HP ProtectTools
Guia do Usuário

Primeira edição: outubro de 2009

Número de peça: 572661-201

Conteúdo

1 Introdução à segurança

Recursos do HP ProtectTools 2
Alcançando os principais objetivos de segurança 3
Proteção contra roubo direcionado 3
Restrição de acesso a dados importantes 3
Prevenção contra acesso não-autorizado a partir de locais internos ou externos 3
Criação de políticas de senhas fortes 4
Elementos adicionais de segurança 5
Atribuição de perfis de segurança 5
Gerenciamento de senhas do HP ProtectTools 5
Criação de uma senha segura 7
Backup e restauração de credenciais do HP ProtectTools 7

2 Passos iniciais

Inicialização do Console Administrativo do HP ProtectTools 9
Ativação de recursos de segurança 10
Registro de impressões digitais 11
Configuração de um smart card 12
Utilização do Console Administrativo 13

3 Configuração do sistema

Configuração de autenticação para seu computador 15
Política de login 15
Política de sessão 15
Configurações 16
Gerenciamento de usuários 17
Especificação de configurações de dispositivos 18
Impressões digitais 18
Smart Card 18

4 Configuração dos aplicativos

Guia Geral 20
Guia Aplicativos 21

5 Adição de ferramentas de gerenciamento

6 HP ProtectTools Security Manager

Procedimentos de configuração ... 24
Passos iniciais ... 24
Registro de credenciais ... 24
Registro de impressões digitais ... 24
Alteração da senha do Windows ... 25
Configuração de um smart card ... 25
Utilização do painel de controle do Security Manager ... 25
Inicialização do HP ProtectTools Security Manager ... 26
Tarefas básicas ... 27
Gerenciador de Senhas ... 27
Para páginas da Web ou programas para os quais não foi criado um login ... 27
Para páginas da Web ou programas para os quais já foi criado um login ... 28
Adição de logins ... 28
Edição de logins ... 29
Utilização do menu de logins ... 29
Organização de logins em categorias ... 29
Gerenciamento de logins ... 30
Avaliação da força de sua senha ... 30
Configurações do ícone do Gerenciador de Senhas ... 31
Configurações ... 31
Credenciais ... 31
Seu ID card pessoal ... 32
Configuração de preferências ... 32
Backup e restauração de dados ... 33
Adição de aplicativos ... 34
Status dos Aplicativos de Segurança ... 34

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

Procedimentos de configuração ... 36
Inicialização do Drive Encryption ... 36
Tarefas básicas ... 37
Ativação do Drive Encryption ... 37
Desativação do Drive Encryption ... 37
Login após o Drive Encryption ser ativado ... 37
Proteger seus dados criptografando a unidade de disco rígido ... 38
Exibição do status da criptografia ... 38
Tarefas avançadas ... 39
Gerenciamento do Drive Encryption (tarefa do administrador) ... 39
Criptografia ou descriptografia de unidades individuais ... 39

Backup e recuperação (tarefa do administrador) 39
Criação de chaves de backup 39
Execução de uma recuperação 40

8 Privacy Manager for HP ProtectTools (somente em determinados modelos)
Procedimentos de configuração 42
Inicialização do Privacy Manager 42
Gerenciamento de Certificados do Privacy Manager 42
Solicitação e instalação de um Certificado do Privacy Manager 42
Solicitação de um Certificado do Privacy Manager 43
Aquisição de um Certificado Corporativo pré-assinado do Privacy Manager 43
Instalação de um Certificado do Privacy Manager 43
Visualização dos detalhes do Certificado do Privacy Manager 44
Renovação de um Certificado do Privacy Manager 44
Configuração de um Certificado do Privacy Manager padrão 44
Exclusão de um Certificado do Privacy Manager 44
Restauração de um Certificado do Privacy Manager 45
Revogação do seu Certificado do Privacy Manager 45
Gerenciamento de Contatos Confiáveis 46
Adição de Contatos Confiáveis 46
Inclusão de um Contato Confiável 46
Adição de Contatos Confiáveis usando os contatos do Microsoft Outlook 47
Visualização de detalhes de Contatos Confiáveis 48
Exclusão de um Contato Confiável 48
Teste de status de revogação para um Contato Confiável 48
Tarefas básicas 49
Utilização do Privacy Manager no Microsoft Outlook 49
Configuração do Privacy Manager for Microsoft Outlook 49
Assinatura e envio de uma mensagem de e-mail 50
Selagem e envio de uma mensagem de e-mail 50
Visualização de uma mensagem de e-mail selada 50
Utilização do Privacy Manager em um documento do Microsoft Office 2007 50
Configuração do Privacy Manager for Microsoft Office 51
Assinatura de um documento do Microsoft Office 51
Acréscimo de uma linha de assinatura ao assinar um documento do Microsoft Word ou Microsoft Excel 51
Acréscimo de assinantes sugeridos a um documento do Microsoft Word ou Microsoft Excel 52
Acréscimo de um assinante sugerido à linha de assinatura 52
Criptografia de um documento do Microsoft Office 53
Remoção da criptografia de um documento do Microsoft Office 53
Envio de um documento do Microsoft Office criptografado 53

Visualização de um documento assinado do Microsoft Office 54
Visualização de um documento do Microsoft Office criptografado 54
Utilização do Privacy Manager no Windows Live Messenger 54
Inicialização de uma sessão do Privacy Manager Chat 55
Configuração do Privacy Manager for Windows Live Messenger 56
Bate-papo na janela do Privacy Manager Chat 56
Visualização do histórico de bate-papo 57
Revelar Todas as Sessões 57
Revelar sessões para uma conta específica 57
Visualização da ID de uma sessão 58
Visualização de uma sessão 58
Pesquisa de um texto específico nas sessões 58
Exclusão de uma sessão 58
Adição ou remoção de colunas 59
Filtragem de sessões exibidas 59
Tarefas avançadas 60
Migração de Certificados do Privacy Manager e contatos confiáveis para um computador diferente 60
Backup de Certificados do Privacy Manager e de Contatos Confiáveis 60
Restauração de Certificados do Privacy Manager e de Contatos Confiáveis 60
Administração central do Privacy Manager 61

9 File Sanitizer for HP ProtectTools

Fragmentação 63
Purificação de espaço livre 64
Procedimentos de configuração 65
Inicialização do File Sanitizer 65
Configuração de uma programação de fragmentação 65
Configuração de uma programação de limpeza de espaço livre 66
Seleção ou criação de um perfil de fragmentação 66
Seleção de um perfil de fragmentação predefinido 66
Personalização de um perfil de fragmentação 67
Personalização de um perfil de exclusão simples 67
Tarefas básicas 69
Uso de uma seqüência de chave para iniciar a fragmentação 69
Uso do ícone do File Sanitizer 70
Fragmentação manual de um ativo 70
Fragmentação manual de todos os arquivos selecionados 71
Ativação manual da limpeza de espaço livre 71
Interrupção de uma operação de fragmentação ou de purificação de espaço livre 71
Exibição dos arquivos de registro 71

10 Device Access Manager for HP ProtectTools (somente em determinados modelos)

Procedimentos de Configuração 74
Inicialização do Device Access Manager 74
Configuração do acesso a dispositivos 74
Grupo Administradores de dispositivos 74
Configuração Simples 75
Inicialização do serviço de segundo plano 75
Configuração de Classe de Dispositivo 76
Negarção de acesso a um usuário ou grupo 78
Permissão de acesso para um usuário ou grupo 78
Remoção do acesso para um usuário ou grupo 79
Permissão de acesso a uma classe de dispositivos para o usuário de um grupo 79
Permitissão de acesso a dispositivos específicos para o usuário de um grupo 79
Restauração das configurações 80
Tarefas avançadas 81
Controle do acesso aos parâmetros de configuração 81
Garantir acesso a um grupo ou usuário existente 81
Negação de acesso para um grupo ou usuário existente 82
Inclusão de um novo grupo ou usuário 82
Remoção do acesso de um grupo ou usuário 82
Documentação relacionada 82

11 LoJack Pro for HP ProtectTools

12 Solução de problemas

HP ProtectTools Security Manager 85
Device Access Manager for HP ProtectTools 87
Diversos 89

Glossário 90

Índice 95

1 Introdução à segurança

O software HP ProtectTools Security Manager fornece recursos de segurança que ajudam na proteção contra o acesso não autorizado ao computador, às redes e aos dados críticos. A administração do HP ProtectTools Security Manager é regida pelo recurso Console Administrativo.

Usando o console, o administrador local pode executar as seguintes tarefas:

- Ativar ou desativar recursos de segurança
- Registrar as impressões digitais dos usuários deste computador
- Configurar um smart card
- Especificar as credenciais necessárias para a autenticação
- Gerenciar usuários do computador
- Ajustar parâmetros específicos de dispositivos
- Configurar aplicativos instalados do Security Manager
- Adicionar aplicativos ao Security Manager

Os módulos de software disponíveis para seu computador podem variar de acordo com o modelo.

Os módulos de software do HP ProtectTools podem estar pré-instalados, pré-carregados ou disponíveis para download no website da HP. Para obter mais informações, acesse http://www.hp.com.

NOTA: As instruções neste guia foram escritas considerando-se que os módulos do software HP ProtectTools aplicáveis já estão instalados.

Recursos do HP ProtectTools

A tabela a seguir detalha os principais recursos dos módulos do HP ProtectTools.

Módulo	Principais recursos
Credential Manager for HP ProtectTools	• O Gerenciador de Senhas atua como um cofre de senhas pessoal, otimizando o processo de login com o recurso Single Sign On, que lembra e aplica as credenciais do usuário automaticamente. • O recurso Single Sign On também oferece proteção adicional, pois exige uma combinação de diferentes tecnologias de segurança, como Java™ Card e biometria, para efetuar a autenticação de usuários. • O armazenamento de senhas é protegido por meio de criptografia de software, e essa proteção pode ser aprimorada com o uso da autenticação via dispositivos de segurança, como o Java Cards ou dados biométricos. **NOTA:** A funcionalidade do Credential Manager pode ser encontrada na opção Gerenciador de Senhas do HP ProtectTools Security Manager
Drive Encryption for HP ProtectTools (somente em determinados modelos)	• O Drive Encryption fornece criptografia completa para uma unidade de disco inteira ("full-volume"). • O Drive Encryption força uma autenticação durante a pré-inicialização para que os dados sejam descriptografados e possam ser acessados.
Privacy Manager for HP ProtectTools (somente em determinados modelos)	• O Privacy Manager utiliza técnicas de login avançadas para verificar a origem, a integridade e a segurança da comunicação ao enviar e receber e-mails, utilizar documentos do Microsoft® Office ou trocar mensagens instantâneas.
File Sanitizer for HP ProtectTools	• O File Sanitizer permite fragmentar com segurança ativos digitais (informações confidenciais que incluem arquivos de aplicativos, conteúdo histórico ou da Web, ou outros dados confidenciais) em seu computador e periodicamente limpar sua unidade de disco rígido.
Device Access Manager for HP ProtectTools (somente em determinados modelos)	• O Device Access Manager permite aos gerentes de TI controlar o acesso aos dispositivos com base em perfis de usuário. • O Device Access Manager evita que usuários não-autorizados removam dados utilizando mídia de armazenamento externo e introduzam vírus no sistema provenientes de mídia externa. • O administrador pode desativar o acesso a dispositivos graváveis para determinados indivíduos ou grupos de usuários.

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:

- Proteção contra roubo direcionado
- Restrição de acesso a dados confidenciais
- Prevenção contra acesso não-autorizado a partir de locais internos ou externos
- Criação de políticas de senhas fortes
- Tratar de questões de segurança regulamentares

Proteção contra roubo direcionado

Um exemplo de roubo direcionado poderia ser o de um computador que contém dados confidenciais e informações de clientes no ponto de controle de segurança de um aeroporto. Os seguintes recursos ajudam a proteger contra roubo direcionado:

- O recurso de autenticação na pré-inicialização, se ativado, ajuda a evitar o acesso ao sistema operacional. Consulte os seguintes procedimentos:
  - Security Manager
  - Drive Encryption

Restrição de acesso a dados importantes

Suponha que um auditor contratado esteja trabalhando localmente em uma empresa e tenha obtido acesso ao computador para analisar dados financeiros confidenciais; não é desejável que o auditor possa imprimir os arquivos ou salvá-los em um dispositivo gravável, como um CD. O seguinte recurso ajuda a restringir o acesso aos dados:

- O Device Access Manager for HP ProtectTools permite aos gerentes de TI restringirem o acesso a dispositivos de gravação de modo que informações confidenciais não possam ser impressas ou copiadas da unidade de disco rígido para uma mídia removível.

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

O acesso não autorizado a um PC comercial desprotegido representa um risco bastante tangível aos recursos de rede corporativos, como informações de serviços financeiros, de um executivo ou da equipe de P&D, e informações confidenciais como registros de patente ou registros financeiros pessoais. Os seguintes recursos ajudam a evitar o acesso não-autorizado:

- O recurso de autenticação na pré-inicialização, se ativado, ajuda a evitar o acesso ao sistema operacional. Consulte os seguintes procedimentos:
  - Gerenciador de Senhas
  - Drive Encryption
- O Gerenciador de Senhas ajuda a garantir que um usuário não autorizado não obtenha senhas ou acesse aplicativos protegidos por senha.

- O Device Access Manager for HP ProtectTools permite que os gerentes de TI restrinjam o acesso a dispositivos de gravação de modo que informações confidenciais não possam ser copiadas da unidade de disco rígido.
- O DriveLock ajuda a garantir que os dados não possam ser acessados mesmo se a unidade de disco rígido for removida e instalada em um sistema desprotegido.

Criação de políticas de senhas fortes

Se entrar em vigor uma ordem que exige o uso de uma política de senha forte para diversos aplicativos baseados na web e bancos de dados, o Security Manager fornecerá um repositório de senhas protegido e o conveniente recurso Single Sign On.

Elementos adicionais de segurança

Atribuição de perfis de segurança

No gerenciamento da segurança de computador (principalmente em grandes organizações), 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, as obrigações e os privilégios da segurança podem ser divididos nas seguintes funções:

- Diretor de segurança - Define o nível de segurança para a empresa ou rede e determina os recursos de segurança a implementar, como Java™ Cards, leitores biométricos ou tokens USB.

  NOTA: Diversos recursos do HP ProtectTools podem ser personalizados pelo responsável pela segurança em conjunto com a HP. Para obter mais informações, consulte o Web site da HP em http://www.hp.com.br.

- Administrador de TI – Aplica e gerencia os recursos de segurança definidos pelo diretor de segurança. Pode também ativar e desativar alguns recursos. Por exemplo, se o responsável pela segurança tiver decidido implementar Java Cards, o administrador de TI pode ativar o modo de segurança do BIOS por Java Card.

- Usuário - Utiliza os recursos de segurança. Por exemplo, se o responsável pela segurança e o administrador de TI tiverem ativado Java Cards para o sistema, o usuário pode definir o PIN do Java Card e usar o cartão para autenticação.

CUIDADO: Os administradores são encorajados a seguir as "melhores práticas" restringindo os privilégios do usuário final e o acesso do usuário.

Usuários não-autorizados não devem receber privilégios administrativos.

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 definidas e usadas somente por administradores de TI também são indicadas nesta tabela. Todas as outras senhas podem ser definidas por usuários ou administradores comuns.

Senha do HP ProtectTools	Definida neste módulo do HP ProtectTools	Função
Senha de login do Security Manager	Security Manager	Esta senha oferece duas opções: • Pode ser usada como login do Security Manager para acessá-lo após o login no Windows. • Pode ser usada para permitir o acesso ao Windows e ao Security Manager simultaneamente.

Senha do HP ProtectTools	Definida neste módulo do HP ProtectTools	Função
Senha do arquivo de recuperação do Security Manager	Security Manager, pelo administrador de TI	Protege o acesso ao arquivo de recuperação do Security Manager.
PIN do Java™ Card	Java Card Security	Protege o acesso ao conteúdo do Java Card e autentica usuários do Java card. Ao ser usado para autenticação na inicialização, o PIN do Java Card também protege o acesso ao utilitário de configuração do computador e ao conteúdo do computador. Autentica usuários do Drive Encryption, se o token de Java Card estiver selecionado.
Senha de login do Windows	Painel de Controle do Windows®	Pode ser usada no login manual ou salva no Java Card.

Criação de uma senha segura

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.
- Divida 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 e restauração de credenciais do HP ProtectTools

Você pode usar o Drive Encryption for HP ProtectTools para selecionar e fazer backup de credenciais do HP ProtectTools.

2 Passos iniciais

NOTA: A administração do HP ProtectTools requer privilégios de administrador.

O Assistente de Configuração do HP ProtectTools guiará você pelo processo de configuração dos recursos mais utilizados do Security Manager. No entanto, há uma série de funcionalidades adicionais disponíveis por meio do Console Administrativo do HP ProtectTools. As mesmas configurações encontradas no assistente, bem como recursos de segurança adicionais, podem ser encontradas em todo o console, que é acessado pelo menu Iniciar do Windows®. Essas configurações aplicam-se ao computador e a todos os usuários que o compartilham.

1. Na página de boas vindas, você pode desativar exibições futuras do assistente selecionando uma das opções.
2. Uma semana após a configuração do computador, ou quando algum usuário com direitos administrativos deslizar o dedo no leitor de impressões digitais pela primeira vez, o Assistente de Configuração do HP ProtectTools se abrirá automaticamente para guiá-lo pelas etapas básicas de configuração do programa. Um tutorial em vídeo sobre a configuração de seu computador será iniciado automaticamente.
3. Siga as instruções na tela até que a configuração seja concluída.

Se você não concluir o assistente, ele abrirá automaticamente mais duas vezes. Após isso e até que a configuração esteja concluída, você poderá acessar o assistente por meio do balão de notificação próximo à área de notificação da barra de tarefas (a não ser que você tenha desativado o assistente, conforme descrito na etapa 2 acima).

Para usar os aplicativos do HP ProtectTools Security Manager, abra o HP ProtectTools Security Manager por meio do menu Iniciar ou clique com o botão direito no ícone do Security Manager na área de notificação, localizada à extrema direita da barra de tarefas. O Console Administrativo do HP ProtectTools e seus aplicativos estão disponíveis para todos os usuários que compartilham o computador.

Inicialização do Console Administrativo do HP ProtectTools

Para tarefas de administrador, tais como estabelecimento de políticas de sistema ou configurações de software, abra o console da seguinte forma:

- Clique em **Iniciar**, **Todos os Programas**, **HP** e, em seguida, em **Console Administrativo do HP Protect Tools**.

  – ou –

  No painel esquerdo do Security Manager, clique em **Administração**.

Para acessar as tarefas do usuário, como o registro das impressões digitais ou a utilização do Security Manager, abra o console da seguinte maneira:

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

  – ou –

  Clique duas vezes no ícone do **HP ProtectTools Security Manager** na área de notificação, à direita da barra de tarefas.

Ativação de recursos de segurança

O Assistente de Configuração solicitará a verificação de sua identidade.

1. Leia a tela "Bem-vindo" e, em seguida, clique em **Avançar**.
2. Verifique sua identidade, seja digitando sua senha do Windows, se você ainda não registrou suas impressões digitais, ou fornecendo sua impressão digital por meio do leitor de impressão digital. Clique em **Avançar**.

   Se você não tiver uma senha para o Windows, será solicitado que crie uma. A senha do Windows é necessária para impedir que sua conta do Windows seja acessada por pessoas não-autorizadas e para que você usufrua dos recursos do HP ProtectTools Security Manager.

O Assistente de Configuração guiará você ao longo do processo de ativação dos recursos de segurança que se aplicam a todos os usuários do computador:

- A Segurança do Windows protege sua(s) conta(s) do Windows solicitando o uso de credenciais específicas para acesso.
- O Drive Encryption protege seus dados criptografando sua(s) unidade(s) de disco rígido, tornando assim as informações ilegíveis para pessoas sem a devida autorização.
- O Pre-Boot Security protege seu computador proibindo o acesso de pessoas não-autorizadas antes da inicialização do Windows.

Para ativar um recurso de segurança, marque a caixa de seleção correspondente. Quanto mais recursos marcar, mais segurança terá o seu computador.

NOTA: O Pre-Boot Security não estará disponível se seu BIOS não suportá-lo.

Registro de impressões digitais

Se você tiver selecionado "Impressão digital" e seu computador tiver um leitor de impressões digitais integrado ou conectado a ele, você será guiado pelo processo de configuração ou "registro" de suas impressões digitais:

1. É exibido o desenho de duas mãos. Os dedos que já estão registrados são realçados em verde. Clique em um dedo do desenho.

   NOTA: Para excluir uma impressão digital já registrada, clique no dedo correspondente.

2. Quando tiver selecionado um dedo para ser registrado, será solicitado que você o deslize sobre o leitor até que a impressão digital seja registrada com sucesso. Os dedos registrados são realçados em verde no desenho.

3. Você deve registrar pelo menos dois dedos; de preferência o indicador e o médio. Repita as etapas 1 a 3 para registrar outro dedo.

4. Clique em **Avançar**.

NOTA: Quando você registra impressões digitais por meio do processo Passos iniciais, elas não são salvas até que você clique em **Avançar**. Se você deixar o computador inativo por algum tempo ou fechar o painel de controle, as alterações realizadas **não** serão salvas.

Configuração de um smart card

Se você selecionar "Smart card" e houver um leitor de cartão smart card integrado ou conectado ao seu computador, o Assistente de Configuração do HP ProtectTools solicitará que você configure o PIN (número de identificação pessoal) do smart card.

Para configurar um PIN de smart card:

1. Na página “Configurar smart card”, digite e confirme um PIN.

   Você também pode alterar o seu PIN. Insira seu PIN antigo e, em seguida, escolha um novo.

2. Para continuar, clique em **Avançar**.

Utilização do Console Administrativo

O Console Administrativo do HP ProtectTools é o ponto central para administrar os recursos e aplicativos do HP ProtectTools Security Manager.

O console é composto pelos seguintes componentes:

- **Ferramentas**: Exibe as seguintes categorias para a configuração da segurança do computador:
  - **Página Inicial**: Permite selecionar as tarefas de segurança a serem realizadas.
  - **Sistema**: Permite configurar recursos de segurança e autenticações para usuários e dispositivos.
  - **Aplicativos**: Exibe configurações gerais para o HP ProtectTools Security Manager e para aplicativos do Security Manager.
  - **Dados**: Oferece um menu expansível de links para aplicativos do Security Manager que protegem seus dados.
- **Ferramentas Administrativas**: Oferece informações acerca de ferramentas adicionais. O painel abaixo exibe as seguintes opções:
  - **Assistente de Configuração do HP ProtectTools**: Guiará você pelo processo de configuração do Security Manager.
  - **Ajuda**: Exibe o arquivo de Ajuda, que fornece informações sobre o Security Manager e seus aplicativos pré-instalados. A Ajuda para os aplicativos que você pode vir a adicionar é fornecida junto com eles.
  - **Sobre**: Exibe informações sobre o HP ProtectTools Security Manager, tais como o número da versão e o aviso de direitos autorais.
- **Área principal**: Exibe telas específicas dos aplicativos.

Para abrir o Console Administrativo do HP ProtectTools, clique em **Iniciar**, **Todos os Programas**, **HP** e, em seguida, em **Console Administrativo do HP ProtectTools**.

3 Configuração do sistema

O grupo Sistema é acessado a partir do painel do menu Ferramentas, do lado esquerdo da tela do Console Administrativo do HP ProtectTools. É possível usar os aplicativos deste grupo para gerenciar políticas e configurações para o computador, seus usuários e seus dispositivos.

Os aplicativos a seguir estão incluídos no grupo Sistema:

- **Segurança**: Gerencie recursos, autenticações e configurações referentes a como os usuários interagem com o computador.
- **Usuários**: Estabeleça, gerencie e registre usuários do computador.
- **Dispositivos**: Gerencie configurações para dispositivos de segurança integrados ou conectados ao computador.

Configuração de autenticação para seu computador

Dentro do aplicativo Autenticação, é possível escolher que recursos de segurança devem ser implementados no computador, estabelecer políticas referentes ao acesso ao computador e configurar opções avançadas adicionais. É possível especificar as credenciais necessárias para autenticar cada classe de usuário ao se fazer login no Windows ou login em sites da Web e em programas durante uma sessão de usuário.

Para configurar a autenticação em seu computador:

1. No painel de menu Segurança, clique em **Autenticação**.
2. Para configurar a autenticação de login, clique na guia **Política de login**, faça as alterações e clique em **Aplicar**.
3. Para configurar a autenticação de sessão, clique na guia **Política de sessão**, faça as alterações e clique em **Aplicar**.

Política de login

Para definir as políticas referentes às credenciais necessárias para autenticar um usuário ao efetuar login no Windows:

1. No menu Ferramentas, clique em **Segurança** e, em seguida, em **Autenticação**.
2. Na guia **Política de login**, clique em uma categoria de usuário.
3. Especifique a credencial ou credenciais de autenticação necessárias para a categoria de usuário selecionada. É necessário especificar ao menos uma credencial.
4. Escolha se ALGUMA (somente uma) das credenciais especificadas ou se TODAS elas são necessárias para a autenticação dos usuários. Também é possível impedir o acesso de qualquer usuário ao computador.
5. Clique em **Aplicar**.

Política de sessão

Para definir as políticas referentes às credenciais necessárias para acessar os aplicativos HP ProtectTools durante uma sessão do Windows:

1. No menu Ferramentas, clique em **Segurança** e, em seguida, em **Autenticação**.
2. Na guia **Política de sessão**, clique em uma categoria de usuário.
3. Especifique a credencial ou credenciais de autenticação necessárias para a categoria de usuário selecionada.
4. Escolha se ALGUMA (somente uma) das credenciais especificadas ou se TODAS elas serão necessárias para a autenticação dos usuários. Também é possível escolher o acesso sem autenticação ao software HP ProtectTools.
5. Clique em **Aplicar**.

Configurações

Você pode permitir uma ou mais das seguintes configurações de segurança:

- **Permitir login único**: Permite que os usuários do computador pulem o login do Windows se a autenticação já tiver sido realizada no nível do BIOS ou do disco criptografado.
- **Permitir autenticação HP SpareKey para login no Windows**: Permite que os usuários deste computador usem o recurso HP SpareKey para efetuar login no Windows, independentemente de qualquer outra política de autenticação solicitada pelo Security Manager.

Para editar as configurações:

1. Clique para ativar ou desativar uma configuração específica.
2. Clique em **Aplicar** para salvar as alterações realizadas.

Gerenciamento de usuários

Dentro do aplicativo Usuários, é possível monitorar e gerenciar os usuários do HP ProtectTools do computador.

Todos os usuários do HP ProtectTools são listados e verificados quanto às políticas estabelecidas no Security Manager, e se registraram ou não as credenciais apropriadas para que estejam em conformidade com tais políticas.

Para adicionar usuários, clique em **Adicionar**.

Para excluir um usuário, clique no usuário e, em seguida, em **Excluir**.

Para registrar impressões digitais ou estabelecer credenciais adicionais para o usuário, clique no usuário e, a seguir, clique em **Registrar**.

Para visualizar as políticas para um usuário específico, selecione o usuário e, a seguir, clique em **Visualizar Políticas**.

Especificação de configurações de dispositivos

Dentro do aplicativo Dispositivo, é possível especificar configurações disponíveis para qualquer dispositivo de segurança integrado ou conectado ao computador que seja reconhecido pelo HP ProtectTools Security Manager.

Impressões digitais

A página Impressões digitais tem três guias: Registro, Sensibilidade e Avançado.

Registro

Você pode escolher o número mínimo ou máximo de impressões digitais que um usuário pode registrar.

Também é possível apagar todos os dados do leitor de impressão digital.

⚠ **AVISO!** Todos os dados de impressão digital de todos os usuários, incluindo administradores, serão apagados. Se a política de login exigir apenas impressões digitais, todos os usuários podem ficar impossibilitados de fazer login no computador.

Sensibilidade

Para ajustar a sensibilidade usada pelo leitor de impressão digital ao ler uma impressão digital, mova o controle deslizante.

Se sua impressão digital muitas vezes não é reconhecida, pode ser necessária uma configuração com menos sensibilidade. Uma configuração mais alta aumenta a sensibilidade a variações na leitura de impressões digitais e, portanto, diminui o risco de uma aprovação falsa. A configuração Média-Alta oferece uma boa combinação de segurança e praticidade.

Avançado

Você pode configurar o leitor de impressão digital para economizar energia quando o computador estiver sendo operado por bateria.

Smart Card

É possível configurar o computador para que fique automaticamente bloqueado quando o smart card for removido. No entanto, o computador só será bloqueado se o smart card tiver sido usado como uma credencial de autenticação no login do Windows. A remoção de um smart card que não foi usado para o login do Windows não bloqueará o computador.

- Marque a caixa de seleção para ativar ou desativar o bloqueio do computador quando o smart card for removido.

4 Configuração dos aplicativos

O grupo Aplicativos é acessado por meio do painel de menu Aplicativos de Segurança do lado esquerdo do Console Administrativo do HP ProtectTools. Você pode usar as Configurações para personalizar o comportamento dos aplicativos do HP ProtectTools Security Manager instalados no momento.

Para editar as configurações dos aplicativos:

1. No menu Ferramentas, a partir do grupo **Aplicativos**, clique em **Configurações**.
2. Clique para ativar ou desativar uma configuração específica.
3. Clique em **Aplicar** para salvar as alterações realizadas.

Guia Geral

As seguintes configurações estão disponíveis na guia Geral:

- **Não abrir automaticamente o Assistente de Configuração para administradores**: Selecione esta opção para impedir que o assistente seja iniciado automaticamente após o login.
- **Não abrir automaticamente o assistente de passos inicias para usuários**: Selecione esta opção para impedir que as configurações do usuário abram automaticamente após o login.

Guia Aplicativos

As configurações aqui exibidas podem mudar quando novos aplicativos são adicionados ao Security Manager. As configurações mínimas exibidas por padrão são as seguintes:

- **Security Manager**: Permite o acesso ao aplicativo Security Manager a todos os usuários do computador .
- **Ativar botão Descobrir mais**: Permite que todos os usuários do computador adicionem aplicativos ao HP ProtectTools Security Manager clicando no botão **[+] Descobrir mais**.

Para restaurar todos os aplicativos às suas configurações de fábrica, clique no botão **Restaurar padrões**.

5 Adição de ferramentas de gerenciamento

Outros aplicativos podem estar disponíveis para adicionar ferramentas de gerenciamento ao Security Manager. O administrador do computador pode desativar esse recurso por meio do aplicativo Configurações.

Para incluir ferramentas de gerenciamento adicionais, clique em **[+] Ferramentas de gerenciamento**.

Você pode acessar o site da DigitalPersona na Web para verificar se há novos aplicativos, ou pode configurar um agendamento para atualizações automáticas.

6 HP ProtectTools Security Manager

O HP ProtectTools Security Manager permite que você aumente a segurança de seu computador de maneira significativa.

Você pode usar aplicativos pré-carregados do Security Manager, bem como aplicativos adicionais disponíveis para download direto da Web, para:

- Gerenciar seu login e senhas
- Mudar com facilidade sua senha do sistema operacional Windows®
- Definir preferências de programa
- Usar impressões digitais para maior segurança e praticidade
- Definir um smart card para autenticação
- Fazer backup e restaurar seus dados de programa
- Adicionar mais aplicativos

Procedimentos de configuração

Passos iniciais

O Assistente de Configuração do HP ProtectTools será exibido automaticamente como a página-padrão do HP ProtectTools Security Manager até que a configuração seja concluída.

Para configurar o Security Manager, siga as etapas abaixo:

NOTA: Caso não haja um leitor de impressão digital ou smart card disponível, realize apenas as etapas 1, 5 e 6.

1. Na página “Bem-vindo”, clique em **Avançar**.
2. A página a seguir lista os métodos de autenticação disponíveis no computador. Clique em **Avançar** para prosseguir.
3. Na página “Verifique sua Identidade”, digite sua senha do Windows e, em seguida, clique em **Avançar**.
4. Consulte um ou mais dos tópicos a seguir, dependendo da configuração do seu computador.
   - Se houver um leitor de impressões digitais disponível, consulte Registro de impressões digitais na página 24.
   - Se houver um leitor de cartões smart card disponível, consulte Configuração de um smart card na página 25.
5. Se não houver um leitor de impressão digital nem um smart card disponível, será solicitado que você digite sua senha do Windows. Você deverá usar essa senha posteriormente, sempre que uma autenticação for solicitada.
6. Na última página do assistente, clique em **Concluir**.

   O painel de controle do Security Manager é exibido.

Registro de credenciais

É possível usar a página “Minha Identidade” para registrar diversos métodos de autenticação ou credenciais. Após o registro, é possível usar esses métodos para fazer login no Security Manager.

Registro de impressões digitais

Se seu computador possui um leitor de impressões digitais integrado ou conectado, o Assistente do HP ProtectTools guiará você pelo processo de configuração ou registro de suas impressões digitais.

1. Leia a tela "Bem-vindo" e, em seguida, clique em **Avançar**.
2. Verifique sua identidade, seja digitando sua senha do Windows, se você ainda não registrou suas impressões digitais, ou fornecendo sua impressão digital por meio do leitor de impressão digital. Clique em **Avançar**.

   Se você não tiver uma senha para o Windows, será solicitado que crie uma. A senha do Windows é necessária para impedir que sua conta do Windows seja acessada por pessoas não-autorizadas e para que você usufrua dos recursos do HP ProtectTools Security Manager.
3. É exibido o desenho de duas mãos. Os dedos que já estão registrados são realçados em verde. Clique em um dedo do desenho.

NOTA: Para excluir uma impressão digital já registrada, clique na impressão digital correspondente.

4. Quando tiver selecionado um dedo para ser registrado, será solicitado que você o deslize sobre o leitor até que a impressão digital seja registrada com sucesso. Os dedos registrados são realçados em verde no desenho.

5. Você deve registrar pelo menos dois dedos; de preferência o indicador e o médio. Repita as etapas 3 e 4 para registrar outro dedo.

6. Clique em **Avançar**.

NOTA: Quando você registra impressões digitais por meio do processo Passos iniciais, elas não são salvas até que você clique em **Avançar**. Se você deixar o computador inativo por algum tempo ou fechar o painel de controle, as alterações realizadas **não** serão salvas.

Alteração da senha do Windows

O Security Manager torna a alteração de sua senha do Windows mais simples e rápida do que por meio do Painel de Controle do Windows.

Para alterar sua senha do Windows, siga as etapas abaixo:

1. No painel de controle do Security Manager, clique em **Minha Identidade**, **Credenciais**, **Senha**.

2. Digite a senha atual na caixa de texto **Senha do Windows atual**.

3. Digite uma nova senha na caixa de texto **Nova senha do Windows** e, a seguir, digite-a novamente na caixa de texto **Confirmar nova senha**.

4. Clique em **Alterar** para mudar imediatamente sua senha atual para a nova senha digitada.

Configuração de um smart card

Se houver um leitor de smart card integrado ou conectado ao computador, o Security Manager solicitará que você defina um PIN (número de identificação pessoal) para o smart card.

- Para configurar um PIN de smart card: na página "Configurar smart card", insira e confirme um PIN.

- Para alterar seu PIN: primeiro digite o PIN antigo e, em seguida, escolha um novo.

Utilização do painel de controle do Security Manager

O painel de controle do Security Manager é o ponto central para se ter acesso fácil aos recursos, aplicativos e configurações do HP ProtectTools Security Manager.

O painel de controle é composto pelos seguintes componentes:

- **ID Card**: Exibe o nome de usuário do Windows e uma imagem selecionada identificando a conta de usuário que efetuou o login.
- **Aplicativos de Segurança**: Exibe um menu expansível de links para configuração das seguintes categorias de segurança:
  - **Minha Identidade**
  - **Meus Dados**
  - **Meu Computador**
- **Descobrir mais**: Abre uma página em que é possível encontrar aplicativos adicionais para aprimorar a segurança de sua identidade, dados e comunicações.
- **Área principal**: Exibe telas específicas dos aplicativos.
- **Administração**: Abre o Console Administrativo do HP ProtectTools.
- **Botão de ajuda**: Exibe informações acerca da tela atual.
- **Avançado**: Permite o acesso às opções a seguir:
  - **Preferências**: Permite que você personalize as configurações do Security Manager.
  - **Backup e Restauração**: Permite que você faça backup ou restaure dados.
  - **Sobre**: Exibe informações da versão do Security Manager.

Para abrir o painel do Security Manager, clique em **Iniciar**, **Todos os Programas**, **HP** e, em seguida, em **HP ProtectTools Security Manager**.

Inicialização do HP ProtectTools Security Manager

É possível iniciar o HP ProtectTools Security Manager de qualquer uma das seguintes maneiras:

- Clique em **Iniciar**, **Todos os Programas**, **HP** e, em seguida, em **HP ProtectTools Security Manager**.
- Clique duas vezes no ícone do **HP ProtectTools** na área de notificação, à direita da barra de tarefas.
- Clique com o botão direito no ícone do **HP ProtectTools** e, a seguir, em **Abrir o HP ProtectTools Security Manager**.
- Clique no gadget **Security Manager ID Card** na Barra Lateral do Windows.
- Aperte a combinação de teclas de atalho ctrl+alt+H para abrir o menu Links Rápidos do Security Manager.

Tarefas básicas

Os aplicativos incluídos neste grupo ajudam você a gerenciar vários aspectos da sua identidade digital.

- **Security Manager**: Cria e gerencia Links Rápidos, os quais permitem que você inicialize e faça login em websites e programas pela autenticação com sua senha do Windows, suas impressões digitais ou um smart card.
- **Credenciais**: Fornece um meio de alterar sua senha do Windows, registrar impressões digitais ou configurar um smart card com facilidade.

Para adicionar aplicativos, clique no botão **Descobrir mais** [+] no canto inferior esquerdo do painel de controle. Esse botão pode ser desativado pelo administrador.

Gerenciador de Senhas

Fazer login no Windows, em sites da Web e em aplicativos é mais fácil e mais seguro com o Gerenciador de Senhas. Você pode usá-lo para criar senhas mais fortes, as quais você não precisa anotar ou memorizar, e então fazer login fácil e rapidamente por meio de impressão digital, smart card ou da senha do Windows.

O Gerenciador de Senhas oferece as seguintes opções:

- Adicionar, editar ou excluir logins a partir da guia Gerenciar.
- Usar Links Rápidos para abrir seu navegador padrão e fazer login em qualquer site da Web ou programa após sua configuração.
- Arrastar e soltar ícones para organizar seus Links Rápidos em categorias.
- Saber rapidamente se alguma de suas senhas é um risco à segurança e gerar automaticamente uma senha forte e complexa para ser usada em novos sites.

Muitos recursos do Gerenciador de Senhas também estão disponíveis a partir do ícone do Gerenciador de Senhas que é exibido quando a tela de login de uma página da Web ou programa está em foco. Clique no ícone para exibir um menu de contexto em que você pode escolher entre as seguintes opções:

Para páginas da Web ou programas para os quais não foi criado um login

As opções abaixo são exibidas no menu de contexto:

- **Adicionar [nomedodomínio.com] ao Gerenciador de Senhas**: Permite que você adicione um login para a tela de login atual.
- **Abrir Gerenciador de Senhas**: Abre o Gerenciador de Senhas.
- **Configurações do Ícone**: Permite que você especifique as condições em que o ícone do Gerenciador de Senhas é exibido.
- **Ajuda**: Exibe a ajuda do software Gerenciador de Senhas.

Para páginas da Web ou programas para os quais já foi criado um login

As opções abaixo são exibidas no menu de contexto:

- **Preencher dados de login**: Insere seus dados de login nos campos de login e, em seguida, envia a página (se o envio foi especificado quando o login foi criado ou editado da última vez).
- **Editar login**: Permite que você modifique seus dados de login para o respectivo site da Web.
- **Adicionar nova conta**: Permite que você adicione uma conta a um login.
- **Abrir Gerenciador de Senhas**: Abre o aplicativo Gerenciador de Senhas.
- **Ajuda**: Exibe a ajuda do software Gerenciador de Senhas.

NOTA: O administrador do computador pode ter configurado o Security Manager de forma a exigir mais de uma credencial ao verificar sua identidade.

Adição de logins

Você pode adicionar facilmente um login para um site da Web ou programa fornecendo as informações de login uma única vez. Feito isso, o Gerenciador de Senhas passa a inserir automaticamente as informações para você. Você pode usar esses logins após navegar até o site da Web ou programa, ou clicar em um login a partir do menu **Logins** para que o Gerenciador de Senhas abra o site da Web ou programa e efetue o login para você.

Para adicionar um login:

1. Abra a tela de login para um site da Web ou programa.
2. Clique na seta exibida no ícone do **Gerenciador de Senhas** e, a seguir, clique em uma das seguintes opções, dependendo de a tela de login ser de um site da Web ou programa:
   - Para um site da Web, clique em **Adicionar [nome do domínio] ao Gerenciador de Senhas**.
   - Para um programa, clique em **Adicionar esta tela de login ao Gerenciador de Senhas**.
3. Digite seus dados de login. Os campos de login na tela, e seus campos correspondentes na caixa de diálogo, são identificados com uma borda realçada em laranja. Você também pode visualizar essa caixa de diálogo clicando em **Adicionar Login** a partir da guia **Gerenciar** do **Gerenciador de Senhas**. Algumas opções dependem dos dispositivos de segurança conectados ao computador; por exemplo, o uso do atalho ctrl+alt+H, a leitura de sua impressão digital ou a inserção de um smart card.
   - Para preencher um campo de login com uma das escolhas pré-formatadas, clique nas setas à direita do campo.
   - Para adicionar outros campos da tela ao seu login, clique em **Escolher outros campos**.
   - Para que os campos de login sejam preenchidos, mas não enviados, desmarque a caixa de seleção **Enviar dados de login**.
   - Para visualizar a senha para este login, clique em **Exibir senha**.
4. Clique em **OK**.

   O sinal de adição é removido do ícone do Gerenciador de Senhas a fim de avisar que o login foi criado.

Toda vez que você acessar aquele site da Web ou abrir aquele programa, o ícone do Gerenciador de Senhas será exibido, indicando que você pode usar sua(s) credencial(is) registrada(s) para fazer o login.

Edição de logins

Para editar um login, siga as etapas abaixo:

1. Abra a tela de login para um site da Web ou programa.
2. Para exibir uma caixa de diálogo em que você possa editar suas informações de login, clique na seta exibida no ícone do **Gerenciador de Senhas** e, a seguir, em **Editar login**. Os campos de login na tela, e seus campos correspondentes na caixa de diálogo, são identificados com uma borda realçada em laranja.

   Você também pode visualizar essa caixa de diálogo clicando em **Editar o login desejado** na guia **Gerenciar o Gerenciador de Senhas**.
3. Edite suas informações de login.
   - Para preencher um campo de login com uma das escolhas pré-formatadas, clique nas setas à direita do campo.
   - Para adicionar outros campos da tela ao seu login, clique em **Escolher outros campos**.
   - Para que os campos de login sejam preenchidos, mas não enviados, desmarque a caixa de seleção **Enviar dados de login**.
   - Para visualizar a senha para este login, clique em **Exibir senha**.
4. Clique em **OK**.

Utilização do menu de logins

O Gerenciador de Senhas oferece uma maneira rápida e fácil de abrir sites da Web e programas para os quais você criou logins. Clique duas vezes no login de um programa ou site da Web a partir do menu **Logins**, ou da guia **Gerenciar** no **Gerenciador de Senhas**, para abrir a tela de login e, então, preencha seus dados de login.

Quando um login é criado, ele é automaticamente adicionado ao menu Logins do Gerenciador de Senhas.

Para exibir o menu Logins:

1. Pressione a combinação de teclas de atalho do **Gerenciador de Senhas**. A configuração de fábrica é ctrl+alt+h. Para alterar a combinação de teclas de atalho, clique em **Gerenciador de Senhas** e depois em **Configurações**.
2. Forneça sua impressão digital (em computadores com leitor de impressão digital integrado ou conectado).

Organização de logins em categorias

Use categorias para manter seus logins em ordem criando uma ou mais categorias. Em seguida, arraste e solte seus logins nas categorias desejadas.

Para adicionar uma categoria:

1. No painel de controle do Security Manager, clique em **Gerenciador de Senhas**.
2. Clique na guia **Gerenciar** e depois em **Adicionar Categoria**.
3. Digite um nome para a categoria.
4. Clique em **OK**.

Para adicionar um login a uma categoria:

1. Posicione o ponteiro do mouse sobre o login desejado.
2. Pressione e segure o botão esquerdo do mouse.
3. Em seguida, arraste o login para dentro da lista de categorias. As categorias serão realçadas quando você posicionar o mouse sobre elas.
4. Solte o botão do mouse quando a categoria desejada for realçada.

Seus logins não são movidos, mas apenas copiados para a categoria selecionada. É possível adicionar o mesmo login para mais de uma categoria e visualizar todos os seus logins clicando em **Todos**.

Gerenciamento de logins

O Gerenciador de Senhas facilita o gerenciamento de nossas informações de login para nomes de usuário, senhas e várias contas de login a partir de um único ponto central.

Seus logins são listados na guia Gerenciar. Se vários logins foram criados para o mesmo site da Web; então, cada um é listado sob o nome do site da Web e aninhado na lista de logins.

Para gerenciar seus logins:

No painel de controle do Security Manager, clique em **Gerenciador de Senhas** e, a seguir, na guia **Gerenciar**.

- **Adicionar um login**: Clique em **Adicionar login** e siga as instruções na tela.
- **Editar um login**: Clique em um login, clique em **Editar** e, então, modifique os dados de login.
- **Excluir um login**: Clique em um login e depois em **Excluir**.

Para incluir um login adicional para um site da Web ou programa:

1. Abra a tela de login para o site da Web ou programa.
2. Clique no ícone do **Gerenciador de Senhas** para exibir seu menu de atalhos.
3. Clique em **Adicionar outro login** e, então, siga as instruções na tela.

Avaliação da força de sua senha

O uso de senhas fortes para fazer login em sites da Web e programas é um aspecto importante para proteger sua identidade.

O Gerenciador de Senhas torna o monitoramento e aperfeiçoamento de sua segurança mais fácil, com análises instantâneas e automatizadas da força de cada senha usada para fazer login em seus sites da Web e programas.

Configurações do ícone do Gerenciador de Senhas

O Gerenciador de Senhas tenta identificar telas de login para sites da Web e programas. Quando detecta uma tela de login para a qual ainda não foi criado um login, ele solicita que você adicione um login para ela exibindo o ícone do Gerenciador de Senhas com um sinal de “+”.

Clique na seta do ícone e, em seguida, clique em **Configurações do Ícone** para personalizar a forma como o **Gerenciador de Senhas** trata possíveis sites de login.

- **Sugerir a adição de logins para telas de login**: Clique nesta opção para que o Gerenciador de Senhas solicite que você adicione um login quando for exibida uma tela de login para a qual ainda não exista um login configurado.
- **Excluir esta tela**: Marcar essa caixa de seleção fará com que o Gerenciador de Senhas não solicite outra vez que você adicione um login para a tela exibida.

Para acessar configurações adicionais do Gerenciador de Senhas, clique em **Gerenciador de Senhas** e depois em **Configurações** no painel de controle do Security Manager.

Configurações

É possível especificar configurações para personalizar o HP ProtectTools Security Manager:

1. **Sugerir a adição de logins para telas de login**: O ícone do Gerenciador de Senhas com um sinal de mais é exibido sempre que a tela de login de um site da Web ou programa é detectada, indicando que você pode adicionar um login para essa tela no arquivo de senhas. Para desativar esse recurso, na caixa de diálogo **Configurações do Ícone**, desmarque a caixa de seleção ao lado de **Sugerir a adição de logins para telas de login**.
2. **Abrir o Gerenciador de Senhas com ctrl+alt+H**: O atalho padrão que abre o menu de Links Rápidos do Gerenciador de Senhas é ctrl+alt+H. Para alterar o atalho, clique nesta opção e digite uma nova combinação de teclas. 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 salvar as alterações.

Credenciais

Suas credenciais do Security Manager são usadas para confirmar que você é realmente você. O administrador local deste computador pode definir as credenciais que serão utilizadas para comprovar sua identidade quando você efetua login em sua conta do Windows, sites da Web ou programas.

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

As credenciais disponíveis, as solicitações e o status atual são listados e podem incluir o seguinte:

- Impressões digitais
- Senha
- Smart Card

Para registrar ou mudar uma credencial, clique no link e siga as instruções na tela.

Seu ID card pessoal

Seu ID card identifica você de forma única como sendo o dono da conta do Windows em questão, e exibe seu nome e uma imagem de sua escolha. Ele é exibido de forma destacada no canto superior esquerdo das páginas do Security Manager e como um gadget na Barra Lateral do Windows.

Uma das diversas maneiras de obter acesso rápido ao Security Manager é clicando no seu ID Card na Barra Lateral do Windows.

Você pode alterar sua imagem e a maneira como seu nome é exibido. Por padrão, são exibidos seu nome de usuário do Windows completo e a imagem que você selecionou durante a instalação do Windows.

Para mudar o nome exibido:

1. No painel de controle do Security Manager, clique em **ID Card** no canto superior esquerdo.
2. Clique na caixa que exibe o nome inserido para sua conta no Windows. O sistema exibirá seu nome de usuário do Windows para essa conta.
3. Para alterar esse nome, digite o novo nome e clique no botão **Salvar**.

Para mudar a imagem exibida:

1. No painel de controle do Security Manager, clique em **Minha Identidade** e depois em **ID Card** no canto superior esquerdo.
2. Clique no botão **Escolher imagem**, clique em uma imagem e clique no botão **Salvar**.

Configuração de preferências

É possível personalizar as configurações do HP ProtectTools Security Manager. No painel de controle do Security Manager, clique em **Avançado** e depois em **Preferências**. As configurações disponíveis são exibidas em duas guias: Geral e Impressão digital.

Geral

As seguintes configurações estão disponíveis na guia Geral:

Aparência: **Exibir ícone na barra de tarefas**

Para ativar a exibição do ícone na barra de tarefas, marque a caixa de seleção.

Para desativar a exibição do ícone na barra de tarefas, desmarque a caixa de seleção.

Impressão digital

As seguintes configurações estão disponíveis na guia Impressão digital:

Ações Rápidas: Use as Ações Rápidas para selecionar a tarefa do Security Manager a ser realizada quando você mantém pressionada uma determinada tecla durante a leitura da sua impressão digital.

Para designar uma Ação Rápida a uma das teclas listadas:

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

Resposta da Leitura de Impressão Digital: Exibida apenas quando há um leitor disponível. Use essa configuração para ajustar a resposta que ocorre quando você informa sua impressão digital no leitor.

- **Ativar resposta sonora**: O Security Manager reproduz uma resposta sonora quando uma impressão digital é lida, reproduzindo sons diferentes para eventos de programa específicos. É possível atribuir novos sons a esses eventos por meio da guia Sons no Painel de Controle do Windows, ou desativar a resposta sonora desmarcando esta opção.
- **Exibir a qualidade de digitalização**: Por padrão, o Security Manager exibe a imagem de uma impressão digital com um ponto de interrogação sempre que a qualidade da digitalização da impressão digital não é boa o bastante para autenticar a pessoa. É possível desativar a exibição dessa imagem desmarcando essa opção.

Backup e restauração de dados

É recomendável que você faça backup de seus dados do Security Manager com regularidade. A frequência com que você deve fazer backup depende da frequência com que seus dados são alterados. Por exemplo, se você adicionar novos logins todos os dias, é aconselhável que você faça backup todos os dias.

Os backups também podem ser usados para passar dados de um computador para outro, o que também é chamado de importação e exportação.

NOTA: Esse recurso faz backup somente dos dados.

O HP ProtectTools Security Manager deve estar instalado no computador que receberá o backup dos dados para que estes possam ser restaurados.

Para fazer backup de seus dados:

1. No painel esquerdo, clique em **Avançado** e depois em **Backup e Restauração**.
2. Clique em **Fazer backup de dados**.
3. Selecione os módulos que você deseja incluir no backup. Na maioria dos casos, você selecionará todos eles.
4. Insira um nome para o arquivo de armazenamento. Por padrão, o arquivo será salvo na pasta Documentos. Clique em **Procurar** para especificar um local diferente.
5. Insira uma senha para proteger o arquivo.
6. Verifique sua identidade.
7. Clique em **Concluir**.

Para restaurar seus dados:

1. No painel esquerdo, clique em **Avançado** e depois em **Backup e Restauração**.
2. Clique em **Restaurar dados**.
3. Selecione o arquivo de armazenamento criado anteriormente. Você pode inserir o caminho no campo fornecido ou clicar em **Editar**.
4. Insira a senha usada para proteger o arquivo.

5. Selecione os módulos cujos dados você deseja restaurar. Na maioria dos casos, você selecionará todos os módulos listados.

6. Clique em **Concluir**.

Adição de aplicativos

É possível que se encontrem disponíveis aplicativos adicionais que oferecem novos recursos a este programa.

No painel de controle do Security Manager, clique em **[+] Descobrir mais** para procurar por aplicativos adicionais.

NOTA: Se não houver um link **[+] Descobrir mais** na parte inferior esquerda do painel de controle, é porque ele foi desativado pelo administrador do computador.

Status dos Aplicativos de Segurança

A página Status de Aplicativos do Security Manager exibe o estado geral de seus aplicativos de segurança instalados. Ele exibe os aplicativos que estão configurados e o estado de configuração de cada um. O resumo é exibido automaticamente quando o painel de controle do Security Manager é aberto ou quando você clica em **Aplicativos de Segurança**.

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

△ **CUIDADO:** Se decidir desinstalar o módulo Drive Encryption, você deve primeiro descriptografar todas as unidades criptografadas. Se isso não for feito, não será possível acessar os dados nas unidades criptografadas a menos que você tenha se registrado no serviço de recuperação do Drive Encryption. A reinstalação do módulo Drive Encryption não permitirá a você acessar as unidades criptografadas.

O Drive Encryption for HP ProtectTools oferece proteção de dados completa, criptografando a unidade de disco rígido do seu computador. Quando o Drive Encryption está ativado, é necessário efetuar login na tela de login do Drive Encryption, exibida antes da inicialização do sistema operacional Windows®.

O Assistente de Configuração do HP ProtectTools permite que os administradores ativem o Drive Encryption, façam backup da chave de criptografia, adicionem e removam usuários e desativem o Drive Encryption. Para obter mais informações, consulte a Ajuda do software HP ProtectTools Security Manager.

As seguintes tarefas podem ser executadas com o Drive Encryption:

- Gerenciamento de criptografia
  - Criptografar ou descriptografar unidades individuais

    NOTA: Apenas unidades de disco rígido internas podem ser criptografadas.
- Recuperação
  - Criar chaves de backup
  - Executar uma recuperação

Procedimentos de configuração

Inicialização do Drive Encryption

1. Clique em **Iniciar**, **Todos os Programas**, **HP** e, em seguida, em **Console Administrativo do HP ProtectTools**.
2. No painel esquerdo, clique em **Drive Encryption**.

Tarefas básicas

Ativação do Drive Encryption

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

NOTA: Esse assistente é utilizado também para adicionar e remover usuários.

– ou –

1. Clique em **Iniciar**, **Todos os Programas**, **HP** e, em seguida, em **Console Administrativo do HP ProtectTools**.
2. No painel esquerdo, clique em **Segurança** e, em seguida, clique em **Recursos**.
3. Marque a caixa de seleção **Drive Encryption** e clique em **Avançar**.
4. Em **Unidades para criptografar**, marque a caixa de seleção da unidade de disco rígido que deseja criptografar.
5. Insira o dispositivo de armazenamento no slot apropriado.

   NOTA: Para salvar a chave de criptografia, é preciso utilizar um dispositivo de armazenamento USB com formato FAT32.

6. Em **Dispositivo de armazenamento externo no qual salvar a chave de criptografia**, marque a caixa de seleção do dispositivo de armazenamento onde a chave de criptografia será salva.
7. Clique em **Aplicar**.

   A criptografia da unidade é iniciada.

Para obter mais informações, consulte a ajuda do software HP ProtectTools Security Manager.

Desativação do Drive Encryption

Use o Assistente de Configuração do HP ProtectTools para desativar o Drive Encryption. Para obter mais informações, consulte a Ajuda do software HP ProtectTools Security Manager.

– ou –

1. Clique em **Iniciar**, **Todos os Programas**, **HP** e, em seguida, em **Console Administrativo do HP ProtectTools**.
2. No painel esquerdo, clique em **Segurança** e, em seguida, clique em **Recursos**.
3. Desmarque a caixa de seleção **Drive Encryption** e clique em **Aplicar**.

   A descriptografia da unidade é iniciada.

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 houver ativado o recurso Pre-boot Security (segurança pré-início) no HP ProtectTools Security Manager, você fará o login no computador assim que ele for ligado, e não na tela de login do Drive Encryption.

1. Clique em seu nome de usuário, em seguida digite sua senha do Windows ou PIN do Java™ Card, ou forneça uma impressão digital registrada.
2. Clique em **OK**.

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.

Proteger seus dados criptografando a unidade de disco rígido

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

1. No Security Manager, clique em **Passos iniciais** e, em seguida, clique no ícone **Configuração do Security Manager**. É iniciada uma demonstração que descreve os recursos do Security Manager. É possível iniciar o Security Manager também a partir da página “Drive Encryption”.
2. No painel esquerdo, clique em **Drive Encryption** e, em seguida, clique em **Gerenciamento de criptografia**.
3. Clique em **Alterar criptografia**.
4. Selecione a(s) unidade(s) a criptografar.

NOTA: É altamente recomendável que você criptografe a unidade de disco rígido.

Exibição do status da criptografia

Os usuários podem exibir o status da criptografia a partir do HP ProtectTools Security Manager.

NOTA: A alteração do status da criptografia da unidade deve ser realizada com o Console Administrativo do HP ProtectTools.

1. Abra o **HP ProtectTools Security Manager**.
2. Em **Meus dados**, clique em **Status da criptografia**.

   Se o Drive Encryption estiver ativo, o status da unidade exibirá um dos seguintes códigos de status:

   - Ativo
   - Inativo
   - Não criptografado
   - Criptografado
   - Criptografando
   - Descriptografando

   Se a unidade de disco rígido estiver no processo de ser criptografada ou descriptografada, a barra de progresso exibirá o percentual concluído e o tempo restante para conclusão da criptografia ou descriptografia.

Tarefas avançadas

Gerenciamento do Drive Encryption (tarefa do administrador)

A página “Gerenciamento de criptografia” permite aos administradores visualizarem e alterarem o status do Drive Encryption (ativo ou inativo) e visualizarem o status de criptografia de todas as unidades de disco rígido do computador.

- Se o status estiver inativo, significa que o Drive Encryption ainda não foi ativado pelo administrador do Windows no HP ProtectTools Security Manager e, portanto, não está protegendo a unidade de disco rígido. Use o Assistente de Configuração do HP ProtectTools Security Manager para ativar o Drive Encryption.
- Se o status for Ativo, o Drive Encryption foi ativado e configurado. A unidade se encontra em um dos seguintes estados:
  - Não criptografado
  - Criptografado
  - Criptografando
  - Descriptografando

Criptografia ou descriptografia de unidades individuais

Para criptografar uma ou mais unidades de disco rígido no computador ou descriptografar uma unidade que já foi criptografada, use o recurso Alterar criptografia:

1. Abra o **Console Administrativo do HP ProtectTools**, clique em **Drive Encryption** e em **Gerenciamento de criptografia**.
2. Clique em **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)

A página “Recuperação” permite aos administradores fazerem o backup e a recuperação de chaves de criptografia.

Backup local da chave do Drive Encryption: permite fazer o backup de chaves de criptografia em mídia removível quando o Drive Encryption está ativado.

Criação de chaves de backup

É possível fazer o backup da chave de criptografia de uma unidade criptografada em um dispositivo de armazenamento removível:

△ **CUIDADO:** Certifique-se de guardar o dispositivo de armazenamento com a chave de backup em um local seguro, pois se esquecer a sua senha ou perder seu Java Card, este dispositivo será sua única forma de acesso ao disco rígido.

1. Abra o **Console Administrativo do HP ProtectTools**, clique em **Drive Encryption** e em **Recuperação**.
2. Clique em **Backup das chaves**.
3. Na página “Selecione o disco de backup”, marque a caixa de seleção do dispositivo onde deseja fazer o backup da chave de criptografia e, 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. Quando a caixa de diálogo de confirmação for exibida, clique em **Concluir**.

Execução de uma recuperação

Para executar uma recuperação caso tenha esquecido sua senha, siga estas etapas:

1. Ligue o computador.
2. Insira o dispositivo de armazenamento removível que contém sua chave de backup.
3. Quando a caixa de diálogo de login do Drive Encryption for HP ProtectTools for exibida, clique em **Cancelar**.
4. Clique em **Opções** no canto inferior esquerdo da tela e, em seguida, clique em **Recuperação**.
5. Selecione o arquivo que contém sua chave de backup ou clique em **Procurar** para procurá-lo e, em seguida clique em **Avançar**.
6. Quando a caixa de diálogo de confirmação for exibida, clique em **OK**.

   O computador é iniciado.

NOTA: É altamente recomendável que você redefina sua senha após a execução de uma recuperação.

8 Privacy Manager for HP ProtectTools (somente em determinados modelos)

O Privacy Manager for HP ProtectTools permite usar métodos avançados de login de segurança (autenticação) para verificar a origem, integridade e segurança da comunicação ao utilizar e-mail, documentos do Microsoft® Office ou troca de mensagens instantâneas.

O Privacy Manager eleva a infraestrutura de segurança fornecida pelo HP ProtectTools Security Manager, que inclui os seguintes métodos de login de segurança:

- Autenticação por impressão digital
- Senha do Windows®
- HP ProtectTools Java™ Card

Você pode usar qualquer um dos métodos de login de segurança acima no Privacy Manager.

O Privacy Manager requer o seguinte:

- HP ProtectTools Security Manager 5.00 ou superior
- Sistema operacional Windows® 7, Windows Vista® ou Windows XP
- Microsoft Outlook 2007 ou Microsoft Outlook 2003
- Uma conta de e-mail válida

NOTA: O Certificado do Privacy Manager (um certificado digital) é solicitado e instalado a partir do Privacy Manager antes do acesso aos recursos de segurança. Para obter mais informações sobre como solicitar um Certificado do Privacy Manager, consulte Solicitação e instalação de um Certificado do Privacy Manager na página 42.

Procedimentos de configuração

Inicialização do Privacy Manager

Para abrir o Privacy Manager:

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

– ou –

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

– ou –

Na barra de ferramentas de uma mensagem de e-mail do Microsoft Outlook, clique na seta para baixo ao lado de **Enviar com Segurança** e, em seguida, clique em **Certificados** ou **Contatos Confiáveis**.

– ou –

Na barra de ferramentas de um documento do Microsoft Office, clique na seta para baixo ao lado de **Assinar e Codificar** e, em seguida, clique em **Certificados** ou **Contatos Confiáveis**.

Gerenciamento de Certificados do Privacy Manager

Os certificados do Privacy Manager protegem dados e mensagens utilizando uma tecnologia de criptografia chamada de public key infrastructure – infraestrutura de chaves públicas (PKI). PKI exige que os usuários obtenham chaves de criptografia e um Certificado do Privacy Manager emitido por uma autoridade certificadora (certificate authority - CA). Ao contrário da maioria dos softwares de autenticação e criptografia que exigem apenas uma autenticação periódica, o Privacy Manager exige a autenticação toda vez que você assina uma mensagem de e-mail ou um documento do Microsoft Office utilizando uma chave de criptografia. O Privacy Manager torna seguro o processo de salvar e enviar suas informações importantes.

As seguintes tarefas podem ser executadas:

- Solicitação e instalação de um Certificado do Privacy Manager
- Visualização dos detalhes do Certificado do Privacy Manager
- Renovação de um Certificado do Privacy Manager
- Quando vários certificados estão disponíveis, defina um Certificado do Privacy Manager padrão para ser utilizado pelo Privacy Manager
- Exclusão e revogação de um Certificado do Privacy Manager (avançado)

Solicitação e instalação de um Certificado do Privacy Manager

Antes que você possa utilizar os recursos do Privacy Manager, precisa solicitar e instalar um Certificado do Privacy Manager (a partir do Privacy Manager) utilizando um endereço de e-mail válido. O endereço de e-mail precisa ser ajustado como uma conta dentro do Microsoft Outlook no mesmo computador a partir do qual você está solicitando um Certificado do Privacy Manager.

Solicitação de um Certificado do Privacy Manager

1. Abra o Privacy Manager e clique em **Gerenciador de Certificado**.
2. Clique em **Solicitar um certificado Privacy Manager**.
3. Na página “Bem-vindo”, leia o texto e, em seguida, clique em **Avançar**.
4. Na página “Contrato de Licença”, leia o contrato de licença.
5. Certifique-se de que a caixa de seleção perto de **Marque aqui para aceitar os termos deste contrato de licença** esteja selecionada e depois clique em **Avançar**.
6. Na página “Detalhes de Seu Certificado”, digite as informações necessárias e depois clique em **Avançar**.
7. Na página “Solicitação de Certificado Aceitada”, clique em **Concluir**.
8. Clique em **OK** para fechar o certificado.

Você vai receber um e-mail no Microsoft Outlook com seu Certificado do Privacy Manager anexado.

Aquisição de um Certificado Corporativo pré-assinado do Privacy Manager

1. No Outlook, abra o e-mail que você recebeu informando que um Certificado Corporativo foi pré-assinado para você.
2. Clique em **Obter**.
3. Você receberá um e-mail no Microsoft Outlook com seu Certificado do Privacy Manager anexado.
4. Para instalar o certificado, consulte Instalação de um Certificado do Privacy Manager na página 43

Instalação de um Certificado do Privacy Manager

1. Quando você receber o e-mail com seu Certificado do Privacy Manager anexado, abra o e-mail e clique no botão **Configurar**, no canto inferior direito da mensagem no Outlook 2007, ou no canto superior esquerdo no Outlook 2003.
2. Faça a autenticação utilizando o método de login de segurança de sua escolha.
3. Clique em **Avançar** na página “Certificado Instalado”.
4. Na página “Backup do Certificado”, digite uma localização e um nome para o arquivo de backup, ou clique em **Procurar** para procurar uma localização.

△ **CUIDADO:** Certifique-se de haver salvo o arquivo em outro local que não seja a sua unidade de disco rígido e guarde-o em um lugar seguro. Este arquivo deve ser utilizado somente por você e será necessário caso precise restaurar seu Certificado do Privacy Manager e as chaves associadas.

5. Insira e confirme uma senha e, em seguida, clique em **Avançar**.
6. Faça a autenticação utilizando o método de login de segurança de sua escolha.
7. Caso opte por iniciar o processo de convite para o Contato Confiável, siga as instruções na tela que se iniciam no passo 2 do tópico Adição de Contatos Confiáveis usando os contatos do Microsoft Outlook na página 47.

– ou –

Se você clicar em **Cancelar**, consulte Inclusão de um Contato Confiável na página 46 para obter informações sobre como adicionar um Contato Confiável posteriormente.

Visualização dos detalhes do Certificado do Privacy Manager

1. Abra o Privacy Manager e clique em **Gerenciador de Certificado**.
2. Clique em um Certificado do Privacy Manager.
3. Clique em **Detalhes do certificado**.
4. Quando terminar de ver os detalhes, clique em **OK**.

Renovação de um Certificado do Privacy Manager

Quando o seu Certificado do Privacy Manager estiver próximo do vencimento, você será notificado do que precisa para renová-lo:

1. Abra o Privacy Manager e clique em **Gerenciador de Certificado**.
2. Clique em **Renovar certificado**.
3. Siga as instruções apresentadas na tela para comprar um novo Certificado do Privacy Manager.

NOTA: O processo de renovação do Certificado do Privacy Manager não substitui o seu Certificado do Privacy Manager antigo. Você precisará comprar um novo Certificado do Privacy Manager e instalá-lo utilizando os mesmos procedimentos que estão em Solicitação e instalação de um Certificado do Privacy Manager na página 42.

Configuração de um Certificado do Privacy Manager padrão

Apenas Certificados do Privacy Manager são visíveis de dentro do Privacy Manager, mesmo se certificados adicionais de outras autoridades certificadoras estiverem instalados no seu computador.

Caso você tenha mais de um Certificado do Privacy Manager no seu computador que foram instalados a partir do Privacy Manager, você pode especificar um deles como o certificado padrão:

1. Abra o Privacy Manager e clique em **Gerenciador de Certificado**.
2. Clique no Certificado do Privacy Manager que deseja utilizar como padrão e em seguida clique em **Definir padrão**.
3. Clique em **OK**.

NOTA: Você não precisa usar o seu Certificado do Privacy Manager padrão. A partir das várias funções do Privacy Manager, você pode selecionar qualquer um dos seus Certificados do Privacy Manager para uso.

Exclusão de um Certificado do Privacy Manager

Se você excluir um Certificado do Privacy Manager, não poderá abrir quaisquer arquivos ou exibir quaisquer dados que tenha criptografado com aquele certificado. Se você excluiu acidentalmente um Certificado do Privacy Manager, poderá restaurá-lo utilizando o arquivo de backup que criou quando o instalou. Consulte Restauração de um Certificado do Privacy Manager na página 45 para obter mais informações.

Para excluir um Certificado do Privacy Manager:

1. Abra o Privacy Manager e clique em **Gerenciador de Certificado**.
2. Clique no Certificado do Privacy Manager que deseja excluir e em seguida clique em **Avançado**.
3. Clique em **Excluir**.
4. Quando a caixa de diálogo de confirmação for exibida, clique em **Sim**.
5. Clique em **Fechar** e em **Aplicar**.

Restauração de um Certificado do Privacy Manager

Durante a instalação do seu Certificado do Privacy Manager, você é solicitado a criar uma cópia de backup do certificado. Também é possível criar uma cópia de backup a partir da página Migração. Essa cópia de backup pode ser usada na migração para outro computador ou para restaurar um certificado para o mesmo computador.

1. Abra o Privacy Manager e clique em **Migração**.
2. Clique em **Restaurar**.
3. Na página “Arquivo de Migração”, clique em **Navegar** para buscar o arquivo .dppsm que você criou durante o processo de backup e, em seguida, clique em **Avançar**.
4. Digite a senha que utilizou ao criar o backup e clique em **Avançar**.
5. Clique em **Concluir**.
6. Clique em **OK**.

Consulte Instalação de um Certificado do Privacy Manager na página 43 ou Backup de Certificados do Privacy Manager e de Contatos Confiáveis na página 60 para obter mais informações.

Revogação do seu Certificado do Privacy Manager

Se você acha que a segurança do seu Certificado do Privacy Manager foi ameaçada, você pode revogar seu próprio certificado:

NOTA: Um Certificado do Privacy Manager revogado não é excluído. O certificado ainda pode ser utilizado para ver arquivos que estão criptografados.

1. Abra o Privacy Manager e clique em **Gerenciador de Certificado**.
2. Clique em **Avançado**.
3. Clique no Certificado do Privacy Manager que deseja revogar e em seguida clique em **Revogar**.
4. Quando a caixa de diálogo de confirmação for exibida, clique em **Sim**.
5. Faça a autenticação utilizando o método de login de segurança de sua escolha.
6. Siga as instruções na tela.

Gerenciamento de Contatos Confiáveis

Contatos Confiáveis são usuários com quem você trocou Certificados do Privacy Manager, permitindo que vocês se comuniquem em segurança.

O Gerenciador de Contatos Confiáveis permite executar as seguintes tarefas:

- Visualizar detalhes de Contatos Confiáveis
- Excluir Contatos Confiáveis
- Testar status de revogação para Contatos Confiáveis (avançado)

Adição de Contatos Confiáveis

O acréscimo de Contatos Confiáveis é um processo de 3 etapas:

1. Você envia um convite por e-mail para um destinatário de Contato Confiável.
2. O destinatário de Contato Confiável responde ao e-mail.
3. Você recebe o e-mail de resposta do destinatário de Contato Confiável e clica em **Aceitar**.

Você pode enviar e-mails de convite de Contato Confiável para destinatários individuais ou pode enviar o convite a todos os contatos na sua lista de endereços do Microsoft Outlook.

Consulte as seguintes seções para adicionar Contatos Confiáveis.

NOTA: Para responder ao seu convite e tornar-se um Contato Confiável, os destinatários de Contato Confiável precisam ter o Privacy Manager instalado nos seus computadores ou ter um cliente alternativo instalado. Para obter informações sobre como instalar o cliente alternativo, acesse o website DigitalPersona em http://DigitalPersona.com/PrivacyManager.

Inclusão de um Contato Confiável

1. Abra o Privacy Manager, clique em **Gerenciador de Contatos Confiáveis** e depois clique em **Convidar contatos**.

   – ou –

   No Microsoft Outlook, clique na seta para baixo perto de **Enviar com Segurança** e depois clique em **Convidar contatos**.

2. Se a caixa de diálogo Selecionar Certificado for exibida, clique no Certificado do Privacy Manager que deseja utilizar e, em seguida, clique em **OK**.
3. Quando a caixa de diálogo Convite a Contato Confiável for exibida, leia o texto e clique em **OK**.

   Um e-mail será gerado automaticamente.

4. Digite um ou mais endereços de e-mail dos recipientes que deseja acrescentar como Contatos Confiáveis.
5. Edite o texto e assine o seu nome (opcional).
6. Clique em **Enviar**.

NOTA: Caso não tenha obtido um Certificado do Privacy Manager, uma mensagem lhe informará que você deve ter um Certificado do Privacy Manager para enviar uma solicitação de Contato Confiável. Clique em **OK** para iniciar o Assistente de Solicitação de Certificado. Consulte Solicitação e instalação de um Certificado do Privacy Manager na página 42 para obter mais informações.

7. Faça a autenticação utilizando o método de login de segurança de sua escolha.

NOTA: Quando o e-mail é recebido pelo destinatário de Contato Confiável, o destinatário precisa abrir o e-mail e clicar em **Aceitar** no canto inferior esquerdo do e-mail e depois clicar em **OK** quando a caixa de diálogo de confirmação se abrir.

8. Quando receber um e-mail de resposta de um destinatário aceitando o convite para tornar-se um Contato Confiável, clique em **Aceitar** no canto inferior direito do e-mail.

   Será exibida uma caixa de diálogo, confirmando que o destinatário foi acrescentado com sucesso à sua lista de Contatos Confiáveis.

9. Clique em **OK**.

Adição de Contatos Confiáveis usando os contatos do Microsoft Outlook

1. Abra o Privacy Manager, clique em **Gerenciador de Contatos Confiáveis** e clique em **Convidar contatos**.

   – ou –

   No Microsoft Outlook, clique na seta para baixo perto de **Enviar com Segurança** e clique em **Convidar Todos os Meus Contatos do Outlook**.

2. Quando a página “Convite de Contato Confiável” for exibida, selecione os endereços de e-mail dos destinatários que deseja adicionar como Contatos Confiáveis e clique em **Avançar**.

3. Quando a página “Enviar Convite” for exibida, clique em **Concluir**.

   Um e-mail listando os endereços de e-mail selecionados do Microsoft Outlook será gerado automaticamente.

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

5. Clique em **Enviar**.

NOTA: Caso não tenha obtido um Certificado do Privacy Manager, uma mensagem lhe informará que você deve ter um Certificado do Privacy Manager para enviar uma solicitação de Contato Confiável. Clique em **OK** para iniciar o Assistente de Solicitação de Certificado. Consulte Solicitação e instalação de um Certificado do Privacy Manager na página 42 para obter mais informações.

6. Faça a autenticação utilizando o método de login de segurança de sua escolha.

NOTA: Quando o e-mail é recebido pelo destinatário do Contato Confiável, este precisa abrir o e-mail, clicar em **Aceitar** no canto inferior esquerdo do e-mail e depois clicar em **OK** quando a caixa de diálogo de confirmação for exibida.

7. Quando você receber um e-mail de resposta de um destinatário aceitando o convite para tornar-se um Contato Confiável, clique em **Aceitar** no canto inferior direito do e-mail.

Será exibida uma caixa de diálogo confirmando que o destinatário foi adicionado com sucesso à sua lista de Contatos Confiáveis.

8. Clique em **OK**.

Visualização de detalhes de Contatos Confiáveis

1. Abra o Privacy Manager e clique em **Gerenciador de Contatos Confiáveis**.
2. Clique em um Contato Confiável.
3. Clique em **Detalhes de Contato**.
4. Quando você houver terminado de ver os detalhes, clique em **OK**.

Exclusão de um Contato Confiável

1. Abra o Privacy Manager e clique em **Gerenciador de Contatos Confiáveis**.
2. Clique no Contato Confiável que deseja excluir.
3. Clique em **Excluir contato**.
4. Quando a caixa de diálogo de confirmação for exibida, clique em **Sim**.

Teste de status de revogação para um Contato Confiável

Para verificar se um Contato Confiável teve o seu Certificado do Privacy Manager revogado:

1. Abra o Privacy Manager e clique em **Gerenciador de Contatos Confiáveis**.
2. Clique em um Contato Confiável.
3. Clique no botão **Avançado**.

   A caixa de diálogo Gerenciador Avançado de Contatos Confiáveis é exibida.
4. Clique em **Verificação Revogação**.
5. Clique em **Fechar**.

Tarefas básicas

É possível utilizar o Privacy Manager com os seguintes produtos Microsoft:

- Microsoft Outlook
- Microsoft Office
- Windows Live Messenger

Utilização do Privacy Manager no Microsoft Outlook

Quando o Privacy Manager é instalado, o botão Privacidade é exibido na barra de ferramentas do Microsoft Outlook, e o botão Enviar com Segurança é exibido na barra de ferramentas de cada mensagem de e-mail do Microsoft Outlook. Ao clicar na seta para baixo próxima a **Privacidade** ou **Enviar com segurança**, é possível escolher dentre as seguintes opções:

- Assinar e Enviar a mensagem (somente botão Enviar com Segurança) — Esta opção adiciona uma assinatura digital ao e-mail e envia-o depois de sua autenticação utilizando o método de login de segurança escolhido.
- Selar para Contatos Confiáveis e Enviar a mensagem (somente botão Enviar com Segurança) — Esta opção adiciona uma assinatura digital, criptografa o e-mail e envia-o depois de sua autenticação utilizando o método de login de segurança escolhido.
- Convidar Contatos — Esta opção permite que você envie um convite a um Contato Confiável. Consulte Inclusão de um Contato Confiável na página 46 para obter mais informações.
- Convidar Contatos do Outlook — Esta opção permite que você envie um convite de Contato Confiável para todos os seus contatos do catálogo de endereços do Microsoft Outlook. Consulte Adição de Contatos Confiáveis usando os contatos do Microsoft Outlook na página 47 para obter mais informações.
- Iniciar o software Privacy Manager — As opções Certificados, Contatos Confiáveis e Configurações permitem que você abra o software Privacy Manager para adicionar, visualizar ou alterar suas configurações atuais. Consulte Configuração do Privacy Manager for Microsoft Outlook na página 49 para obter mais informações.

Configuração do Privacy Manager for Microsoft Outlook

1. Abra o Privacy Manager, clique em **Configurações** e depois clique na guia **E-mail**.

   – ou –

   Na barra de ferramentas principal do Microsoft Outlook, clique na seta para baixo perto de **Enviar com Segurança** (**Privacidade** no Outlook 2003) e depois em **Configurações**.

   – ou –

   Na barra de ferramentas de uma mensagem de e-mail da Microsoft, clique na seta para baixo perto de **Enviar com Segurança** e depois clique em **Configurações**.

2. Selecione as ações que deseja executar quando um e-mail seguro for enviado e, em seguida, clique em **OK**.

Assinatura e envio de uma mensagem de e-mail

1. No Microsoft Outlook, clique em **Novo** ou **Responder**.
2. Digite sua mensagem de e-mail.
3. Clique na seta para baixo próxima a **Enviar com Segurança** (**Privacidade** no Outlook 2003) e em seguida clique em **Assinar e Enviar a mensagem**.
4. Efetue a autenticação usando o método de login de segurança escolhido.

Selagem e envio de uma mensagem de e-mail

Mensagens de e-mail seladas, que são assinadas e seladas (criptografadas) digitalmente, só podem ser visualizadas pelas pessoas escolhidas por você na sua lista de Contatos Confiáveis.

Para selar e enviar uma mensagem de e-mail para um Contato Confiável:

1. No Microsoft Outlook, clique em **Novo** ou **Responder**.
2. Digite sua mensagem de e-mail.
3. Clique na seta para baixo próxima a **Enviar com Segurança** (**Privacidade** no Outlook 2003) e, em seguida, clique em **Selar para Contatos Confiáveis e Enviar a mensagem**.
4. Efetue a autenticação usando o método de login de segurança escolhido.

Visualização de uma mensagem de e-mail selada

Quando uma mensagem de e-mail selada é aberta, a etiqueta de segurança é exibida no cabeçalho do e-mail. A etiqueta de segurança fornece as seguintes informações:

- Quais credenciais foram utilizadas para verificar a identidade da pessoa que assinou o e-mail
- O produto que foi utilizado para verificar as credenciais da pessoa que assinou o e-mail

Utilização do Privacy Manager em um documento do Microsoft Office 2007

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

Depois de instalar o seu Certificado do Privacy Manager, o botão Assinar e Criptografar é exibido no lado direito da barra de ferramentas de todos os documentos do Microsoft Word, Microsoft Excel e Microsoft PowerPoint. Ao clicar na seta para baixo próximo a **Assinar e Codificar**, é possível escolher as seguintes opções:

- Documento Assinado — Esta opção acrescenta sua assinatura digital ao documento.
- Adicionar Linha de Assinatura Antes de Assinar (somente Microsoft Word e Microsoft Excel) — Por padrão, uma linha de assinatura é adicionada quando um documento do Microsoft Word ou do Microsoft Excel é assinado ou criptografado. Para desativar esta opção, clique em **Adicionar Linha de Assinatura** para remover a marca de seleção.
- Documento Codificado — Esta opção acrescenta sua assinatura digital e criptografa o documento.

- Remover Codificação — Esta opção remove a criptografia do documento.
- Iniciar o software Privacy Manager — As opções Gerenciador de Certificado, Contatos Confiáveis e Configurações permitem que você abra o software Privacy Manager para adicionar, visualizar ou alterar suas configurações atuais. Consulte Gerenciamento de Certificados do Privacy Manager na página 42, Gerenciamento de Contatos Confiáveis na página 46 ou Configuração do Privacy Manager for Microsoft Office na página 51 para obter mais informações.

Configuração do Privacy Manager for Microsoft Office

1. Abra o Privacy Manager, clique em **Configurações** e depois clique na guia **Documentos**.

   – ou –

   Na barra de ferramentas de um documento do Microsoft Office, clique na seta para baixo perto de **Assinar e Codificar** e depois clique em **Configuração**.

2. Selecione as ações que deseja configurar e, em seguida, clique em **OK**.

Assinatura de um documento do Microsoft Office

1. No Microsoft Word, Microsoft Excel ou Microsoft PowerPoint, crie e salve um documento.
2. Clique na seta para baixo próxima a **Assinar e Codificar** e, em seguida, clique em **Documento Assinado**.
3. Efetue a autenticação usando o método de login de segurança escolhido.
4. Quando a caixa de diálogo de confirmação for exibida, leia o texto e clique em **OK**.

Se mais tarde você decidir editar o documento, siga estas etapas:

1. Clique no botão **Office** no canto superior esquerdo da tela.
2. Clique em **Preparar** e depois em **Marcar como Final**.
3. Quando a caixa de diálogo de confirmação for exibida, clique em **Sim** para continuar trabalhando.
4. Quando completar sua edição, assine novamente o documento.

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

O Privacy Manager permite acrescentar uma linha de assinatura quando você assina um documento do Microsoft Word ou Microsoft Excel:

1. Crie e salve um documento no Microsoft Word ou Microsoft Excel.
2. Clique no menu **Início**.
3. Clique na seta para baixo próxima a **Assinar e Codificar** e, em seguida, em **Adicionar Linha de Assinatura Antes de Assinar**.

NOTA: Uma marca de seleção é exibida junto a Adicionar Linha de Assinatura Antes de Assinar quando esta opção é selecionada. Por padrão, esta opção vem ativada.

4. Clique na seta para baixo próxima a **Assinar e Codificar** e, em seguida, clique em **Documento Assinado**.

5. Efetue a autenticação usando o método de login de segurança escolhido.

Acréscimo de assinantes sugeridos a um documento do Microsoft Word ou Microsoft Excel

Você pode acrescentar mais de uma linha de assinatura ao seu documento indicando assinantes sugeridos. Um assinante sugerido é um usuário designado pelo proprietário de um documento do Microsoft Word ou do Microsoft Excel para acrescentar uma linha de assinatura ao documento. Os assinantes sugeridos podem ser você ou qualquer outra pessoa que você queira que assine seu documento. Por exemplo, se você preparou um documento que precisa ser assinado por todos os membros do seu departamento, pode incluir linhas de assinatura para esses usuários na parte inferior da página final do documento com instruções para assiná-lo em uma data específica.

Para acrescentar um assinante sugerido a um documento do Microsoft Word ou Microsoft Excel:

1. Crie e salve um documento no Microsoft Word ou Microsoft Excel.

2. Clique no menu **Inserir**.

3. No grupo **Texto** na barra de ferramentas, clique na seta para baixo perto de **Linha de Assinatura** e depois em **Privacy Manager Signature Provider**.

   A caixa de diálogo Configuração de Assinatura é exibida.

4. Na caixa abaixo de **Signatário sugerido**, insira o nome do assinante sugerido.

5. Na caixa abaixo de **Instruções para o signatário**, insira uma mensagem para este assinante sugerido.

   NOTA: Esta mensagem aparecerá no lugar de um título e será excluída ou substituída pelo título do usuário quando o documento for assinado.

6. Selecione a caixa de seleção **Exibir data de assinatura na linha de assinatura** para exibir a data.

7. Selecione a caixa de seleção **Exibir função do signatário na linha de assinatura** para exibir o título.

   NOTA: Como o proprietário do documento indica assinantes sugeridos para seu documento, se as caixas de seleção **Exibir data de assinatura na linha de assinatura** e/ou **Exibir função do signatário na linha de assinatura** não forem selecionadas, o assinante sugerido não será capaz de visualizar a data e/ou título na linha de assinatura, mesmo que as configurações do documento do assinante sugerido estejam configuradas para fazê-lo.

8. Clique em **OK**.

Acréscimo de um assinante sugerido à linha de assinatura

Quando assinantes sugeridos abrirem o documento, verão seu nome entre parênteses, indicando que a sua assinatura é necessária.

Para assinar o documento:

1. Clique duas vezes na linha de assinatura apropriada.

2. Efetue a autenticação usando o método de login de segurança escolhido.

A linha de assinatura será exibida de acordo com as configurações especificadas pelo proprietário do documento.

Criptografia de um documento do Microsoft Office

Você pode criptografar um documento do Microsoft Office para você e para os seus Contatos Confiáveis. Quando você criptografa um documento e o fecha, você e o(s) contato(s) confiável(eis) selecionados na lista precisam autenticá-lo antes de abri-lo.

Para criptografar um documento do Microsoft Office:

1. No Microsoft Word, Microsoft Excel ou Microsoft PowerPoint, crie e salve um documento.
2. Clique no menu **Início**.
3. Clique na seta para baixo próxima a **Assinar e Codificar** e, em seguida, clique em **Documento Codificado**.

   A caixa de diálogo Selecionar Contatos Confiáveis é aberta.
4. Clique no nome de um Contato Confiável que será capaz de abrir o documento e exibir o seu conteúdo.

NOTA: Para selecionar vários nomes de Contatos Confiáveis, mantenha a tecla ctrl pressionada enquanto clica em cada nome.

5. Clique em **OK**.

Se mais tarde você decidir editar o documento, siga as etapas em Remoção da criptografia de um documento do Microsoft Office na página 53. Quando a criptografia é removida, é possível editar o documento. Siga as etapas nesta seção para criptografar o documento novamente.

Remoção da criptografia de um documento do Microsoft Office

Ao remover a criptografia de um documento do Microsoft Office, você e seus Contatos Confiáveis não precisam mais fazer autenticação para abrir e visualizar seus conteúdos.

Para remover a criptografia de um documento do Microsoft Office:

1. Abra um documento criptografado do Microsoft Word, Microsoft Excel ou Microsoft PowerPoint.
2. Efetue a autenticação usando o método de login de segurança escolhido.
3. Clique no menu **Início**.
4. Clique na seta para baixo próxima a **Assinar e Codificar** e, em seguida, em **Remover Codificação**.

Envio de um documento do Microsoft Office criptografado

Você pode anexar um documento criptografado do Microsoft Office a uma mensagem de e-mail sem assinar ou criptografar o próprio e-mail. Para fazer isso, crie e envie um e-mail com um documento criptografado ou assinado como faria normalmente com um e-mail comum com anexo.

Contudo, para o máximo de segurança, é recomendado que você criptografe o e-mail quando anexar um documento criptografado ou assinado do Microsoft Office.

Para enviar um e-mail selado com um documento do Microsoft Office assinado e/ou criptografado anexado, siga estas etapas:

1. No Microsoft Outlook, clique em **Novo** ou **Responder**.
2. Digite sua mensagem de e-mail.
3. Anexe o documento do Microsoft Office.
4. Consulte Selagem e envio de uma mensagem de e-mail na página 50 para obter instruções adicionais.

Visualização de um documento assinado do Microsoft Office

NOTA: Você não precisa ter um Certificado do Privacy Manager para visualizar um documento assinado do Microsoft Office.

Quando um documento assinado do Microsoft Office é aberto, um ícone denominado Assinatura Digital é exibido na barra de status na parte inferior da janela do documento.

1. Clique no ícone **Assinaturas Digitais** para alternar a exibição da caixa de diálogos Assinaturas, que mostra o nome de todos os usuários que assinaram o documento e a data da assinatura de cada um deles.
2. Para obter informações detalhadas sobre cada assinatura, clique com o botão direito do mouse na caixa de diálogo Assinaturas e selecione Detalhes da Assinatura.

Visualização de um documento do Microsoft Office criptografado

Para visualizar um documento criptografado do Microsoft Office em outro computador, o Privacy Manager precisa ser instalado nele. Além disso, você precisa restaurar o Certificado do Privacy Manager que foi usado para criptografar o arquivo.

Um Contato Confiável que deseje visualizar um documento criptografado do Microsoft Office precisa ter um Certificado do Privacy Manager, e este precisa estar instalado no computador dele. Além disso, o Contato Confiável precisa ser selecionado pelo proprietário do documento criptografado do Microsoft Office.

Utilização do Privacy Manager no Windows Live Messenger

O Privacy Manager acrescenta os seguintes recursos de comunicação segura ao Windows Live Messenger:

- **Bate-papo seguro** — As mensagens são transmitidas usando a SSL/TLS (Camada de Soquetes Segura/Segurança da Camada de Transporte) sobre o protocolo XML, a mesma tecnologia que garante a segurança de transações de comércio eletrônico.
- **Identificação do destinatário** — É possível confirmar a presença e a identidade de uma pessoa antes de enviar uma mensagem.
- **Mensagens assinadas** — Permite que você assine suas mensagens eletronicamente. Dessa forma, se a mensagem for adulterada, será marcada como inválida quando for recebida pelo destinatário.
- **Recurso Ocultar/Exibir** — É possível ocultar uma ou todas as mensagens da janela do Privacy Manager Chat. Você também pode enviar uma mensagem na qual o conteúdo está oculto. A autenticação é requerida antes da exibição da mensagem.

- **Histórico seguro do bate-papo** — Os registros de suas sessões de bate-papo são criptografados antes de serem salvos e requerem autenticação para serem visualizados.
- **Bloqueio/Desbloqueio automático** — É possível bloquear e desbloquear a janela do Privacy Manager Chat ou configurá-la para que seja bloqueada automaticamente após um período específico de inatividade.

Inicialização de uma sessão do Privacy Manager Chat

NOTA: Para que possam ser utilizados os recursos do Privacy Manager Chat, ambos os usuários precisam ter o Privacy Manager e um Certificado do Privacy Manager instalados. Para obter detalhes sobre a instalação do Certificado do Privacy Manager, consulte Solicitação e instalação de um Certificado do Privacy Manager na página 42.

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

   a. Clique com o botão direito em um contato on-line no Live Messenger e depois selecione **Iniciar uma atividade**.

   b. Clique em **Iniciar Chat**.

   – ou –

   a. Clique duas vezes em um contato on-line no Live Messenger e depois selecione o menu **Exibir lista de atividades**.

   b. Clique em **Ação** e depois clique em **Iniciar Chat**.

   – ou –

   a. Clique com o botão direito do mouse no ícone ProtectTools na área de notificação, clique em **Privacy Manager for HP ProtectTools** e, em seguida, selecione **Iniciar Chat**.

   b. No Live Messenger, clique em **Ações: Iniciar uma atividade** e depois selecione **Bate-papo do Privacy Manager**.

   NOTA: Todos os usuários devem estar on-line no Live Messenger e devem ser exibidos na janela on-line do Live Messenger uns dos outros. Clique para selecionar um usuário on-line.

   O Privacy Manager envia um convite ao contato para iniciar o Privacy Manager Chat. Quando o contato aceita o convite, a janela do Privacy Manager Chat se abre. Caso o contato convidado não tenha o Privacy Manager, ele será solicitado a baixá-lo.

2. Clique em **Iniciar** para abrir uma sessão de bate-papo segura.

Configuração do Privacy Manager for Windows Live Messenger

1. No Privacy Manager Chat, clique no botão **Configurações**.

   – ou –

   No Privacy Manager, clique em **Configurações** e depois na guia **Bate-papo**.

   – ou –

   No Visualizador de Histórico do Live Messenger do Privacy Manager, clique no botão **Configurações**.

2. Para especificar a quantidade de tempo que o Privacy Manager Chat esperará antes de bloquear sua sessão, coloque um número na caixa **Bloquear sessão após _ minutos de inatividade**.

3. Para especificar uma pasta de histórico para suas sessões de bate-papo, clique em **Navegar** para buscar uma pasta e, em seguida, clique em **OK**.

4. Para criptografar e salvar automaticamente suas sessões quando forem fechadas, selecione a caixa de seleção **Salvar automaticamente o histórico do bate-papo com segurança**.

5. Clique em **OK**.

Bate-papo na janela do Privacy Manager Chat

Depois de inicializar o Privacy Manager Chat, uma janela do Private Manager Chat se abrirá no Windows Live Messenger. O Privacy Manager Chat é parecido com o Windows Live Messenger básico, a não ser pelos seguintes recursos adicionais que estão disponíveis na janela Privacy Manager Chat:

- **Salvar** — Clique neste botão para salvar a sua sessão de bate-papo na pasta especificada nas suas definições de configuração. Você também pode configurar o Privacy Manager Chat para salvar automaticamente todas as sessões quando forem fechadas.
- **Ocultar todas** e **Exibir todas** — Clique no botão apropriado para expandir ou ocultar as mensagens exibidas na janela Comunicações Seguras. Você também pode ocultar ou exibir mensagens clicando no cabeçalho da mensagem.
- **Você está aí?** — Clique neste botão para solicitar a autenticação do seu contato.
- **Bloquear** — Clique neste botão para fechar a janela Privacy Manager Chat e voltar à janela Entrada de Bate-papo. Para exibir novamente a janela Comunicações Seguras, clique em **Retomar sessão** e depois efetue a autenticação utilizando o método de login de segurança escolhido.
- **Enviar** — Clique neste botão para enviar uma mensagem criptografada ao seu contato.
- **Enviar assinada** — Selecione esta caixa de seleção para assinar e criptografar eletronicamente suas mensagens. Dessa forma, se a mensagem for adulterada, será marcada como inválida quando for recebida pelo destinatário. Você deverá efetuar a autenticação toda vez que enviar uma mensagem assinada.
- **Enviar oculta** — Selecione esta caixa de seleção para criptografar e enviar uma mensagem exibindo apenas seu cabeçalho. O seu contato precisa se autenticar para ler o conteúdo da mensagem.

Visualização do histórico de bate-papo

O Privacy Manager Chat: O Visualizador de Histórico do Live Messenger exibe arquivos de sessão criptografados do Privacy Manager Chat. As sessões podem ser salvas clicando em **Salvar** na janela do Privacy Manager Chat ou configurando o salvamento automático na guia Bate-papo do Privacy Manager. No visualizador, cada sessão exibe o Nome de Tela do Contato (criptografado) e a data e hora em que a sessão começou e terminou. Por padrão, as sessões são exibidas para todas as contas de e-mail que você configurou. Você pode usar o menu **Exibir histórico para** a fim de selecionar apenas as contas específicas que poderão visualizá-las.

O visualizador permite que você execute as seguintes tarefas:

- Revelar Todas as Sessões na página 57
- Revelar sessões para uma conta específica na página 57
- Visualização da ID de uma sessão na página 58
- Visualização de uma sessão na página 58
- Pesquisa de um texto específico nas sessões na página 58
- Exclusão de uma sessão na página 58
- Adição ou remoção de colunas na página 59
- Filtragem de sessões exibidas na página 59

Para iniciar o Visualizador de Histórico do Live Messenger:

▲ Na área de notificação, à direita da barra de tarefas, clique com o botão direito no ícone **HP ProtectTools**, em **Privacy Manager: for HP ProtectTools** e depois em **Visualizar Histórico do Live Messenger**.

– ou –

▲ Em uma sessão de bate-papo, clique em **Visualizar Histórico** ou **Histórico**.

Revelar Todas as Sessões

A opção de revelar todas as sessões exibe o Nome de Tela do Contato descriptografado para a(s) sessão(ões) atualmente selecionada(s) e todas as sessões na mesma conta.

Para revelar todas as sessões salvas do histórico do bate-papo:

1. No Visualizador de Histórico do Live Messenger, clique com o botão direito em qualquer sessão e depois selecione **Revelar Todas as Sessões**.
2. Efetue a autenticação usando o método de login de segurança escolhido.

   Os Nomes de Tela dos Contatos são descriptografados.
3. Clique duas vezes em qualquer sessão para visualizar seu conteúdo.

Revelar sessões para uma conta específica

Revelar uma sessão exibe o Nome de Tela do Contato descriptografado para a sessão atualmente selecionada.

Para exibir uma sessão específica do histórico do bate-papo:

1. No Visualizador de Histórico do Live Messenger, clique com o botão direito em qualquer sessão e depois selecione **Revelar Sessão**.
2. Efetue a autenticação usando o método de login de segurança escolhido.

   O Nome de Tela do Contato é descriptografado.
3. Clique duas vezes na sessão exibida para visualizar seu conteúdo.

NOTA: Sessões adicionais criptografadas com o mesmo certificado mostrarão um ícone desbloqueado, indicando que você pode vê-las clicando duas vezes em qualquer uma dessas sessões sem autenticação adicional. Sessões criptografadas com um certificado diferente mostrarão um ícone bloqueado, indicando que uma autenticação adicional é necessária para essas sessões antes de exibir os Nomes de Tela dos Contatos ou o conteúdo.

Visualização da ID de uma sessão

Para visualizar a ID de uma sessão:

- No Visualizador de Histórico do Live Messenger, clique com o botão direito em qualquer sessão revelada e selecione **Visualizar Identificação de Sessão**.

Visualização de uma sessão

Visualizar uma sessão abre o arquivo para visualização. Se a sessão não foi revelada (exibindo o Nome de Tela do Contato descriptografado) anteriormente, ela é revelada ao mesmo tempo.

Para visualizar uma sessão do histórico do Live Messenger:

1. No Visualizador de Histórico do Live Messenger, clique com o botão direito em qualquer sessão e depois selecione **Visualizar**.
2. Se solicitado, faça a autenticação utilizando o método de login de segurança escolhido.

   O conteúdo da sessão é descriptografado.

Pesquisa de um texto específico nas sessões

Você só pode buscar um texto em sessões reveladas (descriptografadas) que são exibidas na janela do visualizador. Estas são as sessões onde o Nome de Contato de Tela é mostrado em texto simples.

Para pesquisar textos em sessões do histórico de bate-papo:

1. NoVisualizador de Histórico do Live Messenger, clique no botão **Pesquisar**.
2. Digite o texto da busca, configure os parâmetros de busca desejados e depois clique em **OK**.

   Sessões que contêm o texto são realçadas na janela do visualizador.

Exclusão de uma sessão

1. Selecione uma sessão de histórico de bate-papo.
2. Clique em **Excluir**.

Adição ou remoção de colunas

Por padrão, as 3 colunas mais utilizadas são exibidas no Visualizador de Histórico do Live Messenger. Você pode acrescentar colunas adicionais à exibição ou remover colunas da exibição.

Para acrescentar colunas à exibição:

1. Clique com o botão direito em qualquer cabeçalho de coluna e selecione **Adicionar/Remover Colunas**.
2. Selecione um cabeçalho de coluna no painel esquerdo e depois clique em **Adicionar** para movê-lo para o painel direito.

Para remover colunas da exibição:

1. Clique com o botão direito em qualquer cabeçalho de coluna e selecione **Adicionar/Remover Colunas**.
2. Selecione um cabeçalho de coluna no painel direito e depois clique em **Remover** para movê-lo para o painel esquerdo.

Filtragem de sessões exibidas

Uma lista de sessões para todas as suas contas é exibida no Visualizador de Histórico do Live Messenger. Também é possível filtrar sessões exibidas por:

- Contas específicas. Para detalhes, consulte Exibição de sessões para uma conta específica na página 59.
- Intervalo de datas. Para detalhes, consulte Exibição de sessões para um intervalo de datas na página 59.
- Pastas diferentes. Para detalhes, consulte Exibição de sessões salvas em uma pasta diferente da pasta padrão na página 59.

Exibição de sessões para uma conta específica

▲ No Visualizador de Histórico do Live Messenger, selecione uma conta a partir do menu **Exibir histórico para**.

Exibição de sessões para um intervalo de datas

1. No Visualizador do Windows Live Messenger, clique no ícone **Filtro avançado**.

   A caixa de diálogo Filtro Avançado é exibida.

2. Selecione a caixa de seleção **Exibir sessões somente do período definido**.
3. Nas caixas **Dt. inicial** e **Dt. final**, digite o dia, mês e/ou ano, ou clique na seta junto ao calendário para selecionar as datas.
4. Clique em **OK**.

Exibição de sessões salvas em uma pasta diferente da pasta padrão

1. No Visualizador de Histórico do Live Messenger, clique no ícone **Filtro avançado**.
2. Selecione a caixa de seleção **Usar pasta alt. arq. históricos**.

3. Digite o local da pasta ou clique em **Procurar** para buscar uma pasta.
4. Clique em **OK**.

Tarefas avançadas

Migração de Certificados do Privacy Manager e contatos confiáveis para um computador diferente

Você pode migrar com segurança os seus Certificados e Contatos Confiáveis do Privacy Manager para outro computador ou fazer o backup de seus dados como medida de precaução. Para isso, faça um backup dos dados na forma de um arquivo protegido por senha em um local da rede ou em qualquer dispositivo de armazenamento removível, em seguida restaure o arquivo no novo computador.

Backup de Certificados do Privacy Manager e de Contatos Confiáveis

Para fazer o backup de seus Certificados e Contatos Confiáveis do Privacy Manager em um arquivo protegido por senha, siga estas etapas:

1. Abra o Privacy Manager e clique em **Migração**.
2. Clique em **Fazer backup**.
3. Na página “Dados Selecionados”, selecione as categorias de dados a serem incluídas no arquivo de migração e depois clique em **Avançar**.
4. Na página “Arquivo de Migração”, digite um nome de arquivo ou clique em **Navegar** para encontrar uma localização de arquivo e depois clique em **Avançar**.
5. Insira e confirme uma senha e, em seguida, clique em **Avançar**.

NOTA: Armazene esta senha em um lugar seguro, pois precisará dela quando restaurar o arquivo de migração.

6. Faça a autenticação utilizando o método de login de segurança de sua escolha.
7. Na página “Arquivo de Migração Salvo”, clique em **Concluir**.

Restauração de Certificados do Privacy Manager e de Contatos Confiáveis

Para restaurar seus Certificados e Contatos Confiáveis do Privacy Manager em um computador diferente como parte do processo de migração ou no mesmo computador, siga estas etapas:

1. Abra o Privacy Manager e clique em **Migração**.
2. Clique em **Restaurar**.
3. Na página “Arquivo de Migração”, clique em **Navegar** para procurar uma localização e depois clique em **Avançar**.
4. Digite a senha que utilizou ao criar o arquivo de backup e clique em **Avançar**.
5. Na página “Arquivo de Migração”, clique em **Concluir**.

Administração central do Privacy Manager

Sua instalação do Privacy Manager pode fazer parte de uma instalação centralizada, personalizada pelo seu administrador. Um ou mais dos seguintes recursos podem estar ativados ou desativados:

- **Política de uso de certificados**: você pode estar limitado a usar certificados do Privacy Manager emitidos pela Comodo, ou pode ter permissão para usar certificados digitais emitidos por outras autoridades de certificação.
- **Política de criptografia**: as capacidades de criptografia podem ser ativadas ou desativadas individualmente no Microsoft Office ou Outlook e no Windows Live Messenger.

9 File Sanitizer for HP ProtectTools

O File Sanitizer é uma ferramenta que permite fragmentar com segurança ativos de dados (informações pessoais ou arquivos, dados de histórico ou relacionados à Web, ou outros componentes de dados) do computador e periodicamente limpar sua unidade de disco rígido.

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

Fragmentação

A fragmentação é diferente da exclusão padrão do Windows® (também conhecida como exclusão simples no File Sanitizer), pois quando você fragmenta um ativo usando o File Sanitizer, um algoritmo que oculta os dados é executado, tornando praticamente impossível recuperar o ativo original. Uma exclusão simples do Windows pode deixar o arquivo (ou ativo) intacto na unidade de disco rígido ou em um estado no qual métodos investigativos podem ser usados para recuperar o arquivo (ou ativo).

Quando você seleciona um perfil de fragmentação (alta segurança, média segurança ou baixa segurança), uma lista predefinida de ativos e um método de apagamento são automaticamente selecionados para a fragmentação. Também é possível personalizar um perfil de fragmentação, que permite especificar o número de ciclos de fragmentação, quais ativos serão incluídos na fragmentação, quais ativos deverão ser confirmados antes da fragmentação e quais ativos serão excluídos da fragmentação. Para obter mais informações, consulte Seleção ou criação de um perfil de fragmentação na página 66.

Você pode configurar uma programação de fragmentação automática e pode também fragmentar ativos manualmente sempre que desejar. Para obter mais informações, consulte Configuração de uma programação de fragmentação na página 65, Fragmentação manual de um ativo na página 70 ou Fragmentação manual de todos os arquivos selecionados na página 71.

NOTA: Um arquivo .dll somente é fragmentado e removido do sistema se tiver sido movido para a lixeira.

Purificação de espaço livre

Excluir um ativo no Windows não remove completamente o conteúdo desse ativo do seu disco rígido. O Windows exclui somente a referência ao ativo. O conteúdo do ativo permanece no disco rígido até que outro ativo sobrescreva essa mesma área no disco rígido com novas informações.

A purificação de espaço livre permite gravar com segurança dados aleatórios sobre os ativos excluídos, evitando que os usuários visualizem os conteúdos originais do ativo excluído.

NOTA: A purificação de espaço livre é para os ativos que você exclui utilizando a Lixeira do Windows ou manualmente. A purificação de espaço livre não oferece segurança adicional aos ativos fragmentados.

Você pode definir uma programação de purificação de espaço livre automática ou pode ativar manualmente a purificação de espaço livre usando o ícone **HP ProtectTools** na área de notificação, no lado direito da barra de tarefas. Para obter mais informações, consulte Configuração de uma programação de limpeza de espaço livre na página 66 ou Ativação manual da limpeza de espaço livre na página 71.

Procedimentos de configuração

Inicialização do File Sanitizer

Para abrir o File Sanitizer:

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

– ou –

▲ Clique duas vezes no ícone **File Sanitizer** localizado na área de trabalho.

– ou –

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

Configuração de uma programação de fragmentação

NOTA: Para obter informações sobre a seleção de um perfil de fragmentação predefinido ou a criação de um perfil de fragmentação, consulte Seleção ou criação de um perfil de fragmentação na página 66.

NOTA: Para obter informações sobre como fragmentar ativos manualmente, consulte Fragmentação manual de um ativo na página 70.

1. Abra o File Sanitizer e clique em **Fragmentar**.
2. Selecione uma opção de fragmentação:
   - **Desligamento do Windows** — Selecione essa opção para fragmentar todos os ativos selecionados no desligamento do Windows.

     NOTA: Quando essa opção é selecionada, uma caixa de diálogo é exibida no desligamento, perguntando se você quer continuar com a fragmentação dos ativos selecionados ou se deseja ignorar o procedimento. Clique em **Sim** para ignorar o procedimento de fragmentação ou clique em **Não** para continuar com a fragmentação.
   - **Abertura do navegador da web** — Selecione essa opção para fragmentar todos os ativos relacionados à Web selecionados, como o histórico de URL do navegador, quando você abrir um navegador da Web.
   - **Ao sair do navegador da web** — Selecione essa opção para fragmentar todos os ativos relacionados à Web selecionados, como o histórico de URL do navegador, quando você fechar um navegador da Web.
   - **Seqüência de chave** — Selecione essa opção para iniciar a fragmentação usando uma seqüência de teclas.
   - **Programador** — Marque a caixa de seleção **Ativar Programador**, insira sua senha do Windows e, em seguida, insira o dia e a hora para fragmentar os ativos selecionados.

NOTA: Um arquivo .dll somente é fragmentado e removido do sistema se tiver sido movido para a lixeira.

3. Clique em **Aplicar** e em **OK**.

Configuração de uma programação de limpeza de espaço livre

NOTA: A purificação de espaço livre funciona para os ativos que você exclui utilizando a Lixeira do Windows ou manualmente. A purificação de espaço livre não oferece segurança adicional aos ativos fragmentados.

Para configurar uma programação de purificação de espaço livre:

1. Abra o File Sanitizer e clique em **Purificação de 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 limpeza do disco rígido.
3. Clique em **Aplicar** e em **OK**.

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

Seleção ou criação de um perfil de fragmentação

Você pode especificar um método para apagar e selecionar os ativos para fragmentação selecionando um perfil predefinido ou criando seu próprio perfil.

Seleção de um perfil de fragmentação predefinido

Quando se escolhe um perfil de fragmentação predefinido (Segurança Máxima, Segurança Média ou Segurança Baixa), um método de exclusão e uma lista de ativos predefinidos são automaticamente selecionados. Clique no botão **Visualizar detalhes** para exibir a lista predefinida de ativos que estão selecionados para fragmentação.

Para selecionar um perfil de fragmentação predefinido:

1. Abra o File Sanitizer e clique em **Configurações**.
2. Clique em um perfil de fragmentação predefinido.
3. Clique em **Visualizar detalhes** para exibir a lista de ativos que estão selecionados para fragmentação.
4. Em **Fragmentar o seguinte**, marque a caixa de seleção de cada ativo que você deseja confirmar antes da fragmentação.
5. Clique em **Aplicar** e em **OK**.

Personalização de um perfil de fragmentação

Ao criar um perfil de fragmentação, especifique o número de ciclos de fragmentação, quais ativos incluir na fragmentação, quais ativos confirmar antes da fragmentação e quais ativos excluir da fragmentação:

1. Abra o File Sanitizer, clique em **Configurações**, em **Configurações Avançadas de Segurança** e, em seguida, clique em **Visualizar detalhes**.
2. Especifique o número de ciclos de fragmentação.

NOTA: O número selecionado de ciclos de fragmentação será executado para cada ativo. Por exemplo, se escolher 3 ciclos de fragmentação, um algoritmo que oculta os dados é executado 3 vezes separadas. Se escolher os ciclos de fragmentação de maior segurança, a fragmentação poderá demorar um tempo significativo; no entanto, quanto maior o número de ciclos de fragmentação especificado, menor a probabilidade dos dados poderem ser recuperados.

3. Selecione os ativos que deseja fragmentar:
   a. Em **Opções de fragmentação disponíveis**, clique em um ativo e em **Adicionar**.
   b. Para adicionar um ativo personalizado, clique em **Adicionar Opção Personalizada**, em seguida navegue até o arquivo ou pasta ou digite o respectivo caminho. Clique em **Abrir**, em seguida clique em **OK**. Em **Opções de fragmentação disponíveis**, clique no ativo personalizado e clique em **Adicionar**.

NOTA: Para remover um ativo das opções de fragmentação disponíveis, clique no ativo e, em seguida, clique em **Excluir**.

4. Em **Fragmentar o seguinte**, marque a caixa de seleção de cada ativo que deseja confirmar antes da fragmentação

NOTA: Para remover um ativo da lista de fragmentação, clique no ativo e, em seguida, clique em **Excluir**.

5. Para proteger arquivos ou pastas contra a fragmentação automática, na seção **Não fragmentar o seguinte**, clique em **Adicionar** e navegue até o arquivo ou pasta ou digite o respectivo caminho. Clique em **Abrir**, em seguida clique em **OK**.

NOTA: Para remover um ativo da lista de extensões, clique no ativo e, em seguida, clique em **Excluir**.

6. Quando terminar de configurar o perfil de fragmentação, clique em **Aplicar** e em **OK**.

Personalização de um perfil de exclusão simples

O perfil de exclusão simples executa a exclusão de um ativo padrão sem a fragmentação. Quando você personaliza um perfil de exclusão simples, pode especificar quais ativos serão incluídos em uma exclusão simples, quais ativos deverão ser confirmados antes de uma exclusão simples ser executada e quais ativos serão removidos de uma exclusão simples.

NOTA: Se você usar a opção de exclusão simples, a purificação de espaço livre poderá ser executada ocasionalmente nos ativos que foram excluídos manualmente ou através da Lixeira do Windows.

Para personalizar um perfil de exclusão simples:

1. Abra o File Sanitizer, clique em **Configurações**, clique em **Configuração de Exclusão Simples** e, em seguida, clique em **Visualizar detalhes**.
2. Selecione os ativos que deseja excluir:
   a. Em **Opções de exclusão disponíveis**, clique no ativo e, em seguida, clique em **Adicionar**.
   b. Para adicionar um ativo personalizado, clique em **Adicionar Opção Personalizada**, digite um nome de arquivo ou nome de pasta e clique em **OK**. Clique no ativo personalizado e, em seguida, clique em **Adicionar**.

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

3. Em **Excluir o seguinte**, marque a caixa de seleção de cada ativo que deseja confirmar antes da exclusão.

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

4. Em **Não excluir o seguinte**, clique em **Adicionar** para selecionar os ativos específicos que deseja excluir da fragmentação.

NOTA: Para remover um ativo da lista de extensões, clique no ativo e, em seguida, clique em **Excluir**.

5. Quando terminar de configurar o perfil de exclusão simples, clique em **Aplicar** e em **OK**.

Tarefas básicas

Você pode usar o File Sanitizer para executar as seguintes tarefas:

- Utilizar uma sequência de teclas para iniciar a fragmentação — Este recurso permite que você crie uma sequência de teclas (por exemplo, ctrl+alt+s) para iniciar a fragmentação. Para detalhes, consulte Uso de uma seqüência de chave para iniciar a fragmentação na página 69.
- Utilizar o ícone File Sanitizer para iniciar a fragmentação — Este recurso é parecido com o recurso de arrastar e soltar do Windows. Para detalhes, consulte Uso do ícone do File Sanitizer na página 70.
- Fragmentar manualmente um ativo específico ou todos os ativos selecionados — Esses recursos permitem que você fragmente itens manualmente sem ter de esperar que a programação de fragmentação regular seja executada. Para detalhes, consulte Fragmentação manual de um ativo na página 70 ou Fragmentação manual de todos os arquivos selecionados na página 71.
- Ativar manualmente a limpeza de espaço livre — Este recurso permite que você ative manualmente a limpeza de espaço livre. Para detalhes, consulte Ativação manual da limpeza de espaço livre na página 71.
- Interromper uma operação de limpeza de espaço livre ou fragmentação — Este recurso permite que você interrompa uma operação de fragmentação ou de limpeza de espaço livre. Para detalhes, consulte Interrupção de uma operação de fragmentação ou de purificação de espaço livre na página 71.
- Visualizar arquivos de registro — Este recurso permite que você visualize os arquivos de registro da limpeza de espaço livre e da fragmentação, os quais contêm os erros e falhas da última operação de fragmentação ou limpeza de espaço livre. Para detalhes, consulte Exibição dos arquivos de registro na página 71.

NOTA: A operação de limpeza de espaço livre ou de fragmentação pode demorar bastante. Mesmo que a limpeza de espaço livre e a fragmentação sejam executadas em segundo plano, seu computador pode ter a capacidade reduzida pelo aumento no uso do processador.

Uso de uma seqüência de chave para iniciar a fragmentação

Para especificar uma seqüência de teclas, siga estas etapas:

1. Abra o File Sanitizer e clique em **Fragmentar**.
2. Marque a caixa de seleção **Seqüência de chave**.
3. Digite um caractere na caixa disponível.
4. Selecione a caixa **CTRL** ou **ALT** e, em seguida, a caixa **SHIFT**.

   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 seqüência de teclas diferente das outras seqüências de teclas que você configurou.

Para iniciar a fragmentação usando uma seqüência de teclas:

1. Mantenha pressionada a tecla shift, ctrl ou alt (ou qualquer outra combinação especificada) enquanto pressiona o caractere escolhido.
2. Se a caixa de diálogo de confirmação for exibida, clique em **Sim**.

Uso do ícone do File Sanitizer

△ **CUIDADO:** Ativos fragmentados não podem ser recuperados. Considere cuidadosamente quais itens selecionar para uma fragmentação manual.

1. Navegue até o documento ou pasta que deseja fragmentar.
2. Arraste o ativo para o ícone do 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:** Ativos fragmentados não podem ser recuperados. Considere cuidadosamente quais itens selecionar para uma fragmentação manual.

1. Clique com o botão direito no ícone do **HP ProtectTools** na área de notificação, à direita da barra de tarefas, clique em **File Sanitizer** e, depois, em **Fragmentar Um**.
2. Quando a caixa de diálogo Navegar for exibida, navegue até o ativo que deseja fragmentar e clique em **OK**.

   NOTA: O ativo selecionado pode ser um arquivo único 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 for exibida, navegue até o ativo que deseja fragmentar e clique em **OK**.
3. Quando a caixa de diálogo de confirmação for exibida, clique em **Sim**.

– ou –

1. Abra o File Sanitizer e clique em **Fragmentar**.
2. Clique no botão **Navegar**.
3. Quando a caixa de diálogo Navegar for exibida, navegue até o ativo que deseja fragmentar e clique em **OK**.
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 do **HP ProtectTools** na área de notificação, à direita da barra de tarefas, clique em **File Sanitizer** e, depois, 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**.

– ou –

1. Abra o File Sanitizer e clique em **Fragmentar**.
2. Clique no botão **Fragmentar Agora**.
3. Quando a caixa de diálogo de confirmação for exibida, clique em **Sim**.

Ativação manual da limpeza de espaço livre

1. Clique com o botão direito no ícone do **HP ProtectTools** na área de notificação, à direita da barra de tarefas, clique em **File Sanitizer** e, depois, em **Purificar Agora**.
2. Quando a caixa de diálogo de confirmação for exibida, clique em **Sim**.

– ou –

1. Abra o File Sanitizer e clique em **Purificação de Espaço Livre**.
2. Clique em **Purificar Agora**.
3. Quando a caixa de diálogo de confirmação for exibida, clique em **Sim**.

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

Quando uma operação de fragmentação ou de purificação de espaço livre está em andamento, uma mensagem é exibida acima do ícone do HP ProtectTools Security Manager, na área de notificação. A mensagem fornece detalhes sobre o processo de fragmentação ou de purificação de espaço livre (porcentagem completa) e oferece a opção de interromper 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 log é criado para operações de fragmentação e um outro arquivo de log é criado para operações de purificação de espaço livre. Ambos os arquivos de log se encontram na unidade de 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

10 Device Access Manager for HP ProtectTools (somente em determinados modelos)

Os administradores do sistema operacional Windows® utilizam o Device Access Manager for HP ProtectTools para controlar o acesso aos dispositivos em um sistema e para proporcionar proteção contra acessos não-autorizados:

- Os perfis de dispositivo são criados para cada usuário a fim de definir os dispositivos aos quais eles possuem ou não possuem permissão de acesso.
- Os usuários são organizados em grupos, como o grupo predefinido Administradores de dispositivos, ou outros grupos podem ser definidos utilizando a opção Gerenciamento do Computador na seção Ferramentas Administrativas do Painel de Controle.
- O acesso a dispositivos pode ser concedido ou negado com base nas associações dos grupos.
- Para as classes de dispositivos como as unidades de CD-ROM e DVD, o acesso de leitura ou gravação pode ser permitido ou negado separadamente.

Um número limitado de usuários também pode receber permissão para ler e modificar a política de controle de acesso ao dispositivo.

Procedimentos de Configuração

Inicialização do Device Access Manager

Para iniciar o Device Access Manager, siga as etapas abaixo:

1. Clique em **Iniciar**, **Todos os Programas**, **HP** e, em seguida, em **Console Administrativo do HP ProtectTools**.
2. No painel esquerdo, clique em **Device Access Manager**.

Configuração do acesso a dispositivos

O Device Access Manager for HP ProtectTools oferece três tipos de visualização:

- A visualização Configuração Simples é utilizada para permitir ou negar o acesso a classes de dispositivos para membros do grupo Administradores de dispositivos.
- A visualização Configuração de Classe de Dispositivo é utilizada para permitir ou negar o acesso a tipos de dispositivo ou dispositivos específicos para usuários ou grupos específicos.
- A visualização Configurações de acesso do usuário é utilizada para especificar quais usuários podem visualizar ou modificar as informações das visualizações Configuração Simples e Configuração de Classe de Dispositivo.

Grupo Administradores de dispositivos

Quando o Device Access Manager é instalado, o grupo Administradores de dispositivos é criado.

O administrador do sistema pode implementar uma política simples de controle de acesso a dispositivos negando o acesso a um conjunto de classes de dispositivo a menos que o usuário esteja classificado como confiável (em relação ao acesso a dispositivos). A maneira recomendada de distinguir entre usuários "confiáveis quanto a dispositivos" e "não-confiáveis quanto a dispositivos" é tornar todos os usuários "confiáveis quanto a dispositivos" membros do grupo Administradores de dispositivos. Conceder acesso aos membros do grupo Administradores de dispositivos por meio das visualizações Configuração Simples ou Configuração de Classe de Dispositivo garantirá, dessa forma, que os usuários "confiáveis quanto a dispositivos" tenham acesso total ao conjunto de classes de dispositivo especificado.

NOTA: Adicionar um usuário ao grupo Administradores de dispositivos não permite automaticamente que ele acesse os dispositivos. No entanto, a visualização Configuração Simples pode ser utilizada para garantir acesso ao conjunto de classes de dispositivos requerido para usuários "confiáveis quanto a dispostivos".

Para adicionar usuários ao grupo Administradores de dispositivos, siga as etapas abaixo:

- Para o Windows 7, Vista ou XP Professional, utilize o snap-in padrão do MMC "Usuários e Grupos Locais".
- Para versões home do Windows 7, Vista® ou XP, em uma conta privilegiada, digite o seguinte em uma janela do prompt de comando:

```
c:\> net localgroup "Administradores de dispositivos" nomedousuário /ADD
```

Configuração Simples

Os administradores e os usuários autorizados podem utilizar a visualização Configuração Simples para modificar o acesso às seguintes classes de dispositivos para todos que não fazem parte do grupo Administradores de dispositivos:

NOTA: A fim de utilizar esta visualização para ler as informações de acesso a dispositivos, o usuário ou o grupo pode receber permissão para "ler" na visualização **Configurações de acesso do usuário**. A fim de utilizar esta visualização para modificar as informações de acesso a dispositivos, o usuário ou o grupo deve receber permissão para "alteração" na visualização **Configurações de acesso do usuário**.

- Toda mídia removível (disquetes, unidades flash USB etc.)
- Todas as unidades de DVD/CD-ROM
- Todas as portas seriais e paralelas
- Todos os dispositivos Bluetooth®
- Todos os dispositivos de infravermelho
- Todos os dispositivos de modem
- Todos os dispositivos PCMCIA
- Todos os dispositivos 1394

Para permitir ou negar o acesso a uma classe de dispositivos para todos os usuários que não fazem parte do grupo Administradores de dispositivos, siga estas etapas:

1. No painel esquerdo do **Console Administrativo do HP ProtectTools**, clique em **Device Access Manager** e, em seguida, em **Configuração Simples**.
2. No painel direito, para negar o acesso, marque a caixa de seleção de uma classe de dispositivos ou de um dispositivo específico. Desmarque a caixa de seleção para permitir o acesso àquela classe de dispositivos ou dispositivo específico.

   Se uma caixa de seleção está acizentada, significa que os valores que afetam o cenário de acesso foram alterados na visualização Configuração de Classe de Dispositivo. Para redefinir os valores de volta às configurações simples, marque ou desmarque a caixa de seleção e clique em **Sim** para confirmar.
3. Clique no ícone **Salvar**.

   NOTA: Se o serviço de segundo plano não estiver sendo executado, uma caixa de diálogo se abrirá perguntando se você deseja iniciá-lo. Clique em **Sim**.
4. Clique em **OK**.

Inicialização do serviço de segundo plano

Antes de os perfis de dispositivos serem aplicados, o HP ProtectTools Security Manager abre uma caixa de diálogo perguntando se você deseja iniciar o serviço de segundo plano Bloqueio de Dispositivos/Auditoria do HP ProtectTools. Clique em **Sim**. O serviço de segundo plano é iniciado e será executado automaticamente sempre que o sistema inicializar.

NOTA: Um perfil de dispositivo deve ser definido antes que o prompt do serviço de segundo plano seja exibido.

Os administradores também podem iniciar ou interromper este serviço:

1. Clique em **Iniciar** e, em seguida, em **Painel de Controle**.
2. Clique em **Ferramentas Administrativas** e em **Serviços**.
3. Procure o serviço **Bloqueio de Dispositivos/Auditoria do HP ProtectTools**.

A interrupção do serviço Bloqueio de Dispositivos/Auditoria não interrompe o bloqueio de dispositivos. Dois componentes asseguram o bloqueio de dispositivos:

- O serviço Bloqueio/Auditoria de dispositivos
- O driver DAMDrv.sys

A inicialização do serviço inicia o driver do dispositivo, mas a interrupção do serviço não interrompe o driver.

Para determinar se o serviço de segundo plano está sendo executado, abra a janela do prompt de comando e digite sc query flcdlock.

Para determinar se o driver do dispositivo está sendo executado, abra a janela do prompt de comando e digite sc query damdrv.

Configuração de Classe de Dispositivo

Os adminstradores e os usuários autorizados podem visualizar e modificar as listas de usuários e grupos com ou sem permissão para acessar classes de dispositivos ou dispositivos específicos.

NOTA: A fim de utilizar esta visualização para ler as informações de acesso a dispositivos, o usuário ou o grupo pode receber permissão para "ler" na visualização **Configurações de acesso do usuário**. A fim de utilizar esta visualização para modificar as informações de acesso a dispositivos, o usuário ou o grupo deve receber permissão para "alteração" na visualização **Configurações de acesso do usuário**.

A visualização Configuração de Classe de Dispositivo possui as seguintes seções:

- **Lista de dispositivos** — Mostra todas as classes de dispositivos e dispositivos instalados no sistema ou que foram instalados anteriormente.
  - A proteção costuma ser aplicada a uma classe de dispositivos. Um usuário ou grupo selecionado terá permissão para acessar qualquer dispositivo da classe de dispositivos.
  - A proteção também pode ser aplicada em dispositivos específicos.
- **Lista de usuários** — Exibe todos os usuários e grupos com ou sem permissão de acesso à classe de dispositivos ou dispositivo específico selecionados.
  - A entrada na Lista de usuários pode ser para um usuário específico ou para um grupo do qual este usuário é membro.
  - Quando uma entrada de usuário ou grupo na Lista de usuários não está disponível, a configuração foi herdada da classe de dispositivos da Lista de dispositivos ou da pasta Classe.
  - Algumas classes de dispositivos, como DVD e CD-ROM, também podem ser controladas permitindo ou negando acesso separadamente a operações de leitura ou de gravação.

Quanto a outros dispositivos e classes, o direito de acesso de leitura ou gravação pode ser herdado. Por exemplo, o acesso de leitura pode ser herdado de uma classe superior, mas o acesso de gravação pode ser negado especificamente para um usuário ou grupo.

NOTA: Se a caixa de seleção Leitura estiver em branco, significa que a entrada de controle de acesso não terá efeito no acesso de leitura ao dispositivo. O acesso de leitura ao dispositivo não será concedido nem negado.

Exemplo 1 — Se um usuário ou grupo não tiver permissão de acesso de leitura para um dispositivo ou classe de dispositivos:

O mesmo usuário, o mesmo grupo ou um membro do grupo terá permissão de acesso de leitura ou leitura+gravação somente para dispositivos abaixo desse na hierarquia de dispositivos.

Exemplo 2 — Se um usuário ou grupo tiver permissão de acesso de leitura para um dispositivo ou classe de dispositivos:

O mesmo usuário, o mesmo grupo ou um membro do grupo não terá permissão de acesso de gravação ou leitura+gravação somente para esse dispositivo ou para dispositivos abaixo dele na hierarquia.

Exemplo 3 — Se um usuário ou grupo tiver permissão de acesso de leitura para um dispositivo ou classe de dispositivos:

O mesmo usuário, o mesmo grupo ou um membro do grupo não terá permissão de acesso de leitura ou leitura+gravação somente para esse dispositivo ou para dispositivos abaixo dele na hierarquia.

Exemplo 4 — Se um usuário ou grupo não tiver permissão de acesso de leitura para um dispositivo ou classe de dispositivos:

O mesmo usuário, o mesmo grupo ou um membro do grupo terá permissão de acesso de leitura ou de acesso de leitura+gravação somente para dispositivos abaixo dele na hierarquia de dispositivos.

Exemplo 5 — Se um usuário ou grupo tiver permissão de acesso de leitura+gravação para um dispositivo ou classe de dispositivos:

O mesmo usuário, o mesmo grupo ou um membro do grupo não terá permissão de acesso de gravação ou leitura+gravação somente para esse dispositivo ou para dispositivos abaixo dele na hierarquia.

Exemplo 6 — Se um usuário ou grupo não tiver permissão de leitura+gravação para um dispositivo ou classe de dispositivos:

O mesmo usuário, o mesmo grupo ou um membro do grupo terá permissão de acesso ou de acesso de leitura+gravação somente para dispositivos abaixo desse na hierarquia de dispositivos.

Negarção de acesso a um usuário ou grupo

Para evitar que um usuário ou grupo acesse um dispositivo ou classe de dispositivos, siga estas etapas:

1. No painel esquerdo do **Console Administrativo do HP ProtectTools** clique em **Device Access Manager** e, em seguida, em **Configuração de Classe de Dispositivo**.
2. Na lista de dispositivos, clique na classe de dispositivos que deseja configurar.
   - Classe de dispositivos
   - Todos os dispositivos
   - Dispositivo individual
3. Em **Usuário/Grupos**, clique no usuário ou grupo ao qual o acesso será negado.
4. Clique em **Negar** próximo a um usuário ou grupo.
5. Clique no ícone **Salvar**.

NOTA: Quando as configurações de negar e permitir são definidas no mesmo nível de dispositivos para um usuário; a negação do acesso tem prioridade sobre sua permissão.

Permissão de acesso para um usuário ou grupo

Para permitir o acesso de um usuário ou grupo a um dispositivo ou classe de dispositivos, siga estas etapas:

1. No painel esquerdo do **Console Administrativo do HP ProtectTools** clique em **Device Access Manager** e, em seguida, em **Configuração de Classe de Dispositivo**.
2. Na lista de dispositivos, clique em um dos itens a seguir:
   - Classe de dispositivos
   - Todos os dispositivos
   - Dispositivo individual
3. Clique em **Adicionar**.

   A caixa de diálogo **Selecionar Usuários ou Grupos** é aberta.
4. Clique em **Avançado** e, em seguida, em **Localizar Agora** para pesquisar usuários ou grupos a serem adicionados.
5. Clique no usuário ou grupo a ser adicionado à lista de usuários e grupos disponíveis e, em seguida, clique em **OK**.
6. Clique em **OK** outra vez.
7. Clique em **Permitir** para conceder acesso esse usuário ou grupo.
8. Clique no ícone **Salvar**.

Remoção do acesso para um usuário ou grupo

Para remover a permissão de acesso a um dispositivo ou classe de dispositivos para um usuário ou grupo, siga estas etapas:

1. No painel esquerdo do **Console Administrativo do HP ProtectTools** clique em **Device Access Manager** e, em seguida, em **Configuração de Classe de Dispositivo**.
2. Na lista de dispositivos, clique na classe de dispositivos que deseja configurar.
   - Classe de dispositivos
   - Todos os dispositivos
   - Dispositivo individual
3. Em **Usuário/Grupos**, clique no usuário ou grupo que deseja remover e, em seguida, clique em **Remover**.
4. Clique no ícone **Salvar**.

Permissão de acesso a uma classe de dispositivos para o usuário de um grupo

Para permitir que um usuário acesse uma classe de dispositivos e, ao mesmo tempo, negar o acesso de todos os outros membros do grupo desse mesmo usuário, siga estas etapas:

1. No painel esquerdo do **Console Administrativo do HP ProtectTools** clique em **Device Access Manager** e, em seguida, em **Configuração de Classe de Dispositivo**.
2. Na lista de dispositivos, clique na classe de dispositivos que deseja configurar.
   - Classe de dispositivos
   - Todos os dispositivos
   - Dispositivo individual
3. Em **Usuário/Grupos**, selecione o grupo que terá o acesso negado e, em seguida, clique em **Negar**.
4. Em seguida, acesse a pasta abaixo da classe requerida e adicione o usuário específico.
5. Clique em **Permitir** para conceder acesso a ele.
6. Clique no ícone **Salvar**.

Permitissão de acesso a dispositivos específicos para o usuário de um grupo

Os administradores podem permitir que um usuário acesse um dispositivo específico ao mesmo tempo que negam o acesso de todos os outros membros do grupo desse usuário a todos os dispositivos da mesma classe:

1. No painel esquerdo do **Console Administrativo do HP ProtectTools** clique em **Device Access Manager** e, em seguida, em **Configuração de Classe de Dispositivo**.
2. Na lista de dispositivos, clique na classe de dispositivos que deseja configurar e, em seguida, navegue até a pasta abaixo dela.
3. Clique em **Adicionar**. A caixa de diálogo **Selecionar Usuários ou Grupos** é aberta.

4. Clique em **Avançado** e, em seguida, em **Localizar Agora** para pesquisar o grupo do usuário, grupo este que terá acesso negado a todos os dispositivos da classe.
5. Selecione o grupo e clique em **OK**.
6. Navegue até o dispositivo específico dentro da classe de dispositivos à qual o usuário terá acesso.
7. Clique em **Adicionar**. A caixa de diálogo **Selecionar Usuários ou Grupos** é aberta.
8. Clique em **Avançado** e, em seguida, em **Localizar Agora** para pesquisar usuários ou grupos a serem adicionados.
9. Clique no usuário que terá acesso permitido e clique em **OK**.
10. Clique em **Permitir** para conceder acesso a esse usuário.
11. Clique no ícone **Salvar**.

Restauração das configurações

△ **CUIDADO:** A restauração das configurações descarta todas as mudanças feitas na configuração do dispositivo e redefine todas as configurações estabelecidas na fábrica.

Para restaurar as definições de configuração aos valores de fábrica, siga estas etapas:

1. No painel esquerdo do **Console Administrativo do HP ProtectTools** clique em **Device Access Manager** e, em seguida, em **Configuração de Classe de Dispositivo**.
2. Clique no botão **Restaurar**.
3. Clique em **Sim** para confirmar.
4. Clique no ícone **Salvar**.

Tarefas avançadas

Controle do acesso aos parâmetros de configuração

Na visualização **Configurações de acesso do usuário**, os administradores especificam os grupos ou usuários que podem utilizar as páginas Configuração Simples e Configuração de Classe de Dispositivo.

NOTA: Um usuário ou grupo deve ter "direitos totais de administrador" para que possa modificar as configurações na visualização Configurações de acesso do usuário.

- Um usuário ou grupo deve ter a permissão de acesso à "visualização (somente leitura) dos parâmetros de configuração" na visualização Configurações de acesso do usuário a fim de visualizar as informações da Configuração Simples e da Configuração de Classe de Dispositivo.
- Um usuário ou grupo deve ter permissão de acesso à "alteração dos parâmetros de configuração" na visualização Configurações de acesso do usuário a fim de alterar as informações da Configuração Simples e da Configuração de Classe de Dispositivo.

NOTA: Até mesmo os membros do grupo Administradores precisam ter acesso de "leitura" para visualizar a Configuração Simples e a Configuração de Classe de Dispositivo, bem como precisam der acesso de "alteração" para modificar dados utilizando as visualizações Configuração Simples e Configuração de Classe de Dispositivo.

NOTA: Se, após a avaliação dos níveis de acesso para todos os usuário e grupos, algum usuário não tiver Permitir ou Negar selecionado para um nível de acesso específico, ele terá seu acesso negado a esse nível.

Garantir acesso a um grupo ou usuário existente

Para conceder permissão para um grupo ou usuário existente visualizar ou modificar os parâmetros de configuração, siga estas etapas:

1. No painel esquerdo do **Console Administrativo do HP ProtectTools**, clique em **Device Access Manager** e, em seguida, clique em **Configurações de acesso do usuário**.
2. Clique no usuário ou grupo que terá o acesso permitido.
3. Em **Permissões**, clique em **Permitir** para cada tipo de permissão que será concedido ao grupo ou usuário selecionado:

   NOTA: As permissões concedidas são cumulativas. Por exemplo, um usuário que recebeu a permissão para a "alteração dos parâmetros de configuração" recebe automaticamente permissão para a "visualização (somente leitura) dos parâmetros de configuração". Um usuário que recebeu a permissão de "direitos totais de administrador" recebe automaticamente as permissões a "visualização (somente leitura) dos parâmetros de configuração" e "visualização (somente leitura) dos parâmetros de configuração".

   - Todos os direitos para usuário-administrador
   - Mudar as opções de configuração
   - Ver (Somente leitura) as opções de configuração
4. Clique no ícone **Salvar**.

Negação de acesso para um grupo ou usuário existente

Para negar a permissão de visualização ou alteração dos parâmetros de configuração para um grupo ou usuário existente, siga estas etapas:

1. No painel esquerdo do **Console Administrativo do HP ProtectTools**, clique em **Device Access Manager** e, em seguida, clique em **Configurações de acesso do usuário**.
2. Clique no usuário ou grupo que terá a permissão negada.
3. Em **Permissões**, clique em **Negar** para cada tipo de permissão que será negado ao grupo ou usuário selecionado:
   - Todos os direitos para usuário-administrador
   - Mudar as opções de configuração
   - Ver (Somente leitura) as opções de configuração
4. Clique no ícone **Salvar**.

Inclusão de um novo grupo ou usuário

Para permitir que um novo grupo ou usuário visualize ou modifique os parâmetros de configuração, siga estas etapas:

1. No painel esquerdo do **Console Administrativo do HP ProtectTools**, clique em **Device Access Manager** e, em seguida, clique em **Configurações de acesso do usuário**.
2. Clique em **Adicionar**. A caixa de diálogo **Selecionar Usuários ou Grupos** é aberta.
3. Clique em **Avançado** e, em seguida, em **Localizar Agora** para pesquisar os usuários ou grupos que serão adicionados.
4. Clique no grupo ou usuário, clique em **OK** e, em seguida, em **OK** novamente.
5. Clique em **Permitir** para conceder acesso a esse usuário.
6. Clique no ícone **Salvar**.

Remoção do acesso de um grupo ou usuário

Para remover a permissão de visualização ou alteração dos parâmetros de configuração para um grupo ou usuário, siga estas etapas:

1. No painel esquerdo do **Console Administrativo do HP ProtectTools**, clique em **Device Access Manager** e, em seguida, clique em **Configurações de acesso do usuário**.
2. Clique no grupo ou usuário e, em seguida, em **Remover**.
3. Clique no ícone **Salvar**.

Documentação relacionada

O Device Access Manager for ProtectTools é compatível com o produto corporativo HP ProtectTools Enterprise Device Access Manager. Ao trabalhar com um produto corporativo, o Device Access Manager for HP ProtectTools permite o acesso somente leitura a seus próprios recursos.

Mais informações sobre o Device Access Manager for HP ProtectTools estão disponíveis na web em http://www.hp.com/hps/security/products.

11 LoJack Pro for HP ProtectTools

O Computrace LoJack Pro, desenvolvido pela Absolute Software (adquirido separadamente), visa ao crescente problema de computadores roubados ou perdidos.

A ativação desse software habilita o Computrace Agent, que permanece ativo em seu computador mesmo que o disco rígido seja reformatado ou substituído.

O LoJack Pro permite o monitoramento, o gerenciamento e o rastreamento remotos de seu computador. Se ele for roubado ou perdido, a Equipe de Recuperação da Absolute auxiliará você na recuperação.*

NOTA: *Esse recurso depende do local geográfico. Consulte o contrato de licenciamento da Absolute Software para obter detalhes adicionais.

12 Solução de problemas

HP ProtectTools Security Manager

Descrição resumida	Detalhes	Solução
Smart cards e tokens USB não estarão disponíveis no Security Manager se tiverem sido instalados após o mesmo.	Para usar smart cards ou tokens USB no Security Manager, o software de suporte (drivers, fornecedores de PKCS#11 etc.) deve ser instalado antes do Security Manager. Se o Security Manager já estiver instalado, execute as seguintes etapas após a instalação do software de suporte do smart card ou token:	Efetue login no Gerenciador de Senhas. No HP ProtectTools Security Manager, clique em **Gerenciador de Senhas** e, em seguida, em **Credenciais** e **Smart Card**. Reinicie o computador, se solicitado.
Algumas páginas web de aplicativos geram erros que evitam que o usuário execute ou conclua tarefas.	Alguns aplicativos web param de funcionar e relatam erros devido ao padrão de funcionalidade de desativação do Single Sign On. Por exemplo, um **!** em um triângulo amarelo é exibida no Internet Explorer, indicando a ocorrência de um erro.	O Single Sign On do Security Manager não suporta todas as interfaces web de software. Desative o suporte ao Single Sign On para a página web específica desligando o suporte ao Single Sign On. Consulte a documentação completa sobre o Single Sign On, disponível nos arquivos de Ajuda do software do Security Manager. Se um Single Sign On específico não puder ser desativado para um determinado aplicativo, entre em contato com o suporte técnico da HP e solicite suporte de nível 3 através do seu contato na HP Service.
A opção **Browse for Virtual Token** (Procurar token virtual) não é exibida durante o processo de login.	O usuário não pode mover o local de um token virtual registrado no Gerenciador de Senhas, pois a opção para procura foi removida visando reduzir os riscos de segurança.	A opção de procura foi removida porque permitia a não-usuários excluir e renomear arquivos e controlar o Windows.
Os administradores de domínio não podem alterar a senha do Windows, mesmo com autorização.	Isso acontece após um administrador do domínio fazer login e registrar a identidade do domínio com o Gerenciador de Senhas utilizando uma conta com direitos de administrador no domínio e no PC local. Quando o administrador do domínio tenta alterar a senha do Windows no Gerenciador de Senhas, ocorre uma falha de erro no login: **Restrição da conta do usuário**.	O Gerenciador de Senhas não pode alterar a senha da conta de um usuário do domínio por meio da opção **Alterar senha do Windows**. O Security Manager pode alterar somente senhas de contas no computador local. O usuário de um domínio pode alterar sua senha por meio da opção **Alterar senha** em **Segurança do Windows**, mas, uma vez que não possui uma conta física no computador local, o Gerenciador de Senhas só poderá alterar a senha utilizada para login.
O Gerenciador de Senhas tem problemas de incompatibilidade com a biblioteca GINA de senhas do Corel WordPerfect 12.	Se o usuário efetua login no Gerenciador de Senhas, cria um documento no WordPerfect e salva com proteção por senha, o Gerenciador de Senhas não detecta ou reconhece, seja de forma	A HP está pesquisando uma solução alternativa para aprimoramentos futuros do produto.

Descrição resumida	Detalhes	Solução
	manual ou automática, a biblioteca GINA de senhas.	
O Gerencaidor de Senhas não reconhece o botão **Conectar** na tela.	Se as credenciais do Single Sign On para o Remote Desktop Connection (RDP) forem definidas para **Conectar**, quando o Single Sign On reiniciado, ele sempre irá inserir **Salvar como** em vez de **Conectar**.	A HP está pesquisando uma solução alternativa para aprimoramentos futuros do produto.
O usuário não é capaz de efetuar login no Gerenciador de Senhas após passar do modo de suspensão para a hibernação somente no Windows XP Service Pack 1.	Após permitir que o sistema alterne entre a hibernação e o modo de suspensão, o administrador ou o usuário não consegue fazer login no Gerenciador de Senhas e a tela de login do Windows permanece sendo exibida, independentemente da credencial de login (senha, impressão digital ou Java Card) selecionada.	Atualize o Windows com o Service Pack 2 usando o Windows Update. Consulte o artigo 813301 da base de conhecimento da Microsoft em http://www.microsoft.com para obter mais informações sobre a causa do problema. Para efetuar o login, o usuário deve selecionar o Gerenciador de Senhas e efetuá-lo. Após efetuar o login no Gerenciador de Senhas, o usuário é solicitado a efetuar o login no Windows (o usuário pode ter que selecionar a opção de login do Windows) para concluir o processo de login. Se o usuário efetuar o login no Windows primeiro, então ele deve efetuar o login no Gerenciador de Senhas manualmente.
O processo de segurança **Restore Identity** (Restaurar identidade) perde a associação com o token virtual.	Quando o usuário restaurar a identidade, o Gerenciador de Senhas poderá perder a associação ao local do token virtual na tela de login. Embora o Gerenciador de Senhas tenha o token virtual registrado, o usuário deve registrá-lo novamente para restaurar a associação.	Esta é uma decisão de projeto. Ao desinstalar o Security Manager sem manter as identidades, a parte sistema (servidor) do token é destruída, de modo que o token não possa mais ser utilizado para efetuar o login, mesmo se a parte cliente do token for restaurada por meio da restauração de identidade. A HP está investigando opções de longo prazo para uma solução.

Device Access Manager for HP ProtectTools

Os usuários tiveram o acesso a dispositivos negado no Device Access Manager, mas os dispositivos ainda estão acessíveis.

- **Explicação**: as visualizações Configuração Simples e/ou Configuração de Classe de Dispositivo foram utilizadas no Device Access Manager para negar o acesso de usuários a dispositivos. Apesar de terem o acesso negado, os usuários ainda podem acessar os dispositivos.
- **Solução:**
  - Verifique se o serviço de bloqueio de dispositivos do HP ProtectTools foi iniciado.
  - Como um usuário administrativo, clique em **Painel de Controle** e, em seguida, clique em **Sistema e Manutenção**. Na janela Ferramentas Administrativas, clique em **Serviços** e procure o serviço **Bloqueio de Dispositivos/Auditoria do HP ProtectTools**. Verifique se o serviço foi iniciado e se o tipo de inicialização é **Automático**.

Um usuário teve acesso a um dispositivo de modo inesperado, ou um usuário teve o acesso negado a um dispositivo de modo inesperado.

- **Explicação**: o Device Access Manager foi utilizado para negar o acesso de usuários a alguns dispositivos e permitir o acesso de usuários a outros dispositivos. Quando o usuário está utilizando o sistema, ele pode acessar dispositivos para os quais acredita que o Device Access Manager tenha negado acesso, e ter o acesso negado a dispositivos para os quais acredita que o Device Access Manager devesse permitir o acesso.
- **Solução:**
  - Use a visualização Configuração de Classe de Dispositivo no Device Access Manager para investigar as configurações de dispositivo dos usuários.
  - Clique em **Security Manager**, **Device Access Manager** e, em seguida, clique em **Configuração de Classe de Dispositivo**. Expanda os níveis na árvore de classes de dispositivos e reveja as configurações aplicáveis ao usuário. Verifique se há permissões do tipo “Negar” definidas para o usuário ou qualquer grupo do Windows ao qual ele possa pertencer, p.ex., Usuários, Administradores.

Permitir ou negar – qual dos dois tem precedência?

- **Explicação**: no Configuração de Classe de Dispositivo, a seguinte configuração foi definida:
  - A permissão Permitir foi concedida a um grupo do Windows (p.ex., BUILTIN\Administradores) e a permissão Negar foi concedida a um outro grupo do Windows (p.ex., BUILTIN\Usuários) no mesmo nível na hierarquia de classe de dispositivo (p.ex., Unidades de DVD/CD-ROM).
  - Se um usuário for membro de ambos os grupos (p.ex., Administrador), o que tem precedência?
- **Solução:**
  - O usuário tem o acesso negado ao dispositivo. Negar tem precedência a Permitir.
  - O acesso é negado devido ao modo como o Windows determina a permissão efetiva para o dispositivo. Um grupo tem o acesso negado e outro grupo tem o acesso permitido, mas o usuário é membro de ambos os grupos. O usuário tem o acesso negado pois a negação de acesso precede a permissão de acesso.

- Uma solução provisória é negar o acesso ao grupo de usuários no nível de Unidades de DVD/CD-ROM e permitir o acesso ao grupo de administradores no nível abaixo de Unidades de DVD/CD-ROM.
- Uma solução alternativa é criar grupos do Windows específicos, um para permitir o acesso a DVD/CD e outro para negar o acesso a DVD/CD. Usuários específicos poderiam então ser adicionados aos grupos apropriados.

A visualização Configuração Simples foi usada para definir uma política de controle de acesso ao dispositivo, mas os usuários administrativos não podem acessar os dispositivos.

- **Explicação**: A visualização Configuração Simples nega o acesso a usuários e convidados e permite o acesso a administradores de dispositivo.
- **Solução:** Adicione o usuário administrativo ao grupo Administradores de dispositivos.

Diversos

Impactado por software – Descrição resumida	Detalhes	Solução
Security Manager — Advertência recebida: **The security application can not be installed until the HP Protect Tools Security Manager is installed** (O aplicativo de segurança não pode ser instalado até que o HP Protect Tools Security Manager esteja instalado).	Todos os aplicativos de segurança, como o Java Card Security e dispositivos biométricos, são plug-ins expansíveis para a interface do Security Manager. O Security Manager deve ser instalado antes que um plug-in de segurança aprovado pela HP possa ser carregado.	O software Security Manager deve ser instalado antes da instalação de qualquer plug-in de segurança.
HP ProtectTools Security Manager — Intermitente, um erro é exibido ao fechar a interface do Security Manager.	Intermitente (1 em 12 instâncias), um erro é gerado ao utilizar o botão fechar no canto superior direito da tela, para fechar o Security Manager antes que todos os aplicativos de plug-ins tenham sido totalmente carregados.	Isso está relacionado a uma dependência de sincronização no tempo de carregamento de serviços do plug-in, ao fechar e reiniciar o Security Manager. Sendo PTHOST.exe uma carcaça (shell) que comporta outros aplicativos (plug-ins), ela depende da capacidade do plug-in em completar seu tempo de carregamento (serviços). A causa do problema é o ato de fechar a carcaça antes que o plug-in tenha sido completamente carregado. Permita que o Security Manager conclua a mensagem de carregamento de serviços (vista na parte superior da janela do Security Manager) e todos os plug-ins listados na coluna da esquerda. Para evitar falhas, aguarde um tempo razoável para que os plug-ins sejam carregados.
HP ProtectTools — Acesso irrestrito ou privilégios de administrador não-controlados apresentam risco à segurança.	Diversos riscos são possíveis com o acesso irrestrito ao PC cliente, incluindo os seguintes: • Exclusão da PSD • Modificação mal-intencionada das configurações do usuário • Desativação de políticas e funções de segurança	Os administradores são encorajados a seguir as "melhores práticas" restringindo os privilégios do usuário final e o acesso do usuário. Usuários não-autorizados não devem receber privilégios administrativos.

Glossário

administrador *Veja* administrador do Windows.

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

arquivo de recuperação de emergência Área de armazenamento protegida que permite criptografar novamente as chaves de usuário básico, a partir de uma chave de proprietário de plataforma a outra.

assinante sugerido Um usuário que é designado pelo proprietário de um documento do Microsoft Word ou do Microsoft Excel para acrescentar uma linha de assinatura ao documento.

assinatura digital Dados enviados junto com um arquivo que verificam o remetente do material, e que o arquivo não foi modificado depois de assinado.

ativação A tarefa que deve ser concluída antes de qualquer um dos recursos do Drive Encryption poder ser acessado. O Drive Encryption é ativado pelo Assistente de Instalação do HP ProtectTools. Somente um administrador pode ativar o Drive Encryption. O processo de ativação consiste na ativação do software, criptografia da unidade, criação de uma conta de usuário e criação do backup inicial da chave de criptografia em um dispositivo de armazenamento removível.

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

ATM Automatic Technology Manager, que 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 algumas formas de autenticação, como um Java Card, um chip de segurança ou uma senha, quando o computador é ligado.

autoridade de certificação Serviço que emite certificados necessários para executar uma infra-estrutura de chave pública.

backup A utilização do recurso de backup permite que seja feita uma cópia das informações importantes do programa para um local fora dele. Também pode ser utilizado para restaurar as informações posteriormente para o mesmo ou outro computador.

biométrica Categoria de credenciais de autenticação que utilizam um recurso físico, como a impressão digital para identificar um usuário.

botão Assinar e Codificar Um botão de software que é exibido na barra de ferramentas dos aplicativos do Microsoft Office. Clicar no botão permite assinar, criptografar ou remover a criptografia de um documento do Microsoft Office.

botão Envio Seguro Um botão de software que é exibido na barra de ferramentas das mensagens de e-mail do Microsoft Outlook. Clicar no botão permite assinar e/ou criptografar uma mensagem de e-mail do Microsoft Outlook.

certificado digital Credenciais eletrônicas que confirmam a identidade de um indivíduo ou empresa, vinculando a identidade do proprietário do certificado digital a um par de chaves eletrônicas que são utilizadas para assinar a informação digital.

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.

classe de dispositivo Todos os dispositivos de um tipo específico, como as unidades, por exemplo.

codificação Procedimento, com a utilização de um algoritmo, empregado na criptografia para converter texto simples em texto cifrado, para evitar que destinatários não-autorizados leiam os dados. Existem diversos tipos de codificação de dados e eles formam a base da segurança de rede. Alguns tipos comuns incluem o padrão de criptografia de dados e criptografia por chave pública.

comunicação de IM confiável Uma sessão de comunicação durante a qual mensagens confiáveis são enviadas por um remetente confiável para um contato confiável.

console Um local central em que é possível acessar e gerenciar recursos e configurações deste programa.

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.

Contato Confiável Uma pessoa que aceitou um convite para se tornar um contato confiável.

convite de Contato Confiável Um e-mail que é enviado para uma pessoa perguntando se ela deseja se tornar um contato confiável.

credenciais Método no qual um usuário comprova sua elegibilidade para determinada tarefa no processo de autenticação.

criptografia Prática de codificar e decodificar dados, para que possam ser decodificados apenas por indivíduos específicos.

descriptografia Procedimento utilizado na criptografia para converter dados criptografados em texto simples.

destinatário de Contato Confiável Uma pessoa que recebe um convite para tornar-se um contato confiável.

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.

Drive Encryption Protege seus dados criptografando seu(s) disco(s) rígido(s), tornando informações ilegíveis por usuários sem a autorização adequada.

DriveLock Recurso de segurança que vincula o disco rígido a um usuário e requer que o usuário digite corretamente a senha do DriveLock quando o computador é inicializado.

EFS (Encryption File System, sistema de criptografia de arquivo) Sistema que decodifica todos os arquivos e subpastas dentro do diretório selecionado.

exclusão simples Exclusão da referência do Windows para um ativo. O conteúdo do ativo permanece no disco rígido até que os dados ocultos sejam sobregravados pela Purificação de Espaço Livre.

fragmentação automática A fragmentação programada que o usuário define no File Sanitizer.

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.

grupo Um grupo de usuário que possui o mesmo nível de acesso ou que tem o acesso negado a uma classe de dispositivos ou dispositivo específico.

HP SpareKey Cópia de segurança da chave do Drive Encryption.

ID card Uma barra lateral no Windows que serve para identificar visualmente sua área de trabalho com seu nome de usuário e uma foto de sua escolha. Clique no ID card para abrir o Console Administrativo do HP ProtectTools.

identidade No HP ProtectTools Security Manager, um grupo de credenciais e configurações que são tratadas como a conta ou perfil de um determinado usuário.

impressão digital Uma reprodução digital da imagem de suas impressão digitais. A imagem real de suas impressões digitais nunca será armazenada pelo Security Manager.

Java Card Um cartão removível que é inserido no computador. Ele contém informações de identificação para o login. O login usando um Java Card na tela de login do Drive Encryption requer que você insira o Java Card e digite seu nome de usuário e o PIN do Java Card.

linha de assinatura É um local reservado para a exibição visual de uma assinatura digital. Quando um documento é assinado, o nome do assinante e o método de verificação são exibidos. A data de assinatura e o título do assinante também podem ser incluídos.

lista de Contatos Confiáveis Uma listagem de contatos confiáveis.

login Um objeto dentro do Security Manager composto por um nome de usuário e uma senha (e possivelmente outras informações selecionadas) e que pode ser utilizado para efetuar login em websites e outros programas.

mensagem confiável Uma sessão de comunicação durante a qual mensagens confiáveis são enviadas por um remetente confiável para um contato confiável.

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

migração Uma tarefa que permite gerenciar, restaurar e transferir certificados do Privacy Manager e contatos confiáveis.

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

painel Um local central em que é possível acessar e gerenciar recursos e configurações deste programa.

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

PKI Public Key Infrastructure – Infraestrutura de chave pública, padrão que define as interfaces para criação, utilização e administração de certificados e chaves criptográficas.

política de controle de acesso a dispositivos A lista de dispositivos aos quais o usuário tem acesso permitido ou não.

Privacy Manager Certificate Um certificado digital que exige autenticação toda vez que é usado para operações de criptografia, como assinar e criptografar mensagens de e-mail e documentos do Microsoft Office.

provedor de serviços de criptografia (CSP) Prestador ou biblioteca de algoritmos criptográficos que podem ser utilizados em uma interface bem definida para realizar determinadas funções criptográficas.

PSD Personal secure drive – Unidade pessoal protegida, que fornece uma área de armazenamento protegida para informações importantes.

Purificação de Espaço Livre A gravação segura de dados aleatórios sobre os ativos excluídos para alterar o conteúdo do ativo excluído.

reinicializar Processo de reinicialização do computador.

remetente confiável Um contato confiável que envia e-mails e documentos do Microsoft Office assinados e/ou criptografados.

restauração Um processo que copia as informações do programa a partir de um arquivo de backup salvo previamente neste programa.

revelar Uma tarefa que permite ao usuário descriptografar uma ou mais sessões de histórico de bate-papo, exibindo o(s) nome(s) de tela do(s) contato(s) em texto simples e tornando a sessão disponível para exibição.

Segurança de Login no Windows Protege sua(s) conta(s) do Windows solicitando o uso de credenciais específicas de acesso.

Selar para Contatos Confiáveis Uma tarefa que acrescenta uma assinatura digital, criptografa o e-mail e o envia depois que você realiza sua autenticação utilizando o método de login de segurança de sua escolha.

senha de revogação Uma senha que é criada quando um usuário solicita um certificado digital. Uma senha que é necessária quando o usuário deseja revogar seu certificado digital. Isso garante que só o usuário pode revogar o certificado.

seqüência de teclas Uma combinação de teclas específicas que, quando pressionadas, iniciam uma fragmentação automática; por exemplo: ctrl+alt+s.

serviço de segundo plano Refere-se ao serviço de segundo plano Bloqueio/Auditoria de dispositivos do HP ProtectTools, que deve estar em execução para que as políticas de controle de acesso sejam aplicadas. Ele pode ser visualizado a partir do aplicativo Serviços, na opção Ferramentas Administrativas do Painel de Controle. Se o serviço não estiver sendo executado, o HP ProtectTools Security Manager tentará iniciá-lo quando as políticas de controle de acesso forem aplicadas.

sessão de histórico de bate-papo Um arquivo criptografado que contém um registro dos dois lados de uma conversa em uma sessão de bate-papo.

Single Sign On (Login Único) Recurso que armazena informações de autenticação e permite o uso do Security Manager para acessar aplicativos da Internet e do Windows que requeiram autenticação por senha.

smart card Pequena peça de hardware, similares a um cartão de crédito em tamanho e formato, que armazena informações identificáveis sobre o proprietário. Utilizado para autenticar o proprietário de um computador.

tela de login do Drive Encryption A tela de login exibida antes do Windows ser iniciado. Os usuários devem inserir seu nome de usuário e a senha do Windows ou o PIN do Java Card. Na maioria das vezes, a inserção da informação correta na tela de login do Drive Encryption permite o acesso direto ao Windows sem precisar efetuar login novamente na tela de login do Windows.

token Vide método de login de segurança.

token USB Dispositivo de segurança que armazena informações de identificação de um usuário. Como um Java Card ou leitor biométrico, ele é utilizado para autenticar o proprietário de um computador.

token virtual Recurso de segurança que funciona de forma muito semelhante a um Java Card e leitor de cartão. O token é salvo no disco rígido do computador ou no registro do Windows. Ao efetuar login com um token virtual, será solicitado um PIN de usuário para completar a autenticação.

TXT Trusted Execution Technology (Tecnologia de execução confiável).

usuário Qualquer pessoa registrada no Drive Encryption. Usuários não-administradores têm direitos limitados no Drive Encryption. Eles podem apenas se registrar (com aprovação do administrador) e efetuar login.

usuário autorizado Um usuário que recebeu permissão de acesso nas Configurações de acesso do usuário para visualizar ou modificar os parâmetros de configuração nas visualizações Configuração Simples ou Configuração de Classe de Dispositivo.

Visualizar Histórico do Live Messenger Um componente do Privacy Manager Chat que permite procurar e visualizar sessões de histórico de bate-papo.

Índice

A

acesso
  controle 73
  garantir acesso a grupos ou usuários existentes 81
  negação para grupos ou usuários existentes 82
  negar 78
  permissão 78
  prevenção contra acesso não-autorizado 3
acesso não-autorizado, prevenção 3
acréscimo
  assinantes sugeridos 52
  linha de assinatura 51
  linha de assinatura do assinante sugerido 52
administração central 61
aplicativos, configuração dos 19
Aplicativos, configurações da guia 34
assinante sugerido
  acréscimo 52
  acréscimo de uma linha de assinatura 52
assinatura
  documento do Microsoft Office 51
  mensagem de e-mail 50
Assistente
  configuração do HP ProtectTools 8
Assistente de Configuração 8, 24
ativação
  Drive Encryption 37
  limpeza de espaço livre 71
autenticação 15

B

backup, criação de
  Certificados do Privacy Manager 60
  Contatos Confiáveis 60
  credenciais do HP ProtectTools 7
  dados 33
bate-papo na janela Comunicações 56

C

certificado, pré-assinado 43
certificado digital
  configuração de padrão 44
  detalhes de visualização 44
  exclusão 44
  instalação 43
  recebimento 43
  renovação 44
  restauração 45
  revogação 45
  solicitação 43
Certificado do Privacy Manager
  configuração de padrão 44
  detalhes de visualização 44
  exclusão 44
  instalação 43
  recebimento 43
  renovação 44
  restauração 45
  revogação 45
  solicitação 43
chaves de backup, criação de 39
ciclo de fragmentação 67
classe de dispositivo
  configuração 76
  permissão de acesso para um usuário 79
configuração
  acesso a dispositivos 74
  aplicativos 19
  classe de dispositivo 76
  Console Administrativo do HP ProtectTools 14
  controle de acesso 81
  fragmentação, programação de 65
  parâmetros 81
  Privacy Manager for Microsoft Outlook 49
  Privacy Manager for Windows Live Messenger 56
  Privacy Manager para um documento do Microsoft Office 51
  programação de limpeza de espaço livre 66
  restauração 80
  simples 75
Configuração Simples 75
configurações
  adição 25, 34
  aplicativos 21, 25, 34
  guia Geral 20
  ícone 31
  inclusão 21
configurações da guia Aplicativos 21
Console Administrativo do HP ProtectTools
  configuração 14
  inicialização 9
  utilização 13
Contatos Confiáveis
  adição 46
  detalhes de visualização 48

exclusão 48
Verificação do status de revogação 48
controle de acesso a dispositivos 73
credenciais 31, 32
credenciais, registro de 24
criação
chaves de backup 39
perfil de fragmentação 66
criptografia
documento do Microsoft Office 53
unidades 35, 38, 39
criptografia, exibição do status da 38

D
dados
backup, criação de 33
restauração 33
restrição de acesso a 3
definição
quais ativos serão confirmados antes da exclusão 68
definindo
quais ativos serão confirmados antes da fragmentação 67
desativação do Drive Encryption 37
descriptografia de unidades 35, 39
Device Access Manager for HP ProtectTools
inicialização 74
solução de problemas 87
dispositivo, configurações de
especificação 18
impressão digital 18
smart card 18
dispositivo para um usuário, permissão de acesso a um 79
Drive Encryption for HP ProtectTools
ativação 37
backup e recuperação 39
criptografia de unidades individuais 39
desativação 37
descriptografia de unidades individuais 39
gerenciamento do Drive Encryption 39
inicialização 36
login após o Drive Encryption ser ativado 37

E
efetuando login no computador 37
envio por e-mail de um documento do Microsoft Office criptografado 53
especificação das configurações de segurança 16
Excel, acréscimo de uma linha de assinatura no 51
exclusão de ativos da exclusão automática 68
exclusão simples 67

F
ferramentas, adição de 22
File Sanitizer for HP ProtectTools
ícone 70
inicialização 65
procedimentos de configuração 65
fragmentação manual
todos os itens selecionados 71
um ativo 70
funções de segurança 5

G
Geral, configurações da guia 20
Gerenciador de Senhas 27, 28
gerenciamento
credenciais 31
senhas 21, 27, 28
usuários 17
gerenciamento, adição de ferramentas de 22
grupo
negar acesso 78
permissão de acesso 78
remoção 79

H
histórico de bate-papo, visualização do 57
HP ProtectTools, recursos 2
HP ProtectTools Security Manager
Assistente de Configuração 8
inicialização 26
procedimentos de configuração 24
senha do arquivo de recuperação 6
solução de problemas 85

I
ID card 32
impressões digitais
configurações 18
registro 11, 24
inclusão
grupo 82
usuário 82
inicialização
Console Administrativo do HP ProtectTools 9
Device Access Manager for HP ProtectTools 74
Drive Encryption for HP ProtectTools 36
File Sanitizer for HP ProtectTools 65
HP ProtectTools Security Manager 26
Privacy Manager for HP ProtectTools 42
inicialização de uma sessão do Privacy Manager Chat 55
interrupção de uma operação de fragmentação ou de purificação 71

J
Java Card Security for HP ProtectTools, PIN 6

L
limpeza de espaço livre 66
logins
adição 28
categorias 29
edição 29

gerenciamento 30
menu 29
LoJack Pro for HP ProtectTools 84

M
mensagem de e-mail
assinatura 50
Selagem para Contatos Confiáveis 50
visualização de uma mensagem selada 50
Microsoft Excel, acréscimo de uma linha de assinatura no 51
Microsoft Office
assinatura de um documento 51
criptografia de um documento 53
envio por e-mail de um documento criptografado 53
remoção da criptografia 53
visualização de um documento assinado 54
visualização de um documento criptografado 54
Microsoft Word, acréscimo de uma linha de assinatura no 51

N
negar acesso 78

O
objetivos, segurança 3

P
painel de controle, configurações do 25
perfil de fragmentação predefinido 66
permissão de acesso 78
personalização
perfil de exclusão simples 67
perfil de fragmentação 67
preferências, configuração das 32
principais objetivos de segurança 3
Privacy Manager
utilização com o Microsoft Outlook 49
utilização com um documento do Microsoft Office 50
utilização no Windows Live Messenger 54
Privacy Manager for HP ProtectTools
autenticação, métodos de 41
gerenciamento de certificados do Privacy Manager 42
gerenciamento de contatos confiáveis 46
inicialização 42
métodos de login de segurança 41
migração de Certificados do Privacy Manager e de contatos confiáveis para um outro computador 60
Privacy Manager Certificate 42
procedimentos de configuração 42
requisitos do sistema 41
proteção de ativos contra a fragmentação automática 67

R
recuperação, execução de uma 40
recursos do HP ProtectTools 2
registro de credenciais 24
remoção
acesso de grupo 82
acesso de usuário 82
criptografia de um documento do Microsoft Office 53
requisitos do sistema 41
restauração
Certificados do Privacy Manager e Contatos Confiáveis 60
credenciais do HP ProtectTools 7
dados 33
restrição
acesso a dados importantes 3
acesso a dispositivos 73
roubo, proteção contra 3, 84

S
Security Manager
Assistente de Configuração 24
senha de login 5
segurança
perfis 5
principais objetivos 3
resumo 34
segurança, ativação de recursos de 10
selagem 50
seleção
ativos para fragmentação 66
perfil de fragmentação 66
senha
alteração 25
força 30
gerenciamento 5
HP ProtectTools 5
instruções 7
políticas 4
segura 7
Senha de login do Windows 6
seqüência de teclas 69
serviço de segundo plano 75
smart card
configurações 18
Smart Card
configuração 12
solicitação de um certificado digital 43
solução de problemas
Device Access Manager 87
diversos 89
Security Manager 85
Status dos Aplicativos de Segurança 34

U
usuário
negar acesso 78
permissão de acesso 78
remoção 79

V
visualização
arquivos de registro 71
documento assinado do Microsoft Office 54

documento criptografado do Microsoft Office 54
histórico de bate-papo 57
mensagem de e-mail selada 50

W

Windows Live Messenger, bate-papo no 56
Word, acréscimo de uma linha de assinatura no 51