **Definições do Acesso do Utilizador**. Para utilizar esta vista para modificar as informações de acesso ao dispositivo, deve conceder acesso de "alteração" ao utilizador ou grupo na vista **Definições do Acesso do Utilizador**.

- Todos os suportes amovíveis (disquetes, unidades flash USB, etc.)
- Todas as unidades DVD/CD-ROM
- Todas as portas de série e paralelas
- Todos os dispositivos Bluetooth®
- Todos os dispositivos infravermelhos
- Todos os dispositivos tipo modem
- Todos os dispositivos PCMCIA
- Todos os dispositivos 1394

Para permitir ou recusar o acesso a uma classe de dispositivos a todos os Utilizadores que não sejam Administradores, cumpra estes passos:

1. No painel da esquerda da **HP ProtectTools Administrative Console**, clique em **Device Access Manager** e em **Configuração Simples**.
2. No painel direito, para recusar acesso, seleccione a caixa de verificação de uma classe do dispositivo ou um dispositivo específico. Desmarque a caixa de verificação para permitir o acesso a essa classe do dispositivo ou dispositivo específico.

   Se uma caixa de verificação estiver acinzentada, os valores que afectam o cenário de acesso foram alterados a partir da vista Configuração da Classe do Dispositivo. Clique na caixa de verificação para a desmarcar ou definir e depois clique em **Sim** para confirmar para reinicializar os valores das definições simples.
3. Clique no ícone do **Guardar**.

   **NOTA:** Surge uma caixa de diálogo no ecrã com uma mensagem a perguntar se quer iniciar o serviço de fundo, caso não esteja a funcionar. Clique em **Sim**.
4. Clique em **OK**.

### Iniciar serviço de fundo

O HP ProtectTools Security Manager abre uma caixa de diálogo para perguntar se quer iniciar o serviço de fundo de Bloqueio/Desbloqueio do dispositivo do HP ProtectTools antes de poder aplicar perfis do dispositivo. Clique em **Sim**. O serviço de fundo é iniciado e é activado automaticamente daí em diante sempre que o sistema arrancar.

**NOTA:** Deve definir um perfil do dispositivo para apresentar o pedido de serviço de fundo.

Os administradores também podem iniciar ou parar este serviço:

1. Clique em **Iniciar** e depois em **Painel de controlo**.
2. Clique em **Ferramentas Administrativas** e depois em **Serviços**.
3. Procure o serviço de **Bloqueio/Auditoria do Dispositivo do HP ProtectTools**.

Parar o serviço de Bloqueio/Auditoria do Dispositivo não interrompe o bloqueio do dispositivo. O bloqueio do dispositivo é activado por dois componentes:

- Serviço de Bloqueio/Auditoria do Dispositivo
- controlador DAMDrv.sys

O controlador do dispositivo é iniciado quando o serviço arranca, mas parar o serviço não interrompe o controlador.

Para determinar se o serviço de fundo está a ser executado, abra uma janela de pedido de comando e digite sc query flcdlock.

Para determinar se o controlador do dispositivo está a ser executado, abra uma janela de pedido de comando e digite sc query damdrv.

## Configuração da Classe do Dispositivo

Os administradores e utilizadores autorizados podem ver e modificar as listas de utilizadores e grupos, cujo acesso a classes de dispositivos ou dispositivos específicos é permitido ou negado.

**NOTA:** Para utilizar esta vista para ler as informações de acesso ao dispositivo, deve conceder acesso de "leitura" ao utilizador ou grupo na vista **Definições do Acesso do Utilizador**. Para utilizar esta vista para modificar as informações de acesso ao dispositivo, deve conceder acesso de "alteração" ao utilizador ou grupo na vista **Definições do Acesso do Utilizador**.

A vista Configuração da Classe do Dispositivo tem as seguintes secções:

- **Lista de Dispositivos**—Apresenta todas as classes de dispositivos e dispositivos instalados no sistema ou que possam ter sido previamente instalados no sistema.
  - Normalmente a protecção é aplicada a uma classe do dispositivo. Um utilizador ou grupo seleccionado poderá aceder a qualquer dispositivo na classe do dispositivo.
  - A protecção também pode ser aplicada a dispositivos específicos.
- **Lista de Utilizadores**—Apresenta todos os utilizadores e grupos cujo acesso à classe do dispositivo seleccionada ou dispositivo específico é permitido ou negado.
  - A entrada Lista de Utilizadores pode ser efectuada para um utilizador específico ou para um grupo do qual o utilizador é membro.
  - A definição foi herdada da classe do dispositivo na Lista de Dispositivos ou da pasta Classe se uma entrada de utilizador ou grupo da Lista de Utilizadores estiver indisponível.
  - Algumas classes de dispositivos, como DVD e CD-ROM, também podem ser mais controladas permitindo ou recusando o acesso separadamente para operações de leitura e escrita.

Os direitos de acesso de leitura e escrita podem ser herdados no caso de outros dispositivos e classes. Por exemplo, o acesso de Leitura pode ser herdado de uma classe mais elevada, mas o acesso de Escrita pode ser negado especificamente para um utilizador ou grupo.

**NOTA:** Se a caixa de verificação Leitura estiver em branco, então a entrada do controlo de acesso não tem qualquer efeito no acesso de leitura ao dispositivo. Não concede nem recusa acesso de leitura ao dispositivo.

**Exemplo 1**—Se o acesso de escrita para um dispositivo ou classe de dispositivos for negado a um utilizador ou grupo:

Pode ser concedido acesso de leitura ou acesso de leitura+escrita apenas para um dispositivo abaixo deste dispositivo na hierarquia de dispositivos ao mesmo utilizador, ao mesmo grupo ou a um membro do mesmo grupo.

**Exemplo 2**—Se o acesso de escrita para um dispositivo ou classe de dispositivos for permitido a um utilizador ou grupo:

Pode ser negado acesso de escrita ou acesso de leitura+escrita apenas para o mesmo dispositivo ou um dispositivo abaixo deste dispositivo na hierarquia de dispositivos ao mesmo utilizador, ao mesmo grupo ou a um membro do mesmo grupo.

**Exemplo 3**—Se o acesso de leitura para um dispositivo ou classe de dispositivos for permitido a um utilizador ou grupo:

Pode ser negado acesso de leitura ou acesso de leitura+escrita apenas para o mesmo dispositivo ou um dispositivo abaixo deste dispositivo na hierarquia de dispositivos ao mesmo utilizador, ao mesmo grupo ou a um membro do mesmo grupo.

**Exemplo 4**—Se o acesso de leitura para um dispositivo ou classe de dispositivos for negado a um utilizador ou grupo:

Pode ser concedido acesso de leitura ou acesso de leitura+escrita apenas para um dispositivo abaixo deste dispositivo na hierarquia de dispositivos ao mesmo utilizador, ao mesmo grupo ou a um membro do mesmo grupo.

**Exemplo 5**—Se o acesso de leitura+escrita para um dispositivo ou classe de dispositivos for permitido a um utilizador ou grupo:

Pode ser negado acesso de escrita ou acesso de leitura+escrita apenas para o mesmo dispositivo ou um dispositivo abaixo deste dispositivo na hierarquia de dispositivos ao mesmo utilizador, ao mesmo grupo ou a um membro do mesmo grupo.

**Exemplo 6**—Se o acesso de leitura+escrita para um dispositivo ou classe de dispositivos for negado a um utilizador ou grupo:

Pode ser concedido acesso de leitura ou acesso de leitura+escrita apenas para um dispositivo abaixo deste dispositivo na hierarquia de dispositivos ao mesmo utilizador, ao mesmo grupo ou a um membro do mesmo grupo.

### Recusar o acesso a um utilizador ou grupo

Para impedir um utilizador ou grupo de aceder um dispositivo ou uma classe de dispositivos, cumpra estes passos:

1. No painel da esquerda da **HP ProtectTools Administrative Console**, clique em **Device Access Manager** e em **Configuração da Classe do Dispositivo**.
2. Na lista de dispositivos, clique na classe de dispositivos que pretende configurar.
   - Classe do dispositivo
   - Todos os dispositivos
   - Dispositivo individual
3. Em **Utilizador/Grupos**, clique no utilizador ou grupo ao qual pretende negar o acesso.
4. Clique na opção **Recusar** ao lado de um utilizador ou grupo.
5. Clique no ícone do **Guardar**.

**NOTA:** Quando as definições de recusa e permissão são definidas ao mesmo nível do dispositivo de um utilizador, a recusa do acesso tem precedência em relação à autorização do acesso.

### Permitir o acesso de um utilizador ou um grupo

Para conceder a permissão a um utilizador ou grupo de acesso a um dispositivo ou uma classe de dispositivos, cumpra estes passos:

1. No painel da esquerda da **HP ProtectTools Administrative Console**, clique em **Device Access Manager** e em **Configuração da Classe do Dispositivo**.
2. Na lista de dispositivos, clique numa das seguintes opções:
   - Classe do dispositivo
   - Todos os dispositivos
   - Dispositivo individual
3. Clique em **Add** (Adicionar).

   É apresentada a caixa de diálogo **Seleccionar Utilizadores ou Grupos**.
4. Clique em **Avançado** e depois em **Encontrar Agora** para procurar utilizadores ou grupos a adicionar.
5. Clique num utilizador ou um grupo a adicionar à lista de utilizadores e grupos disponíveis, e clique depois em **OK**.
6. Clique em **OK** novamente.
7. Clique em **Permitir** para conceder o acesso a esse utilizador ou grupo.
8. Clique no ícone do **Guardar**.

### Remover o acesso de um utilizador ou um grupo

Para remover a permissão a um utilizador ou grupo de acesso a um dispositivo ou uma classe de dispositivos, cumpra estes passos:

1. No painel da esquerda da **HP ProtectTools Administrative Console**, clique em **Device Access Manager** e em **Configuração da Classe do Dispositivo**.
2. Na lista de dispositivos, clique na classe de dispositivos que pretende configurar.
   - Classe do dispositivo
   - Todos os dispositivos
   - Dispositivo individual
3. Em **Utilizador/Grupos**, clique no utilizador ou grupo que quer remover e depois em **Remover**.
4. Clique no ícone do **Guardar**.

### Permitir o acesso a uma classe de dispositivos a um utilizador de um grupo

Para permitir o acesso a uma classe de dispositivos a um utilizador enquanto recusa o acesso a todos os outros membros do grupo desse utilizador, cumpra os seguintes passos:

1. No painel da esquerda da **HP ProtectTools Administrative Console**, clique em **Device Access Manager** e em **Configuração da Classe do Dispositivo**.
2. Na lista de dispositivos, clique na classe de dispositivos que pretende configurar.
   - Classe do dispositivo
   - Todos os dispositivos
   - Dispositivo individual
3. Em **Utilizador/Grupos**, seleccione o grupo ao qual vai negar o acesso e clique em **Negar**.
4. Navegue até à pasta por baixo da referente à classe pretendida e adicione então o utilizador específico.
5. Clique em **Allow** (Permitir) para permitir o acesso a esse utilizador.
6. Clique no ícone do **Guardar**.

### Permitir acesso a um dispositivo específico a um utilizador de um grupo

Os administradores podem conceder o acesso a um dispositivo específico a um utilizador, e negar o acesso a todos os dispositivos dessa classe a todos os outros membros do grupo desse utilizador.

1. No painel da esquerda da **HP ProtectTools Administrative Console**, clique em **Device Access Manager** e em **Configuração da Classe do Dispositivo**.
2. Na lista de dispositivos, clique na classe de dispositivos que pretende configurar e, em seguida, navegue até à pasta por baixo dessa.
3. Clique em **Add** (Adicionar). É apresentada a caixa de diálogo **Seleccionar Utilizadores ou Grupos**.

4. Clique em **Avançado** e depois em **Encontrar Agora** para procurar o grupo desse utilizador ao qual vai negar o acesso a todos os dispositivos na classe.
5. Clique no grupo e depois em **OK**.
6. Navegue até ao dispositivo específico na classe do dispositivo à qual vai ser permitido o acesso ao utilizador.
7. Clique em **Add** (Adicionar). É apresentada a caixa de diálogo **Seleccionar Utilizadores ou Grupos**.
8. Clique em **Avançado** e depois em **Encontrar Agora** para procurar utilizadores ou grupos a adicionar.
9. Clique no utilizador para permitir o acesso e, em seguida, clique em **OK**.
10. Clique em **Allow** (Permitir) para permitir o acesso a esse utilizador.
11. Clique no ícone do **Guardar**.

## Reinicializar a configuração

△ **CUIDADO:** A reinicialização da configuração descarta todas as alterações da configuração do dispositivo efectuadas e repõe todas as predefinições de fábrica dos valores.

Para reinicializar as predefinições da configuração, cumpra estes passos:

1. No painel da esquerda da **HP ProtectTools Administrative Console**, clique em **Device Access Manager** e em **Configuração da Classe do Dispositivo**.
2. Clique no botão **Reinicializar**.
3. Clique em **Sim** para confirmar.
4. Clique no ícone do **Guardar**.

# Tarefas avançadas

## Controlar o acesso às definições da configuração

Na vista **Definições de Acesso do Utilizador**, os administradores especificam os grupos ou utilizadores autorizados a utilizar as páginas Configuração Simples e Configuração da Classe do Dispositivo.

**NOTA:** Um utilizador ou grupo deve ter "Direitos completos de Administrador" para modificar as definições na vista Definições do Acesso do Utilizador.

- Permita o acesso "Ver Definições de Configuração (Apenas leitura)" ao utilizador ou grupo na vista Definições do Acesso do Utilizador para ver as informações da Configuração Simples e Configuração do Classe do Dispositivo.
- Permita o acesso "Alterar Definições de Configuraçã" ao utilizador ou grupo na vista Definições do Acesso do Utilizador para alterar as informações da Configuração Simples e Configuração do Classe do Dispositivo.

**NOTA:** O acesso de "leitura" deve ser permitido até mesmo a membros do grupo Administradores para ver as vistas Configuração Simples e Configuração da Classe do Dispositivo e o acesso de "alteração" deve ser permitido para alterar dados com as vistas Configuração Simples e Configuração da Classe do Dispositivo.

**NOTA:** Depois de avaliar os níveis de acesso de todos os utilizadores e grupos, se um utilizador não tiver seleccionado Permitir ou Negar para um determinado nível de acesso, o acesso nesse nível é negado ao utilizador.

### Permitir o acesso a um grupo ou utilizador existente

Para permitir que um grupo ou utilizador existente veja ou altere as definições de configuração, cumpra os seguintes passos:

1. No painel da esquerda da **HP ProtectTools Administrative Console**, clique em **Device Access Manager** e em **Definições do Acesso do Utilizador**.
2. Clique para permitir o acesso de um grupo ou utilizador.
3. Em **Permissões**, clique em **Permitir** para cada tipo de permissão a ser concebida ao grupo ou utilizador seleccionado:

   **NOTA:** As permissões concedidas são cumulativas. Por exemplo, a permissão “Ver Definições de Configuração (Apenas leitura)” é automaticamente concedida a um utilizador autorizado a “Alterar Definições da Configuração”. Um utilizador com “Direitos completos de Administrador” tem também as permissões “Alterar Definições da Configuração” e“Ver Definições da Configuração (Apenas leitura)”.

   - Direitos Completos de Administrador
   - Alterar Definições da Configuração
   - Ver Definições da Configuração (Apenas leitura)
4. Clique no ícone do **Guardar**.

## Negar o acesso a um grupo ou utilizador existente

Para negar que um grupo ou utilizador existente veja ou altere as definições de configuração, cumpra os seguintes passos:

1. No painel da esquerda da **HP ProtectTools Administrative Console**, clique em **Device Access Manager** e em **Definições do Acesso do Utilizador**.
2. Clique para negar o acesso de um grupo ou utilizador.
3. Em **Permissões**, clique em **Negar** para cada tipo de permissão a ser negada ao grupo ou utilizador seleccionado:
   - Direitos Completos de Administrador
   - Alterar Definições da Configuração
   - Ver Definições da Configuração (Apenas leitura)
4. Clique no ícone do **Guardar**.

## Adicionar um novo grupo ou utilizador

Para permitir que um novo grupo ou utilizador veja ou altere as definições de configuração, cumpra os seguintes passos:

1. No painel da esquerda da **HP ProtectTools Administrative Console**, clique em **Device Access Manager** e em **Definições do Acesso do Utilizador**.
2. Clique em **Add** (Adicionar). É apresentada a caixa de diálogo **Seleccionar Utilizadores ou Grupos**.
3. Clique em **Avançado** e depois em **Encontrar Agora** para procurar utilizadores ou grupos a adicionar.
4. Clique num grupo ou utilizador, em **OK** e depois em **OK** novamente.
5. Clique em **Allow** (Permitir) para permitir o acesso a esse utilizador.
6. Clique no ícone do **Guardar**.

## Remover o acesso do grupo ou utilizador

Para negar que um grupo ou utilizador veja ou altere as definições de configuração, cumpra os seguintes passos:

1. No painel da esquerda da **HP ProtectTools Administrative Console**, clique em **Device Access Manager** e em **Definições do Acesso do Utilizador**.
2. Clique num grupo ou utilizador e depois em **Remover**.
3. Clique no ícone do **Guardar**.

## Documentação relacionada

O Device Access Manager for HP ProtectTools é compatível com o produto empresarial HP ProtectTools Enterprise Device Access Manager. O Device Access Manager for HP ProtectTools permite o acesso de leitura apenas às suas próprias funcionalidades ao trabalhar com o produto empresarial.

Encontram-se disponíveis mais informações acerca do Device Access Manager for HP ProtectTools na Web em http://www.hp.com/hps/security/products.

# 11 LoJack Pro for HP ProtectTools

O Computrace LoJack Pro, alimentado pelo Absolute Software (adquirido em separado), lida com o crescente problema dos computadores que são perdidos ou roubados.

Aactivação deste software activa o agente da Computrace, que permanece activo no computador mesmo que a unidade do disco rígido seja reformatada ou substituída.

O LoJack Pro possibilita a monitorização remota, gestão e rastreio do seu computador. A Equipa de Recuperação do Absolute irá ajudar à recuperação do seu computador, em caso de roubo ou perda.*

**NOTA:** *Esta funcionalidade depende da localização geográfica. Consulte o contrato de subscrição do Absolute Software para obter informações adicionais.

# 12 Resolução de problemas

## HP ProtectTools Security Manager

| Descrição breve | Detalhes | Solução |
|---|---|---|
| Os Smart cards e tokens USB não se encontram disponíveis no Security Manager se forem instalados depois do Security Manager. | Deve instalar o software de suporte (controladores, fornecedores de PKCS#11, etc.) antes do Security Manager para poder utilizar smart cards ou tokens USB no Security Manager.<br><br>Se já tiver instalado o Security Manager, cumpra os seguintes passos após a instalação do software de suporte do smart card ou token: | Inicie a sessão no Password Manager.<br><br>No HP ProtectTools Security Manager, clique em **Password Manager**, **Credenciais** e depois em **Smart Card**<br><br>Reinicie o computador, se solicitado. |
| Algumas páginas de Web de aplicações criam erros que impedem o utilizador de efectuar ou concluir tarefas. | Algumas aplicações baseadas na Web deixam de funcionar e relatam erros devido ao padrão de desactivação de funcionalidades do Início de sessão único. Por exemplo, um **!** dentro de um triângulo amarelo é apresentado no Internet Explorer para indicar a ocorrência de um erro. | A aplicação Security Manager Single Sign On não suporta todas as interfaces de software da Web. Desactive o suporte da aplicação Single Sign On para a página da Web específica desactivando a opção do suporte da aplicação Single Sign On. Consulte a documentação completa da aplicação Single Sign On, disponível nos ficheiros da Ajuda do software Security Manager.<br><br>Se não for possível desactivar um Início de sessão único específico para uma determinada aplicação, ligue para o suporte técnico da HP e solicite suporte de nível três através do seu contacto de Assistência HP. |
| A opção para **Browse for Virtual Token** (Procurar token virtual) não é apresentada durante o processo de início de sessão. | O utilizador não pode mover a localização de um token virtual registado no Password Manager porque a opção de procura foi removida para reduzir riscos de segurança. | A opção de procura foi removida pois permitia que não utilizadores eliminassem e mudassem o nome de ficheiros e controlassem o Windows. |
| Os administradores de domínio não podem alterar a palavra-passe do Windows mesmo com autorização. | Isto ocorre após o início de sessão de um administrador num domínio e registo da identidade do domínio com o Password Manager através de uma conta com direitos de Administrado no domínio e no PC local. O administrador do domínio recebe um erro de falha do início de sessão quando tenta alterar a palavra-passe do Windows a partir do Password Manager: **Restricção da conta de utilizador**. | 'O Password Manager não consegue alterar uma palavra-passe da conta do utilizador através da opção **Alterar palavra-passe do Windows**. O Security Manager só consegue alterar as palavras-passe de contas locais do PC. O utilizador do domínio pode mudar a sua palavra-passe através da opção **Alterar palavra-passe** da **Segurança do Windows**, mas como o utilizador do domínio não tem uma conta física no PC local, o Password Manager só pode mudar a palavra-passe utilizada para iniciar a sessão. |
| O Password Manager tem problemas de incompatibilidade com a | Se o utilizador iniciar a sessão no Password Manager, criar um documento no WordPerfect e oi guardar com | A HP está a desenvolver uma solução para melhoramentos futuros do produto. |

| Descrição breve | Detalhes | Solução |
|---|---|---|
| palavra-passe GINA do Corel WordPerfect 12. | protecção de palavra-passe, o Password Manager não consegue detectar ou reconhecer, manual ou automaticamente, a palavra-passe GINA. | |
| O Password Manager não reconhece o botão **Ligar** no ecrã. | Se as credenciais de Início de sessão único para RDP (Remote Desktop Connection) estiverem definidas para **Ligar**, quando o Início de sessão único é reiniciado, apresenta sempre **Guardar como** em vez de **Ligar**. | A HP está a desenvolver uma solução para melhoramentos futuros do produto. |
| O utilizador não consegue iniciar a sessão no Password Manager depois de passar do modo de Suspensão para o de Hibernação apenas no Windows XP Service Pack 1. | Depois de permitir a transição do sistema para o modo de Hibernação e Suspensão, o Administrador ou utilizador não consegue iniciar a sessão no Password Manager e o ecrã do início de sessão do Windows continua a ser apresentado independentemente da credencial de início de sessão (palavra-passe, impressão digital ou Java Card) seleccionada. | Actualizar o Windows para o Service Pack 2, através da Actualização do Windows. Consulte a base de conhecimentos da Microsoft, artigo 813301, disponível em http://www.microsoft.com, para obter mais informações sobre as causas deste problema.<br><br>Para iniciar a sessão, o utilizador tem de seleccionar o Password Manager e iniciar a sessão. Depois de iniciar a sessão no Password Manager, é pedido ao utilizador que inicie a sessão no Windows (o utilizador pode ter de seleccionar a opção de início de sessão do Windows) para concluir o processo de início de sessão.<br><br>O utilizador tem de iniciar a sessão no Password Manager manualmente se iniciar a sessão no Windows primeiro. |
| O processo de segurança **Restore Identity** (Restaurar identidade) perde a associação a um token virtual. | Quando o utilizador restaurar a identidade, o Password Manager pode perder a associação à localização do token virtual no ecrã do início de sessão. O utilizador tem de registar novamente o token para restaurar a associação embora o Password Manager tenha o token virtual registado. | Esta é uma característica intencional do produto.<br><br>A parte do sistema (servidor) do token é destruída quando desinstala o Security Manager sem manter as identidades, pelo que não é possível voltar a utilizar o token para iniciar a sessão, mesmo que a parte do cliente do token seja restaurada através da funcionalidade de restauro da identidade.<br><br>A HP está a investigar possíveis soluções a longo prazo. |

# Device Access Manager for HP ProtectTools

**Foi negado acesso a dispositivos no Device Access Manager aos utilizadores, mas os dispositivos continuam acessíveis.**

- **Explicação**—As opções Configuração Simples e/ou Configuração da Classe do Dispositivo foram utilizadas a partir do Device Access Manager para negar acesso a dispositivos aos utilizadores. Os utilizadores conseguem aceder ainda aos dispositivos, embora o acesso lhes tenha sido negado.
- **Solução:**
  - Certifique-se de que o serviço de Bloqueio do Dispositivo do HP ProtectTools foi iniciado.
  - Como administrador, clique em **Painel de Controlo** e depois em **Sistema e Manutenção**. Na janela Ferramentas Administrativas, clique em **Serviços** e procure o serviço de **Bloqueio/ Auditoria do Dispositivo do HP ProtectTools**. Certifique-se de que o serviço foi iniciado e que o tipo de arranque escolhido é **Automático**

**Um utilizador tem acesso inesperado a um dispositivo ou o acesso a um dispositivo é inesperadamente negado a um utilizador.**

- **Explicação**—O Device Access Manager foi utilizado para negar o acesso de utilizadores a alguns dispositivos e permitir o acesso de utilizadores a outros dispositivos. Quando o utilizador utiliza o sistema pode aceder a dispositivos cujo acesso acha que foi negado pelo Device Access Manager e ser-lhe negado acesso a dispositivos, para os quais achava que tinha permissão pelo Device Access Manager.
- **Solução:**
  - Use a funcionalidade Configuração da Classe do Dispositivo no Device Access Manager para investigar as definições do dispositivo do utilizador.
  - Clique em **Security Manager**, **Device Access Manager** e depois em **Configuração da Classe do Dispositivo**. Expanda os níveis na árvore da Classe do Dispositivo e reveja as definições aplicáveis a este utilizador. Verifique se existem quaisquer permissões “Negar” que possam ter sido definidas para o utilizador ou qualquer grupo do Windows do qual o utilizador possa fazer parte, como Utilizadores e Administradores.

**Permitir ou negar—qual tem precedência?**

- **Explicação**—Na Configuração da Classe do Dispositivo foi definida a seguinte configuração:
  - A permissão Permitir foi concedida a um grupo do Windows (por ex., BUILTIN \Administradores) e a permissão Recusar foi concedida a outro grupo do Windows (por ex., BUILTIN\Utilizadores) ao mesmo nível na hierarquia da classe do dispositivo (por ex., Unidades de DVD/CD-ROM).
  - Se um utilizador for um membro destes dois grupos (por ex., Administrador), qual tem precedência?
- **Solução:**
  - O acesso ao dispositivo é negado ao utilizador. A opção Negar tem precedência sobre a opção Permitir.
  - Oacesso é negado por causa do modo como o Windows determina a permissão efectiva do dispositivo. O acesso de um grupo é negado e o de outro grupo é permitido, mas o utilizador é membro dos dois grupos. O acesso do utilizador é negado porque a recusa de acesso tem precedência sobre a permissão de acesso.
  - Uma solução para esta situação é negar o acesso ao grupo Utilizador ao nível das Unidades de DVD/CD-ROM e permitir o acesso do grupo Administradores ao nível abaixo das Unidades de DVD/CD-ROM.
  - Uma solução alternativa é criar grupos específicos do Windows, um para permitir o acesso às unidades de DVD/CD e um para negar o acesso às unidades de DVD/CD. Os utilizadores específicos seriam adicionados então ao grupo apropriado.

**A vista Configuração Simples foi utilizada para definir uma política de controlo do acesso ao dispositivo, mas os administradores não podem aceder aos dispositivos.**

- **Explicação**—A opção Configuração Simples nega o acesso aos Utilizadores e Convidados e permite o acesso dos Administradores do dispositivo.
- **Solução:** Adicione o Administrado ao grupo Administradores do dispositivo.

# Diversos

| Software — Descrição breve | Detalhes | Solução |
|---|---|---|
| Security Manager – Aviso recebido: **A aplicação de segurança não pode ser instalada até o HP ProtectTools Security Manager ser instalado**. | Todas as aplicações de segurança, como a Java Card Security e biométrica são plug-ins extensíveis para a interface do Security Manager. Tem de instalar o Security Manager para poder carregar um plug-in de segurança aprovado pela HP. | O software Security Manager deve ser instalado antes qualquer plug-in de segurança. |
| HP ProtectTools Security Manager — Intermitentemente, é devolvido um erro ao fechar a interface do Security Manager. | Intermitentemente (1 em 12 casos), é criado um erro pela utilização do botão de fecho no canto superior direito do ecrã para fechar o Security Manager antes de todas as aplicações plug-in terem concluído o respectivo carregamento. | Isto está relacionado com uma dependência de temporização no tempo de carregamento de serviços plug-in quando o Security Manager é fechado ou reiniciado. Visto que o PTHOST.exe é o alojamento da shell das outras aplicações (plug-ins), está dependente da capacidade do plug-in para concluir o respectivo tempo de carregamento (serviços). Fechar a shell antes do plug-in ter tido tempo de concluir o carregamento é a causa raiz.<br><br>Deixe que o Security Manager conclua a mensagem de carregamento dos serviços (apresentada na parte superior da janela do Security Manager) e todos os plug-ins listados na coluna esquerda. Para evitar falhas, conceda um tempo razoável para estes plug-ins serem carregados. |
| HP ProtectTools — Acesso não restringido ou privilégios de administrador não controlados constituem um risco de segurança. | Vários riscos são possíveis com o acesso não restringido ao PC cliente, incluindo os seguintes:<br>• Eliminação do PSD<br>• Modificação maliciosa de definições dos utilizadores<br>• Desactivação de políticas e funções de segurança | Os administradores são encorajados a cumprir as “melhores práticas” no que diz respeito a restringir privilégios do utilizador final bem como de acesso dos utilizadores.<br><br>Não devem ser concedidos privilégios administrativos a utilizadores não autorizados. |

# Glossário

**activação** A tarefa que tem de ser concluída para aceder a quaisquer funcionalidades do Drive Encryption. O Drive Encryption é activado através do Assistente de Configuração do HP ProtectTools. Só um administrador pode activar o Drive Encryption. O processo de activação consiste em activar o software, encriptar a unidade, criar uma conta de utilizador e criar uma cópia de segurança inicial da chave de encriptação num dispositivo de armazenamento amovível.

**activo** Um componente de dados, que consiste em informação pessoal ou ficheiros, dados históricos e relacionados com a Web, e outros dados do género, localizado no disco rígido.

**administrador** *Ver* o administrador do Windows.

**administrador do Windows** Um utilizador com todos os direitos para modificar permissões e gerir outros utilizadores.

**arquivo de recuperação de emergência** Área de armazenamento protegida que permite a reencriptação das chaves de utilizador básico de uma chave de proprietário da plataforma para outra.

**assinatura digital** Dados enviados com um ficheiro que verifica o remetente do material e que o ficheiro não foi modificado após ser assinado.

**assinatura sugerida** Um utilizador que é designado pelo titular dum documento do Microsoft Word ou Microsoft Excel, para adicionar uma linha de assinatura ao documento.

**ATM** O Automatic Technology Manager permite aos administradores da rede gerir sistemas remotamente ao nível do BIOS.

**autenticação** Processo de verificar se um utilizador está autorizado a efectuar uma tarefa, tal como aceder a um computador, modificar as definições de um programa específico ou ver dados protegidos.

**autenticação na ligação** Funcionalidade de segurança que requer alguma forma de autenticação, tal como um Java Card, chip de segurança ou palavra-passe, quando o computador é ligado.

**autoridade de certificação** Serviço que emite os certificados requeridos para a execução de uma infra-estrutura de chaves públicas.

**biométrico** Categoria de credenciais de autenticação que utilizam uma característica física, tal como uma impressão digital, para identificar um utilizador.

**Botão Assinar e Encriptar** Um botão do software, que é exibido na barra de ferramentas das aplicações do Microsoft Office. Se clicar neste botão, pode assinar, encriptar ou remover a encriptação de um documento do Microsoft Office.

**Botão Enviar Segurança** Um botão do software, que é exibido na barra de ferramentas das mensagens de e-mail do Microsoft Outlook. Se clicar neste botão, pode assinar e/ou encriptar uma mensagem de e-mail do Microsoft Outlook.

**cartão de identificação** Um acessório da Barra lateral do Windows que serve para identificar visualmente o seu ambiente de trabalho com o seu nome de utilizador e imagem seleccionada. Clique no cartão de identificação para abrir a HP ProtectTools Administrative Console.

**certificado digital** Credenciais electrónicas que confirmam a identidade de um indivíduo ou empresa através da associação da identidade do proprietário do certificado digital a um par de chaves electrónicas que é utilizado para assinar informações digitais.

**Certificado do Privacy Manager** Um certificado digital, que requer autenticação de cada vez que o utiliza em operações de encriptação, tais como assinatura e encriptação de mensagens de e-mail e documentos do Microsoft Office.

**ciclo de destruição** O número de vezes que o algoritmo de fragmentação é executado em cada activo. Quanto mais elevado for o número de ciclos de fragmentação que seleccionar, mais protegido fica o computador.

**classe do dispositivo** Todos os dispositivos de um determinado tipo, como as unidades.

**comunicação por mensagens instantâneas fidedigna** Uma sessão de comunicação, durante a qual mensagens fiáveis são enviadas de um remetente de confiança para um Contacto de confiança.

**consola** Uma localização central a partir da qual pode aceder e gerir as funcionalidades e definições deste programa.

**conta de rede** Conta de utilizador ou administrador do Windows num computador local, grupo de trabalho ou domínio.

**Conta de utilizador do Windows** Perfil que permite que um indivíduo autorizado inicie sessão numa rede ou num computador individual.

**Convite de Trusted Contacto** Um e-mail que é enviado para uma pessoa, solicitando-lhe que se torne num Contacto de confiança.

**cópia de segurança** Utilizar a funcionalidade da cópia de segurança para guardar uma cópia de informações importantes do programa para uma localização fora do programa. Esta cópia pode ser utilizada posteriormente para restaurar as informações no mesmo computador ou noutro computador.

**credenciais** Método pelo qual um utilizador prova a elegibilidade para uma tarefa específica no processo de autenticação.

**criptografia** Encriptação e desencriptação de dados, para que estes só possam ser descodificados por indivíduos específicos.

**cryptographic service provider (CSP)** Fornecedor ou biblioteca de algoritmos criptográficos que podem ser utilizados numa interface bem definida para a execução de funções criptográficas específicas.

**desencriptação** Procedimento utilizado na criptografia para converter os dados encriptados em texto simples.

**Destinatário Trusted Contact** Uma pessoa que recebe um convite para se tornar um Contacto de confiança.

**destruição automática** Fragmentação programada que o utilizador define no File Sanitizer.

**destruição manual** Fragmentação imediata de um activo ou activos seleccionados, que contorna o calendário de fragmentação automática.

**destruir** A execução de um algoritmo que oculta os dados contidos num activo.

**domínio** Grupo de computadores que faz parte de uma rede e partilha uma base de dados de directórios comum. Os domínios têm nomes exclusivos e cada um tem um conjunto de regras e procedimentos comuns.

**Drive Encryption** Protege os seus dados encriptando a(s) sua(s) unidade(s) de disco rígido, impossibilitando a leitura das informações por pessoas sem a devida autorização.

**DriveLock** Funcionalidade de segurança, que associa a unidade de disco rígido a um utilizador e que requer que o utilizador introduza a palavra-passe correcta do DriveLock durante o arranque do computador.

**Ecrã de início de sessão do Drive Encryption** Um ecrã de início de sessão, que é apresentado antes do Windows ser iniciado. Os utilizadores devem introduzir o respectivo nome de utilizador e a palavra-passe do Windows ou o PIN do Java Card. Na maioria dos casos, a introdução das informações correctas no ecrã de início de sessão do Drive Encryption permite ter acesso directo ao Windows, sem ser necessário iniciar sessão novamente no ecrã de início de sessão do Windows.

**eliminação simples** Eliminação da referência do Windows a um activo. O conteúdo do activo permanece no disco rígido até que sejam gravados dados de ocultação por cima do mesmo, através do branqueamento do espaço livre.

**encriptação** Procedimento, como a utilização de um algoritmo, utilizado na criptografia para converter texto simples em texto cifrado para impedir a leitura dos dados por pessoas não autorizadas. Existem muitos tipos de encriptação de dados, constituindo a base da segurança da rede. Os tipos comuns incluem o Data Encryption Standard e a encriptação de chaves públicas.

**grupo** Um grupo de utilizadores com o mesmo nível de acesso ou recusa a uma classe de dispositivos ou um dispositivo específico.

**HP SpareKey** Cópia de segurança da chave de encriptação da unidade.

**identidade** No In the HP ProtectTools Security Manager, um grupo de credenciais e definições que é tratado como uma conta ou perfil de um utilizador específico.

**impressão digital** Uma extracção digital da imagem da sua impressão digital. A imagem real da sua impressão digital nunca é armazenada pelo Security Manager.

**início de sessão** Um objecto no Security Manager constituído por um nome de utilizador e palavra-passe (e possivelmente outras informações seleccionadas) que podem ser utilizadas para iniciar a sessão em sites da Web ou outros programas.

**Java Card** Um cartão amovível, que é inserido no computador. Contém informação de identificação para o início de sessão. Iniciar sessão com um Java Card no ecrã de início de sessão do Drive Encryption, requer que o utilizador introduza o Java Card e escreva o respectivo nome de utilizador, assim como o PIN do Java Card.

**limpeza do espaço livre** A gravação protegida de dados aleatórios por cima de activos eliminados, para distorcer os conteúdos dos activos eliminados.

**linha da assinatura** Um espaço em branco para a exibição visual duma assinatura digital. Quando um documento é assinado, o nome e método de verificação do signatário são exibidos. A data de assinatura e o título do signatário também podem ser incluídos.

**Lista de Trusted Contacts** Uma listagem dos Contactos de confiança.

**Live Messenger History Viewer** Um componente do Privacy Manager Chat, que lhe permite pesquisar e visualizar o histórico encriptado de sessões de conversação.

**mensagem fidedigna** Uma sessão de comunicação, durante a qual mensagens fiáveis são enviadas de um remetente de confiança para um Contacto de confiança.

**método de início de sessão em segurança** O método utilizado para iniciar a sessão no computador.

**migração** Uma tarefa que permite a gestão, restauro e transferência de Privacy Manager Certificates e Trusted Contacts.

**Modo do dispositivo SATA** Modo de transferência de dados entre um computador e dispositivos de armazenamento em massa, tais como unidades de disco rígido e unidades ópticas.

**painel** Uma localização central a partir da qual pode aceder e gerir as funcionalidades e definições deste programa.

**palavra-passe de revogação** Uma palavra-passe que é criada quando um utilizador solicita um certificado digital. A palavra-passe é pedida quando o utilizador pretender revogar o seu certificado digital. Isto assegura que apenas o utilizador pode revogar o certificado.

**perfil de destruição** Um método de eliminação específico e lista de activos.

**PKI** Public Key Infrastructure é uma norma que define as interfaces para a criação, utilização e administração de certificados e chaves criptográficas.

**política de controlo do acesso ao dispositivo** A lista de dispositivos aos quais é permitido ou negado o acesso ao utilizador.

**PSD** Unidade pessoal segura que fornece uma área de armazenamento protegida para informações confidenciais.

**reiniciar** Processo de reiniciar o computador.

**remetente fidedigno** Um Contacto de confiança que envia e-mails e documentos do Microsoft Office assinados e/ou encriptados.

**restaurar** Um processo que copia informações do programa para este programa a partir de um ficheiro de cópia de segurança criado previamente.

**revelar** Uma tarefa que permite ao utilizador desencriptar uma ou mais sessões do histórico de conversação, apresentando o(s) nome(s) do Contact Screen sob a forma de texto simples e fazendo com que a sessão fique disponível para visualização.

**selo para contactos fidedignos** Uma tarefa que adiciona uma assinatura digital, encripta o e-mail e envia o mesmo, depois do utilizador o autenticar, utilizando o método por ele seleccionado de início de sessão de segurança.

**sequência de teclas** Uma combinação de teclas específicas que, quando premidas, iniciam uma fragmentação automática - por exemplo ctrl+alt+s.

**serviço de fundo** As políticas de controlo do acesso do dispositivo só são aplicadas se o serviço de fundo Bloqueio/Auditoria do Dispositivo do HP ProtectTools estiver a ser executado. Pode ser visualizado através da aplicação Serviços na opção Ferramentas Administrativas no Painel de Controlo. Se este serviço não estiver a ser executado, o HP ProtectTools Security Manager tenta iniciá-lo quando as políticas de controlo do acesso do dispositivo forem aplicadas.

**sessão do histórico de conversação** Um ficheiro encriptado, que contém um registo de ambos os lados de uma conversação numa sessão de conversação (chat).

**Single Sign On** Funcionalidade que armazena informações de autenticação e permite a utilização do Security Manager para aceder a aplicações da Internet e do Windows que requerem a autenticação por palavra-passe.

**Sistema de ficheiros de encriptação (EFS, Encryption File System)** Sistema que encripta todos os ficheiros e subpastas da pasta seleccionada.

**smart card** Cartão de tamanho e forma semelhantes a um cartão de crédito, que armazena informações de identificação do proprietário. É utilizado para autenticar o proprietário perante um computador.

**token** Ver método de início de sessão em segurança.

**Token USB** Dispositivo de segurança que armazena informações identificativas de um utilizador. Tal como um Java Card ou leitor biométrico, é utilizado para autenticar o proprietário perante um computador.

**token virtual** Funcionalidade de segurança que tem um funcionamento muito semelhante ao de um Java Card e do respectivo leitor. O token é guardado na unidade de disco rígido do computador ou no registo do Windows. Quando inicia sessão com um token virtual, é-lhe pedido para introduzir um PIN para concluir a autenticação.

**Trusted Contact** Uma pessoa que tenha aceitado um convite de Contacto de confiança.

**TXT** Trusted Execution Technology.

**utilizador** Qualquer pessoa registada no Drive Encryption. Os utilizadores não administradores têm direitos limitados no Drive Encryption. Apenas se podem registar (com a aprovação do administrador) e iniciar sessão.

**utilizador autorizado** Um utilizador autorizado na vista Definições do Acesso do Utilizador a ver ou modificar definições da configuração nas vistas Configuração Simples ou Configuração da Classe do Dispositivo.

**Windows Logon Security** Protege a(s) sua(s) conta(s) do Windows exigindo a utilização de credenciais específicas para fins de acesso.

# Índice Remissivo