Software HP ProtectTools for Small Business Security, Versão 5.10

Guia do Usuário

Software HP ProtectTools for Small Business Security Versão 5.10 Guia do Usuário

HP Business PC

Segunda edição: maio de 2010

Número de peça: 610663-202

Sobre este guia

Este guia fornece informações sobre o Software HP ProtectTools para Segurança das Pequenas Empresas.

⚠ **AVISO!** O texto apresentado dessa maneira indica que a não-observância das orientações poderá resultar em lesões corporais ou morte.

△ **CUIDADO:** O texto apresentado dessa maneira indica que, se as instruções não forem seguidas, provavelmente haverá danos ao equipamento ou perda de informações.

NOTA: O texto apresentado dessa maneira fornece importante informação adicional.

Conteúdo

1 Introdução à segurança

A HP entende que seu tempo é extremamente valioso, e você precisa se concentrar no funcionamento e crescimento de seus negócio – não se preocupar com software de segurança adequado para proteger seu PC, seus dados e seus negócios.

É importante que você considere proativamente soluções de segurança que sejam fáceis de usar mas que forneçam forte proteção para seus ativos empresariais. Segurança não é “agradável de ter” – ela é uma “obrigação!”

A HP fornece proteção que é fácil de implantar e simples para usar…ela é chamada HP ProtectTools for Small Business.

O HP ProtectTools for Small Business é um software de segurança que fornece recursos para ajudam proteger contra acesso não autorizado ao computador e dados críticos. A funcionalidade de segurança aprimorada é fornecida pelos vários módulos do software HP ProtectTools:

O HP ProtectTools for Small Business oferece duas versões que podem ser utilizadas: Console Administrativo do HP ProtectTools Security Manager e HP ProtectTools Security Manager (para usuários em geral). Ambas as versões, do Administrador e do usuário estão disponíveis no menu **Iniciar** > **Todos os Programas**.

Função	Recursos
Console Administrativo do HP ProtectTools Security Manager	• Requer direitos de administrador no sistema Microsoft Windows para obter acesso • Acesso a módulos a ser configurados por um administrador e não disponíveis para usuários em geral • Permite configuração de segurança inicial e opções de configuração ou requisitos para todos os usuários
HP ProtectTools Security Manager (para usuários em geral)	• Permite que os usuários configurem opções fornecidas por um administrador • O acesso pode ser restrito e permite somente um usuário com controles limitados a alguns módulos HP ProtectTools

Os módulos do software HP ProtectTools podem ser pré-instalados, pré-carregados ou disponibilizados como uma opção configurável ou como uma opção pós-venda. Visite http://www.hp.com.br para obter mais informações.

Recursos do HP ProtectTools

A tabela seguinte detalha os principais recursos dos módulos do HP ProtectTools for Small Business:

Módulo	Principais recursos
Console Administrativo do HP ProtectTools Security Manager	• O assistente de configuração do Security Manager é utilizado pelos administradores para definir e configurar os níveis de segurança e métodos seguros para login. • Opções de configuração ocultas de usuários básicos. • Configura as definições do Device Access Manager e acesso de usuários. • As ferramentas para administradores são utilizadas para adicionar e remover usuários do HP ProtectTools e visualizar o status dos usuários.
HP ProtectTools Security Manager (para usuários em geral)	• Organiza, configura e altera nomes de usuários e senhas. • Configura e altera credenciais de usuários tais como senha do Windows e Smart Card. • Configura e altera Fragmentação, Purificação e Configurações do File Sanitizer. • Visualiza as configurações do Device Access Manager. • Configura Preferências e opções de Backup e Restauração.
Credential Manager for HP ProtectTools (Gerenciador de Senhas)	• Está desenvolvido para salvar, organizar e proteger seus nomes de usuário e senhas. • Permite que você defina a tela de login de websites e programas para acesso rápido e seguro. • Como você acessa vários websites e deseja salvar seu nome de usuário e senhas, digite-os no Gerenciador de Senhas para que você não tenha que lembrá-los novamente. A próxima vez que você visitar este site, o Gerenciador de Senhas irá inserir e enviar os dados automaticamente. • Permite que você crie senhas difíceis que não terá que escrever ou relembrar, e manterá suas contas mais seguras.
Drive Encryption for HP ProtectTools	• Fornece criptografia completa do volume total da unidade de disco rígido. • Força a autenticação de pré-inicialização para decodificar e acessar os dados na unidade de disco rígido. • Ajuda você atender os requisitos legais ou industriais para proteger dados confidenciais e sensíveis. • Proteja seus dados contra o acesso não autorizado criptografando totalmente a unidade de disco rígido. Se alguma vez o PC for roubado e a unidade for removida do sistema original e colocada em um sistema diferente, os dados não serão comprometidos.

Módulo	Principais recursos
File Sanitizer for HP ProtectTools	• Excluir dados no Windows não remove completamente os conteúdos de sua unidade de disco rígido. O Windows exclui somente a referência para os dados. Os dados ainda permanecerão na unidade de disco rígido até que outro arquivo seja sobregravado na mesma área da unidade de disco rígido com nova informação. Entretanto, com o File Sanitizer, você pode apagar completamente e automaticamente documentos, histórico do navegador arquivos temporários, etc. • Permite que você apague arquivos e pastas críticos (ou compartilhados) com segurança (informações ou arquivos pessoais, históricos ou dados relatados na Web, ou outros componentes de dados) em seu computador e periodicamente limpar sua unidade de disco rígido (gravar sobre dados previamente excluídos).
Device Access Manager for HP ProtectTools	• Pode ser usado para controlar o acesso às unidades de mídia, USB e outros dispositivos de hardware com base nos perfis do usuário. • Permite que você limite o recurso de um usuário para armazenar dados críticos. • Evita que usuários utilizem dispositivos de armazenamento externo, como um reprodutor de música pessoal, que copie dados de um PC ou de sua rede. • Evita que usuários introduzam vírus no sistema através de mídia externa. • Permite que você desative seletivamente um grupo de dispositivos (como chaves, dispositivos de gravação, reprodutores de música pessoais, etc.) para usuários ou grupos de usuários. A pessoa com uma senha de administrador pode efetuar login e copiar informações do PC, mas outros usuários não podem.

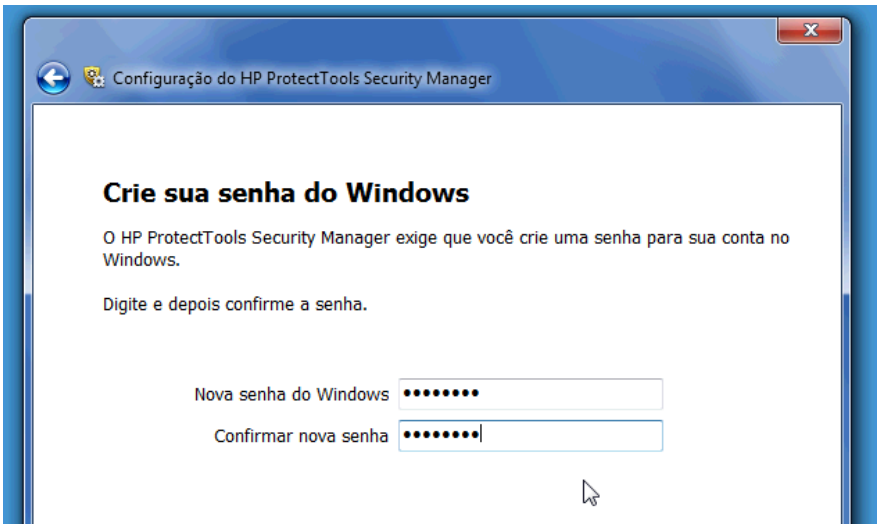
2 Guia de Configuração Fácil para a maioria das opções úteis

Este Guia de Configuração Fácil foi desenvolvido para demonstrar os passos básicos para ativar a maioria das opções úteis e comuns com o HP ProtectTools for Small Business. Existem numerosas ferramentas e opções disponíveis neste software que irão permitir que você ajuste suas preferências e defina seu controle de acesso. O Guia de Configuração Fácil focará em fazer com que cada módulo execute com o menor esforço e tempo de configuração. Para obter informação adicional, apenas selecione o módulo no qual está interessado e clique na “?” ou no botão Ajuda no canto superior direito. Este botão irá fornecer a informação automaticamente para ajudá-lo com a janela atualmente exibida.

Passos iniciais

1. Abra o HP ProtectTools Security Manager a partir do ícone Gadget, ícone na barra de tarefas (escudo dourado), ou clique em **Iniciar** > **Todos os Programas** > **HP**.

2. Digite sua senha do Windows ou crie uma senha do Windows.

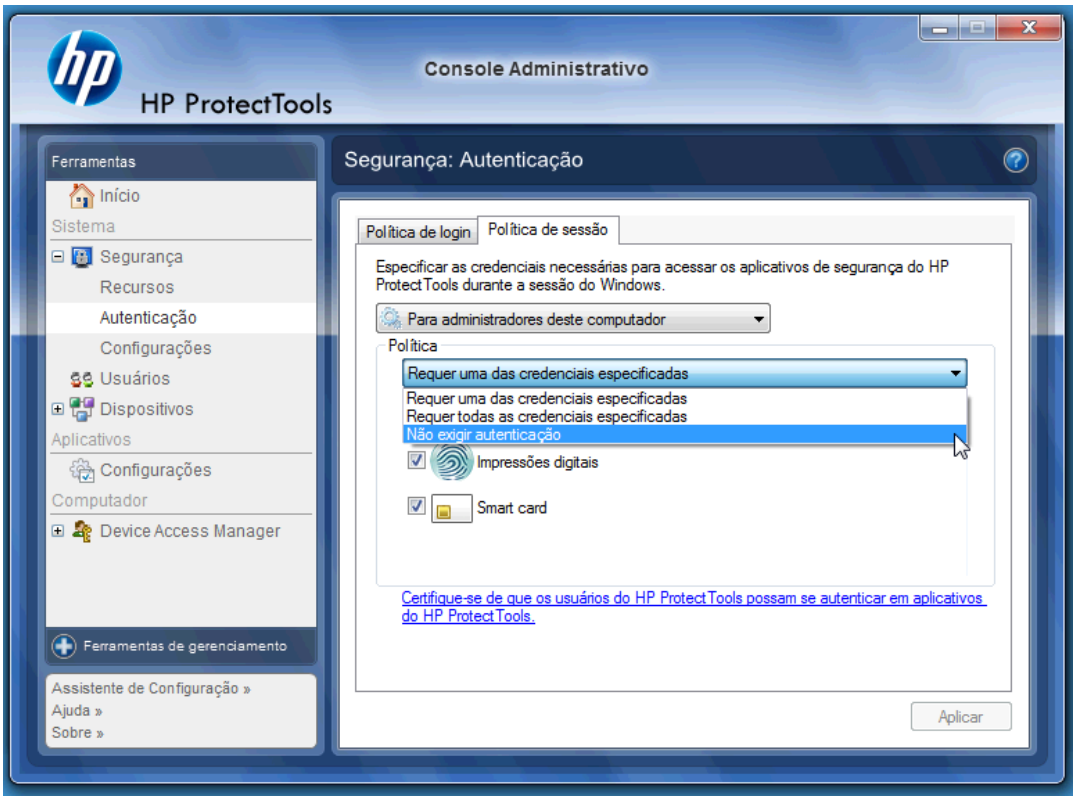


3. Conclua o assistente de configuração.

NOTA: Por padrão, o HP ProtectTools Security Manager está definido para Diretiva de Autenticação Forte.

Esta definição é destinada a evitar o acesso não autorizado enquanto estiver acessando o Windows e será usado quando for necessária alta segurança ou se os usuários estiverem frequentemente ausentes de seus sistemas no decorrer do dia. Se você desejar alterar esta configuração, clique na guia Política de sessão, e faça suas seleções.

Para configurar o HP ProtectTools Security Manager para usar somente o login inicial do Windows para a sessão completa, altere a configuração seguinte.



Para ter o HP ProtectTools Security Manager autenticado somente uma vez durante o login no Windows:

1. Clique em **Iniciar** > **Todos os Programas** > **HP** > **Console Administrativo HP ProtectTools**.
2. Na tela da esquerda **Ferramentas**, selecione **Autenticação** a partir do grupo **Segurança**.
3. Clique na guia **Política de sessão** e selecione **Não exigir autenticação** a partir do menu instantâneo embaixo de **Política**.
4. Quando concluir clique no botão **Aplicar**.

Credential Manager for HP ProtectTools (Gerenciador de Senhas)

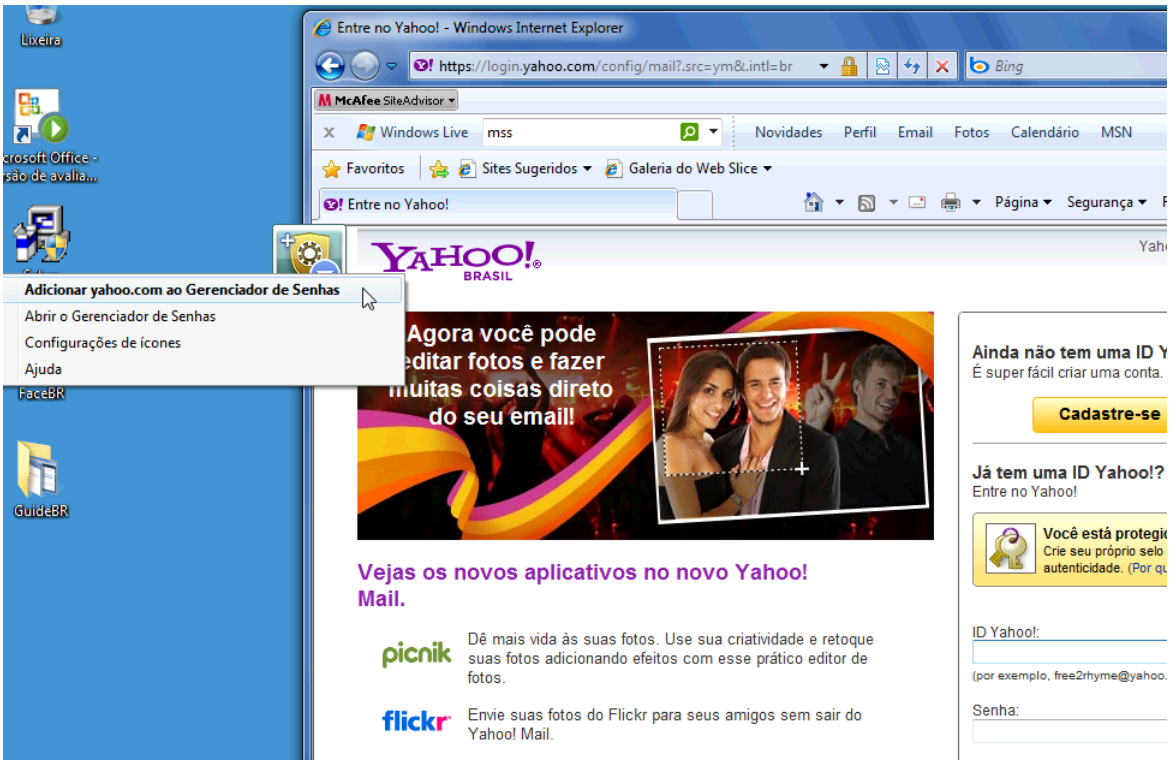
Senhas! Todos temos bastante delas – especialmente se você acessa websites regularmente ou usa aplicativos que requerem login. O usuário comum usa a mesma senha para todos os aplicativos e websites, ou às vezes, se torna muito criativo e rapidamente esquece quais senhas vão com quais aplicativos.

Não seria ótimo ter um software que lembre automaticamente suas senhas para sites que não são críticos ou dão a você ao recurso para discernir quais sites deve lembrar e quais deve omitir? Credential Manager for HP ProtectTools é a resposta. Credential Manager é o gerenciador de senhas que oferece a você esse recurso. Uma vez que você conecta o PC, Credential Manager irá fornecer sua senha ou credenciais, o que for necessário.

Quando você acessa qualquer aplicativo ou website requerendo credenciais, o Credential Manager reconhecerá automaticamente o site, e perguntará se deseja que o software lembre sua informação. Se você aceitar, nunca precisará se lembrar qual é a senha novamente. Você pode recusar o pedido para lembrar sua informação se desejar excluir certos sites.

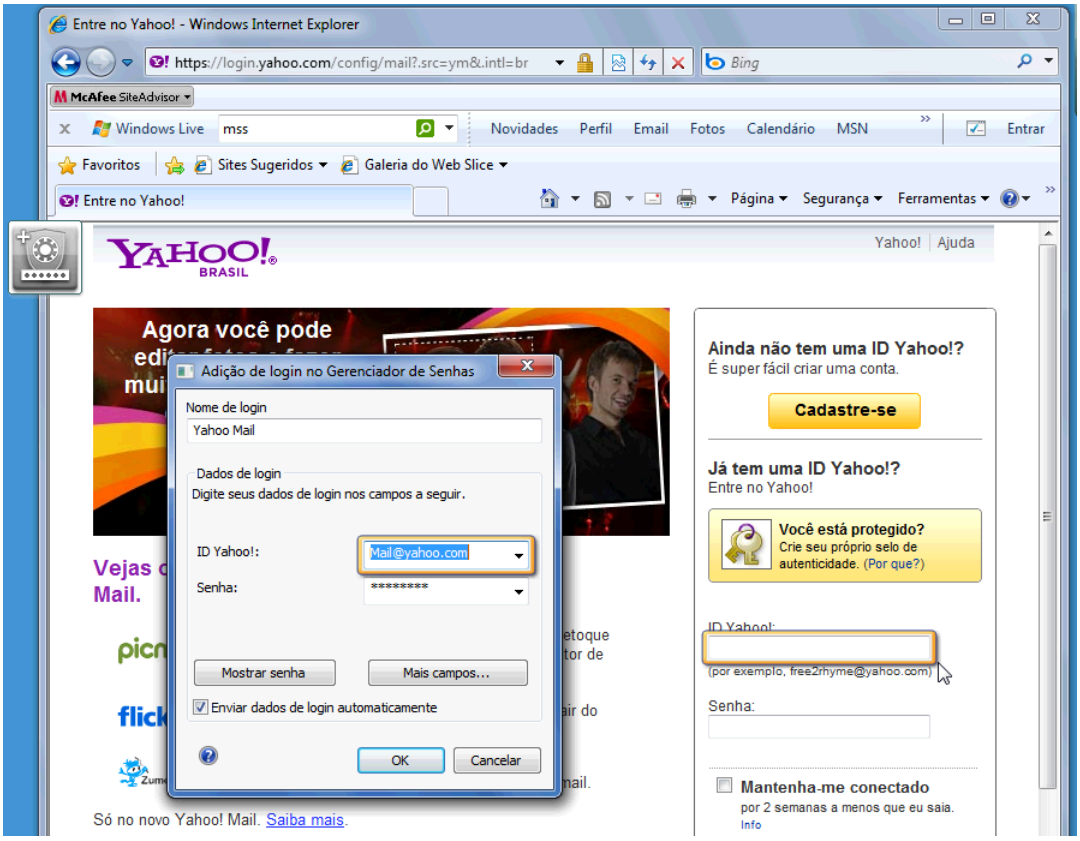
Para Iniciar salvando locais na web, nomes de usuário e senhas:

1. Como um exemplo, navegue em sua conta de web mail e informe para o Credential Manager (clique em um ícone) para adicionar a autenticação na web.



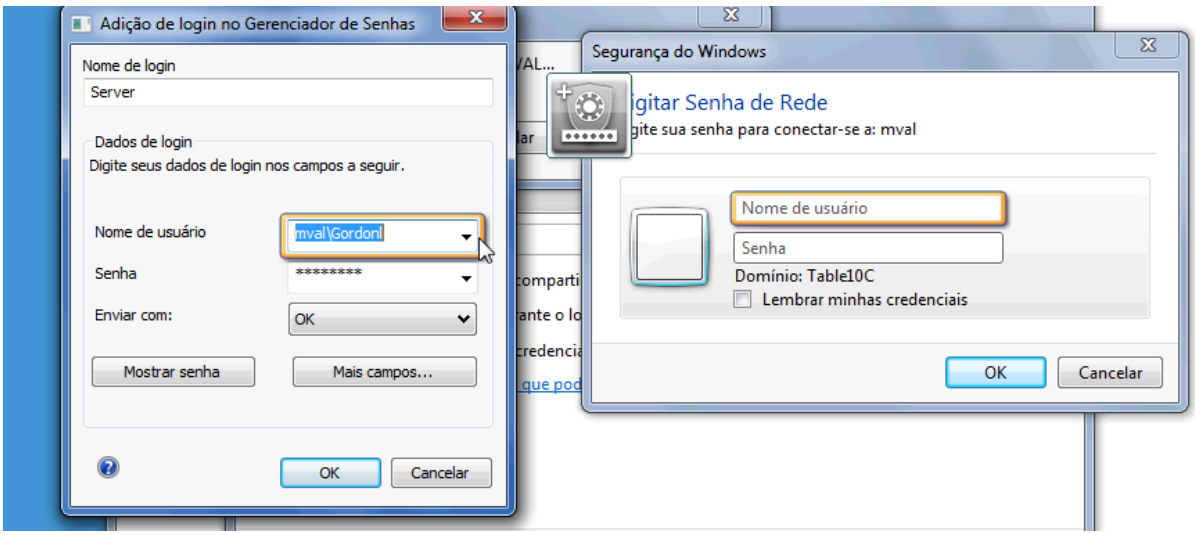
2. Nomeie o link (opcional) e digite um nome de usuário e senha no Credential Manager.

NOTA: A página da web irá realçar as áreas do Credential Manager que usará agora e para visitas subsequentes.



3. Quando concluir, clique no botão **OK**.

4. O Credential Manager também pode salvar seu nome de usuário e senha para compartilhar rede ou mapear unidades na rede.



Visualizar e gerenciar autenticações salvas no Credential Manager

As vantagens do Credential Manager são que você pode visualizar, gerenciar, fazer backup e iniciar suas autenticações a partir de um local central. Credential Manager também admite a inicialização de sites salvos a partir do Windows.

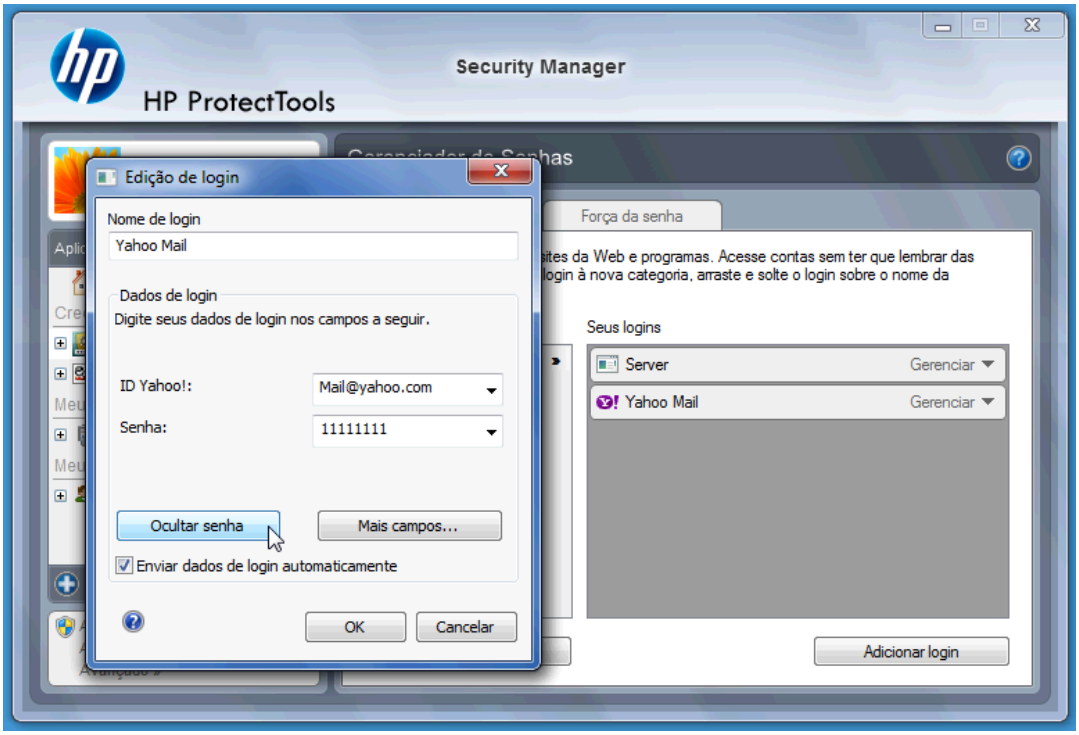
Para abrir o HP Recovery Manager, utilize um dos seguintes métodos:

- Use a combinação no teclado de Ctrl + Windows + H para abrir o Gerenciador de Senhas. Selecionando **Abrir** irá iniciar e autenticar rapidamente o atalho salvo.

OU

- Selecione a guia **Gerenciar** no Gerenciador de Senhas para abrir o HP ProtectTools Security Manager onde as credenciais podem ser editadas.

A opção **Editar** do Credential Manager permite que você visualize e modifique nome, nome de login, e até revele as senhas.



HP ProtectTools for Small Business permite que faça backup e/ou copie em outro PC todas as credenciais e configurações.

File Sanitizer for HP ProtectTools

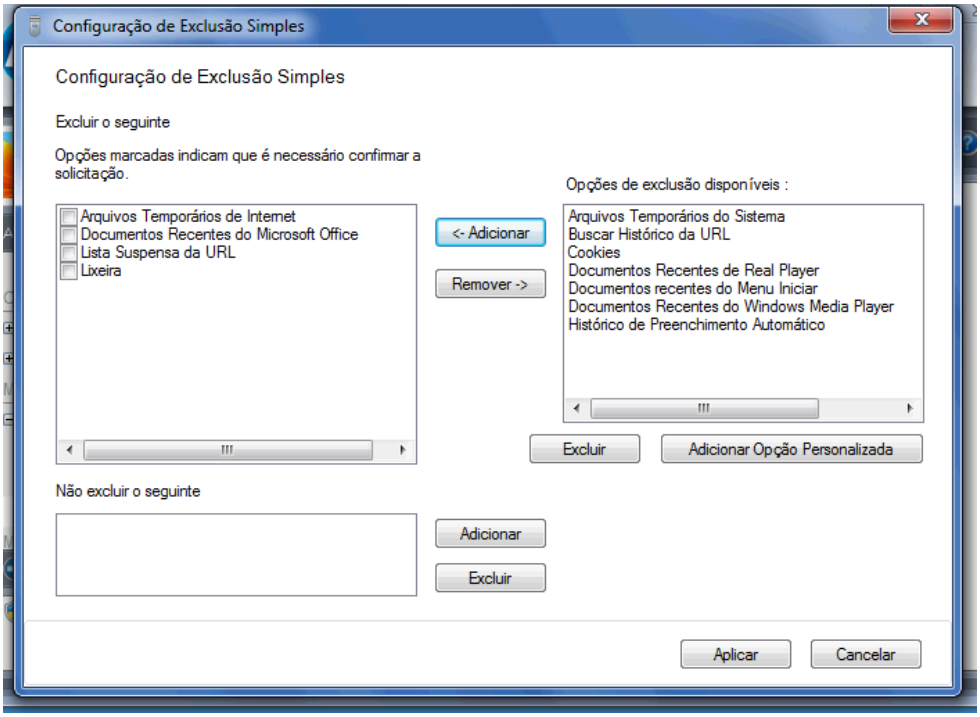
File Sanitizer está destinado a tornar verdadeiramente difícil que uma pessoa não autorizada recupere dados que você tenha excluído. Existem várias opções disponíveis para você apagar manualmente ou estabelecer uma programação regular para apagar arquivos e pastas selecionados incluindo histórico do navegador.

Abaixo estão algumas definições de configuração simples.

Para iniciar apagando permanentemente seus dados excluídos, selecione os arquivos ou pastas que você precisa mais.

1. Navegue para **Security Manager** > **File Sanitizer** > **Configurações**. Selecione **Configuração de Exclusão Simples** e clique no botão **Visualizar Detalhes**.

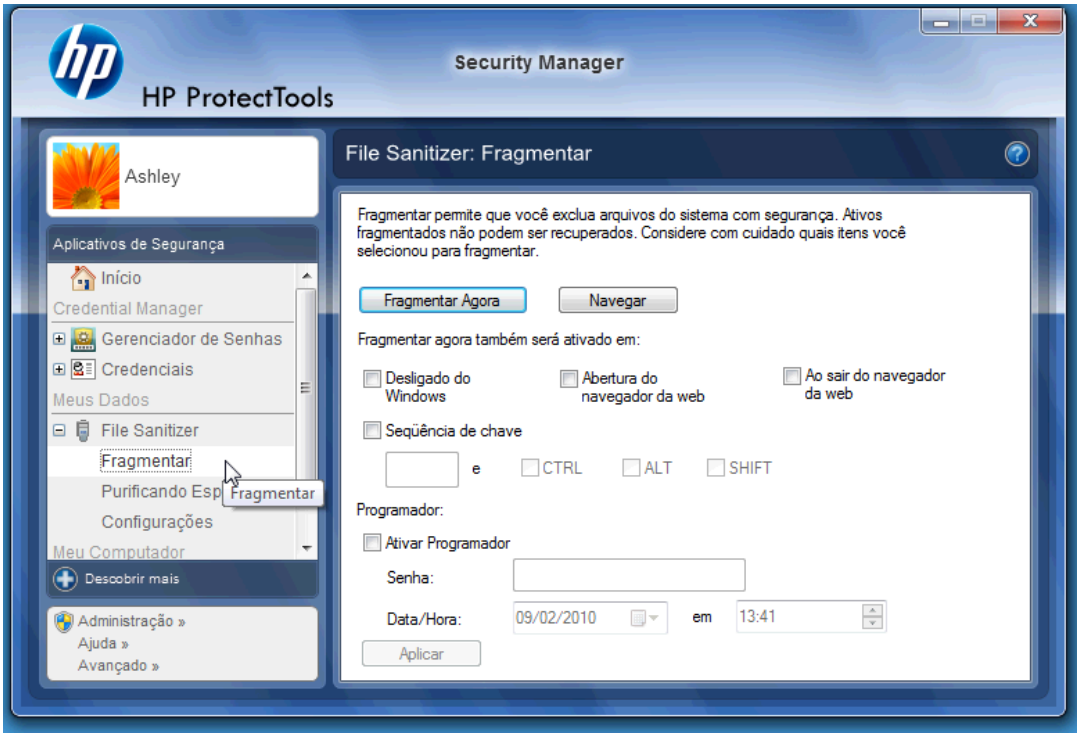
2. Selecione os itens no lado direito da janela do Configuração de Exclusão Simples que você deseja excluir permanentemente em períodos regulares e clique no botão **<-Adicionar** para mover os itens selecionados para o lado de Excluir.



3. Inicie com a Lixeira e adicione outros itens que você deseja Fragmentar.

4. Clique no botão **Aplicar** quando você tiver selecionado tudo que deseja apagar permanentemente.

5. Navegue até a opção **Fragmentar** e configure quando você deseja que a ação seja executada. O botão **Fragmentar Agora** apaga imediatamente os itens selecionados na janela Configuração de Exclusão Simples que você acabou de configurar.



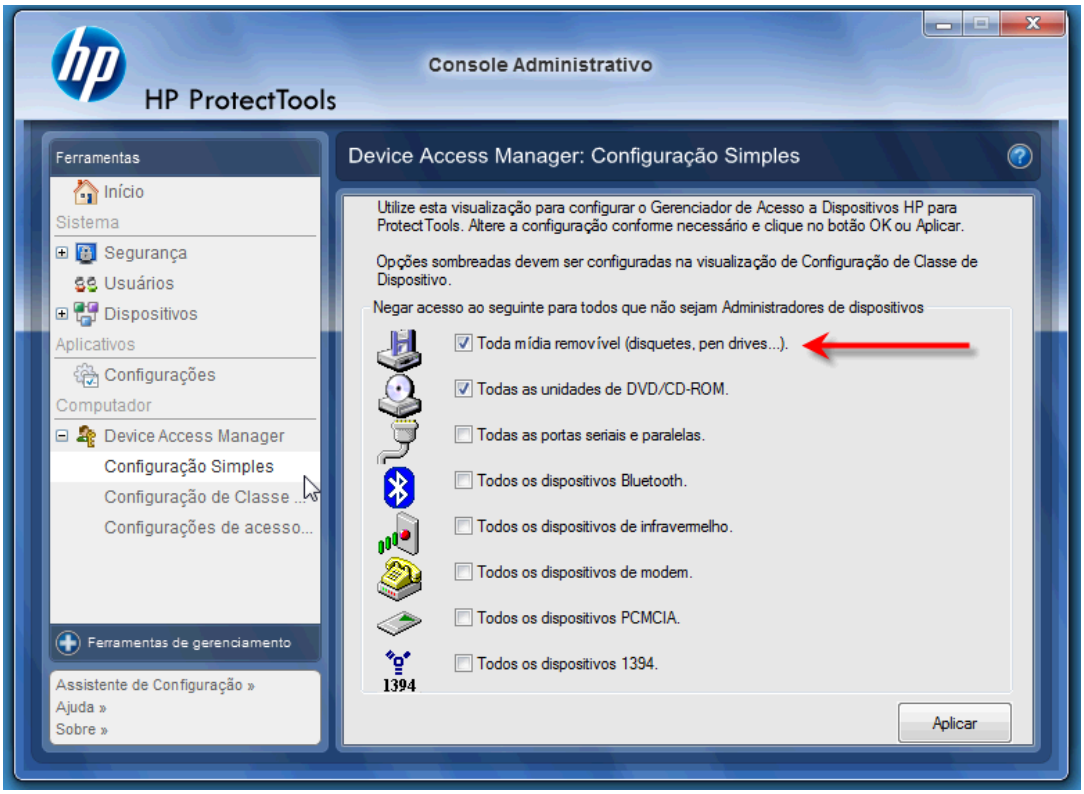
6. Um pequeno pop-up aparece na área de trabalho todo o tempo desde que Fragmentar é iniciada até concluir.

Device Access Manager for HP ProtectTools

O Device Access Manager pode ser usado para restringir o uso de vários dispositivos de armazenamento internos e externos para que seus dados permaneçam seguros na unidade de disco rígido e não saiam de sua empresa. Um exemplo de como seria permitir que um usuário acesse seus dados mas os bloqueia para cópia em um CD reprodutor de música pessoal ou dispositivo de memória USB. Abaixo está uma maneira fácil de fazer isso.

1. Clique em **Iniciar** > **Todos os Programas** > **HP** > **Console Administrativo** > **Device Access Manager** > **Configuração Simples**.

2. Selecione o dispositivo de hardware que você deseja restringir e clique no botão **Aplicar** para finalizar o processo.

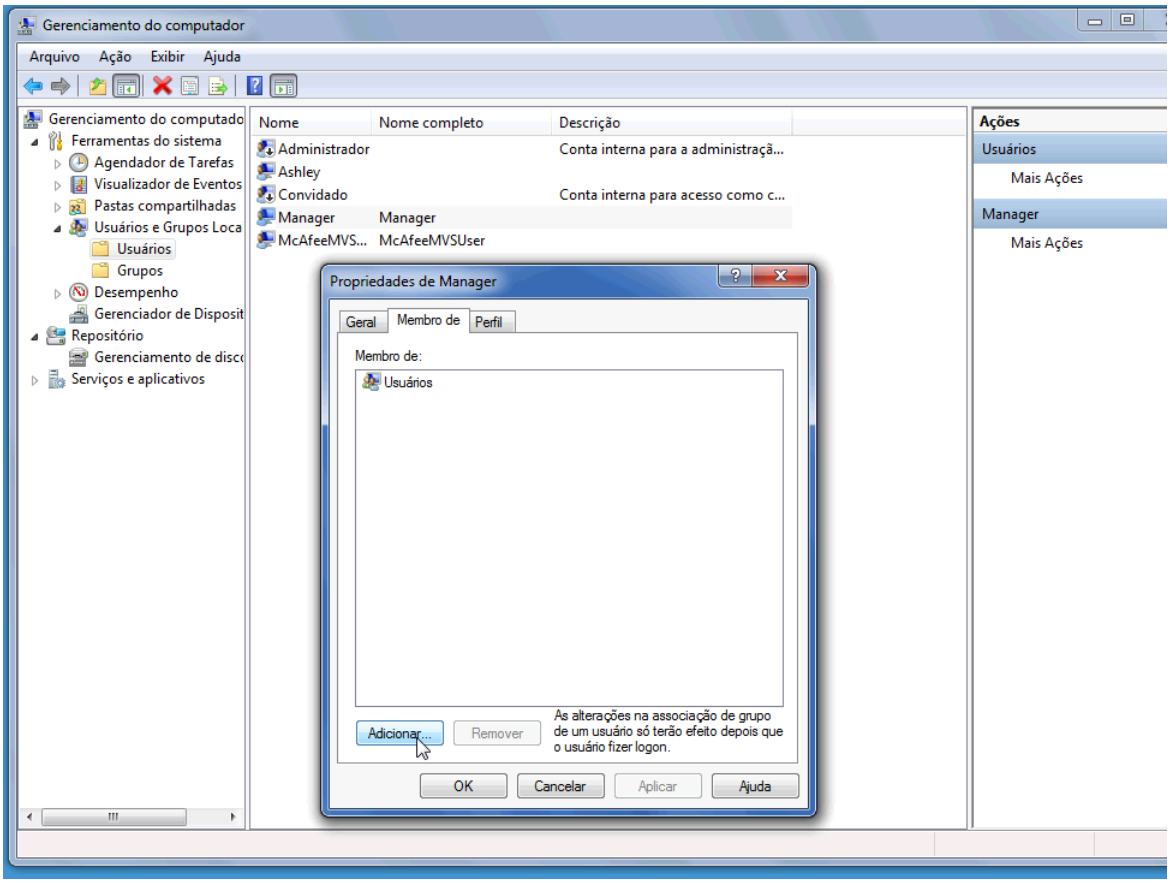


3. O próximo passo abaixo é para selecionar quem continua tendo acesso enquanto qualquer outra pessoa é bloqueada.

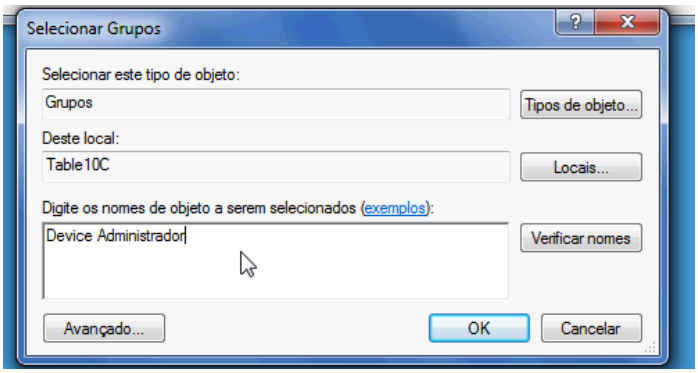
4. Navegue e selecione **Meu Computador**, clique com o botão direito e selecione **Gerenciar** > **Gerenciamento do Computador** > **Ferramentas do Sistema** > **Usuários e Grupos Locais** > **Usuários**.

5. Clique duas vezes no usuário (neste exemplo “Gerenciador”) que você deseja restringir o acesso ao hardware bloqueado.

6. Na guia **Membro de**, clique no botão **Adicionar**.



7. Na janela **Selecionar Grupos** você pode usar a opção **Avançado** ou apenas digitar no grupo “Administradores de Dispositivo”. Clique no botão **OK** e finalize fechando a janela clicando nos botões OK. Você deve fazer logoff e fazer login novamente para obter as permissões.



Agora todas as unidades de armazenamento internas e externas incluindo unidades de CD, unidades USB, reprodutores de música pessoal etc. não funcionam exceto para a pessoa(s) no grupo “Administradores de Dispositivo”.

Drive Encryption for HP ProtectTools

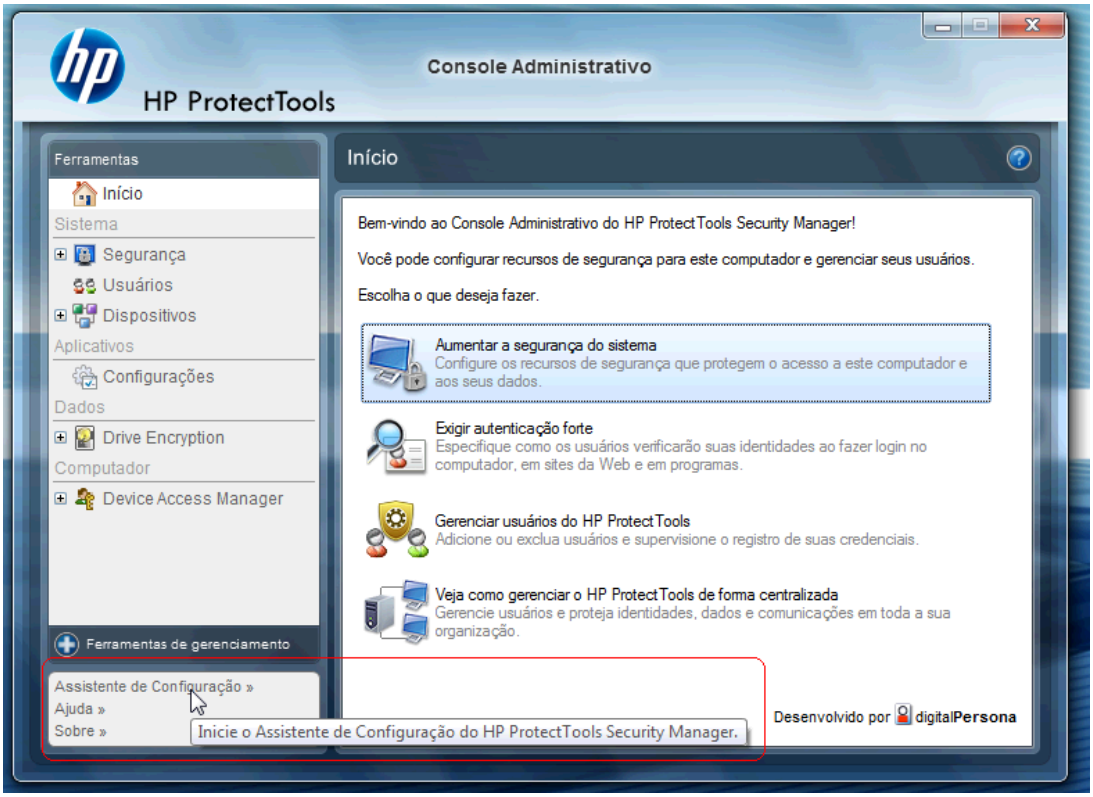
Drive Encryption for HP ProtectTools é um software usado para proteger seus dados criptografando toda a unidade de disco rígido. Os dados em sua unidade de disco rígido permanecerão protegidos se seu PC alguma vez for roubado e/ou se a unidade de disco rígido for removida do sistema original e colocada em um sistema diferente.

Um benefício de segurança adicional é que o Drive Encryption requer autenticação correta usando seu nome e senha de usuário antes que o sistema possa inicializar. Este processo é chamado de Autenticação antes da inicialização.

Para tornar fácil para você, usuários do Windows, domínio, Credential Manager for HP ProtectTools e HP ProtectTools Security Manager todos interagem com Drive Encryption permitindo fácil sincronização de senhas.

Siga as etapas abaixo para ativar o Drive Encryption for HP ProtectTools.

1. Clique em **Iniciar** > **Todos os programas** > **HP** > **Console Administrativo do HP ProtectTools** > **Ferramentas de gerenciamento** > **Assistente de Configuração**. A seguinte tela é exibida



2. Selecione **Avançar** na tela Bem-vindo.
3. É requerida a senha do Windows para iniciar o assistente de ativação > **Avançar**.
4. Verifique a caixa do **Drive Encryption** e selecione **Avançar**.

5. A janela de configuração do Drive Encryption abaixo exibe as unidades disponíveis para serem criptografas e irá requerer uma unidade flash USB para armazenar a chave de recuperação da criptografia. Mantenha esta chave de recuperação salva e segura pois ela será usada para recuperar os dados ou para acessar a unidade se a senha de pré-inicialização for perdida ou falhar.

6. Selecione **Avançar**, conclua o processo e selecione **Finalizar**. Quando for solicitado, remova a unidade flash USB e reinicie o sistema quando estiver pronto.

7. Quando o sistema reiniciar a partir da unidade de disco rígido, o Drive Encryption solicitará sua senha do Windows. Digite a senha e clique em **OK**.

NOTA: O computador pode mostrar-se executando lentamente enquanto a unidade é criptografada. Uma vez que esteja totalmente criptografada, o sistema retorna ao normal. Uma vez que os dados na unidade são acessados, eles serão criptografados ou decodificados como for necessário.

Também observe que a autenticação do Drive Encryption será em “cadeia” através do login do Windows no Credential Manager diretamente na área de trabalho sem ter que digitar a senha duas vezes.

3 Benefícios do HP ProtectTools for Small Business

Acesso ao Software HP ProtectTools para Segurança das Pequenas Empresas

Para acessar o HP ProtectTools Security Manager a partir do menu Iniciar do Windows:

- No Windows, clique em **Iniciar**, clique em **Todos os Programas**, em seguida clique em **HP ProtectTools Security Manager**.

Para acessar o Console Administrativo do HP ProtectTools Security Manager a partir do menu Iniciar do Windows:

- No Windows, clique em **Iniciar**, clique em **Todos os Programas**, em seguida clique em **Console Administrativo do HP ProtectTools**.

Alcançando os principais objetivos de segurança

Os módulos do HP ProtectTools podem funcionar em conjunto para fornecer soluções para diversos problemas de segurança, incluindo os principais objetivos de segurança a seguir:

- Restrição de acesso a dados confidenciais
- Prevenção contra acesso não-autorizado a partir de locais internos ou externos
- Criação de políticas de senhas fortes

Restrição de acesso a dados sensíveis

Suponha que um auditor de contratos estiver trabalhando no local e tenha recebido acesso para revisar dados financeiros sensíveis; você não deseja que o auditor possa imprimir os arquivos ou salvá-los em um dispositivo de gravação como um CD. O recurso seguinte ajuda a restringir o acesso a dados:

O Device Access Manager for HP ProtectTools permite aos administradores restringir o acesso a dispositivos de gravação, assim informações sensíveis não podem ser impressas ou copiadas a partir da unidade de disco rígido em uma mídia removível. Consulte Configuração de classe de dispositivo (avançado) na página 49.

Prevenção contra acesso não-autorizado a partir de locais internos ou externos

O acesso não autorizado a um business PC desprotegido apresenta um verdadeiro risco tangível a dados críticos como informações sobre serviços financeiros, um executivo ou de uma equipe de Pesquisa e Desenvolvimento, e a informações privadas como registro de pacientes ou registros financeiros pessoais. Os recursos seguintes ajudam a evitar acesso não autorizado:

- O recurso de autenticação de pré-inicialização, se ativado, ajuda a impedir o acesso ao sistema operacional. Consulte os seguintes capítulos:
  - Credential Manager for HP ProtectTools (Gerenciador de Senhas) na página 36
  - Drive Encryption for HP ProtectTools na página 33
- O Credential Manager for HP ProtectTools ajuda a assegurar que um usuário não autorizado não obtenha senhas de acesso aos aplicativos protegidos por senha. Veja o seguinte capítulo:
  - Credential Manager for HP ProtectTools (Gerenciador de Senhas) na página 36
- O Device Access Manager for HP ProtectTools permite aos administradores restringirem o acesso aos dispositivos de gravação, assim informações sensíveis não podem ser copiadas a partir da unidade de disco rígido. Veja o seguinte capítulo:
  - Device Access Manager for HP ProtectTools na página 48
- O File Sanitizer permite que você exclua dados com segurança triturando arquivos e pastas críticos ou purificando espaço livre na unidade de disco rígido (gravar sobre dados que você tenha previamente excluído, mas ainda estão presentes na unidade de disco rígido para tornar mais difícil a recuperação dos dados). Consulte o seguinte capítulo:
  - File Sanitizer for HP ProtectTools na página 41

Criação de políticas de senhas fortes

Se você requer o uso do critério de senha forte (uma senha complicada que seja difícil para hacker) para dúzias de aplicativos e bancos de dados com base na Web, o Credential Manager for HP ProtectTools fornece um repositório protegido para senhas e conveniência de uma única autenticação. Veja o seguinte capítulo:

- Credential Manager for HP ProtectTools (Gerenciador de Senhas) na página 36

Elementos adicionais de segurança

Atribuição de funções de segurança

Para proteger adequadamente os dados, uma prática importante é dividir as responsabilidades e os direitos entre vários tipos de administradores e usuários.

NOTA: Em uma organização pequena ou para uso individual, esses perfis podem ser mantidos pela mesma pessoa.

Para o HP ProtectTools for Small Business, as obrigações e os privilégios da segurança podem ser divididos entre as seguintes funções:

- Administrador - Aplica e gerencia os recursos de segurança. Pode também ativar e desativar alguns recursos.
- Usuário - Utiliza os recursos de segurança.

Gerenciamento de senhas do HP ProtectTools

A maioria dos recursos do HP ProtectTools Security Manager são protegidos por senhas. A tabela a seguir lista as senhas mais usadas, o módulo de software em que a senha é definida e a função da senha.

As senhas que são definidas e usadas somente por administradores são indicadas nesta tabela. Todas as outras senhas podem ser definidas por usuários regulares.

Senha do HP ProtectTools	Definida neste módulo do HP ProtectTools	Função
Senha de login do Gerenciador de Senhas	Password Manager	Esta senha oferece duas opções: • Pode ser usado em um login separado para acessar o Gerenciador de Senhas após o login no Windows. • Pode ser usada em lugar do processo de login do Windows, permitindo acessar simultaneamente o Windows e o Gerenciador de Senhas.
Senha do Utilitário de configuração **NOTA:** Também conhecida como senha de administrador do BIOS, de Configuração F10 ou configuração de segurança	BIOS, pelo administrador	Protege o acesso ao utilitário Computer Setup.
Senha de inicialização	BIOS	Protege o acesso ao conteúdo do computador quando este for ligado, reiniciado ou sair da hibernação.
Senha de login do Windows	Painel de controle do Windows	Pode ser usada para login normal.

Criação de uma senha de segurança

Ao criar senhas, é preciso primeiro seguir as especificações definidas pelo programa. Em geral, entretanto, considere as instruções a seguir para ajudar a criar senhas fortes e reduzir as chances de sua senha ser comprometida:

- Use senhas com mais de 6 caracteres, de preferência mais de 8.
- Misture letras maiúsculas e minúsculas na senha.
- Sempre que possível, misture caracteres alfanuméricos e inclua caracteres especiais e sinais de pontuação.

- Substitua caracteres especiais ou números por letras em uma palavra-chave. Por exemplo, use o número 1 para substituir as letras I ou L.
- Combine palavras de 2 ou mais idiomas.
- Divide uma palavra ou frase com números ou caracteres especiais no meio, por exemplo, “Mary2-2Cat45.”
- Não use uma senha que poderia aparecer em um dicionário.
- Não use seu nome como senha, ou qualquer outra informação pessoal, como data de aniversário, nomes de animais de estimação, ou nome de solteira da mãe, mesmo se soletrar invertido.
- Altere as senhas regularmente. É possível mudar uma senha apenas adicionando dois caracteres.
- Se escrever sua senha, não a guarde em um local bastante visível, muito perto do computador.
- Não guarde a senha em um arquivo, como um e-mail, no computador.
- Não compartilhe contas nem informe sua senha a qualquer pessoa.

Backup de credenciais e configurações

Utilize a ferramenta Backup and Recovery no HP ProtectTools Security Manager como um local centralizado do qual você possa fazer backup e restaurar credenciais com segurança a partir de módulos instalados do HP ProtectTools.

4 Console Administrativo do HP ProtectTools Security Manager

Sobre o Console Administrativo do HP ProtectTools

A administração do HP ProtectTools Security Manager é fornecida através do Console Administrativo.

Utilizando o console, o administrador local pode:

- Ativar ou desativar recursos de segurança
- Gerenciar usuários do computador
- Ajustar parâmetros específicos de dispositivo
- Configurar aplicativos do Security Manager
- Adicionar aplicativos adicionais do Security Manager

Uso do Console Administrativo

O Console Administrativo do Security Manager é o local central para administrar o HP ProtectTools Security Manager.

Para abrir o console:

- Selecione **Iniciar** > **Todos os Programas** > **Console Administrativo do HP ProtectTools**, ou
- Clique no link **Administração** no canto inferior esquerdo do console Security Manager.

O Console Administrativo consiste de duas telas: uma tela à esquerda e uma à direita. A tela da esquerda contém as ferramentas administrativas. A tela da direita contém a área de trabalho para configurar as ferramentas.

A tela da esquerda do Console Administrativo consiste do seguinte:

- **Início** - Fornece fácil acesso para tarefas comumente usadas, incluindo ativação de recursos de segurança, especificação de credenciais de segurança e gerenciamento de usuários.
- **Sistema** - Gerencia configurações dos recursos de segurança de todo o sistema, usuários e dispositivos de autenticação como leitores de smart card.
- **Aplicativos** - Inclui ferramentas para configuração do comportamento do Security Manager e seus aplicativos.
- **Dados** - Fornece ferramentas para fazer backup e recuperação de chaves de criptografia.

- **Computador** - Fornece opções de segurança avançada para desautorizar seletivamente vários tipos de dispositivos que podem comprometer a segurança do PC e definir permissões de acesso para vários usuários e grupos.
- **Ferramentas de Gerenciamento** - Abre seu navegador padrão em uma página da web onde você pode descobrir aplicativos e ferramentas de gerenciamento adicionais que aumentam os recursos do Security Manager bem como meios para permanecer notificado quando novos aplicativos e atualizações estiverem disponíveis.
- **Links** - Fornece o seguinte:
  - **Assistente de Configuração** - Inicia o Assistente de Configuração, que guia você através da configuração inicial do Security Manager.
  - **Ajuda** - Abre o arquivo de ajuda que fornece informações sobre o Security Manager e seus aplicativos.
  - **Sobre** - Exibe informações sobre o Security Manager, incluindo o número da versão e aviso sobre direitos autorais.

Passos Iniciais com o Assistente de Configuração

A administração do HP ProtectTools Security Manager requer privilégios administrativos.

O Assistente de Configuração do HP ProtectTools Security Manager guia você através da configuração dos recursos de segurança. Entretanto, existem inúmeras funcionalidades adicionais disponíveis através do Console HP ProtectTools Security Manager. As mesmas configurações encontradas no assistente, bem como os recursos de segurança adicional, podem ser configurados através do console, acessando a partir do menu Iniciar do Windows ou a partir de um link dentro do console Administrativo. Essas configurações aplicam para o computador e todos os usuários que compartilham o computador.

A primeira vez que efetuar login no Windows, você será solicitado a configurar o HP ProtectTools Security Manager. Clique em **OK** para iniciar o assistente de configuração do Security Manager, que guiará você através dos passos básicos na configuração do programa.

NOTA: Você também pode iniciar o Assistente de Segurança clicando no botão **Assistente de Segurança** na seção inferior da tela da esquerda do Console Administrativo.

Siga as instruções na tela até que a configuração do Assistente de Configuração seja concluída.

Se você não concluir o assistente, ele iniciará automaticamente até que você clique em **Não Mostrar este assistente novamente**.

Para usar os aplicativos do HP ProtectTools Security Manager, inicie o HP ProtectTools Security Manager a partir do menu **Iniciar** ou clicando com o botão direito no ícone **Security Manager** na barra de tarefas da área de notificação (bandeja do sistema). O console do Security Manager e seus aplicativos estão disponíveis para todos os usuários que compartilham este computador.

Configuração de seu sistema

O grupo de aplicativos **Sistema** é acessado a partir do menu **Ferramentas** no lado esquerdo do Console Administrativo.

Usando os aplicativos incluídos neste grupo, você pode configurar e gerenciar os critérios e configurações para este computador, seus usuários e dispositivos.

Os seguintes aplicativos estão incluídos no grupo Sistema.

- **Segurança** - Gerencia os recursos de segurança, critérios de autenticação e outras configurações que governam como os usuários autenticam quando efetuam login no computador ou nos aplicativos do HP ProtectTools.
- **Usuários** - Configura, gerencia e inscreve os usuários deste computador.
- **Dispositivos** - Gerencia configurações para dispositivos de segurança integrados ou conectados no computador.

Ativação de recursos de segurança

Os recursos de segurança ativados aqui aplicam a todos os usuários deste computador.

1. Na tela da esquerda do Console Administrativo, expanda **Segurança**, e clique em **Recursos**.
2. Para ativar um recurso de segurança, clique na caixa de verificação correspondente próxima a **Segurança do Login do Windows** e/ou **Drive Encryption**.
   - **Segurança do Login do Windows** - protege sua(s) conta(s) no Windows solicitando o uso de credenciais específicas para acessar.
   - **Drive Encryption** - protege seus dados criptografando sua(s) unidade(s) de disco rígido, tornando as informações ilegíveis para aqueles sem autorização apropriada.
3. Clique no botão **Avançar**.
4. Clique no botão **Aplicar**.

Definição dos critérios de autenticação do Security Manager

Os critérios de autenticação do Security Manager para este computador são definidos em duas guias, Login e Sessão, que especificam as credenciais requeridas para autenticar cada classe de usuário que acessa o computador e os aplicativos do HP ProtectTools durante uma sessão de usuário.

Guia Login

Para especificar as credenciais requeridas para acessar o computador e efetuar login no Windows:

1. Na tela da esquerda do Console Administrativo, expanda **Segurança**, e clique em **Autenticação**.
2. Na guia **Login**, selecione a categoria de usuário a partir da lista suspensa.
3. Na seção **Política**, especifique a(s) credencial(ais) de autenticação requeridas para a categoria de usuário selecionada clicando na caixa de verificação ou caixas próximas às credenciais listadas. Você deve especificar pelo menos uma credencial.
4. Na lista suspensa da seção **Política**, escolha QUALQUER (somente uma) das credenciais especificadas é requerida, ou se TODAS as credenciais especificadas são requeridas para autenticar um usuário.
5. Clique no botão **Aplicar**.

Guia Sessão

Para definir os critérios que governam as credenciais requeridas para autenticar um usuário quando efetua login nos aplicativos do HP ProtectTools durante uma sessão no Windows.

1. Na tela da esquerda do Console Administrativo, expanda **Segurança**, e clique em **Autenticação**.
2. Na guia **Sessão**, selecione a categoria de usuário.
3. Na seção **Política**, especifique a(s) credencial(ais) de autenticação requeridas para a categoria de usuário selecionada clicando na caixa de verificação ou caixas próximas às credenciais listadas. Você deve especificar pelo menos uma credencial.
4. Na lista suspensa da seção **Política**, escolha QUALQUER (somente uma) das credenciais especificadas é requerida, ou se TODAS as credenciais especificadas são requeridas para autenticar um usuário.
5. Clique no botão **Aplicar**.

Definição de Configurações

Você pode especificar quais configurações de segurança avançada permitir. Para editar as configurações:

1. Na tela da esquerda do Console Administrativo, expanda **Segurança**, e clique em **Configurações**.
2. Clique na caixa de verificação apropriada para ativar ou desativar uma configuração específica.
3. Clique no botão **Aplicar** para salvar as alterações.

NOTA: A configuração **Permitir login de Um Passo** permite que o usuário desse computador pule o login no Windows se a autenticação foi executada no nível do BIOS.

Gerenciamento de Usuários

No aplicativo Usuários, o administrador do Windows pode gerenciar os usuários deste computador e os critérios que os afetam. Para acessar o aplicativo Usuários no Console Administrativo, clique em **Usuários**.

Os usuários do HP ProtectTools estão listados e verificados junto aos critérios de autenticação definidos através do Security Manager e junto às credenciais requeridas para atender esses critérios.

Para visualizar os critérios em vigor para um usuário específico, selecione o usuário a partir da lista e clique no botão **Visualizar Políticas**.

Para supervisionar usuários enquanto eles registram credenciais, selecione o usuário a partir da lista e clique no botão **Registrar**.

Adição de um usuário

Este processo adiciona usuários para a lista de login. Antes de você adicionar um usuário, ele já deve ter uma conta de usuário do Windows no computador e deve estar presente durante o seguinte procedimento para fornecer a senha.

Para adicionar um Usuário na lista de usuários:

1. Clique em **Iniciar**, clique em **Todos os Programas**, em seguida clique em **Console Administrativo do HP ProtectTools**.
2. Na tela da esquerda do Console Administrativo, clique em **Usuário**.
3. Clique no botão **Adicionar**. A caixa de diálogo **Selecionar Usuários** é aberta.
4. Clique no botão **Avançado** em seguida clique no botão **Localizar Agora** para pesquisar usuários para adicionar.
5. Clique em um usuário para ser adicionado na lista, em seguida clique em **OK**.
6. Clique em **OK** na caixa de diálogo **Selecionar Usuários**.
7. Digite a senha do Windows para a conta selecionada, em seguida clique em **Concluir**.

NOTA: Você deve usar uma conta do Windows existente e digitá-la exatamente. Você não pode modificar ou adicionar uma conta de usuário do Windows nesta caixa de diálogo.

Remoção de um usuário

NOTA: Este procedimento não exclui a conta de usuário do Windows. Ele apenas remove aquela conta do Security Manager. Para remover completamente o usuário, você deve removê-lo do Security Manager e Windows.

1. Clique em **Iniciar**, clique em **Todos os Programas**, em seguida clique em **Console Administrativo do HP ProtectTools**.
2. Na tela da esquerda do Console Administrativo, clique em **Usuário**.
3. Clique no nome do usuário da conta que você deseja remover, em seguida clique em **Excluir**.
4. Na caixa de diálogo de confirmação, clique em **Sim**.

Verificação do status de usuário

A seção Usuário do Console Administrativo mostra o status atual de cada usuário:

- **Marca de verificação verde** - Indica que o usuário foi configurado e solicitado o(os) método(o) seguros para login.
- **X vermelho** - Indica que o usuário não foi configurado a nenhum método seguro para login requerido e será bloqueado do computador quando tentar efetuar login. O usuário deve executar o assistente de configuração para configurar o(os) método(os) requeridos para login.
- **Em branco** - Indica que o método seguro para login não é requerido.

Definição das Configurações dos Aplicativos

A janela Configurações inclui ferramentas para configuração do comportamento do Security Manager e seus aplicativos. Para modificar as configurações:

1. Clique em **Iniciar**, clique em **Todos os Programas**, em seguida clique em **Console Administrativo do HP ProtectTools**.
2. Na tela da esquerda do Console Administrativo, clique em **Configurações**.

3. Na guia **Geral**, escolha as configurações gerais para o HP ProtectTools Security Manager, em seguida clique no botão **Aplicar**.

4. Na guia **Aplicativos**, selecione os aplicativos que deseja ativar ou desativar, em seguida clique no botão **Aplicar**.

NOTA: Ativação ou desativação de um aplicativo pode não ser efetivada até o computador seja reiniciado.

Codificação de Unidades

O Drive Encryption for HP ProtectTools permite a você criptografar as unidades de disco rígido do computador tornando a unidade de disco rígido ilegível e inacessível para qualquer pessoa não autorizada que estiver tentando acessá-la mesmo se a unidade tiver sido removida do computador ou enviada para um serviço de recuperação de dados.

Para ativar ou desativar o Drive Encryption, clique no Assistente de Configuração no Console Administrativo.

△ **CUIDADO:** É importante que você faça backup das chaves de criptografia em uma unidade USB e armazene o dispositivo em um local seguro. Se você esquecer sua senha, este dispositivo fornece somente a você acesso à sua unidade de disco rígido.

Para obter mais informação sobre o uso do Drive Encryption for HP ProtectTools, consulte o Drive Encryption for HP ProtectTools na página 33.

Gerenciamento Device Access

Device Access Manager for HP ProtectTools fornece opções de segurança avançada para desautorizar seletivamente vários tipos de dispositivos que podem comprometer a segurança de seu PC. Para obter mais informações sobre o uso do Device Access Manager for HP ProtectTools, consulte o Device Access Manager for HP ProtectTools na página 48.

5 HP ProtectTools Security Manager

O HP ProtectTools Security Manager permite que você aumente significativamente a segurança de seu computador. Através do uso dos aplicativos do Security Manager, você pode:

- Gerenciar seu login e senhas
- Alterar facilmente sua senha do Windows
- Definir as credenciais de autenticação, incluindo um smart card
- Fragmentar ou purificar sua unidade de disco rígido
- Visualizar status de criptografia de unidade
- Visualizar configurações de acesso de dispositivo
- Backup e restauração de dados do Security Manager

Gerenciamento de senhas

O Credential Manager for HP ProtectTools (Gerenciador de Senhas) cria e gerencia logins, os quais permitem a você iniciar e efetuar login para web sites e programas autenticando com suas credenciais registradas.

Para obter mais informações sobre o gerenciamento de senhas, consulte Credential Manager for HP ProtectTools (Gerenciador de Senhas) na página 36.

Configuração de credenciais

Você usa suas Credenciais do Security Manager para verificar se você é realmente você. O administrador deste computador pode definir quais credenciais podem ser usadas para provar sua identidade quando efetuar login em sua conta do Windows, web sites ou programas.

As credenciais disponíveis podem variar dependendo do dispositivo de segurança integrado ou conectado no computador. Cada credencial admitida terá uma entrada no grupo de Credenciais.

Alteração de sua senha do Windows

O Security Manager torna simples ou rápido fazer alteração em sua senha do Windows quando o faz através do Painel de Controle do Windows.

Para alterar sua senha do Windows:

1. No HP ProtectTools Security Manager, clique em **Credenciais** na tela da esquerda.
2. Clique em **Senha do Windows**.
3. Digite sua senha atual na caixa **Senha atual do Windows**.
4. Digite sua nova senha nas caixas **Nova senha do Windows** e **Confirmar nova senha**.
5. Clique em **Alterar**.

Fragmentar ou purificar espaço livre de arquivos

O File Sanitizer for HP ProtectTools exclui arquivos substituindo-os por dados sem significado. Este processo, referido como “fragmentação”, melhora bastante a segurança da informação tornando muito mais difícil recuperar os arquivos excluídos. O File Sanitizer, além disso, melhora a segurança da informação substituindo o espaço usado anteriormente na unidade de disco rígido usando um processo conhecido como “Purificando espaço livre.” Os arquivos excluídos usando o File Sanitizer não podem ser recuperados pelo Sistema Operacional ou outro software de recuperação de arquivos normalmente disponível.

Para obter mais informações sobre o uso do File Sanitizer for HP ProtectTools, consulte o File Sanitizer for HP ProtectTools na página 41.

Visualização do status de criptografia de unidade

O Drive Encryption é configurado pelo Administrador do Windows no Console Administrativo. Os usuários podem visualizar o status de sua criptografia no Security Manager.

Para visualizar o status do drive encryption:

1. Clique em **Iniciar**, clique em **Todos os Programas**, em seguida clique em **HP ProtectTools Security Manager**.
2. Na tela da esquerda do Security Manager, clique em **Status de Criptografia**. A página de Status de Criptografia mostra se a criptografia da unidade está ativa ou inativa e quais unidades são ou não criptografadas.

Visualização de Device Access

O Device Access é configurado pelo Administrador do Windows no Console Administrativo. Os usuários podem visualizar a configuração de device access no Security Manager.

Para visualizar configurações de device access:

1. Clique em **Iniciar**, clique em **Todos os Programas**, em seguida clique em **HP ProtectTools Security Manager**.
2. Na tela da esquerda do Security Manager, expanda **Device Access Manager**.
3. Para visualizar quais dispositivos têm acesso negado, clique em **Configuração Simples**. Dispositivos com uma marca de seleção próxima a eles têm acesso negado.

4. Para visualizar quais usuários ou grupos têm acesso negado, clique em **Configuração de Classe de Dispositivo**.

5. Clique em um dispositivo para ver quais usuários ou grupos têm acesso negado ou permitido para um dispositivo.

Adição de aplicativos

Podem estar disponíveis aplicativos adicionais para adicionar novos recursos para este programa.

1. Clique em **Iniciar**, clique em **Todos os Programas**, em seguida clique em **HP ProtectTools Security Manager**.

2. Na tela da esquerda do Security Manager, clique em **Descobrir Mais**.

NOTA: Se não existir um link **Descobrir Mais**, ele pode ter sido desativado pelo administrador de seu computador.

3. Navegue na guia **Adicionar Aplicativos**, para buscar aplicativos adicionais.

4. Na guia **Atualizações e Mensagens**, você pode permanecer informado sobre novos aplicativos e atualizações clicando na caixa de verificação **Mantenha-me informado sobre novos aplicativos e atualizações** e configurar um número de dias para verificar atualizações, ou você pode clicar no botão **Verificar Agora** para verificar imediatamente se existem atualizações.

Definição de preferências

A página Preferências permite que você selecione a caixa de verificação **Mostrar ícone na barra de tarefas** para exibir o ícone do Security Manager na barra de tarefas na área de notificações (bandeja do sistema).

Para acessar a página Preferências:

1. Clique em **Iniciar**, clique em **Todos os Programas**, em seguida clique em **HP ProtectTools Security Manager**.

2. Na tela da esquerda do Security Manager, clique em **Avançado**, em seguida clique em **Preferências**.

3. Marque ou desmarque a caixa de verificação **Mostrar ícone na barra de tarefas** e clique em **Aplicar**.

Backup e Restauração

É uma boa prática efetuar backup de seus dados no Security Manager em períodos regulares. Com que frequência você deve fazer backup de seus dados depende de quantas vezes os dados são alterados. Por exemplo, se você normalmente adiciona novos logins diariamente, deve fazer backups diários de seus dados.

Os backups podem ser usados para migrar de um computador para outro, algumas vezes também chamado de importação e exportação. Contudo, lembre-se de que neste recurso os backups são apenas de dados.

Se você restaurar o arquivo de backup em outro computador ou no mesmo computador depois de reinstalar o sistema operacional, o sistema deve ter o HP ProtectTools Security Manager já instalado antes de restaurar os dados a partir do arquivo de backup.

Backup de seus dados

Quando efetuar backup de seus dados, está salvando suas informações de login e credenciais em um arquivo criptografado, protegido por uma senha que você digitou.

Para fazer backup dos dados:

1. Clique em **Iniciar**, clique em **Todos os Programas**, em seguida clique em **HP ProtectTools Security Manager**.
2. Na tela da esquerda do Security Manager, clique em **Avançado**, em seguida clique em **Backup e Restauração**.
3. Clique em **Backup**.
4. Selecione os módulos que você deseja incluir no backup. Na maioria dos casos, você desejará selecionar todos. Clique em **Avançar**.
5. Digite sua senha para verificar sua identidade, em seguida clique no botão de seta.
6. Digite um caminho e nome para armazenar o arquivo. Por padrão, o arquivo será salvo em sua pasta Documentos. Clique em **Pesquisar** para especificar um local diferente. Clique em **Avançar**.
7. Digite e confirme uma senha para proteger o arquivo.
8. Clique em **Concluir**.

Restauração de seus dados

Você restaura seus dados a partir de um arquivo criptografado, protegido por senha, que foi previamente criado através do recurso Backup e Restauração do Security Manager.

Para restaurar seus dados:

1. Clique em **Iniciar**, clique em **Todos os Programas**, em seguida clique em **HP ProtectTools Security Manager**.
2. Na tela da esquerda do Security Manager, clique em **Avançado**, em seguida clique em **Backup e Restauração**.
3. Clique em **Restaurar**.
4. Digite o caminho e nome para o armazenamento do arquivo ou clique em **Pesquisar** e selecione o arquivo.
5. Digite a senha usada para proteger o arquivo e clique em **Avançar**.
6. Selecione os módulos cujos dados você deseja restaurar. Na maioria dos casos, todos os módulos serão listados. Clique em **Avançar**.
7. Clique em **Concluir**.

Alteração de seu nome de usuário e imagem no Windows

Seu nome de usuário e imagem no Windows serão exibidos no canto superior esquerdo do Security Manager.

Para alterar seu nome de usuário e/ou imagem:

1. Clique na seção superior esquerda no Security Manager com seu nome de usuário e imagem.
2. Para alterar seu nome de usuário, digite um nome na caixa **Nome de usuário no Windows**.
3. Para alterar sua imagem, clique no botão **Escolher Imagem** e navegue para selecionar uma imagem.
4. Clique no botão **Salvar** para salvar suas alterações.

6 Drive Encryption for HP ProtectTools

NOTA: O Drive Encryption for HP ProtectTools está disponível somente em alguns modelos.

No mundo atual, um computador que pertence a você ou qualquer pessoa de sua equipe poderá ser roubado, e informações críticas sobre sua companhia poderão ser seriamente comprometidas. Tudo que estiver criptografado em sua unidade de disco rígido torna-se ilegível e inacessível para qualquer pessoa não autorizada que estiver tentando acessá-la mesmo se a unidade tiver sido removida do computador ou enviada para um serviço de recuperação de dados.

O software Drive Encryption for HP ProtectTools fornece completa proteção aos dados criptografando sua unidade de disco rígido. Quando o Drive Encryption é ativado, você deve efetuar login na tela de login no Drive Encryption, que é exibida antes de iniciar o Windows.

O Drive Encryption não evita o acesso não autorizado durante a mesma sessão do Windows. Uma vez que o PC é iniciado e você digita seu nome e senha de usuário, os dados na unidade de disco rígido ainda estão criptografados, mas estão disponíveis para qualquer usuário do sistema. Assegure-se de proteger a senha de sua sessão do Windows quando estiver longe de seu computador.

NOTA: O Drive Encryption for HP ProtectTools pode ser ativado somente através do Assistente de Configuração no Console Administrativo do HP ProtectTools.

NOTA: O Drive Encryption não é admitido em sistemas operacionais de 64 bits quando configurado com RAID em sistemas que usam um processador AMD.

NOTA: O Drive Encryption não admite prevenção de Ataque por Dicionário.

Drive Encryption (Criptografia de Unidade):

- Permite que você criptografe tudo em suas unidades de disco rígido internas
- Oferece a você fácil acesso a senha e autenticação na preinicialização
- Suporte para Microsoft Windows XP, Windows Vista e Windows 7

Várias tarefas podem ser executadas no Drive Encryption for HP ProtectTools:

- Gerenciamento do Drive Encryption
  - Criptografar e descriptografar unidades individuais
- Backup and Recovery
  - Criar chaves de backup
  - Executar uma recuperação

△ **CUIDADO:** É importante que você faça backup das chaves de criptografia em uma unidade USB e armazene o dispositivo em um local seguro. Se você esquecer sua senha, este dispositivo fornece somente a você acesso à sua unidade de disco rígido.

CUIDADO: Se você decidir pela desinstalação do módulo Drive Encryption ou se você utilizar uma solução de backup e restauração, você deve primeiro decodificar todas as unidades criptografadas. Se você não o fizer, você não será capaz de acessar os dados em unidades criptografadas. Reinstalação do módulo Drive Encryption não permitirá acesso às unidades criptografadas.

Procedimentos de configuração

Abertura do Drive Encryption

1. Clique em **Iniciar**, clique em **Todos os Programas**, em seguida clique em **Console Administrativo do HP ProtectTools**.
2. Clique em **Drive Encryption**.

Tarefas básicas

Ativação do Drive Encryption

Use o Assistente de Configuração do Console Administrativo do HP ProtectTools para ativar Drive Encryption.

Desativação do Drive Encryption

Use o Assistente de Configuração do Console Administrativo do HP ProtectTools para desativar Drive Encryption.

Login após o Drive Encryption ser ativado

É preciso efetuar login na tela de login do Drive Encryption quando o computador é ligado após o Drive Encryption ter sido ativado e sua conta de usuário ter sido registrada:

NOTA: Se o administrador do Windows tiver ativado a Segurança de Pré-inicialização no Console Administrativo do HP ProtectTools, você deve efetuar login para o computador imediatamente após o computador ser ligado, em vez de fazê-lo na tela de logon do Drive Encryption.

NOTA: Se utilizar uma chave de recuperação para efetuar login na tela de login do Drive Encryption, você será solicitado também a selecionar seu nome de usuário do Windows e digitar sua senha na tela de login do Windows.

Tarefas avançadas

Gerenciamento do Drive Encryption (tarefa do administrador)

A janela do Drive Encryption permite aos administradores do Windows visualizar e alterar o status do Drive Encryption (ativo ou inativo) e visualizar o status da criptografia de todas as unidades de disco rígido do computador.

Criptografia ou descriptografia de unidades individuais

1. Na tela da esquerda do Console Administrativo, expanda **Drive Encryption** em seguida clique em **Gerenciamento de Criptografia**.
2. Clique no botão **Alterar Criptografia**.
3. Na caixa de diálogo Alterar criptografia, marque ou desmarque a caixa de seleção próxima a cada unidade de disco rígido que deseja criptografar ou descriptografar e, em seguida, clique em **OK**.

NOTA: Quando a unidade está sendo criptografada ou descriptografada, a barra de progresso exibe o tempo restante para concluir o processo durante a sessão atual. Se o computador for desligado ou iniciar a suspensão ou a hibernação durante o processo de criptografia e, em seguida, for reiniciado, o campo Tempo restante exibido é reiniciado mas a criptografia é retomada de onde foi interrompida. A exibição do tempo restante e do progresso se alterará mais rapidamente para refletir o progresso anterior.

Backup e recuperação (tarefa do administrador)

O Drive Encryption: A janela de Backup and Recovery permite que os administradores do Windows façam backup e recuperem chaves de criptografia.

Criação de chaves de backup

CUIDADO: Assegure-se de manter o dispositivo de armazenamento contendo o backup da chave em um local seguro, porque se você esquecer sua senha, este dispositivo fornece somente a você o acesso à sua unidade de disco rígido.

1. Na tela da esquerda do Console Administrativo, expanda **Drive Encryption** em seguida clique em **Backup and Recovery**.
2. Clique no botão **Chaves de Backup**.
3. Na página “Selecione o disco de backup”, clique no nome do dispositivo em que deseja fazer o backup da chave de criptografia, em seguida clique em **Avançar**.
4. Leia as informações na próxima página exibida e, em seguida, clique em **Avançar**.

   A chave de criptografia é salva no dispositivo de armazenamento selecionado.
5. Clique em **OK** quando a caixa de diálogo de confirmação for exibida.

NOTA: Consulte o arquivo Ajuda do Drive Encryption for HP ProtectTools para obter informações sobre gerenciamento e execução de uma recuperação.

7 Credential Manager for HP ProtectTools (Gerenciador de Senhas)

É mais fácil e mais seguro efetuar login no Windows, websites e programas quando você usa o Gerenciador de Senhas.

O Gerenciador de Senhas permite que você defina a tela de login de websites e programas para acesso rápido e seguro. Primeiro, o Gerenciador de Senhas é informado sobre logins e os dados específicos que você digitou nas caixas de entrada em cada tela de login. Então, uma vez que você esteja na tela de login, depois de verificar sua identidade, o Gerenciador de Senhas preenche e apresenta os dados automaticamente.

Para acesso ainda mais rápido, você pode exibir um menu de seus logins simplesmente usando uma combinação de tecla de atalho configurável (Ctrl+Windows+H é o padrão). No menu, apenas selecione um login, e o Gerenciador de Senhas inicia o website ou programa, navega na tela de login e conecta automaticamente.

Para verificar sua identidade você usa as credenciais do HP ProtectTools for Small Business, tal como sua senha do Windows. Isto significa que você irá usar as mesmas credenciais que você configurou para efetuar logon em todas as telas de logon. Portanto, você pode criar senhas difíceis que não terá que escrever ou relembrar, e manterá suas contas mais seguras.

O Gerenciador de Senhas permite que você tenha uma visão geral se quaisquer de suas senhas estão correndo risco de segurança e pode gerar automaticamente uma senha de alta segurança e complexa para usar em novos sites.

Com o Gerenciador de Senhas você pode visualizar seus logins e senhas, e editá-las em qualquer momento. Muitos recursos do Gerenciador de Senhas também estão disponíveis a partir do ícone do Gerenciador de Senhas que é exibido quando o foco está na tela de login de um programa que tenha sido configurado ou em qualquer tela de login de website. Clicando no ícone exibe um menu de contexto onde você pode escolher entre as seguintes opções.

Para páginas da web ou programas onde um login ainda não foi criado:

As seguintes opções são mostradas no menu de contexto.

- Adicionar [somedomain.com] para o Gerenciador de Senhas – Use para adicionar um login para a tela atual de login.
- Abrir o Gerenciador de Senhas – Inicia o Security Manager na página Gerenciador de Senhas.
- Configurações do Ícone do Gerenciador de Senhas – Permite que você especifique as condições nas quais o Ícone do Gerenciador de Senhas será exibido.
- Ajuda – Exibe ajuda on-line para o aplicativo Gerenciador de Senhas.

Para páginas da web ou programas onde um login já foi criado:

As seguintes opções são mostradas no menu de contexto.

- Preencher dados no login – Coloca seus dados de login nos campos de login e envia a página (se o envio foi especificado quando o login foi criado ou editado anteriormente).
- Editar login – Permite que você edite seus dados de login para este website.
- Adicionar login – Use para adicionar outro login para o mesmo website ou programa.
- Abrir o Gerenciador de Senhas – Inicia a tela Security Manager na página do Gerenciador de Senhas.
- Ajuda – Exibe ajuda on-line para o aplicativo Gerenciador de Senhas.

Adicionar logins

Para adicionar um login:

1. Abra a tela de login para um site na web ou programa.
2. Clique na seta do ícone no Gerenciador de Senhas, em seguida selecione um dos seguintes, dependendo se a tela de login é para um site na web ou um programa.
   - Para um site na web - selecione **Adicionar [nome de domínio] para Gerenciador de Senhas**.
   - Para um programa - selecione **Adicionar esta tela de login para Gerenciador de Senhas**.
3. Digite seus dados de login. Os campos de login na tela, e seus campos correspondentes nos diálogos são identificados com uma borda laranja em negrito. Estão disponíveis outras opções para exibir este diálogo, como selecionar Adicionar Login a partir da guia **Gerenciar** do Gerenciador de Senhas. Algumas opções dependem do dispositivo de segurança conectado no computador; por exemplo, usando as Teclas de Atalho Ctrl-H ou inserindo um smart card.
   - Clique nas setas para a direita no campo de login para preenchê-lo com uma das várias opções pré-formatadas.
   - Opcionalmente, clique em **Escolher outros campos** para adicionar campos adicionais na tela de seu login.
   - Desmarque **Enviar dados de login** se você deseja preencher o campo de login, mas não deseja enviá-los.
   - Se você deseja visualizar a senha deste login, clique em **Mostrar senha**.
4. Clique em **OK**. O sinal mais é removido do ícone Gerenciador de Senhas, deixando que você saiba que o login foi criado.

Agora, toda vez que você entrar num site na web ou iniciar um programa, o ícone do Gerenciador de Senhas irá aparecer, indicando que você pode usar sua(s) credencial(ais) registradas para efetuar login.

Editar logins

Para editar um login:

1. Abra a tela de login para um site na web ou programa.
2. Clique na seta no ícone do Gerenciador de Senhas e selecione **Editar login** para exibir um diálogo onde você pode editar sua informação de login. Os campos de login na tela, e seus campos correspondentes nos diálogos, são identificados com uma borda laranja em negrito.
3. Edite sua informação de login.
   - Clique nas setas para a direita no campo de login para preenchê-lo com uma das várias opções pré-formatadas.
   - Opcionalmente, clique em **Escolher outros campos** para agregar campos adicionais na tela de seu login.
   - Desmarque **Enviar dados da conta** se você deseja preencher os campos de login, mas não deseja enviá-los.
   - Se você deseja visualizar a senha deste login, clique em Mostrar senha.
4. Clique em **OK**.

Usar o menu de Logins

O Gerenciador de Senhas fornece uma maneira rápida e fácil de iniciar websites e programas que você tenha criado login para eles. Simplesmente clique duas vezes em um login de programa ou website a partir do menu Logins, ou na guia **Gerenciar** no Gerenciador de Senhas, assim ele inicia a tela de login e preenche seus dados. Por padrão, a informação também é imediatamente enviada para a website, embora você possa escolher não fazê-lo desmarcando **Enviar dados da conta** quando configurar ou editar inicialmente o login.

Quando você criar um login, ele é automaticamente adicionado no menu Logins do Gerenciador de Senhas.

Para exibir o menu Logins, pressione a combinação de Teclas de Atalho do Gerenciador de Senhas. Ctrl-H é o padrão, mas você pode alterar a combinação de Teclas de Atalho a partir de **Gerenciador de Senhas** > **Configurações**.

Organização de logins por categoria

Use categorias para manter seus logins em ordem. É uma maneira simples de criar uma ou mais categorias e arrastar e soltar seus logins nas categorias desejadas.

Para adicionar uma categoria:

1. Na tela da esquerda do Security Manager, selecione **Gerenciador de Senhas**.
2. Selecione a guia **Gerenciar**, clique em **Adicionar Categoria**.
3. Digite um nome para a categoria.
4. Clique em **OK**.

Para adicionar um login em uma categoria:

1. Coloque o apontador de seu mouse sobre o login desejado.
2. Mantenha pressionado o botão esquerdo do mouse.
3. Arraste o login até a lista de categorias. As categorias tornam-se realçadas assim que você move seu mouse sobre elas.
4. Libere o botão do mouse quando a categoria desejada estiver realçada.

Seus logins não serão movidos para a categoria, mas apenas copiados na categoria selecionada. O que significa que você pode adicionar o mesmo login em mais de uma categoria. E você sempre poderá ver todos os seus logins clicando em **Todos**.

Gerenciamento de seus logins

O Gerenciador de Senhas faz o gerenciamento das informações do login – nome de usuário, senhas e várias contas de login – fácil e intuitivo, a partir de um local central.

Seus logins são listados na guia **Gerenciar**. Quando vários logins forem criados para o mesmo website, cada login é então listado no nome da website e entram na lista de login.

Para gerenciar seus logins:

Na tela da esquerda do Security Manager, selecione **Gerenciador de Senhas** e clique na guia **Gerenciar**.

- Adicionar um login – Clique em **Adicionar Login** e siga as instruções na tela.
- Editar um login – Selecione um login e clique em **Editar**. Então altere os dados do login como desejar.
- Excluir um login – Selecione um login e clique em **Excluir**.

Para adicionar um login adicional para uma website ou programa:

1. Inicie a tela de login para a website ou programa.
2. Clique no ícone Gerenciador de Senhas para exibir o menu de atalho.
3. Selecione **Adição de login adicional** e siga as instruções na tela.

Avaliar sua senha forte

O uso de senhas com alta segurança para login em websites e programas é um aspecto importante de proteção de sua identidade.

O Gerenciador de Senhas faz o monitoramento e melhora facilmente sua segurança com análises instantâneas e automatizadas da segurança de cada uma das senhas usadas para efetuar login em websites e programas. Pode verificar a força da senha que você usa para efetuar logins no Gerenciador de Senhas na guia **Força da Senha**.

Configurações do Ícone do Gerenciador de Senhas

O Gerenciador de Senhas tenta identificar as telas de login para websites e programas. Quando ele encontra uma tela de login em que você não criou um login para ela, o Gerenciador de Senhas solicita que você adicione um login para a tela exibindo o ícone Gerenciador de Senhas com um sinal “+”.

As seguintes definições são configuráveis:

- Solicitar sempre – Selecione esta opção para ter uma solicitação do Gerenciador de Senhas para você adicionar um login sempre que exibir uma tela de login que ainda não tenha um login configurado para ela.
- Não solicitar para esta tela – Selecione esta opção para que o Gerenciador de Senhas não solicite novamente adicionar um login para esta tela de login específica.
- Nunca solicitar – Selecione esta opção para assegurar que o Gerenciador de Senhas nunca solicite você para telas de login que não tenham sido definidas.

8 File Sanitizer for HP ProtectTools

File Sanitizer é uma ferramenta que permite que você apague arquivos e pastas críticos com segurança (informações ou arquivos pessoais, históricos ou dados relatados na Web, ou outros componentes de dados) em seu computador e periodicamente limpar sua unidade de disco rígido.

NOTA: O File Sanitizer opera somente no disco rígido.

Sobre fragmentação

Excluir arquivos e/ou pastas no Windows não remove completamente os conteúdos de sua unidade de disco rígido. O Windows exclui apenas a referência. O conteúdo ainda permanecerá na unidade de disco rígido até que outro arquivo seja sobregravado na mesma área da unidade de disco rígido com nova informação.

Fragmentar é diferente do padrão de excluir no Windows (também conhecido como uma simples exclusão no File Sanitizer) porque quando você tritura dados é impossível virtualmente reparar esses dados.

Quando você escolhe um perfil para fragmentar (Segurança Alta, Segurança Média ou Segurança Baixa), uma lista predefinida de arquivos e/ou pastas e um método para apagar são selecionados automaticamente para fragmentar. Você também pode personalizar um perfil para fragmentar, que permite que você especifique o número de ciclos de trituração, quais arquivos serão incluídos na trituração, quais os arquivos deve confirmar antes de fragmentar e quais arquivos serão excluídos da trituração.

Você pode definir uma programação para fragmentar automaticamente, e também pode fragmentar manualmente arquivos e/ou pastas sempre que desejar.

Sobre a purificação de espaço livre

A purificação de espaço livre permite que você grave dados aleatórios com segurança sobre arquivos excluídos, evitando que usuários visualizem os conteúdos originais do arquivo excluído.

NOTA: A purificação de espaço livre é para aqueles arquivos que você excluiu usando a Lixeira do Windows ou quando você excluiu manualmente um arquivo. A purificação de espaço livre não oferece segurança adicional para arquivos triturados.

Você pode definir uma programação de purificação de espaço livre automática ou pode ativar manualmente essa purificação usando o ícone HP ProtectTools na área de notificação, à direita da barra de tarefas.

Procedimentos de configuração

Abertura do File Sanitizer

Para abrir o File Sanitizer:

1. Clique em **Iniciar**, clique em **Todos os Programas**, em seguida clique em **HP ProtectTools Security Manager**.
2. Na tela da esquerda do Security Manager, clique em **File Sanitizer**.

   – ou –

- Clique duas vezes no ícone **File Sanitizer**.

  – ou –

- Clique com o botão direito no ícone HP ProtectTools na área de notificação, no lado direito da barra de tarefas, destaque **File Sanitizer**, em seguida clique em **Abrir File Sanitizer**.

Configuração de uma programação de purificação de espaço livre

Para configurar uma programação de purificação de espaço livre:

1. Na tela da esquerda do Security Manager, expanda **File Sanitizer**, e clique em **Purificando espaço livre**.
2. Marque a caixa de diálogo **Ativar programador**, digite sua senha do Windows e, em seguida, o dia e a hora para executar a purificação do disco rígido.
3. Clique no ícone **Salvar**.

NOTA: A operação de purificação de espaço livre pode demorar bastante. Mesmo que a purificação de espaço livre seja executada no fundo, seu computador pode ter a capacidade reduzida pelo aumento no uso do processador.

Configuração de uma programação de Fragmentação

1. Na tela da esquerda do Security Manager, expanda **File Sanitizer**, e clique em **Fragmentar**.
2. Selecione uma opção de fragmentação:

   - **Desligado do Windows** — Escolha esta opção para fragmentar todos os arquivos selecionados quando desligar o Windows.

     NOTA: Quando esta opção é selecionada, uma caixa de diálogo é exibida pedindo para desligar se você deseja continuar triturando os arquivos selecionados ou se deseja ignorar o procedimento. Clique em Sim para ignorar o procedimento de trituração ou clique em Não para continuar triturando. A opção Sim ou Não deve ser selecionada rapidamente porque o Windows irá fechar o software preparando para desligar e gerar um erro. Se você selecionar Não para continuar a trituração, o Windows pode gerar uma tela de erro indicando que o File Sanitizer não está respondendo. Permita que o File Sanitizer conclua o trituramento, em seguida inicie o desligamento novamente.

   - **Abertura do navegador da web** — Escolha esta opção pra fragmentar todos os arquivos selecionados relatados na Web, como histórico URL do navegador, quando você abrir uma navegador Web.

- **Ao sair do navegador da web** — Escolha esta opção pra fragmentar todos os arquivos selecionados relatados na Web, como histórico URL do navegador, quando você fechar uma navegador Web.
- **Sequência de chave** — Escolha esta opção para iniciar a trituração usando a sequência de chave.
- **Programador** — Selecione a caixa de verificação Ativar Programador, digite sua senha do Windows, em seguida digite um dia e hora para fragmentar os arquivos selecionados.

3. Clique no ícone **Salvar**.

Seleção ou criação de um perfil de fragmentação

Você pode especificar um método de apagar e selecionar os arquivos e/ou pastas para fragmentar selecionando um perfil predefinido ou criando seu próprio perfil.

Seleção de um perfil de fragmentação predefinido

Quando você escolher um perfil predefinido para fragmentar (Segurança Alta, Segurança Média ou Segurança Baixa), um método predefinido para apagar e a lista de arquivos será automaticamente selecionada. Você pode clicar no botão Visualizar Detalhes para visualizar a lista predefinida de arquivos que foram selecionados para trituração.

Para selecionar um perfil de fragmentação predefinido:

1. Na tela da esquerda do Security Manager, expanda **File Sanitizer**, e clique em **Configurações**.
2. Clique em um perfil de fragmentação predefinido.
3. Clique em **Visualizar Detalhes** para visualizar a lista de arquivos que foram selecionados para trituração.
4. Em **Excluir o seguinte**, selecione a caixa de verificação próxima a cada arquivo que você deseja confirmar antes da trituração.
5. Clique em **Aplicar**.

Personalização de um perfil de segurança avançada de trituração

Quando você criar um perfil para fragmentar, você especifica o número de ciclos de trituração, quais arquivos serão incluídos para trituração, quais os arquivos devem confirmar antes de fragmentar e quais arquivos serão excluídos da trituração:

1. Na tela esquerda do Security Manager, expanda **File Sanitizer**, clique em **Configurações**, selecione **Configurações Avançadas de Segurança**, em seguida clique em **Visualizar Detalhes**.
2. Especifique o número de ciclos de fragmentação.

NOTA: O número selecionado de ciclos de trituração será executado para cada arquivo. Por exemplo, se você escolhe 3 ciclos para fragmentar, um algoritmo que apaga os dados será executado em 3 tempos diferentes. Se você escolher os ciclos de trituração de segurança alta, a trituração pode levar um tempo significativo; entretanto, quanto maior o número de ciclos de trituração você especificar, mais seguro estará o computador.

3. Selecione os ativos que deseja fragmentar:

   a. Em **Opções de exclusão disponíveis**, clique em um arquivo, em seguida clique em **Adicionar**.

   b. Para adicionar um arquivo personalizado, clique em **Adicionar Opção Personalizada**, digite ou procure o nome do arquivo ou nome da pasta, em seguida clique em **OK**. Clique no arquivo personalizado, em seguida clique em **Adicionar**.

   NOTA: Para excluir um arquivo de opções de trituração disponíveis, clique no arquivo, em seguida clique em **Excluir**.

4. Em **Excluir o seguinte**, selecione a caixa de verificação próxima a cada arquivo que você deseja confirmar antes da trituração.

NOTA: Para remover um arquivo da lista de trituração, clique no arquivo, em seguida clique em **Remover**.

5. Em **Não excluir o seguinte**, clique em **Adicionar** para selecionar os arquivos específicos que você deseja excluir da trituração.

6. Quando você concluir a configuração do perfil de trituração, clique em **Aplicar**.

Personalização de um perfil de exclusão simples

O perfil de exclusão simples executa uma exclusão padrão dos arquivos sem fragmentar. Quando você personaliza um perfil de exclusão simples, você especifica quais os arquivos para incluir em uma exclusão simples, quais arquivos deve confirmar antes que a exclusão é executada e quais arquivos serão excluídos da exclusão simples:

NOTA: É altamente recomendável que você execute uma purificação de espaço livre regularmente se utilizar a opção de exclusão simples.

1. Na tela esquerda do Security Manager, expanda **File Sanitizer**, clique em **Configurações**, selecione **Configuração de Exclusão Simples**, em seguida clique em **Visualizar Detalhes**.

2. Selecione os arquivos que você deseja excluir:

   a. Em **Opções de exclusão disponíveis**, clique em um arquivo, em seguida clique em **Adicionar**.

   b. Para adicionar um arquivo personalizado, clique em **Adicionar Opção Personalizada**, digite ou procure o nome do arquivo ou nome da pasta, em seguida clique em **OK**. Clique no arquivo personalizado, em seguida clique em **Adicionar**.

   NOTA: Para excluir um arquivo de opções de exclusão disponíveis, clique no arquivo, em seguida clique em **Excluir**.

3. Em **Excluir o seguinte**, selecione a caixa de verificação próxima a cada arquivo que você deseja confirmar antes da exclusão.

NOTA: Para remover um arquivo da lista de exclusão, clique no arquivo, em seguida clique em **Remover**.

4. Em **Não excluir o seguinte**, clique em **Adicionar** para selecionar os arquivos específicos que você deseja excluir da trituração.

5. Quando você concluir a configuração do perfil de exclusão simples, clique em **Aplicar**.

Tarefas básicas

Uso de uma sequência de chave para iniciar a fragmentação

Para especificar uma sequência de chave, siga estas etapas:

1. Na tela da esquerda do Security Manager, expanda **File Sanitizer**, e clique em **Fragmentar**.
2. Marque a caixa de seleção **Sequência de chave**.
3. Digite um caractere na caixa disponível e marque a caixa **CTRL**, **ALT** ou **SHIFT**, ou selecione todas as três opções.

   Por exemplo, para iniciar a fragmentação automática usando a tecla S e Ctrl+Shift, digite S na caixa e, em seguida, marque as opções **CTRL** e **SHIFT**.

NOTA: Certifique-se de selecionar uma sequência de chave diferente das outras sequências de chave que você configurou.

Para iniciar a fragmentação usando uma sequência de chave:

1. Mantenha pressionada as teclas Ctrl, Alt, ou a tecla Shift (ou a que for sua combinação especificada) enquanto pressiona seu caráter escolhido.
2. Se a caixa de diálogo de confirmação for exibida, clique em **Sim**.

Uso do ícone do File Sanitizer

△ **CUIDADO:** Arquivos triturados não podem ser recuperados. Analise cuidadosamente quais itens você seleciona para trituração manual.

1. Navegue até o documento ou pasta que deseja fragmentar.
2. Arraste o arquivo para o ícone File Sanitizer na área de trabalho.
3. Quando a caixa de diálogo de confirmação for exibida, clique em **Sim**.

Fragmentação manual de um ativo

△ **CUIDADO:** Arquivos triturados não podem ser recuperados. Analise cuidadosamente quais itens você seleciona para trituração manual.

1. Clique com o botão direito no ícone **HP ProtectTools** na área de notificação, no lado direito da barra de tarefas, destaque **File Sanitizer**, em seguida clique em **Fragmentar Um**.
2. Quando a caixa de diálogo Procurar é aberta, navegue até ao arquivo que você deseja fragmentar, em seguida clique em **Abrir**.

   NOTA: O arquivo que você seleciona pode ser um simples arquivo ou pasta.

3. Quando a caixa de diálogo de confirmação for exibida, clique em **Sim**.

– ou –

1. Clique com o botão direito no ícone do **File Sanitizer** na área de trabalho e, em seguida, clique em **Fragmentar um**.
2. Quando a caixa de diálogo Procurar é aberta, navegue até ao arquivo que você deseja fragmentar, em seguida clique em **OK**.
3. Quando a caixa de diálogo de confirmação for exibida, clique em **Sim**.

– ou –

1. Na tela da esquerda do Security Manager, expanda **File Sanitizer**, e clique em **Fragmentar**.
2. Clique no botão **Procurar**.
3. Quando a caixa de diálogo Procurar é aberta, navegue até ao arquivo que você deseja fragmentar, em seguida clique em **Abrir**.
4. Quando a caixa de diálogo de confirmação for exibida, clique em **Sim**.

Fragmentação manual de todos os arquivos selecionados

1. Clique com o botão direito no ícone **HP ProtectTools** na área de notificação, no lado direito da barra de tarefas, destaque **File Sanitizer**, em seguida clique em **Fragmentar Agora**.
2. Quando a caixa de diálogo de confirmação for exibida, clique em **Sim**.

– ou –

1. Clique com o botão direito no ícone do **File Sanitizer** na área de trabalho e, em seguida, clique em **Fragmentar Agora**.
2. Quando a caixa de diálogo de confirmação for exibida, clique em **Sim**.

Ativação manual da purificação de espaço livre

1. Clique com o botão direito no ícone **HP ProtectTools** na área de notificação, no lado direito da barra de tarefas, destaque **File Sanitizer**, em seguida clique em **Purificar Agora**.
2. Uma bolha de notificação aparecerá verificando se uma operação de purificação foi iniciada.

– ou –

1. Na tela da esquerda do Security Manager, expanda **File Sanitizer**, e clique em **Purificar**.
2. Clique em **Purificar agora**.
3. Uma bolha de notificação aparecerá verificando se uma operação de purificação foi iniciada.

Interrupção de uma operação de fragmentação ou de purificação de espaço livre

Quando uma operação de trituração ou purificação de espaço livre está em progresso, uma mensagem sobre o ícone do HP ProtectTools Security Manager é exibida na área de notificação. A mensagem fornece detalhes sobre o processo da operação de trituração ou purificação de espaço livre, (porcentagem total), e dá a opção para você abortar a operação.

Para interromper a operação:

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

Exibição dos arquivos de registro

Toda vez que uma operação de fragmentação ou purificação de espaço livre é executada, são gerados arquivos de registro de erros e falhas. Os arquivos de registro são sempre atualizados de acordo com a última operação de fragmentação ou purificação de espaço livre.

NOTA: Os arquivos cuja fragmentação ou purificação tenha sido bem-sucedida não são exibidos nos arquivos de registro.

Um arquivo de registro é criado para operações de fragmentação e outro para operações de purificação de espaço livre. Ambos os arquivos de registro estão localizados no disco rígido em:

- C:\Arquivos de programas\Hewlett-Packard\File Sanitizer\`[Nome_de_usuário]`_ShredderLog.txt
- C:\Arquivos de programas\Hewlett-Packard\File Sanitizer\`[Nome_de_usuário]`_DiskBleachLog.txt

9 Device Access Manager for HP ProtectTools

Essa ferramenta de segurança está disponível somente para administradores. O Device Access Manager for HP ProtectTools possui os seguintes recursos de segurança que fornecem proteção contra acesso não-autorizado a dispositivos anexados a seu sistema de computador:

- Perfis de dispositivos que são criados para cada usuário para definir o device access
- Device access que pode ser concedido ou negado com base em associações de grupos

NOTA: O Device Access Manager utiliza Grupos e Usuários Locais do Windows para gerenciar o acesso. As versões do Windows Home não admitem Usuários e Grupos Locais, portanto, o Device Access Manager não funcionará adequadamente. No entanto, o Device Access Manager irá funcionar na versão do Microsoft Windows Vista Home se você usar os comandos DOS para configurar usuário. Consulte o arquivo de ajuda do Device Access Manager para obter instruções.

Inicializar serviços de segundo plano

Para aplicar perfis de dispositivo, o serviço de segundo plano de Bloqueio/Auditoria de Dispositivo HP ProtectTools deve estar executando. Quando tentar aplicar perfis de dispositivo pela primeira vez, o Console Administrativo do HP ProtectTools abre uma caixa de diálogo para perguntar se deseja iniciar o serviço de segundo plano. Clique em **Sim** para iniciar o serviço de segundo plano e defini-lo para iniciar automaticamente sempre que o sistema inicializar.

Configuração simples

O Device Access Manager cria um novo Grupo de Usuário durante a instalação chamada Administradores de Dispositivo para acessar ou explorar dispositivos como um administrador. Coloque os usuários neste grupo que você deseja para ter acesso administrativo ao dispositivo que você controla através de Configurações simples do Device Access Manager.

Este recurso permite que proíba o acesso às seguintes classes de dispositivos:

- Dispositivos USB para todos que não sejam Administradores de Dispositivos
- Toda mídia removível (unidades de disquete, reprodutores de música pessoais, pen drives, etc.) para todos que não sejam Administradores de Dispositivos
- Toas as unidades de DVD/CD-ROM para todos que não sejam Administradores de Dispositivos
- Todas as portas seriais e paralelas para todos que não sejam Administradores de Dispositivos

Para impedir o acesso a uma classe de dispositivo para todos que não sejam Administradores de Dispositivos:

1. Clique em **Iniciar**, clique em **Todos os Programas**, em seguida clique em **Console Administrativo do HP ProtectTools**.
2. No painel esquerdo, clique em **Device Access Manager**, em seguida, clique em **Configuração simples**.
3. No painel direito, marque a caixa de seleção de um dispositivo para negar acesso.
4. Clique no ícone **Salvar**.

NOTA: Se serviço de segundo plano não tiver executando, ele será solicitado a iniciar agora. Clique em **Sim** para permiti-lo.

5. Clique em **OK**.

Configuração de classe de dispositivo (avançado)

Estão disponíveis mais seleções para permitir que usuários específicos ou grupos de usuários tenham acesso autorizado ou proibido a tipos de dispositivo.

Adição de um usuário ou grupo

1. Clique em **Iniciar**, clique em **Todos os Programas**, em seguida clique em **Console Administrativo do HP ProtectTools**.
2. No painel esquerdo, expanda **Device Access Manager**, em seguida, clique em **Configuração de Classe de Dispositivo**.
3. Na lista de dispositivo, clique na classe de dispositivo que deseja configurar.
4. Clique em **Adicionar**. A caixa de diálogo de **Selecione usuários ou grupos** é aberta.
5. Clique em **Avançado** e, em seguida, clique em **Localizar agora** para pesquisar usuários ou grupos para adicionar.
6. Clique no usuário ou grupo a ser adicionado à lista de usuários e grupos disponíveis e, em seguida, clique em **OK**.
7. Clique em **OK**.

Remoção de um usuário ou grupo

1. Clique em **Iniciar**, clique em **Todos os Programas**, em seguida clique em **Console Administrativo do HP ProtectTools**.
2. No painel esquerdo, expanda **Device Access Manager**, em seguida, clique em **Configuração de Classe de Dispositivo**.
3. Na lista de dispositivo, clique na classe de dispositivo que deseja configurar.
4. Clique no usuário ou grupo que deseja remover e, em seguida clique em **Remover**.

Impedir ou permitir acesso para um usuário ou grupo

1. Clique em **Iniciar**, clique em **Todos os Programas**, em seguida clique em **Console Administrativo do HP ProtectTools**.
2. No painel esquerdo, expanda **Device Access Manager**, em seguida, clique em **Configuração de Classe de Dispositivo**.
3. Na lista de dispositivo, clique na classe de dispositivo que deseja configurar.
4. Em **Usuários/Grupos**, clique no usuário ou grupo ao qual negar o acesso.
5. Clique em **Negar**, próximo ao usuário ou grupo aos quais será impedido acesso.
6. Clique no ícone **Salvar**, em seguida clique em **OK**.

Configuração de acesso a usuário (avançado)

A Configuração de Acesso a Usuário permite aos administradores especificar quais usuários e grupos têm permissão de usar a Configuração Simples e visualizar a Configuração de Classe de Dispositivo.

Um usuário ou grupo deve receber acesso a **Visualização de (somente Leitura) Definições de Configuração** para visualizar a informação de Configuração Simples e Configuração de Classe de Dispositivo.

Um usuário ou grupo deve receber acesso a **Alterar Definições de Configuração** para alterar a informação de Configuração Simples e Configuração de Classe de Dispositivo.

Um usuário ou grupo deve receber de acesso a **Direitos Completos de Administrador do Usuário** para modificar as definições em visualizar Configuração Simples e Configuração de Classe de Dispositivo.

Adição de um usuário ou grupo

1. Clique em **Iniciar**, clique em **Todos os Programas**, em seguida clique em **Console Administrativo do HP ProtectTools**.
2. No painel esquerdo, expanda **Device Access Manager**, em seguida, clique em **Configurações de Acesso do Usuário**.
3. Clique em **Adicionar**. A caixa de diálogo de **Selecionar Usuário ou Grupo** é aberta.
4. Clique em **Avançado**, em seguida clique em **Localizar Agora** para pesquisar usuários ou grupos para adicionar.
5. Clique em um usuário ou grupo para adicionar à lista de usuários e grupos disponível, em seguida clique em **OK**.
6. Clique em **OK**.
7. Clique no ícone **Salvar**.

Remoção de um usuário ou grupo

1. Clique em **Iniciar**, clique em **Todos os Programas**, em seguida clique em **Console Administrativo do HP ProtectTools**.
2. No painel esquerdo, expanda **Device Access Manager**, em seguida, clique em **Configurações de Acesso do Usuário**.
3. Clique no usuário ou grupo que deseja remover e, em seguida clique em **Remover**.
4. Clique no ícone **Salvar**.

Permitir ou Negar Permissões

1. Clique em **Iniciar**, clique em **Todos os Programas**, em seguida clique em **Console Administrativo do HP ProtectTools**.
2. No painel esquerdo, expanda **Device Access Manager**, em seguida, clique em **Configurações de Acesso do Usuário**.
3. Na caixa **Nomes de grupo ou de usuário**, selecione o nome de um usuário ou grupo.

4. Na caixa **Permissões**, selecione as caixas de verificação **Permitir** ou **Negar** para obter as permissões apropriadas.

5. Clique no ícone **Salvar**.

Glossário

Administrador.
Veja administrador do Windows.

Administrador do Windows.
Um usuário com direitos totais para modificar permissões e gerenciar outros usuários.

Ativo.
Um componente de dados contendo informações ou arquivos pessoais, histórico e dados relacionados à Web, localizado no disco rígido.

ATM (Automatic Technology Manager).
Permite que os administradores de rede gerenciem sistemas remotamente no nível do BIOS.

Autenticação.
Processo que verifica se um usuário está autorizado a executar uma tarefa, como acessar um computador, modificar configurações de um determinado programa ou visualizar dados protegidos.

Autenticação na inicialização.
Recurso de segurança que requer alguns formatos de autenticação, como uma senha, quando o computador é ligado.

Ciclo de fragmentação.
O número de vezes que o algoritmo de fragmentação é executado em cada ativo. Quanto mais alto for o número de ciclos de fragmentação selecionado, maior a segurança do computador.

Conta de rede.
Conta de usuário ou administrador Windows, seja em um computador local, em um grupo de trabalho ou em um domínio.

Conta de usuário do Windows.
Perfil de um indivíduo autorizado a acessar uma rede ou um computador individual.

Credenciais.
Método pelo qual o usuário comprova elegibilidade para uma determinada tarefa no processo de autenticação, como nome de usuário e senha.

Domínio.
Grupo de computadores que fazem parte de uma rede e compartilham de um banco de dados de diretórios comum. Os domínios possuem nomes exclusivos, e cada um possui um conjunto de regras e procedimentos.

Exclusão simples.
Informação sensível excluída com segurança inclui arquivos, histórico ou conteúdo relacionado à web, ou outros dados confidenciais.

Fragmentação automática.
Fragmentação programada que o usuário define no File Sanitizer for HP ProtectTools.

Fragmentação manual.
Fragmentação imediata de um ativo ou de ativos selecionados, a qual ignora a programação de fragmentação automática.

Fragmentar.
A execução de um algoritmo que oculta os dados contidos em um ativo.

Método de login de segurança.
O método usado para efetuar login no computador.

Perfil de fragmentação.
Um método de apagamento específico e lista de ativos.

Purificação.
Consulte **Purificando espaço livre**.

Purificando espaço livre.
A gravação segura de dados aleatórios sobre os arquivos excluído da unidade de disco rígido para distorcer o conteúdo do arquivo excluído, torna mais difícil a recuperação dos dados.

Reinicializar.
Processo de reinicialização do computador.

Sequência de chave.
Uma combinação de teclas específicas que, quando pressionadas, iniciam uma fragmentação automática; por exemplo: Ctrl+Alt+S.

Índice