HP ProtectTools

Passos Iniciais

Primeira edição: janeiro de 2011

Número de peça: 638391-201

Conteúdo

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.

Aplicativo	Recursos
Console Administrativo do HP ProtectTools (para administradores)	• Requer direitos de administrador do Microsoft Windows para obter acesso. • Fornece acesso a módulos que são configurados por um administrador e não estão disponíveis para usuários. • Permite a configuração de segurança inicial e configura opções ou requisitos para todos os usuários.
HP ProtectTools Security Manager (para usuários)	• Permite aos usuários configurar opções fornecidas por um administrador. • Permite aos administradores fornecer aos usuários controle limitado sobre alguns módulos do HP ProtectTools.

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.br.

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
Console Administrativo do HP ProtectTools (para administradores)	• Define e configura níveis de segurança e métodos de login de segurança usando o Assistente de Configuração do Security Manager. • Configura opções ocultas de usuários. • Define as configurações do Device Access Manager e o acesso de usuário. • Adiciona e remove usuários do HP ProtectTools e exibe o status de usuário usando as ferramentas do administrador.
HP ProtectTools Security Manager (para usuários)	• Organiza, configura e altera senhas. • Configura e altera credenciais de usuários, como senha do Windows, impressões digitais e smart card. • Configura e altera a fragmentação, a purificação e outras configurações do File Sanitizer. • Exibe as configurações do Device Access Manager. • Configura o Computrace for HP ProtectTools. • Configura preferências e opções de Backup e Restauração.
Credential Manager for HP ProtectTools (Password Manager)	• Salva, organiza e protege nomes de usuário e senhas. • Configura as telas de login de sites da web e programas para acesso rápido e seguro. • Salva nomes e senhas de usuário de sites da web inserindo-os no Password Manager. A próxima vez que você visitar o site, o Password Manager preencherá e enviará as informações automaticamente. • Cria senhas mais fortes para aumentar a segurança da conta. O Password Manager preenche e envia automaticamente as informações.
Drive Encryption for HP ProtectTools (somente em determinados modelos)	• Oferece criptografia completa, de volumes inteiros, para unidades de disco rígido. • Força a autenticação de pré-inicialização para decodificar e acessar dados.
File Sanitizer for HP ProtectTools	• Fragmenta ativos digitais (informações sensíveis, incluindo arquivos de aplicativos, conteúdo de históricos ou da web, ou outros dados confidenciais) em seu computador e, periodicamente, limpa ativos excluídos da unidade de disco rígido.

Módulo	Principais recursos
Device Access Manager for HP ProtectTools (somente em determinados modelos)	• Permite que os gerentes de TI controlem o acesso a dispositivos com base em perfis de usuários. • Impede que usuários não autorizados retirem dados usando uma mídia de armazenamento externa, além da introdução de vírus no sistema usando mídias externas. • Permite aos administradores desativar o acesso de indivíduos específicos ou grupos de usuários a dispositivos graváveis.
Privacy Manager for HP ProtectTools (somente em determinados modelos)	• Usado para a obtenção de certificados de autoridade, que verificam a fonte, a integridade e a segurança de comunicações ao se usar e-mails Microsoft e documentos do Microsoft Office.
Computrace for HP ProtectTools (vendido separadamente)	• Fornece rastreamento seguro de ativo. • Monitora a atividade do usuário, bem como as alterações de hardware e software. • Permanece ativo ainda que o disco rígido seja reformatado ou substituído. • Para ser ativado, requer a aquisição separada de assinaturas de rastreamento e acompanhamento.
Embedded Security for HP ProtectTools (somente em determinados modelos)	• Usa um chip de segurança integrado TPM (Trusted Platform Module) que oferece proteção contra acessos não autorizados a dados e credenciais do usuário armazenados em um computador. • Permite a criação de uma unidade pessoal protegida (PSD), que é útil para a proteção de informações de arquivos e pastas do usuário. • Suporta aplicativos de terceiros (como o Microsoft Outlook e o Internet Explorer) para operações de certificado digital protegido.

Exemplos de uso comum e descrição do produto de segurança HP ProtectTools

A maioria dos produtos de segurança do HP ProtectTools possui autenticação do usuário (geralmente uma senha) e um backup administrativo para se obter acesso caso as senhas sejam perdidas, fiquem indisponíveis ou sejam esquecidas, ou para qualquer momento em que a segurança corporativa exigir acesso.

NOTA: Alguns dos produtos de segurança do HP ProtectTools foram projetados para restringir o acesso a dados. Os dados devem ser criptografados quando forem tão importantes que o usuário preferiria perder as informações a comprometê-las. É recomendável que todos os dados tenham um backup guardado em um local seguro.

Credential Manager for HP ProtectTools

O Credential Manager (parte do Security Manager) armazena nomes de usuário e senhas e pode ser usado para:

- Salvar nomes e senhas de login para acesso à Internet ou e-mail.
- Registrar automaticamente o usuário em um site da web ou e-mail.
- Gerenciar e organizar autenticações.
- Selecionar um ativo de web ou de rede e acessar diretamente o link.
- Exibir nomes e senhas quando necessário.

Exemplo 1: Uma agente de compras de um grande fabricante faz a maioria de suas transações corporativas pela Internet. Ela também visita frequentemente vários sites populares que exigem informações de login. Ela é muito consciente da segurança de modo que não usa a mesma senha para todas as contas. A agente de compras decidiu usar o Credential Manager para associar links da web a diferentes nomes de usuário e senhas. Quando ela acessa um site para fazer login, o Credential Manager apresenta as credenciais automaticamente. Se ela quiser ver os nomes de usuário e senhas, o Credential Manager pode ser configurado para exibi-los.

O Credential Manager também pode ser usado para gerenciar e organizar as autenticações. Essa ferramenta permitirá que um usuário selecione um ativo da web ou de rede e acesse diretamente o link. O usuário também pode exibir os nomes de usuário e as senhas, quando necessário.

Exemplo 2: Um esforçado contador foi promovido e agora gerenciará toda a contabilidade do departamento. A equipe deve fazer login em um grande número de contas de cliente na web, cada uma das quais usa informações de login diferentes. Essas informações de login precisam ser compartilhadas com outros funcionários, portanto a confidencialidade é uma questão. O contador decide organizar todos os links da web, nomes de usuário da empresa e senhas no Credential Manager for HP ProtectTools. Ao concluir, o contador implementa o Credential Manager para os funcionários de modo que eles possam trabalhar nas contas da web e nunca terem conhecimento das credenciais de login que estão utilizando.

Drive Encryption for HP ProtectTools

O Drive Encryption é usado para restringir o acesso aos dados em todo o disco rígido do computador ou uma unidade secundária. O Drive Encryption pode também gerenciar unidades autocriptografadas.

Exemplo 1: Um médico quer ter certeza de que apenas ele pode acessar os dados do disco rígido de seu computador. O médico ativa o Drive Encryption, que requer uma autenticação pré--inicialização, antes do login do Windows. Após a configuração, a unidade de disco rígido não pode ser acessada sem uma senha antes da inicialização do sistema operacional. O médico poderia aprimorar ainda mais a segurança da unidade escolhendo criptografar os dados com a opção SED (unidade autocriptografada).

O Embedded Security for HP ProtectTools e o Drive Encryption for HP ProtectTools não permitem o acesso aos dados criptografados, mesmo quando a unidade é removida, porque ambos são vinculados à placa-mãe original.

Exemplo 2: O administrador de um hospital quer garantir que apenas médicos e o pessoal autorizado possam acessar quaisquer dados em seu computador local, sem compartilhar suas senhas pessoais. O departamento de TI adiciona o administrador, médicos e todo o pessoal autorizado como usuários do Drive Encryption. Agora, apenas o pessoal autorizado pode inicializar o computador ou domínio utilizando o nome de usuário e a senha pessoal.

File Sanitizer for HP ProtectTools

O File Sanitizer for HP ProtectTools é usado para excluir permanentemente os dados, incluindo atividades do navegador da Internet, arquivos temporários, dados excluídos anteriormente ou quaisquer outras informações. O File Sanitizer pode ser configurado de modo que seja executado de forma manual ou automática em uma programação definida pelo usuário.

Exemplo 1: Um procurador lida frequentemente com informações sensíveis dos clientes e quer garantir que os dados nos arquivos excluídos não possam ser recuperados. O procurador usa o File Sanitizer para “fragmentar” arquivos excluídos de modo que seja quase impossível recuperá-los.

Normalmente, quando o Windows exclui dados, ele não apaga realmente os dados da unidade de disco rígido. Em vez disso, ele marca os setores do disco rígido como disponíveis para uso futuro. Até que os dados sejam sobrescritos, eles podem ser facilmente recuperados utilizando-se ferramentas comuns disponíveis na Internet. O File Sanitizer sobrescreve os setores com dados aleatórios (várias vezes quando necessário), tornando, desse modo, os dados excluídos ilegíveis e irrecuperáveis.

Exemplo 2: Uma pesquisadora quer fragmentar automaticamente dados excluídos, arquivos temporários, atividades do navegador, entre outros, quando ela fizer o logoff. Ela usa o File Sanitizer para programar a “fragmentação”, portanto pode selecionar os arquivos comuns ou quaisquer arquivos personalizados para serem removidos automaticamente de forma permanente.

Device Access Manager for HP ProtectTools

O Device Access Manager for HP ProtectTools pode ser usado para bloquear o acesso não autorizado a unidades flash USB, nas quais dados poderiam ser copiados. Ele também pode restringir o acesso a unidades de CD/DVD, controlar dispositivos USB, conexões de rede, entre outros. Um administrador pode também programar quando e por quanto tempo as unidades podem ser acessadas. Um exemplo poderia ser uma situação em que fornecedores externos precisam acessar os computadores da empresa, mas não devem ser capazes de copiar os dados para uma unidade USB. O Device Access Manager for HP ProtectTools permite a um administrador restringir e gerenciar o acesso ao hardware.

Exemplo 1: O gerente de uma empresa de suprimentos médicos frequentemente trabalha com registros médicos pessoais juntamente com informações de sua empresa. Os funcionários precisam acessar esses dados; no entanto, é extremamente importante que os dados não sejam retirados do computador por uma unidade USB ou qualquer outra mídia de armazenamento externo. A rede é protegida, mas os computadores possuem gravadores de CD e portas USB que poderiam permitir

que os dados fossem copiados ou roubados. O gerente usa o Device Access Manager para desativar as portas USB e os gravadores de CD de modo que não possam ser utilizados. Embora as portas USB estejam bloqueadas, mouses e teclados continuarão a funcionar.

Exemplo 2: Uma empresa de seguros não quer que seus funcionários instalem ou carreguem softwares ou dados pessoais de casa. Alguns funcionários precisam acessar a porta USB em todos os computadores. O gerente de TI usa o Device Access Manager para permitir o acesso de alguns funcionários, ao mesmo tempo que bloqueia o acesso externo para outros.

Privacy Manager for HP ProtectTools

O Privacy Manager for HP ProtectTools é usado quando as comunicações por e-mail na Internet precisam ser protegidas. O usuário pode criar e enviar e-mails que podem ser abertos somente por um destinatário autenticado. Com o Privacy Manager, as informações não podem ser comprometidas ou interceptadas por um impostor.

Exemplo 1: Um corretor da bolsa de valores quer ter certeza de que seus e-mails sigam apenas para clientes específicos e que ninguém possa falsificar a conta de e-mail e interceptá-los. O corretor registra a si mesmo e seus clientes com o Privacy Manager. O Privacy Manager emite um Certificado de Autenticação (CA) para cada usuário. Utilizando essa ferramenta, o corretor da bolsa de valores e seus clientes devem fazer a autenticação antes de trocar algum e-mail.

O Privacy Manager for HP ProtectTools facilita o envio e o recebimento de e-mails em que o destinatário foi verificado e autenticado. O serviço de e-mail também pode ser criptografado. O processo de criptografia é semelhante ao utilizado em compras com cartão de crédito pela Internet.

Exemplo 2: Um CEO quer garantir que apenas os membros da diretoria possam visualizar as informações que ele envia por e-mail. O CEO usa a opção de criptografar e-mails enviados e recebidos de diretores. Um Certificado de Autenticação do Privacy Manager permite ao CEO e aos diretores ter uma cópia da chave de criptografia para que apenas eles possam decodificar o e-mail confidencial.

Computrace for HP ProtectTools (anteriormente LoJack Pro)

O Computrace for HP ProtectTools (adquirido separadamente) é um serviço que rastreia a localização de um computador roubado sempre que o usuário acessar a Internet.

Exemplo 1: Um diretor de escola instruiu ao departamento de TI que rastreasse todos os computadores da escola. Após a realização do inventário dos computadores, o administrador de TI registrou todos os computadores com o Computrace de modo que poderiam ser rastreados caso algum dia fossem roubados. Recentemente, a escola verificou que estavam faltando vários computadores, então o administrador de TI alertou as autoridades e os oficiais do Computrace. Os computadores foram localizados e devolvidos à escola pelas autoridades.

O Computrace for HP ProtectTools pode ajudar também a gerenciar e localizar computadores remotamente, bem como monitorar a utilização e os aplicativos do computador.

Exemplo 2: Uma imobiliária precisa gerenciar e atualizar computadores em todo o mundo. Eles usam o Computrace para monitorar e atualizar os computadores sem precisar enviar uma pessoa de TI para cada computador.

Embedded Security for HP ProtectTools (somente em determinados modelos)

O Embedded Security for HP ProtectTools oferece a capacidade de criar uma unidade pessoal protegida. Essa capacidade permite ao usuário criar uma partição de unidade virtual no PC que fica

completamente oculta até ser acessada. O Embedded Security pode ser usado em qualquer lugar em que os dados precisem ser secretamente protegidos, enquanto o restante dos dados não é criptografado.

Exemplo 1: Um gerente de armazém tem um computador que vários trabalhadores acessam esporadicamente durante o dia. O gerente quer criptografar e ocultar dados confidenciais do armazém existentes no computador. Ele quer que os dados estejam tão protegidos que mesmo se alguém roubar a unidade de disco rígido, não possa decodificar os dados nem lê-los. O gerente de armazém decide ativar o Embedded Security e mover os dados confidenciais para a unidade pessoal protegida. O gerente pode inserir uma senha e acessar os dados confidenciais exatamente como em outra unidade de disco rígido. Ao fazer logoff ou reiniciar a unidade pessoal protegida, ela não pode ser vista ou aberta sem a senha correta. Os trabalhadores nunca veem os dados confidenciais quando acessam o computador.

O Embedded Security guarda as chaves de criptografia dentro de um chip de hardware TPM (Trusted Platform Module) localizado na placa-mãe. Trata-se da única ferramenta de criptografia que atende aos requisitos mínimos de resistência a ataques de senha quando alguém tenta adivinhar a senha de criptografia. O Embedded Security também criptografa a unidade inteira e o e-mail.

Exemplo 2: Uma corretora da bolsa de valores quer transportar dados extremamente sensíveis para outro computador usando uma unidade portátil. Ela quer ter certeza de que apenas aqueles dois computadores possam abrir a unidade, mesmo se a senha ficar comprometida. A corretora usa a migração do Embedded Security TPM para permitir que um segundo computador tenha as chaves de criptografia necessárias para decodificar os dados. Durante o processo de transporte, mesmo com a senha, apenas os dois computadores físicos podem decodificar os dados.

Alcançar 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

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 pré-inicialização, se ativado, ajuda a impedir o acesso ao sistema operacional. Consulte os seguintes capítulos:
  - Security Manager for HP ProtectTools
  - Embedded Security for HP ProtectTools
  - Drive Encryption for HP ProtectTools
- O recurso Personal Secure Drive (Unidade pessoal protegida), fornecido pelo módulo Embedded Security for HP ProtectTools, criptografa dados sensíveis para ajudar a garantir que eles não possam ser acessados sem autenticação. Consulte o seguinte capítulo:
  - Embedded Security for HP ProtectTools
- O Computrace pode rastrear a localização do computador após um roubo. Consulte o seguinte capítulo:
  - Computrace for HP ProtectTools

Restrição de acesso a dados importantes

Suponha que um auditor de contrato esteja trabalhando no local e tenha acesso concedido ao computador para rever dados financeiros sensíveis; você pode não querer que o auditor seja capaz de imprimir os arquivos ou salvá-los em um dispositivo gravável, como um CD. O seguinte recurso ajuda a restringir o acesso a dados:

- O Device Access Manager for HP ProtectTools permite aos gerentes de TI restringir o acesso a dispositivos graváveis para que informações sensíveis 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 computador comercial não protegido apresenta um risco muito real aos recursos da rede corporativa, como informações sobre serviços financeiros, sobre um executivo

ou sobre a equipe de P&D, e informações privadas como registros de pacientes ou registros financeiros pessoais. Os seguintes recursos ajudam a impedir o acesso não autorizado:

- O recurso de autenticação pré-inicialização, se ativado, ajuda a impedir o acesso ao sistema operacional. Consulte os seguintes capítulos:
  - Password Manager for HP ProtectTools
  - Embedded Security for HP ProtectTools
  - Drive Encryption for HP ProtectTools
- O Password Manager 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 aos gerentes de TI restringir o acesso a dispositivos graváveis, para que informações sensíveis não possam ser copiadas da unidade de disco rígido.
- O File Sanitizer permite a exclusão segura de dados por meio da fragmentação de arquivos e pastas críticos ou da limpeza de ativos excluídos da unidade de disco rígido (gravação sobre dados excluídos, mas ainda recuperáveis).
- O Privacy Manager permite a obtenção de certificados de autoridade ao se utilizar e-mails Microsoft e documentos do Microsoft Office, tornando o processo de envio e salvamento de informações importantes seguro e protegido.

Criação de políticas de senhas fortes

Se a política da empresa colocar em prática a exigência do uso da política de senha forte para diversos aplicativos e bancos de dados baseados em web, o Security Manager fornece um repositório protegido para senhas e a conveniência do login único (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:

- Responsável pela segurança: define o nível de segurança da empresa ou da rede e determina os recursos de segurança a serem implementados, como Drive Encryption ou Embedded Security.

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

- Administrador de TI: aplica e gerencia os recursos de segurança definidos pelo responsável pela segurança. Pode também ativar e desativar alguns recursos. Por exemplo, se o responsável pela segurança tiver decidido implementar smart cards, o administrador de TI pode ativar o modo de senha e de smart card.

- Usuário: utiliza os recursos de segurança. Por exemplo, se o responsável pela segurança e o administrador de TI tiverem ativado smart cards para o sistema, o usuário pode definir o PIN do smart 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 é protegida 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	Definido no seguinte módulo	Função
Senha de login do Windows	Painel de controle do Windows® ou HP ProtectTools Security Manager	Pode ser usada para efetuar login manual e autenticação para acesso a vários recursos do Security Manager.
Senha do Security Manager Backup and Recovery	Security Manager, por usuário individual	Protege o acesso ao arquivo do Security Manager Backup and Recovery.

Senha do HP ProtectTools	Definido no seguinte módulo	Função
PIN do smart card	Credential Manager	Pode ser usado como autenticação multifatores. Pode ser usado como autenticação do Windows. Autentica usuários do Drive Encryption, se o token do smart card estiver selecionado.
Senha do token de recuperação de emergência (Emergency Recovery Token)	Embedded Security, por administrador de TI	Protege o acesso ao Emergency Recovery Token (token de recuperação de emergência), que é um arquivo de backup para o chip de segurança integrado.
Senha de proprietário	Embedded Security, por administrador de TI	Protege o sistema e o chip TPM de acesso não autorizado a todas as funções do proprietário do Embedded Security.
Senha de administrador do BIOS	Configuração do computador, por administrador de TI	Protege o acesso ao utilitário de configuração do computador.

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 para a senha, ou qualquer outra informação pessoal, como data de aniversário, nomes de animal 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.

Credenciais de backup e restauração do HP ProtectTools

Você pode usar o recurso Backup and Recovery do HP ProtectTools para selecionar e fazer backup de dados e configurações de credenciais do HP ProtectTools.

2 Passos iniciais do Assistente de Configuração

O Assistente de Configuração do Security Manager ajuda você a ativar os recursos de segurança disponíveis que são aplicados a todos os usuários deste computador. Também é possível gerenciar esses recursos na página Recursos de segurança do Console Administrativo.

Para configurar os recursos de segurança por meio do Assistente de Configuração do Security Manager:

1. Abra o HP ProtectTools Security Manager pelo ícone de gadget da área de trabalho do HP ProtectTools, na barra lateral do Windows, ou pelo ícone da barra de tarefas na área de notificação, no lado direito da barra de tarefas.

A cor do banner no ícone de gadget da área de trabalho do HP ProtectTools indica uma das seguintes condições:

- Vermelho: o HP ProtectTools não foi configurado ou há uma condição de erro em um dos módulos do ProtectTools.
- Amarelo: verifique se há alterações de configurações que devem ser realizadas na página Status dos aplicativos no Security Manager.
- Azul: o HP ProtectTools foi configurado e está funcionando corretamente.

Uma mensagem é exibida na parte inferior do ícone de gadget para indicar uma das seguintes condições:

- **Configurar agora**: O administrador deve clicar no ícone de gadget para executar o Assistente de Configuração do Security Manager e configurar credenciais de autenticação para o computador.

  O Assistente de Configuração é um aplicativo independente.

- **Registrar agora**: O usuário deve clicar no ícone de gadget para executar o Assistente de Configuração do Security Manager e registrar credenciais de autenticação.

  O Assistente de Passos iniciais é exibido no painel de controle do Security Manager.

- **Verificar agora**: Clique no ícone de gadget para exibir mais detalhes na página Status de aplicativos de segurança.

NOTA: O ícone de gadget da área de trabalho do HP ProtectTools não está disponível no Windows XP.

– ou –

Clique em **Iniciar**, **Todos os Programas**, **HP** e, em seguida, clique em **Console Administrativo do HP ProtectTools**. No painel esquerdo, clique em **Assistente de Configuração**.

2. Leia a tela Bem-vindo e, em seguida, clique em **Avançar**.

3. Confirme sua identidade digitando sua senha do Windows e, em seguida, clique em **Avançar**.

   Se ainda não tiver criado uma senha do Windows, será solicitado que você a crie. A senha do Windows é necessária para impedir que sua conta do Windows seja acessada por pessoas não autorizadas e para que você utilize os recursos do HP ProtectTools Security Manager.

4. Na página SpareKey do assistente, selecione três perguntas de segurança, insira uma resposta para cada pergunta e, em seguida, clique em **Avançar**.

   Você pode selecionar perguntas diferentes ou alterar suas respostas na página SpareKey em **Credential Manager**, no painel de controle do Security Manager.

NOTA: Essa configuração do SpareKey se aplica somente ao usuário administrativo.

5. Ative os recursos de segurança marcando as respectivas caixas de seleção e, em seguida, clique em **Avançar**.

   Quanto mais recursos marcar, mais segurança terá seu computador.

NOTA: As configurações a seguir se aplicam a todos os usuários. Se alguma caixa de seleção não estiver marcada, o Assistente de Configuração não solicitará aos usuários que registrem essas credenciais.

- **Segurança de login do Windows**: Protege suas contas do Windows solicitando o uso de credenciais específicas de acesso.

- **Drive Encryption**: Protege seus dados criptografando suas unidades de disco rígido, tornando assim as informações ilegíveis para pessoas sem a devida autorização.

- **Pre-Boot Security**: Protege seu computador proibindo o acesso de pessoas não autorizadas antes da inicialização do Windows.

NOTA: O Pre-Boot Security não estará disponível se o BIOS não oferecer suporte a ele.

6. O Assistente de Configuração pedirá que você verifique sua identidade.

   Se não houver um leitor de impressões digitais, um smart card ou uma webcam disponível, será solicitado que você insira sua senha do Windows. Após o registro, você poderá usar qualquer credencial registrada para verificar sua identidade sempre que a autenticação for necessária.

NOTA: O registro dessas credenciais se aplica somente ao usuário administrativo.

7. No final da página do assistente, clique em **Concluir**.

   A página inicial do painel de controle do Security Manager será exibida.

3 Console Administrativo do HP ProtectTools Security Manager

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 realizada por meio do recurso Console Administrativo.

Aplicativos adicionais estão disponíveis (somente em determinados modelos) no painel de controle do Security Manager para auxiliar na recuperação do computador se ele for perdido ou roubado.

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

- Ativação ou desativação dos recursos de segurança
- Especificação das credenciais necessárias para a autenticação
- Gerenciamento de usuários do computador
- Ajuste de parâmetros específicos de dispositivos
- Configuração de aplicativos instalados do Security Manager
- Adição de aplicativos ao Security Manager

Abertura 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, clique em **Console Administrativo do HP ProtectTools**.

  – ou –

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

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.

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

– ou –

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

O console é composto pelos seguintes componentes:

- **Página inicial**: Permite que você configure as seguintes opções de segurança:
  - **Aumentar a segurança do sistema**
  - **Exigir autenticação forte**
  - **Gerenciar os usuários do HP ProtectTools**
  - **Veja como é possível gerenciar centralmente o HP ProtectTools**
- **Sistema**: Permite configurar os recursos de segurança e a autenticação a seguir para usuários e dispositivos:
  - **Segurança**
  - **Usuários**
  - **Credenciais**
- **Aplicativos**: Permite que você defina as configurações 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.
- **Gerenciamento Central**: Exibe guias para acesso a soluções adicionais, atualizações de produto e mensagens.
- **Assistente de Configuração**: Ajuda na configuração do HP ProtectTools Security Manager.
- **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.

  ?: Exibe a ajuda do software Console Administrativo. Este ícone se encontra na parte superior direita do quadro da janela, próximo aos ícones minimizar e maximizar.

Configuração do sistema

O grupo **Sistema** é acessado pelo painel do menu, do lado esquerdo do Console Administrativo do HP ProtectTools. É possível usar os aplicativos desse 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.
- **Credenciais**: Gerencie configurações para dispositivos de segurança integrados ou conectados ao computador.

Configuração de autenticação para seu computador

Dentro do aplicativo Autenticação, é possível estabelecer políticas referentes ao acesso ao computador. 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 esquerdo do Console Administrativo, clique em **Segurança**, em seguida, 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, com o objetivo de autenticar um usuário ao efetuar login no Windows:

1. No painel esquerdo do Console Administrativo, clique em **Segurança**, em seguida, clique em **Autenticação**.
2. Na guia **Política de login**, clique na seta para baixo e, em seguida, selecione uma categoria de usuário:
   - **Para administradores deste computador**
   - **Para usuários que não são administradores**
3. Especifique as credenciais de autenticação necessárias para a categoria de usuário selecionada.
4. Escolha se ALGUMA das credenciais especificadas é necessária ou se TODAS as credenciais especificadas são necessárias para autenticar um usuário.
5. Clique em **Aplicar**.

Política de sessão

Para definir as políticas referentes às credenciais necessárias, com o objetivo de acessar os aplicativos HP ProtectTools durante uma sessão do Windows:

1. No painel esquerdo do Console Administrativo, clique em **Segurança**, em seguida clique em **Autenticação**.
2. Na guia **Política de sessão**, clique na seta para baixo e, em seguida, selecione uma categoria de usuário:
   - **Para administradores deste computador**
   - **Para usuários que não são administradores**
3. Clique na seta para baixo e, em seguida, selecione as credenciais de autenticação necessárias para a categoria de usuário selecionada:
   - **Requer uma das credenciais especificadas**

     NOTA: Desmarcar as caixas de seleção para todas as credenciais tem o mesmo efeito de selecionar **Não exigir autenticação**.
   - **Requer todas as credenciais especificadas**
   - **Não exigir autenticação**: Selecionar essa opção limpa todas as credenciais da janela.
4. Clique em **Aplicar**.

Configurações

1. Marque a caixa de seleção para ativar a seguinte configuração, ou desmarque a caixa de seleção para desativar a configuração:

   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.
2. Clique em **Aplicar**.

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 no que se refere às políticas estabelecidas no Security Manager e se registraram ou não as credenciais apropriadas para que estejam em conformidade com tais políticas.

Para gerenciar usuários, selecione dentre as seguintes configurações:

- Para adicionar usuários, clique em **Adicionar**.
- Para excluir um usuário, clique no usuário e, em seguida, em **Excluir**.
- Para configurar credenciais adicionais para o usuário, clique no usuário e, em seguida, clique em **Registrar**.
- Para visualizar as políticas de um usuário específico, selecione o usuário e visualize as políticas na janela inferior.

Credenciais

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

SpareKey

Você pode configurar se deseja ou não permitir a autenticação do SpareKey para o login do Windows, e gerenciar as perguntas de segurança que serão apresentadas aos usuários durante seu registro no SpareKey.

1. Marque a caixa de seleção para ativar ou desmarque-a para desativar o uso da autenticação do SpareKey para o login do Windows.
2. Selecione as perguntas de segurança que serão apresentadas aos usuários durante seu registro no SpareKey. É possível especificar até três perguntas personalizadas ou permitir que os usuários digitem sua própria combinação de palavras.
3. Clique em **Aplicar**.

Impressões digitais

Se um leitor de impressão digital estiver instalado ou conectado ao computador, a página Impressões digitais exibirá as seguintes guias:

- **Registro**: Escolha o número mínimo e máximo de impressões digitais que um usuário pode registrar.

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

  CUIDADO: A remoção de todos os dados do leitor de impressões digitais apaga todos os dados de impressões digitais de todos os usuários, incluindo administradores. Se a política de login exigir apenas impressões digitais, todos os usuários podem ficar impossibilitados de efetuar login no computador.

- **Sensibilidade**: deslize o controle para ajustar a sensibilidade do leitor de impressão digital durante a leitura.

  Se o não reconhecimento de sua impressão digital ocorrer com frequência, talvez seja necessário selecionar uma configuração de sensibilidade mais baixa. Uma configuração alta aumenta a sensibilidade com relação a variações entre as leituras de uma impressão digital, diminuindo, portanto, a possibilidade de um reconhecimento falso. A configuração **Média-Alta** oferece uma boa combinação entre segurança e conveniência.

- **Avançado**: Selecione uma das seguintes opções para configurar o leitor de impressão digital a fim de economizar energia e melhorar a resposta visual:

  - **Otimizado**: O leitor de impressão digital é ativado quando necessário. Pode haver um pequeno atraso quando o leitor for usado pela primeira vez.
  - **Economizar energia**: O leitor de impressão digital demora um pouco mais para responder, mas usa muito menos energia.
  - **Energia total**: O leitor de impressão digital ficará sempre pronto para uso, mas consumirá mais energia.

Smart card

Se um leitor de smart card estiver instalado ou conectado ao computador, a página Smart card exibirá duas guias:

- **Configurações**: configure o computador para que fique automaticamente bloqueado quando um smart card for removido.

NOTA: 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.

- **Administração**: selecione uma das seguintes opções:
  - **Inicializar o smart card**: prepara um smart card para uso com o HP ProtectTools. Se um smart card foi anteriormente inicializado fora do HP ProtectTools (contém um par de chaves assimétricas e um certificado associado), ele não precisará ser inicializado novamente, a menos que seja desejada uma inicialização com um certificado específico.
  - **Alterar o PIN do smart card**: permite que você altere o PIN usado com o smart card.
  - **Apagar apenas os dados do HP ProtectTools**: apagar apenas o certificado do HP ProtectTools criado durante a inicialização do cartão. Nenhum outro dado é apagado do cartão.
  - **Apagar todos os dados do smart card**: apaga todos os dados no smart card especificado. O cartão não pode ser mais usado com o ProtectTools ou qualquer outro aplicativo.

NOTA: Os recursos não suportados pelo seu smart card não estão disponíveis.

▲ Clique em **Aplicar**.

Rosto

Se uma webcam estiver instalada ou conectada ao computador, e se o programa Face Recognition estiver instalado, será possível definir o nível de segurança do Face Recognition para estabelecer equilíbrio entre a facilidade de uso e a dificuldade de burlar a segurança do computador.

1. Clique em **Iniciar**, **Todos os Programas**, **HP** e, em seguida, clique em **Console Administrativo do HP ProtectTools**.
2. Clique em **Credenciais** e, em seguida, clique em **Rosto**.
3. Para mais conveniência, clique no controle deslizante para movê-lo para a esquerda ou, para mais precisão, clique no controle deslizante para movê-lo para a direita.
   - **Conveniência**: Para tornar mais fácil o acesso de usuários registrados em determinadas situações, clique na barra deslizante para movê-la para a posição **Conveniência**.
   - **Equilíbrio**: Para fornecer uma boa contemporização entre segurança e capacidade de uso, ou se você tiver informações confidenciais ou o computador estiver localizado em uma área onde possam ocorrer tentativas de login não autorizado, clique na barra deslizante para movê-la para a posição **Equilíbrio**.
   - **Precisão**: Para tornar mais difícil o acesso de um usuário se houver cenas registradas ou se as condições de iluminação atuais estiverem abaixo do normal e for menos provável

que ocorra uma falsa aceitação, clique na barra deslizante para movê-la para a posição **Precisão**.

4. Clique em **Avançado** e, em seguida, configure a segurança adicional. Para obter mais informações, consulte Configurações avançadas do usuário na página 41.

5. Clique em **Aplicar**.

Configuração de aplicativos

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 painel esquerdo do Console Administrativo, em **Aplicativos**, clique em **Configurações**.
2. Marque a caixa de seleção próxima a uma configuração específica para ativá-la, ou desmarque a caixa de seleção para desativar a configuração.
3. Clique em **Aplicar**.

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 aberto automaticamente após o login.
- **Não abrir automaticamente o Assistente de Passos iniciais para usuários**: Selecione esta opção para impedir que as configurações do usuário sejam abertas 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:

- **Status de aplicativos**: Permite que o status seja exibido para todos os aplicativos.
- **Password Manager**: Ativa o aplicativo Password Manager para todos os usuários do computador.
- **Privacy Manager**: Ativa o aplicativo Privacy Manager para todos os usuários do computador.
- **Ativar o link Gerenciamento Central**: Permite que todos os usuários do computador adicionem aplicativos ao HP ProtectTools Security Manager clicando no botão **Gerenciamento Central**.

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

Gerenciamento Central

Outros aplicativos podem estar disponíveis para adicionar novas ferramentas de gerenciamento ao Security Manager. O administrador do computador pode desativar esse recurso na página Configurações. A página Gerenciamento Central tem duas guias:

- **Soluções de negócios**: Se houver uma conexão de Internet disponível, você poderá acessar o site da DigitalPersona (http://www.digitalpersona.com/) para verificar se há novos aplicativos.
- **Atualizações e mensagens**
  - Para solicitar informações sobre novos aplicativos e atualizações, marque a caixa de seleção **Mantenha-me informado sobre novos aplicativos e atualizações**.
  - Para programar atualizações automáticas, selecione o número de dias.
  - Para verificar se existem atualizações disponíveis, clique em **Verificar agora**.

4 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.
- Registrar uma ou mais cenas para autenticação.
- Definir um smart card para autenticação.
- Fazer backup e restaurar seus dados de programa.
- Adicionar mais aplicativos.

Abertura do Security Manager

É possível abrir o Security Manager de qualquer uma das seguintes maneiras:

- Clique em **Iniciar**, **Todos os Programas**, **HP** e, em seguida, clique 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 ícone de gadget de área de trabalho **HP ProtectTools**.
- Pressione a combinação de teclas de atalho ctrl+tecla de logo do Windows+h para abrir o menu **Links rápidos do Security Manager**.

  Para obter informações sobre a alteração da combinação de tecla de atalho, consulte Configurações na página 36.

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.

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

O painel de controle exibe os 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:
  - **Início**: Gerencie senhas, configure suas credenciais de autenticação ou verifique o status dos aplicativos de segurança.
  - **Status**: Verifique o status dos aplicativos de segurança do HP ProtectTools.

NOTA: Os aplicativos que não estiverem instalados no computador não serão exibidos na lista a seguir.

- **Meus logins**: Gerencie suas credenciais de autenticação com o Password Manager, Credential Manager, senha, SpareKey, Smart Card, rosto e impressão digital.
- **Meus dados**: Gerencie a segurança de seus dados com Drive Encryption e File Sanitizer.
- **Meu computador**: Gerencie a segurança de seu computador com Device Access Manager.
- **Minhas comunicações**: Gerencie a segurança de suas comunicações com Privacy Manager.
- **Administração**: Permite aos administradores acesso às seguintes opções:
  - **Console Administrativo**: Permite que os administradores gerenciem a segurança e os usuários.
  - **Gerenciamento Central**: Permite que os administradores acessem soluções adicionais, atualizações de produto e mensagens.
- **Avançado**: Exibe comandos para acesso a recursos adicionais, incluindo:
  - **Preferências**: Permite que você personalize as configurações do Security Manager.
  - **Backup e Restauração**: Permite que você faça backup ou restaure dados.
  - **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.
- **?**: Exibe a Ajuda do software Security Manager. Este ícone se encontra na parte superior direita da janela, próximo aos ícones minimizar e maximizar.

Status de Aplicativos de Segurança

O status de seus aplicativos de segurança instalados pode ser visualizado em dois locais:

- **Gadget da área de trabalho do HP ProtectTools**

  A cor do banner na parte superior do ícone de gadget HP ProtectTools muda para refletir o status de segurança geral de seus aplicativos de segurança instalados.

  - **Vermelho** — Advertência
  - **Amarelo** — Atenção: não configurado
  - **Azul** — OK

  Uma mensagem é exibida na parte inferior do ícone de gadget para indicar uma das seguintes condições:

  - **Configurar agora**: O administrador deve clicar no ícone de gadget para executar o Assistente de Configuração do Security Manager e configurar credenciais de autenticação para o computador.

    O Assistente de Configuração é um aplicativo independente.

  - **Registrar agora**: O usuário deve clicar no ícone de gadget para executar o Assistente de Configuração do Security Manager e registrar credenciais de autenticação.

    O Assistente de Passos iniciais é exibido no painel de controle do Security Manager.

  - **Verificar agora**: Clique no ícone de gadget para exibir mais detalhes na página Status de aplicativos de segurança.

- **Página Status de aplicativos de segurança**: Clique em **Status** no painel de controle do Security Manager para exibir o status geral de seus aplicativos de segurança instalados e o status específico de cada aplicativo.

Meus logins

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

- **Password Manager**: Cria e gerencia Links rápidos, que permitem que você abra e faça login em vários sites da web e programas por meio de autenticação com sua senha do Windows, impressão digital ou smart card.
- **Credential Manager**: Fornece um meio de alterar sua senha do Windows, registrar impressões digitais ou configurar um smart card com facilidade.

Os administradores podem adicionar aplicativos clicando em **Administração** e, em seguida, clicando em **Gerenciamento Central** no canto inferior esquerdo do painel de controle.

Password Manager

Fazer login no Windows, em sites da web e em aplicativos é mais fácil e mais seguro com o Password Manager. 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 Password Manager 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.

O ícone do **Gerenciador de Senhas** é exibido no canto superior esquerdo de uma página da Web ou tela de login de aplicativo. Quando um login ainda não tiver sido criado para o site da Web ou aplicativo, um sinal de adição (+) será exibido no ícone.

▲ Clique no ícone do **Password Manager** 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 Password Manager**: Permite que você adicione um login para a tela de login atual.
- **Abrir Password Manager**: Abre o Password Manager.
- **Configurações do ícone**: Permite que você especifique as condições em que o ícone do **Password Manager** é exibido.
- **Ajuda**: Exibe a Ajuda do software Security Manager.

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 login**: Permite que você adicione uma conta a um login.
- **Abrir Password Manager**: Abre o Password Manager.
- **Ajuda**: Exibe a Ajuda do software Security Manager.

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 Password Manager 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 Password Manager 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 **Password Manager** e, a seguir, clique em uma das seguintes opções, de acordo com a tela de login, se de um site da web ou de um programa:
   - Para um site da web, clique em **Adicionar [nome do domínio] ao Password Manager**.
   - Para um programa, clique em **Adicionar esta tela de login ao Password Manager**.
3. Digite seus dados de login. Os campos de login na tela, bem como 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** na guia **Password Manager**. Algumas opções dependem dos dispositivos de segurança conectados ao computador. Por exemplo, o uso do atalho ctrl+tecla de logo do Windows+h, a leitura de sua impressão digital e a inserção de um smart card.
   a. Para preencher um campo de login com uma das escolhas pré-formatadas, clique nas setas à direita do campo.
   b. Para visualizar a senha para este login, clique em **Exibir senha**.
   c. Para que os campos de login sejam preenchidos, mas não enviados, desmarque a caixa de seleção **Enviar dados de login automaticamente**.
   d. Para ativar a segurança VeriSign VIP, marque a caixa de seleção **Eu quero segurança VIP neste site**.

      Essa opção é exibida somente para sites onde VeriSign Identity Protection (VIP) está disponível. Quando suportado pelo site, você também pode escolher que o VIP Security Code seja preenchido automaticamente em conjunto com seu método de autenticação costumeiro.

e. Clique em **OK**, clique no método de autenticação que deseja usar (impressões digitais, senha ou rosto) e, em seguida, faça o login utilizando o método de autenticação selecionado.

   O sinal de adição será removido do ícone do **Password Manager** a fim de avisar que o login foi criado.

f. Se o Password Manager não detectar os campos de login, clique em **Mais campos**.

   - Marque a caixa de seleção de cada campo exigido para o login ou desmarque a caixa de seleção de todos os campos que não são obrigatórios para o login.
   - Se o Password Manager não detectar todos os campos de login, será exibida uma mensagem perguntando se você deseja continuar. Clique em **Sim**.
   - Será exibida uma caixa de diálogo com seus campos de login preenchidos. Clique no ícone de cada campo e arraste-o para o campo de login apropriado e, em seguida, clique no botão para entrar no site da web.

     NOTA: Após o uso do modo manual para inserção de dados de login de um site, você deve continuar a utilizar esse método para efetuar o login no mesmo site da web posteriormente.

     NOTA: O modo manual de inserção de dados de login está disponível somente para o Internet Explorer 8.

   - Clique em **Fechar**.

Toda vez que você acessar aquele site da web ou abrir aquele programa, o ícone do **Password Manager** será exibido no canto superior esquerdo de um site da web ou tela de login de aplicativo, indicando que você pode usar suas credenciais registradas para efetuar 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 **Password Manager** 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 Password Manager**.
3. Edite suas informações de login.

   - Para selecionar um campo de login **Nome de usuário** com uma das escolhas pré-formatadas, clique na seta para baixo à direita do campo.
   - Para selecionar um campo de login **Senha** com uma das escolhas pré-formatadas, clique na seta para baixo à direita do campo.
   - Para ativar a segurança VeriSign VIP, marque a caixa de seleção **Eu quero segurança VIP neste site**.

Essa opção é exibida somente para sites onde a segurança VeriSign VIP está disponível. Quando suportado pelo site, você também pode escolher que o VIP Security Code seja preenchido automaticamente em conjunto com seu método de autenticação costumeiro.

- Para adicionar outros campos da tela ao seu login, clique em **Mais campos**.
- Para visualizar a senha para este login, clique em **Exibir senha**.
- Para que os campos de login sejam preenchidos, mas não enviados, desmarque a caixa de seleção **Enviar dados de login automaticamente**.

4. Clique em **OK**.

Utilização do menu Logins

O Password Manager 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 Password Manager, para abrir a tela de login e, em seguida, preencha seus dados de login.

Quando um login é criado, ele é automaticamente adicionado ao menu **Logins** do Password Manager.

Para exibir o menu **Logins**:

1. Pressione a combinação de teclas de atalho do **Password Manager** (ctrl+tecla de logo do Windows+h é a configuração de fábrica). Para alterar a combinação de tecla de atalho, no painel de controle do Security Manager, clique em **Password Manager** e depois em **Configurações**.
2. Deslize o dedo para fornecer sua impressão digital (em computadores com leitor de impressão digital integrado ou conectado) ou insira sua senha do Windows.

Organização de logins em categorias

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

Para adicionar uma categoria:

1. No painel de controle do Security Manager, clique em **Password Manager**.
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. Arraste o login para dentro da lista de categorias. As categorias serão realçadas quando você posicionar o ponteiro do 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 Password Manager facilita o gerenciamento de suas 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 **Password Manager** e, a seguir, na guia **Gerenciar**.

- **Adicionar um login**: Clique em **Adicionar login** e siga as instruções na tela.
- **Seus logins**: Clique em um login existente, selecione uma das opções a seguir e depois siga as instruções na tela:
  - **Abrir**: Abra um site da web ou programa para o qual você possui um login existente.
  - **Adicionar**: Adicione um login. Para obter mais informações, consulte Adição de logins na página 31.
  - **Editar**: Edite um login. Para obter mais informações, consulte Edição de logins na página 32.
  - **Excluir**: Exclui um site da web ou programa para o qual você possui um login existente.
- **Adicionar categoria**: Clique em **Adicionar categoria** e siga as instruções na tela. Para obter mais informações, consulte Organização de logins em categorias na página 33.

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 **Password Manager** para exibir seu menu de contexto.
3. Clique em **Adicionar login** e 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 Password Manager 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 Password Manager

O Password Manager 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 **Password Manager** com um sinal de adição (+).

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

   - **Sugerir a adição de logins para telas de login**: Clique nesta opção para que o Password Manager 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**: Marque essa caixa de seleção para que o Password Manager não solicite novamente que você adicione um login para esta tela de login.

     Para adicionar um login para uma tela que foi excluída anteriormente:

     ◦ Enquanto a página de login de site da web ou de programa excluída anteriormente estiver exibida, abra o painel de controle do Security Manager e clique em **Password Manager**.

     ◦ Clique em **Adicionar login**.

       A caixa de diálogo Adicionar login é exibida com a tela de login do site da web ou programa listado no campo **Tela atual**.

     ◦ Clique em **Continuar**.

       A tela Adicionar login ao Password Manager é exibida.

     ◦ Siga as instruções na tela. Para obter mais informações, consulte Adição de logins na página 31.

     ◦ O ícone do **Password Manager** será exibido sempre que esta tela de login de site da web ou programa for aberta.

2. Para desativar a opção de exibição de um aviso para adicionar logins para telas de login, marque a caixa de seleção.

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

VeriSign Identity Protection (VIP)

É possível criar tokens do VeriSign VIP Access para uso com sites da web habilitados para VeriSign VIP. Esses tokens são usados pelo Password Manager para criar logins automáticos que incorporam o uso de tokens arrastados e soltos em telas de login habilitadas para VeriSign VIP ou inseridos manualmente em campos específicos.

Você pode ativar o VeriSign VIP e criar um token a partir do painel de controle do Security Manager ou em qualquer site da web habilitado para VeriSign VIP. Para usar o token, você deve registrá-lo em cada site da web no qual será usado.

Após o registro e primeiro uso de um token, ele pode (opcionalmente) ser anexado e enviado com suas credenciais de login normais. Para sites que não permitem anexar o token, você pode arrastar e soltar o token ou inserir manualmente as informações do token.

Para ativar o VeriSign VIP e criar um token VeriSign VIP a partir do painel de controle do Security Manager:

1. Abra o painel de controle do Security Manager. Para obter mais informações, consulte Abertura do Security Manager na página 27.
2. Clique em **Password Manager** e, em seguida, clique em **VIP**.
3. Clique em **Obter VIP**.

   Um token VeriSign VIP é criado e exibido na página VeriSign VIP. Agora, o token será exibido sempre que você acessar essa página.

Para ativar o VeriSign VIP e criar um token VeriSign VIP a partir de um site da web:

1. O Password Manager alerta que você está acessando um site da web habilitado para VeriSign VIP.
2. Crie um login para a tela. Para obter mais informações, consulte Adição de logins na página 31.
3. Na caixa de diálogo Criar login, selecione **Eu quero proteção de conta adicional com VIP**.

Para registrar o token VeriSign VIP a partir de um site da web:

1. Efetue login no site da web habilitado para VeriSign VIP manualmente ou com um login do Password Manager.
2. Clique no balão VeriSign VIP exibido para criar um login para este site.
3. Na caixa de diálogo Adicionar login ao Password Manager, selecione **Eu quero segurança VIP neste site**.

   Essa opção é exibida somente para sites em que a segurança VeriSign VIP está disponível. Quando suportado pelo site, você também pode optar para que o VIP Security Code seja preenchido automaticamente juntamente com seu método de autenticação de costume.

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 **Password Manager** 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 Password Manager com ctrl+win+h**: O atalho-padrão que abre o menu de **Links rápidos do Password Manager** é ctrl+tecla de logo do Windows+h. Para alterar o atalho, clique nessa 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.

Credential Manager

Suas credenciais do Security Manager são usadas para confirmar que você é realmente você. O administrador 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. As credenciais suportadas, os requisitos e o status atual são exibidos quando você clica em **Credential Manager** em **Meus logins**, e pode incluir os seguintes itens:

- Senha
- SpareKey
- Impressões digitais
- Smart Card
- Rosto

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

Alteração da sua 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 **Credential Manager** e, em seguida, clique em **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 sua SpareKey

A SpareKey permite acessar o computador (em plataformas suportadas) respondendo a três perguntas a partir de uma lista definida pelo administrador.

O HP ProtectTools Security Manager solicita a definição de sua SpareKey durante a configuração inicial no Assistente de Passos iniciais.

Para definir sua SpareKey:

1. Na página SpareKey do assistente, selecione três perguntas e, em seguida, insira uma resposta para cada pergunta.
2. Clique em **Avançar**.

Você pode selecionar perguntas diferentes ou alterar suas respostas na página SpareKey em **Credential Manager**.

Após a definição de sua SpareKey, você pode acessar seu computador usando sua SpareKey a partir de uma tela de login de pré-inicialização ou da tela Bem-vindo do Windows.

Registro de impressões digitais

Se seu computador tiver um leitor de impressão digital integrado ou conectado a ele, o HP ProtectTools Security Manager solicita que você defina ou “registre” suas impressões digitais durante a configuração inicial no Assistente de Passos iniciais. Também é possível registrar suas impressões

digitais na página Impressão digital em **Credential Manager** no painel de controle do Security Manager.

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 escolhido um dedo para registro, será solicitado que você deslize o dedo até que sua impressão digital seja registrada com sucesso. O dedo registrado será realçado em verde no desenho.

3. Você deve registrar pelo menos dois dedos; de preferência o indicador e o médio. Repita as etapas 1 e 2 para registrar outro dedo.

4. Clique em **Avançar** e siga as instruções na tela.

CUIDADO: 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 programa, as alterações realizadas **não** serão salvas.

Configuração de um smart card

É necessário que os administradores inicializem e registrem o smart card antes que ele possa ser usado para autenticação.

Inicialização do smart card

O HP ProtectTools Security Manager oferece suporte a diferentes tipos de smart card. O número e o tipo de caracteres usados como código PIN podem variar. O fabricante do smart card deve fornecer ferramentas para instalar um certificado de segurança e um PIN de gerenciamento que o HP ProtectTools usará em seu algoritmo de segurança.

NOTA: O software ActivIdentity precisa estar instalado.

1. Insira o smart card no leitor.

2. Clique em **Iniciar**, **Todos os Programas** e, em seguida, clique em **Ferramenta de inicialização de PIN do ActivClient**.

3. Insira e confirme um PIN.

4. Clique em **Avançar**.

   O software do smart card fornecerá uma chave de desbloqueio. A maioria dos smart cards sofrerá bloqueio se um PIN for inserido incorretamente 5 vezes. A chave é usada para desbloquear o cartão.

5. Clique em **Iniciar**, **Todos os Programas**, **HP** e, em seguida, clique em **Console Administrativo do HP ProtectTools**.

6. Clique em **Credenciais**, e em seguida clique em **Smart card**.

7. Clique na guia **Administração**.

8. Certifique-se de que a opção **Configurar smart card** esteja selecionada.

9. Insira o PIN, clique em **Aplicar** e siga as instruções na tela.

10. Após o smart card ter sido inicializado com sucesso, é necessário registrá-lo.

Registro do smart card

Após inicializar o smart card, os administradores podem registrá-lo como um método de autenticação usando o Console Administrativo do HP ProtectTools:

1. Em **Gerenciamento Central**, clique em **Assistente de Configuração**.

2. Na página Bem-vindo!, clique em **Avançar** e, em seguida, digite sua senha do Windows.

3. Na página SpareKey, clique em **Pular configuração do SpareKey**, a não ser que você queira atualizar suas informações do SpareKey.

4. Na página Ativar recursos de segurança, clique em **Avançar**.

5. Na página Escolher suas credenciais, certifique-se de que a opção **Configurar smart card** esteja selecionada e, em seguida, clique em **Avançar**.

6. Na página Smart card, insira o PIN e clique em **Avançar**.

7. Clique em **Concluir**.

Os usuários também podem registrar um smart card no Security Manager. Para obter mais informações, consulte a Ajuda do software HP ProtectTools Security Manager.

Configuração do smart card

Se um leitor de smart card estiver instalado ou conectado ao computador, a página Smart card exibirá duas guias:

- **Configurações**: configure o computador para que fique automaticamente bloqueado quando um smart card for removido.

NOTA: 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.

- **Administração**: selecione uma das seguintes opções:

  - **Inicializar o smart card**: prepara um smart card para uso com o HP ProtectTools. Se um smart card foi anteriormente inicializado fora do HP ProtectTools (contém um par de chaves assimétricas e um certificado associado), ele não precisará ser inicializado novamente, a menos que seja desejada uma inicialização com um certificado específico.

  - **Alterar o PIN do smart card**: permite que você altere o PIN usado com o smart card.

  - **Apagar apenas os dados do HP ProtectTools**: apagar apenas o certificado do HP ProtectTools criado durante a inicialização do cartão. Nenhum outro dado é apagado do cartão.

  - **Apagar todos os dados do smart card**: apaga todos os dados no smart card especificado. O cartão não pode ser mais usado com o ProtectTools ou qualquer outro aplicativo.

NOTA: Os recursos não suportados pelo seu smart card não estão disponíveis.

▲ Clique em **Aplicar**.

Registro de cenas para login com rosto

Se seu computador tiver uma webcam integrada ou conectada a ele, o HP ProtectTools Security Manager solicita que você defina ou “registre” suas cenas durante a configuração inicial no Assistente de Passos iniciais. Também é possível registrar cenas na página de login Rosto em **Credential Manager** no painel de controle do Security Manager.

É necessário registrar uma ou mais cenas para utilizar o login com rosto. Após ter efetuado um registro com êxito, você poderá registrar uma nova cena caso esteja tendo dificuldades para fazer o login porque uma ou mais das seguintes condições sofreu alteração:

- Seu rosto tiver mudado significativamente desde o último registro.
- A iluminação for muito diferente de qualquer uma dos registros anteriores.
- Você usou óculos (ou não) durante seu último registro.

NOTA: Caso esteja com dificuldades para registrar cenas, experimente chegar mais perto da webcam.

Para registrar uma cena no Assistente de Passos iniciais:

1. Na página Rosto do assistente, clique em **Avançado** e, em seguida, configure a segurança adicional. Para obter mais informações, consulte Configurações avançadas do usuário na página 41.
2. Clique em **OK**.
3. Clique em **Iniciar**, ou se tiver registrado cenas anteriormente, clique em **Registrar nova cena**.
4. Se não tiver selecionado nenhuma opção de segurança adicional, você será solicitado a selecionar uma opção de segurança adicional. Siga as instruções na tela e clique em **Avançar**. Para obter mais informações, consulte Configurações avançadas do usuário na página 41.
5. Clique no ícone **Câmera** e siga as instruções na tela para registrar sua cena.

   Siga as instruções na tela e certifique-se de olhar sua imagem enquanto as cenas estiverem sendo capturadas.
6. Clique em **Avançar**.
7. Clique em **Concluir**.

Também é possível registrar cenas a partir do painel de controle do Security Manager:

1. Abra o painel de controle do Security Manager. Para obter mais informações, consulte Abertura do Security Manager na página 27.
2. Em **Meus logins**, clique em **Credential Manager** e clique em **Rosto**.
3. Clique em **Avançado** e, em seguida, configure a segurança adicional. Para obter mais informações, consulte Configurações avançadas do usuário na página 41.
4. Clique em **OK**.

5. Clique em **Iniciar**, ou se tiver registrado cenas anteriormente, clique em **Registrar nova cena**.

6. Se não tiver selecionado nenhuma opção de segurança adicional, você será solicitado a selecionar uma opção de segurança adicional. Siga as instruções na tela e clique em **Avançar**. Para obter mais informações, consulte Configurações avançadas do usuário na página 41.

7. Clique no ícone **Câmera** e siga as instruções na tela para registrar sua cena.

   Siga as instruções na tela e certifique-se de olhar sua imagem enquanto as cenas estiverem sendo capturadas.

Para obter mais informações, consulte a Ajuda do software Face Recognition clicando no ícone **?** azul na parte superior direita da página de login Rosto.

Configurações avançadas do usuário

Estas opções também são exibidas na página de Segurança Adicional se nenhuma segurança adicional tiver sido selecionada.

1. Abra o painel de controle do Security Manager. Para obter mais informações, consulte Abertura do Security Manager na página 27.

2. Em **Meus logins**, clique em **Credential Manager** e clique em **Rosto**.

3. Clique em **Avançado** para configurar as seguintes opções de segurança:

   a. **Guia Segurança**: selecione uma das seguintes opções:

      - **Nenhuma segurança adicional**: Selecione esta opção se não quiser incluir segurança adicional para login com rosto.
      - **Usar PIN para segurança adicional**: Selecione esta opção para exigir um PIN específico do usuário para efetuar login com rosto.
        - Clique em **Criar PIN**.
        - Digite sua senha do Windows.
        - Insira o novo PIN e, em seguida, confirme o novo PIN inserindo-o novamente.

          Após a criação do PIN, você pode selecionar usando as seguintes opções: **Alterar**, **Redefinir** ou **Remover um PIN**.
      - **Usar Bluetooth para segurança adicional**: Selecione esta opção para corresponder seu telefone com Bluetooth com o software Face Recognition. No login do Windows, depois da autenticação do seu rosto, o Face Recognition também verifica a presença

de telefone Bluetooth para correspondência. Se o telefone estiver presente (com Bluetooth ativado), então você poderá efetuar login no Windows.

- Certifique-se de que o Bluetooth esteja ativado no computador e no telefone.

  Se não houver um telefone com Bluetooth presente, você será solicitado a ativar o telefone Bluetooth para correspondência e reiniciar o processo de login. Após 30 segundos, a janela de login do Face Recognition é pausada. Para iniciar o processo de login, clique no ícone **Câmera**. Se o telefone com Bluetooth não estiver presente, você pode usar sua senha normal do Windows para efetuar o login.

- Clique em **Adicionar**.

- Quando seu dispositivo Bluetooth for exibido, selecione-o e clique em **Avançar**.

Clique em **OK**.

b. **Guia Outras configurações**: Marque as caixas de seleção para ativar uma ou mais das opções a seguir, ou desmarque para desativar a opção. As configurações a seguir se aplicam somente ao usuário atual.

- **Reproduzir som nos eventos de reconhecimento de rosto**: Reproduz um som quando o login com rosto é bem-sucedido ou ocorre falha.

- **Solicitar atualização de cenas quando houver falha no login**: se o login com rosto não for bem-sucedido, mas você inserir sua senha com êxito, você poderá ser avisado para salvar uma série de imagens e aumentar as possibilidades de um login com rosto bem-sucedido.

- **Solicitar registro de uma nova cena quando houver falha no login**: Se o login com rosto não for bem-sucedido, mas você inserir sua senha com êxito, você poderá ser avisado para registrar uma nova cena para aumentar as possibilidades de um login com rosto bem-sucedido.

Clique em **OK**.

Seu ID card pessoal

Seu ID card identifica você de forma exclusiva como sendo o dono da conta do Windows em questão, além disso exibe seu nome e uma imagem de sua escolha. Ele é mostrado de forma destacada no canto superior esquerdo das páginas do Security Manager.

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. Abra o painel de controle do Security Manager. Para obter mais informações, consulte Abertura do Security Manager na página 27.
2. Clique em ID card no canto superior esquerdo do painel de controle.
3. Clique na caixa que exibe o nome de usuário do Windows para esta conta, digite o novo nome e clique em **Salvar**.

Para mudar a imagem exibida:

1. Abra o painel de controle do Security Manager. Para obter mais informações, consulte Abertura do Security Manager na página 27.
2. Clique em ID card no canto superior esquerdo do painel de controle.
3. Clique em **Escolher imagem**, clique em uma imagem e clique em **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**.

Guia Geral

Aparência: **exibe o ícone na área de notificação da 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.

Guia Impressão digital

NOTA: A guia **Impressão digital** está disponível apenas se o computador tiver um leitor de impressão digital, e o driver correto estiver instalado.

- **Ações rápidas**: use as Ações rápidas para selecionar a tarefa do Security Manager a ser realizada quando você mantiver pressionada uma determinada tecla durante a leitura da sua impressão digital.

  Para atribuir a Ação rápida a uma das teclas listadas, clique em uma opção **(Tecla)+Impressão digital** e, em seguida, selecione uma das tarefas disponíveis no menu.

- **Resposta do leitor de impressões digitais**: exibida apenas quando houver um leitor disponível. Use essa configuração para ajustar a resposta ao informar sua impressão digital no leitor.

  - **Ativar resposta sonora**: o Security Manager reproduzirá uma resposta sonora quando uma impressão digital for lida, reproduzindo sons diferentes para eventos específicos de programas. 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 resposta de qualidade de leitura**

    Para exibir todas as leituras, independentemente da qualidade, marque a caixa de seleção.

    Para exibir apenas as leituras de boa qualidade, desmarque a caixa de seleção.

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. Abra o painel de controle do Security Manager. Para obter mais informações, consulte Abertura do Security Manager na página 27.
2. No painel esquerdo do painel de controle, clique em **Avançado** e depois em **Backup e Restauração**.
3. Clique em **Fazer backup de dados**.
4. Selecione os módulos que você deseja incluir no backup. Na maioria dos casos, você selecionará todos os módulos.
5. Verifique sua identidade.
6. 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.

7. Insira uma senha para proteger o arquivo.
8. Clique em **Concluir**.

Para restaurar seus dados:

1. Abra o painel de controle do Security Manager. Para obter mais informações, consulte Abertura do Security Manager na página 27.
2. No painel esquerdo do painel de controle, clique em **Avançado** e depois em **Backup e Restauração**.
3. Clique em **Restaurar dados**.
4. Selecione o arquivo de armazenamento criado anteriormente. Insira o caminho no campo fornecido ou clique em **Procurar**.
5. Insira a senha usada para proteger o arquivo.
6. Selecione os módulos para os quais você quer restaurar dados. Na maioria dos casos, você selecionará todos os módulos listados.
7. Verificar sua senha do Windows.
8. Clique em **Concluir**.

5 Drive Encryption for HP ProtectTools (somente em determinados modelos)

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 Security Manager permite que os administradores do Windows ativem o Drive Encryption, efetuem backup da chave de criptografia e marquem ou desmarquem unidade(s). Para obter mais informações, consulte a Ajuda do software HP ProtectTools Security Manager.

As seguintes tarefas podem ser executadas com o Drive Encryption:

- Seleção de configurações do Drive Encryption:
  - Ativação de uma senha protegida por TPM
  - Criptografia ou decodificação de unidades individuais ou partições utilizando criptografia por software
  - Criptografia ou decodificação de unidades individuais autocriptografadas utilizando criptografia por hardware
  - Adição de mais segurança desativando o modo de suspensão ou de espera para garantir que a autenticação pré-inicialização do Drive Encryption seja sempre exigida

NOTA: Apenas unidades de disco rígido SATA internas e eSATA externas podem ser criptografadas.

- Criação de chaves de backup
- Recuperação de chave do Drive Encryption
- Ativação da autenticação pré-inicialização do Drive Encryption usando uma senha, impressão digital registrada ou PIN do smart card

Abertura do Drive Encryption

Os administradores podem acessar o Drive Encryption pelo Console Administrativo do HP ProtectTools.

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

Tarefas básicas

Ativação do Drive Encryption para unidades de disco rígido padrão

Unidades de disco rígido padrão são criptografadas utilizando-se criptografia por software. Para ativar o Drive Encryption, siga estas etapas:

1. Use o Assistente de Configuração do HP ProtectTools Security Manager para ativar o Drive Encryption.
2. Siga as instruções apresentadas na tela até que a página **Ativar recursos de segurança** seja exibida, em seguida continue com a etapa 4 abaixo.

– ou –

1. Clique em **Iniciar**, **Todos os Programas**, **HP** e, em seguida, clique em **Console Administrativo do HP ProtectTools**.
2. No painel esquerdo, clique no ícone **+** à esquerda de **Segurança** para exibir as opções disponíveis.
3. Clique em **Recursos**.
4. Marque a caixa de seleção **Drive Encryption** e clique em **Avançar**.

NOTA: Se nenhuma unidade de disco rígido estiver selecionada para criptografia, a autenticação pré-inicialização do Drive Encryption será ativada, mas a(s) unidade(s) não será(ão) criptografada(s).

5. Em **Unidades para criptografar**, marque a caixa de seleção da unidade de disco rígido que deseja criptografar, em seguida clique em **Avançar**.
6. Para fazer backup da chave de criptografia, 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. Um disquete, um memory stick USB, um cartão de memória Secure Digital (SD) ou um MMC pode ser usado para backup.

7. Em **Fazer backup de chaves do Drive Encryption**, marque a caixa de seleção do dispositivo de armazenamento onde a chave de criptografia será salva.
8. Clique em **Avançar**.

NOTA: O computador será reiniciado.

O Drive Encryption foi ativado. A criptografia da unidade pode levar algumas horas, dependendo do tamanho da unidade.

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

Ativação do Drive Encryption para unidades autocriptografadas

Unidades autocriptografadas que atendem à especificação OPAL do Trusted Computing Group para gerenciamento de unidade autocriptografada podem ser criptografadas utilizando-se criptografia por

software ou por hardware. Para ativar o Drive Encryption em unidades autocriptografadas, siga estas etapas:

1. Use o Assistente de Configuração do HP ProtectTools Security Manager para ativar o Drive Encryption.
2. Siga as instruções apresentadas na tela até que a página **Ativar recursos de segurança** seja exibida, em seguida continue com a etapa 4 em “Criptografia por software” ou “Criptografia por hardware” abaixo.

NOTA: Se o computador não tiver uma unidade autocriptografada que atenda à especificação OPAL do Trusted Computing Group para gerenciamento de unidade autocriptografada, a opção de criptografia por hardware não estará disponível, e a criptografia por software será utilizada por padrão.

Se houver uma mistura de unidades autocriptografadas e unidades de disco rígido padrão, a opção de criptografia por hardware não estará disponível, e a criptografia por software será utilizada por padrão.

– ou –

Criptografia por software

1. Clique em **Iniciar**, **Todos os Programas**, **HP** e, em seguida, clique em **Console Administrativo do HP ProtectTools**.
2. No painel esquerdo, clique no ícone **+** à esquerda de **Segurança** para exibir as opções disponíveis.
3. Clique em **Recursos**.
4. Marque a caixa de seleção **Drive Encryption** e clique em **Avançar**.
5. Em **Unidades para criptografar**, marque a caixa de seleção da unidade de disco rígido que deseja criptografar, em seguida clique em **Avançar**.
6. Para fazer backup da chave de criptografia, 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. Um disquete, um memory stick USB, um cartão de memória Secure Digital (SD) ou um MMC pode ser usado para backup.

7. Em **Fazer backup de chaves do Drive Encryption**, marque a caixa de seleção do dispositivo de armazenamento onde a chave de criptografia será salva.
8. Clique em **Aplicar**.

NOTA: O computador será reiniciado.

O Drive Encryption foi ativado. A criptografia da unidade pode levar algumas horas, dependendo do tamanho da unidade.

Criptografia por hardware

1. Clique em **Iniciar**, **Todos os Programas**, **HP** e, em seguida, clique em **Console Administrativo do HP ProtectTools**.
2. No painel esquerdo, clique no ícone **+** à esquerda de **Segurança** para exibir as opções disponíveis.
3. Clique em **Recursos**.
4. Marque a caixa de seleção **Drive Encryption** e clique em **Avançar**.

NOTA: Se for exibida apenas uma unidade, a caixa de seleção da unidade será automaticamente marcada e ficará esmaecida.

Se for exibida mais de uma unidade, as caixas de seleção das unidades serão automaticamente marcadas, mas não ficarão esmaecidas.

O botão **Avançar** não estará disponível até que pelo menos uma unidade tenha sido selecionada.

5. Certifique-se de que a caixa de seleção **Usar criptografia de unidade de hardware** esteja selecionada na parte inferior da tela.
6. Em **Unidades para criptografar**, marque a caixa de seleção da unidade de disco rígido que deseja criptografar, em seguida clique em **Avançar**.
7. Para fazer backup da chave de criptografia, 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. Um disquete, um memory stick USB, um cartão de memória Secure Digital (SD) ou um MMC pode ser usado para backup.

8. Em **Fazer backup de chaves do Drive Encryption**, marque a caixa de seleção do dispositivo de armazenamento onde a chave de criptografia será salva.
9. Clique em **Aplicar**.

NOTA: O computador precisará ser reiniciado.

O Drive Encryption foi ativado. A criptografia da unidade pode demorar vários minutos.

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

Desativação do Drive Encryption

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

▲ Siga as instruções apresentadas na tela até que a página **Ativar recursos de segurança** seja exibida, em seguida continue com a etapa 4 abaixo.

– ou –

1. Clique em **Iniciar**, **Todos os Programas**, **HP** e, em seguida, clique em **Console Administrativo do HP ProtectTools**.
2. No painel esquerdo, clique no ícone **+** à esquerda de **Segurança** para exibir as opções disponíveis.
3. Clique em **Recursos**.
4. Desmarque a caixa de seleção **Drive Encryption** e clique em **Avançar**.

   A desativação do Drive Encryption é iniciada.

NOTA: Se a criptografia por software foi utilizada, a decodificação será iniciada. Isso pode levar algumas horas, dependendo do tamanho da unidade. Quando a decodificação for concluída, o Drive Encryption será desativado.

Se a criptografia por hardware foi utilizada, a unidade será descriptografada instantaneamente, o que pode demorar alguns minutos, e então o Drive Encryption será desativado.

Após a unidade ser desativada, o computador precisará ser reiniciado.

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: Em um cenário de criptografia por hardware, certifique-se de que o computador esteja desligado. Se o computador não estiver desligado e então for reiniciado, a tela de autenticação pré--autenticação do Drive Encryption não será exibida.

NOTA: Ao sair do modo de suspensão ou de espera, a autenticação pré-inicialização do Drive Encryption não é exibida para criptografia por software ou por hardware, a menos que isso seja desativado.

Ao sair da hibernação, a autenticação pré-inicialização do Drive Encryption é exibida.

NOTA: Se o administrador do Windows tiver ativado a Segurança pré-inicialização no HP ProtectTools Security Manager, é possível fazer o login no computador imediatamente após este ser ligado, em vez de fazê-lo na tela de login do Drive Encryption.

1. Clique em seu nome de usuário, em seguida insira sua senha do Windows ou PIN do smart card, ou forneça uma impressão digital registrada.

NOTA: Os seguintes smart cards são suportados:

Smart cards

- ActivIdentity 64K V2C Smart Card
- ActivIdentity SIM 48010-B DEC06
- Chave ActivIdentity USB V3.0 ZFG-48001-A

Leitores PCMCIA

- Leitor interno de Express Card 54 SCR3340
- SCR 201
- SCR 243 (também da marca HP)
- ActivCard
- Omnikey 4040
- Cisco

Leitores USB

- ActivCard USB v2
- ActivCard USB v3
- ActivCard USB SCR 3310
- Omnikey Cardman 3121
- Omnikey Cardman 3021
- ACR32
- Terminal de HP Smart Card

2. Clique em **OK**.

NOTA: Se for utilizar uma chave de recuperação para fazer login na tela de login do Drive Encryption, você será solicitado a autenticar sua senha, o PIN do smart card ou a impressão digital registrada na tela de login do Windows.

Proteja seus dados criptografando sua unidade de disco rígido

É altamente recomendado a utilização do Assistente de Configuração do HP ProtectTools Security Manager para proteger seus dados criptografando a unidade de disco rígido:

1. No painel esquerdo, clique no ícone **+** à esquerda de **Drive Encryption** para exibir as opções disponíveis.
2. Clique em **Configurações**.
3. Para unidades criptografadas por software, selecione as partições da unidade a serem criptografadas.

NOTA: Isso também se aplica a um cenário de mistura de unidades, em que uma ou mais unidades de disco rígido padrão e uma ou mais unidades autocriptografadas estão presentes.

– ou –

- Para unidades criptografadas por hardware, selecione a unidade, ou unidades, a ser criptografada. Pelo menos uma unidade deve ser selecionada.

Exibição do status da criptografia

Os usuários podem exibir o status da criptografia pelo HP ProtectTools Security Manager.

NOTA: Os administradores podem alterar o status do Drive Encryption com o Console Administrativo do HP ProtectTools.

1. Abra o HP ProtectTools Security Manager.
2. Em **Meus dados**, clique em **Drive Encryption**.

   Em um cenário de criptografia por software, um dos seguintes códigos de status é exibido em **Status da unidade**:

   - Ativado
   - Desativado
   - Não criptografado
   - Criptografado
   - Criptografando
   - Descriptografando

   Em um cenário de criptografia por hardware, o seguinte código de status é exibido em **Status da unidade**:

   - Criptografado

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

Tarefas avançadas

Gerenciamento do Drive Encryption (tarefa do administrador)

Os administradores podem usar a página Configurações do Drive Encryption para visualizar e alterar o status do Drive Encryption (ativado, inativo ou a criptografia por hardware foi ativada) e visualizar o status da criptografia de todas as unidades de disco rígido do computador.

NOTA: A criptografia por hardware não pode ser alterada na página Configurações.

- Se o status for Desativado, o Drive Encryption ainda não foi ativado pelo administrador do Windows e 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 Ativado, o Drive Encryption foi ativado e configurado. A unidade se encontra em um dos seguintes estados:

Criptografia por software

- Não criptografado
- Criptografado
- Criptografando
- Descriptografando

Criptografia por hardware

- Criptografado

Criptografia ou decodificação de unidades individuais (somente criptografia por software)

Os administradores podem usar a página Configurações para criptografar uma ou mais unidades de disco rígido no computador ou decodificar uma unidade que já foi criptografada.

1. Abra o Console Administrativo do HP ProtectTools.
2. No painel esquerdo, clique no ícone **+** à esquerda de **Drive Encryption** para exibir as opções disponíveis.
3. Clique em **Configurações**.
4. Em **Status da unidade**, marque ou desmarque a caixa de seleção próxima a cada unidade de disco rígido que deseja criptografar ou decodificar, em seguida clique em **Aplicar**.

NOTA: Quando a unidade estiver sendo criptografada ou descriptografada, a barra de progresso exibirá o tempo restante para a conclusão do processo durante a sessão atual.

Se o computador for desligado ou iniciar o modo de suspensão/espera ou hibernação durante o processo de criptografia e, em seguida, reiniciar, o tempo restante na barra de progresso retorna ao início, mas a criptografia real é retomada do ponto em que foi interrompida. A barra de progresso, exibida em porcentagem, e o tempo restante mudam mais rapidamente para refletir o progresso anterior.

NOTA: Partições dinâmicas não são suportadas. Se uma partição for exibida como disponível, mas não puder ser criptografada quando selecionada, a partição é dinâmica. Uma partição dinâmica é resultado do encolhimento de uma partição para a criação de uma nova partição no Gerenciamento de Disco.

É exibido um aviso caso alguma partição for convertida para uma partição dinâmica.

Backup e Restauração (tarefa do administrador)

Quando o Drive Encryption está ativado, os administradores podem usar a página Backup da chave de criptografia para fazer o backup de chaves de criptografia em uma mídia removível e para executar uma recuperação.

Fazer backup de chaves de criptografia

Os administradores podem 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 que contém o backup da chave em um local seguro, pois se você esquecer sua senha, perder seu smart card ou não tiver uma impressão digital registrada, esse dispositivo fornecerá seu único acesso à unidade de disco rígido.

1. Abra o Console Administrativo do HP ProtectTools.
2. No painel esquerdo, clique no ícone **+** à esquerda de **Drive Encryption** para exibir as opções disponíveis.
3. Clique em **Backup da chave de criptografia**.
4. Insira o dispositivo de armazenamento a ser usado para backup da chave de criptografia.
5. Em **Unidade**, marque a caixa de seleção do dispositivo onde deseja fazer backup da chave de criptografia.
6. Clique em **Backup das chaves**.
7. Leia as informações na página exibida, em seguida clique em **Avançar**. A chave de criptografia é salva no dispositivo de armazenamento selecionado.

Recuperação de chaves de criptografia

Os administradores podem recuperar uma chave de criptografia a partir do dispositivo de armazenamento removível em que foi salva anteriormente:

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 **Opções**.
4. 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.

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

O Privacy Manager for HP ProtectTools permite que você utilize métodos avançados de login de segurança (autenticação) para verificar a fonte, a integridade e a segurança das comunicações ao usar e-mail ou documentos do Microsoft® Office.

O Privacy Manager tira proveito da infraestrutura de segurança fornecida pelo HP ProtectTools Security Manager, que inclui os seguintes métodos de login:

- Autenticação por impressão digital
- Senha do Windows®
- Smart card
- Face Recognition

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

Abertura do Privacy Manager

Para abrir o Privacy Manager:

- Para acessar os recursos específicos do Outlook no Microsoft Outlook, clique em **Enviar com segurança**, no grupo **Privacidade** da guia **Mensagem**.
- Para acessar a maioria dos recursos nos documentos do Microsoft Office, clique em **Assinar e codificar**, no grupo **Privacidade** da guia **Início**.
- Para acessar recursos adicionais, acesse o painel de controle do HP ProtectTools Security Manager.
  - Clique em **Iniciar**, depois em **Todos os Programas**, a seguir em **HP**, depois em **HP ProtectTools Security Manager**, e por fim clique em **Privacy Manager**.

    – ou –
  - Clique no ícone de gadget da área de trabalho do **HP ProtectTools**.

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

Procedimentos de configuração

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). A PKI exige que os usuários obtenham chaves de criptografia e um Certificado do Privacy Manager emitido por uma autoridade de certificação (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.

O Gerenciador de Certificados permite executar as seguintes tarefas:

- Solicitação de um Certificado do Privacy Manager na página 59
- Obtenção de um Certificado Corporativo pré-assinado do Privacy Manager na página 60
- Configuração de um certificado-padrão do Privacy Manager na página 61
- Importação de um certificado de terceiros na página 60
- Visualização dos detalhes do Certificado do Privacy Manager na página 61
- Renovação de um Certificado do Privacy Manager na página 61
- Configuração de um certificado-padrão do Privacy Manager na página 61
- Renovação de um Certificado do Privacy Manager na página 62
- Restauração de um Certificado do Privacy Manager na página 62
- Revogação de seu Certificado do Privacy Manager na página 63

Solicitação de um Certificado do Privacy Manager

Antes de ser possível usar os recursos do Privacy Manager, você deve 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 deve ser configurado como uma conta no Microsoft Outlook do mesmo computador do qual foi solicitado o Certificado do Privacy Manager.

1. Abra o Privacy Manager e clique em **Certificados**.
2. Clique em **Solicitar um Certificado do Privacy Manager**.
3. Na página de boas-vindas, leia o texto e, em seguida, clique em **Avançar**.
4. Leia o Contrato de Licença na página respectiva.
5. Certifique-se de que a caixa de seleção próxima a **Marque aqui para aceitar os termos deste acordo de licença** esteja selecionada e clique em **Avançar**.
6. Na página Detalhes de seu certificado, insira as informações exigidas e, em seguida, clique em **Avançar**.
7. Na página Solicitação de certificação aceita, clique em **Concluir**.

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

Obtenção 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**.

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

Para instalar o certificado, consulte Configuração de um Certificado do Privacy Manager na página 60.

Configuração 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 Outlook 2010, 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 ter salvo o arquivo em outro local que não seja a sua unidade de disco rígido e guarde-o em um lugar seguro. Esse 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. Se você quiser iniciar o processo de convite de Contato Confiável, siga as instruções apresentadas na tela começando pela etapa 2 do tópico Adição de Contatos Confiáveis usando os contatos do Microsoft Outlook na página 64.

   – ou –

   Se clicar em **Cancelar**, consulte Gerenciamento de Contatos Confiáveis na página 63 para obter informações sobre a inclusão de um Contato Confiável em um momento posterior.

Importação de um certificado de terceiros

É possível importar um certificado de terceiros no Privacy Manager através do Assistente de Importação de Certificado.

Para usar esse recurso, a configuração **Permitir uso de certificados de terceiros** no Console Administrativo do HP ProtectTools deve ter sido ativada na página Configurações em **Privacy Manager**.

1. Abra o Privacy Manager e clique em **Certificados**.
2. Selecione a guia **Gerenciador de Certificados**, em seguida, clique em **Importar certificados**.

   Este botão não é exibido se a importação de certificados não for permitida.

3. Escolha entre importar um certificado já instalado neste computador ou um certificado armazenado como um arquivo PFX (Personal Information Exchange/PKCS#12), em seguida clique em **Avançar**.

   - Para importar um certificado instalado neste computador, selecione o certificado desejado e, em seguida, clique em **Avançar**.
   - Para selecionar um certificado PFX, clique em **Procurar**, navegue até o local do arquivo PFX, e, em seguida, clique em **Avançar**. Digite a senha do arquivo PFX e clique em **Avançar**.

4. Quando o processo de importação for concluído, clique em **Avançar**.
5. Você terá a opção de fazer backup do certificado importado.

   Recomenda-se fazer backup de seu certificado em outro local que não seja a unidade de disco rígido de seu computador.

Visualização dos detalhes do Certificado do Privacy Manager

1. Abra o Privacy Manager e clique em **Certificados**.
2. Clique em um Certificado do Privacy Manager.
3. Clique em **Detalhes do certificado**.
4. Quando você tiver terminado de visualizar os detalhes, clique em **OK**.

Renovação de um Certificado do Privacy Manager

Quando seu Certificado do Privacy Manager estiver para expirar, você será notificado a renová-lo:

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

NOTA: O processo de renovação do certificado do Privacy Manager não substitui seu certificado antigo do Privacy Manager. É preciso obter um novo Certificado do Privacy Manager e instalá-lo usando os mesmos procedimentos como em Solicitação de um Certificado do Privacy Manager na página 59.

Para certificados corporativos emitidos por sua empresa usando a Autoridade de Certificação da Microsoft, o administrador de Certificados Corporativos deve renovar seu certificado utilizando a mesma chave privada do certificado original, ou emitir para você um novo certificado usando a mesma chave privada.

Configuração de um certificado-padrão do Privacy Manager

Apenas os Certificados do Privacy Manager são visíveis dentro do Privacy Manager, mesmo que certificados adicionais de outras autoridades de certificados estejam instalados em seu computador.

Se você possui mais de um Certificado do Privacy Manager em seu computador instalado dentro do Privacy Manager, é possível definir um como sendo o padrão:

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

NOTA: Você não é obrigado a usar seu Certificado padrão do Privacy Manager. Dentro das diversas funções do Privacy Manager, é possível selecionar para uso qualquer um de seus Certificados do Privacy Manager.

Renovação de um Certificado do Privacy Manager

Se você excluir um Certificado do Privacy Manager, não será possível abrir qualquer arquivo ou visualizar qualquer dado que foi criptografado com esse certificado. Se você excluir acidentalmente um Certificado do Privacy Manager, é possível restaurá-lo usando o arquivo de backup que você criou quando instalou o certificado. Consulte Restauração de um Certificado do Privacy Manager na página 62 para obter mais informações.

Para excluir um Certificado do Privacy Manager:

1. Abra o Privacy Manager e clique em **Certificados**.
2. Clique no Certificado do Privacy Manager que você deseja excluir, 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 seguida, 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**.

Consulte Configuração de um Certificado do Privacy Manager na página 60 ou Backup de Certificados e Contatos Confiáveis do Privacy Manager na página 72 para obter mais informações.

Revogação de seu Certificado do Privacy Manager

Se você sentir que a segurança de seu Certificado do Privacy Manager está em risco, é possível revogar seu próprio certificado:

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

1. Abra o Privacy Manager e clique em **Certificados**.
2. Clique em **Avançado**.
3. Clique no Certificado do Privacy Manager que você deseja revogar, 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 receberá um e-mail de resposta do destinatário do Contato Confiável; em seguida, clique em **Aceitar**.

É possível enviar convites de e-mail para Contato Confiável aos destinatários individuais, ou enviar o convite para todos os contatos em seu catálogo de endereços do Microsoft Outlook.

Consulte as seguintes seções para adicionar Contatos Confiáveis.

NOTA: Para responder a seu convite a fim de se tornarem um Contato Confiável, os destinatários do Contato Confiável devem ter o Privacy Manager instalado em seus computadores ou ter o “alternate client” (cliente alternativo) instalado. Para obter informações sobre a instalação do alternate client, acesse o site da DigitalPersona em http://digitalpersona.com/privacymanager/download.

Acréscimo 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. Insira os endereços de e-mail dos destinatários que você deseja adicionar como Contatos Confiáveis.

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

6. Clique em **Enviar**.

NOTA: Se não tiver obtido um Certificado do Privacy Manager, uma mensagem 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 de um Certificado do Privacy Manager na página 59 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 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.

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 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: Se não tiver obtido um Certificado do Privacy Manager, uma mensagem 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 de um Certificado do Privacy Manager na página 59 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 direito 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 **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 **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 **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 de revogação**.
5. Clique em **Fechar**.

Tarefas básicas

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

- Microsoft Outlook
- Microsoft Office

Utilização do Privacy Manager no Microsoft Outlook

Quando o Privacy Manager é instalado, um botão de privacidade é exibido na barra de ferramentas do Microsoft Outlook, e um botão Enviar com segurança é mostrado na barra de ferramentas de cada mensagem de e-mail do Microsoft Outlook. Quando você clica na seta para baixo perto de **Privacidade** ou **Enviar com segurança**, você pode escolher entre as seguintes opções:

- **Assinar e enviar a mensagem** (apenas o botão Enviar com segurança): Esta opção adiciona uma assinatura digital ao e-mail e envia-o após você autenticar usando o seu método preferido de login de segurança.
- **Selar para Contatos Confiáveis e enviar mensagem** (apenas o botão Enviar com segurança): Esta opção adiciona uma assinatura digital, criptografa o e-mail e envia-o após você autenticar usando o seu método preferido de login de segurança.
- **Convidar contatos**: Esta opção permite que você envie um convite de Contato Confiável. Consulte Acréscimo de um Contato Confiável na página 64 para obter mais informações.
- **Convidar meus contatos do Outlook**: Esta opção permite que você envie um convite de Contato Confiável a todos os contatos do seu catálogo de endereços do Microsoft Outlook. Consulte Adição de Contatos Confiáveis usando os contatos do Microsoft Outlook na página 64 para obter mais informações.
- **Abrir o software Privacy Manager**: As opções Certificados, Contatos Confiáveis e Configurações permitem que você abra o software Privacy Manager para adicionar, visualizar ou alterar as configurações atuais. Consulte Gerenciamento de Certificados do Privacy Manager na página 59, Gerenciamento de Contatos Confiáveis na página 63 ou Configuração do Privacy Manager no Microsoft Outlook na página 66 para obter mais informações.

Configuração do Privacy Manager no 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), em seguida, clique 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 é 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 perto de **Enviar com segurança** (**Privacidade** no Outlook 2003), e depois clique em **Assinar e enviar a mensagem**.
4. Faça a autenticação utilizando o método de login de segurança de sua escolha.

Selagem e envio de uma mensagem de e-mail

Mensagens de e-mail seladas que são digitalmente assinadas e seladas (criptografadas) 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 perto de **Enviar com segurança** (**Privacidade** no Outlook 2003), e depois clique em **Selar para Contatos Confiáveis e enviar a mensagem**.
4. Faça a autenticação utilizando o método de login de segurança de sua escolha.

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. Esta 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

Depois de instalar o seu Certificado do Privacy Manager, um botão Assinar e codificar é exibido no lado direito da barra de ferramentas de todos os documentos do Microsoft Word, Microsoft Excel e Microsoft PowerPoint. Quando você clica na seta para baixo próxima de **Assinar e codificar**, pode escolher entre as seguintes opções:

- **Assinar documento**: Esta opção adiciona sua assinatura digital ao documento.
- **Adicionar linha de assinatura antes de assinar** (apenas no Microsoft Word e Microsoft Excel): Por padrão, uma linha de assinatura é adicionada quando um documento do Microsoft Word ou Microsoft Excel é assinado ou criptografado. Para desativar esta opção, clique em **Adicionar linha de assinatura** para remover a marca de seleção.
- **Criptografar documento**: Esta opção adiciona sua assinatura digital ao documento e o criptografa.
- **Remover criptografia**: Esta opção remove a criptografia do documento.
- **Abrir o software Privacy Manager**: As opções Certificados, Contatos Confiáveis e Configurações permitem que você abra o software Privacy Manager para adicionar, visualizar

ou alterar as configurações atuais. Consulte Gerenciamento de Certificados do Privacy Manager na página 59, Gerenciamento de Contatos Confiáveis na página 63 ou Configuração do Privacy Manager no Microsoft Office na página 68 para obter mais informações.

Configuração do Privacy Manager no Microsoft Office

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

   – ou –

   Na barra de ferramentas de uma mensagem de um documento do Microsoft Office, clique na seta para baixo perto de **Assinar e codificar** e depois clique em **Configurações**.

2. Selecione as ações que deseja configurar, 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. Faça a autenticação utilizando o método de login de segurança de sua escolha.
4. Quando a caixa de diálogo de confirmação for exibida, leia o texto e clique em **OK**.

Se depois 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 clique 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.

Adição 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. No Microsoft Word ou Microsoft Excel, 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 **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. Esta opção vem ativada como padrão.

4. Clique na seta para baixo próxima a **Assinar e codificar** e em seguida clique em **Documento assinado**.
5. Faça a autenticação utilizando o método de login de segurança de sua escolha.

Adição de signatários sugeridos a um documento do Microsoft Word ou Microsoft Excel

É possível adicionar mais de uma linha de assinatura ao seu documento ao apontar signatários sugeridos. Um signatário sugerido é um usuário designado pelo proprietário de um documento em Microsoft Word ou Microsoft Excel para adicionar uma linha de assinatura ao documento. Os signatários sugeridos podem ser você ou outra pessoa que você deseja que assine seu documento. Por exemplo, se você preparar um documento que precisa ser assinado por todos os membros de seu departamento, é possível incluir linhas de assinatura para aqueles usuários na parte inferior da página final do documento, com instruções de assinatura 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** da barra de ferramentas, clique na seta para baixo perto de **Linha de assinatura** e depois clique em **Provedor de assinatura Privacy Manager**.

   A caixa de diálogo Configuração de Assinatura é exibida.
4. Na caixa sob **Signatário sugerido**, insira o nome do assinante sugerido.
5. Na caixa sob **Instruções para o signatário**, insira uma mensagem para este assinante sugerido.

   NOTA: Esta mensagem vai aparecer 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 mostrar a data.
7. Selecione a caixa de seleção **Exibir função do signatário na linha de assinatura** para mostrar o título.

   NOTA: O proprietário do documento designa signatários sugeridos para o seu documento. As caixas de seleção **Exibir data de assinatura na linha de assinatura** e/ou **Exibir função do signatário na linha de assinatura** devem estar marcadas para que o signatário sugerido possa exibir a data e/ou a função na linha de assinatura.
8. Clique em **OK**.

Adição de uma linha de assinatura do signatário sugerido

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

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

Criptografia de um documento do Microsoft Office

É possível criptografar um documento do Microsoft Office para você e para seus Contatos Confiáveis. Quando você criptografa um documento e o fecha, você e seu(s) Contato(s) Confiável(eis) que você selecionou da lista devem realizar a autenticação antes de abrir o documento.

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 perto de **Assinar e criptografar**, em seguida, clique em **Criptografar documento**.

   A caixa de diálogo 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 pressionada a tecla ctrl, e clique nos nomes individuais.
5. Clique em **OK**.

Se você posteriormente decidir editar o documento, siga as etapas em Remoção da criptografia de um documento do Microsoft Office na página 70. Quando a criptografia for 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

Quando remove a criptografia de um documento do Microsoft Office, você e seus Contatos Confiáveis não precisam mais fazer autenticação para abrir e ver os conteúdos do documento.

Para remover a criptografia de um documento do Microsoft Office:

1. Abra um documento criptografado do Microsoft Word, Microsoft Excel ou Microsoft PowerPoint.
2. Faça a autenticação utilizando o método de login de segurança de sua escolha.
3. Clique no menu **Início**.
4. Clique na seta para baixo perto de **Assinar e criptografar**, e clique em **Remover criptografia**.

Envio de um documento criptografado do Microsoft Office

É possível anexar um documento criptografado do Microsoft Office em uma mensagem de e-mail sem a necessidade de assinar ou criptografar o e-mail. Para fazer isso, crie e envie um e-mail com um documento assinado ou criptografado, do mesmo modo como faria para um e-mail regular com um 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 anexado do Microsoft Office assinado e/ou criptografado, 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 67 para obter mais informações.

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 de Assinatura Digital aparece na barra de status, na parte inferior da janela do documento.

1. Clique no ícone **Assinaturas digitais** para alternar a exibição da caixa de diálogo Assinaturas, que exibe o nome de todos os usuários que assinaram o documento e a data em que cada um assinou.
2. Para exibir mais detalhes sobre cada assinatura, clique com o botão direito na caixa de diálogo Assinaturas e selecione **Detalhes da assinatura**.

Envio de um documento criptografado do Microsoft Office

Para ver um documento criptografado do Microsoft Office em outro computador, o Privacy Manager precisa estar instalado nesse computador. Também é necessário restaurar o Certificado do Privacy Manager que foi usado para criptografar o arquivo.

Se o seu certificado foi perdido, para visualizar um documento criptografado do Microsoft Office, será preciso 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.

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 e Contatos Confiáveis do Privacy Manager

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, em seguida, clique em **Avançar**.
4. Na página Arquivos de migração, insira o nome do arquivo ou clique em **Procurar** para localizar um local e, em seguida, 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 e Contatos Confiáveis do Privacy Manager

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 **Procurar** para localizar o arquivo, e, em seguida, 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 Microsoft Outlook.

7 File Sanitizer for HP ProtectTools

O File Sanitizer permite fragmentar ativos com segurança (por exemplo: informações pessoais ou arquivos, dados históricos ou da web, ou outros componentes de dados) existentes em seu computador e, periodicamente, limpa ativos excluídos de sua unidade de disco rígido.

NOTA: Esta versão do File Sanitizer fornece suporte somente à unidade de disco rígido do computador.

Fragmentação

A fragmentação é diferente de uma exclusão padrão do Windows® (também conhecida como exclusão simples no File Sanitizer). Quando você fragmenta um ativo usando o File Sanitizer, os arquivos são substituídos por dados insignificantes, o que torna 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 em que métodos periciais poderiam ser usados para recuperá-lo.

Quando você seleciona um perfil de fragmentação (**Segurança máxima**, **Segurança média** ou **Segurança baixa**), uma lista predefinida de ativos e um método de apagamento são automaticamente selecionados para a fragmentação. Também é possível personalizar um perfil de fragmentação, especificando 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 78.

Você pode definir uma programação de fragmentação ou pode ativar manualmente a fragmentação 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 fragmentação na página 77, Fragmentação manual de um ativo na página 82 ou Fragmentação manual de todos os itens selecionados na página 83.

NOTA: Um arquivo .dll só 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 (ou limpeza) pode ser executada ocasionalmente em ativos excluídos por você selecionando **Configurações de exclusão simples** no File Sanitizer ou movendo os ativos para a Lixeira do Windows ou, ainda, excluindo os ativos manualmente. A purificação de espaço livre não oferece segurança adicional a ativos fragmentados.

Você pode programar uma 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 Programação de uma purificação de espaço livre na página 77 ou Ativação manual de uma limpeza do espaço livre na página 83.

Abertura do File Sanitizer

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

– ou –

- Clique duas vezes no ícone do **File Sanitizer** em sua área de trabalho.

– ou –

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

Procedimentos de configuração

Configuração de uma programação de fragmentação

Você pode selecionar um perfil de fragmentação predefinido ou criar seu próprio perfil de fragmentação. Para obter mais informações, consulte Seleção ou criação de um perfil de fragmentação na página 78. Também é possível fragmentar ativos manualmente em qualquer momento. Para obter mais informações, consulte Utilização de uma sequência de teclas para iniciar a fragmentação na página 81.

NOTA: Uma tarefa programada é iniciada em uma hora específica. Se o sistema for desligado ou estiver no modo de suspensão/espera na hora programada, o File Sanitizer não tentará reiniciar a tarefa.

1. Abra o File Sanitizer e clique em **Fragmentar**.
2. Selecione uma ou mais opções de fragmentação:
   - **Desligamento do Windows**: Fragmenta todos os ativos selecionados no desligamento do Windows.

     NOTA: É exibida uma caixa de diálogo no desligamento, perguntando se você quer continuar fragmentando os ativos selecionados ou se quer ignorar o procedimento.

     Clique em **Sim** para ignorar o procedimento ou clique em **Não** para continuar com a fragmentação.
   - **Início do navegador da web**: Fragmenta todos os ativos relacionados à web selecionados, como o histórico de URL do navegador, quando você abrir um navegador da web.
   - **Saída do navegador da web**: Fragmenta todos os ativos relacionados à web selecionados, como o histórico de URL do navegador, quando você fechar um navegador da web.
   - **Sequência de teclas**: Permite especificar uma sequência de teclas para iniciar a fragmentação. Para obter detalhes, consulte Utilização de uma sequência de teclas para iniciar a fragmentação na página 81.

   NOTA: Um arquivo .dll só é fragmentado e removido do sistema se tiver sido movido para a Lixeira.
3. Para programar uma data futura para fragmentar ativos selecionados, marque a caixa de seleção **Ativar programador**, insira sua senha do Windows e, em seguida, selecione o dia e a hora.
4. Clique em **Aplicar**.

Programação de uma purificação de espaço livre

A purificação de espaço livre (ou limpeza) pode ser executada ocasionalmente sobre ativos excluídos por você selecionando **Configurações de exclusão simples** no File Sanitizer, movendo os ativos para a Lixeira do Windows ou, ainda, excluindo os ativos manualmente. A purificação de espaço livre não oferece segurança adicional a ativos fragmentados.

NOTA: Uma tarefa programada é iniciada em uma hora específica. Se o sistema for desligado ou estiver no modo de suspensão/espera na hora programada, o File Sanitizer não tentará reiniciar a tarefa.

1. Abra o File Sanitizer e clique em **Purificação**.
2. Para programar uma data futura para realizar a limpeza de ativos excluídos da unidade de disco rígido, marque a caixa de seleção **Ativar programador**, insira sua senha do Windows e, em seguida, selecione o dia e a hora.
3. Clique em **Aplicar**.

NOTA: A operação de purificação de espaço livre pode levar um tempo significativo. Embora a purificação de espaço livre seja executada em segundo plano, o aumento da utilização do processador pode afetar o desempenho do computador.

Seleção ou criação de um perfil de fragmentação

Você pode especificar um método de apagamento ou selecionar os ativos a serem fragmentados, selecionando um perfil predefinido ou criando seu próprio perfil.

Seleção de um perfil de fragmentação predefinido

Quando você seleciona um perfil de fragmentação predefinido, uma lista predefinida de ativos e um método de apagamento são automaticamente selecionados. Também é possível visualizar a lista predefinida dos ativos selecionados para a fragmentação.

1. Abra o File Sanitizer e clique em **Configurações**.
2. Clique em um perfil de fragmentação predefinido:
   - **Segurança máxima**
   - **Segurança média**
   - **Segurança baixa**
3. Para visualizar os ativos selecionados para a fragmentação, clique em **Exibir detalhes**.
   a. **Os itens selecionados serão fragmentados e uma mensagem de confirmação será exibida. Os itens não selecionados serão fragmentados sem qualquer mensagem de confirmação.**—Marque a caixa de seleção para exibir uma mensagem de confirmação antes de fragmentar o item ou desmarque-a para fragmentar o item sem exibir uma mensagem de confirmação.

      NOTA: Um ativo será fragmentado ainda que a caixa de seleção referente a ele esteja desmarcada.

   b. Clique em **Aplicar**.
4. Clique em **Aplicar**.

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**, clique em **Configurações avançadas de segurança** e em **Exibir detalhes**.
2. Selecione o número de ciclos de fragmentação.

NOTA: O número de ciclos de fragmentação selecionado será executado em cada ativo. Por exemplo, se escolher 3 ciclos de fragmentação, um algoritmo que obscurece os dados é executado 3 vezes separadas. Se escolher muitos ciclos de fragmentação para mais segurança, a fragmentação pode levar um tempo significativo; no entanto, quanto maior o número de ciclos de fragmentação especificado, menor a probabilidade de os dados serem recuperados.

3. Para selecionar os ativos a serem fragmentados:
   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.
   c. Clique em **Abrir**, em seguida clique em **OK**.
   d. Em **Opções de fragmentação disponíveis**, clique no ativo personalizado e clique em **Adicionar**.

   Para remover um ativo das opções de fragmentação disponíveis, clique no ativo e, em seguida, clique em **Excluir**.
4. **Os itens selecionados serão fragmentados e uma mensagem de confirmação será exibida. Os itens não selecionados serão fragmentados sem qualquer mensagem de confirmação.**—Marque a caixa de seleção para exibir uma mensagem de confirmação antes de fragmentar o item ou desmarque-a para fragmentar o item sem exibir uma mensagem de confirmação.

NOTA: Um ativo será fragmentado ainda que a caixa de seleção referente a ele esteja desmarcada.

   Para remover um ativo da lista de fragmentação, clique no ativo e, em seguida, clique em **Remover**.
5. Para proteger arquivos ou pastas contra a fragmentação automática:
   a. Em **Não fragmentar o seguinte**, clique em **Adicionar**, em seguida navegue até o arquivo ou pasta ou digite o respectivo caminho.
   b. Clique em **Abrir**, em seguida clique em **OK**.

   Para remover um ativo da lista de exclusões, clique no ativo e, em seguida, clique em **Excluir**.
6. Clique em **Aplicar**.

Personalização de um perfil de exclusão simples

O perfil de exclusão simples executa uma exclusão de ativo padrão sem realizar a fragmentação. Você pode personalizar um perfil de exclusão simples, especificando quais ativos serão incluídos na fragmentação, quais ativos deverão ser confirmados antes da exclusão e quais ativos serão excluídos.

NOTA: Se selecionar **Configurações de exclusão simples**, a purificação de espaço livre poderá ser executada ocasionalmente sobre os ativos que foram excluídos manualmente ou por meio da Lixeira do Windows.

1. Abra o File Sanitizer, clique em **Configurações**, clique em **Configurações de exclusão simples** e em **Exibir 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**, navegue até o arquivo ou pasta ou digite o respectivo caminho e, em seguida, clique em **OK**.
   c. Clique no ativo personalizado e clique em **Adicionar**.

   Para excluir um ativo das opções de exclusão disponíveis, clique no ativo e, em seguida, clique em **Excluir**.
3. **Os itens selecionados serão fragmentados e uma mensagem de confirmação será exibida. Os itens não selecionados serão fragmentados sem qualquer mensagem de confirmação.**—Marque a caixa de seleção para exibir uma mensagem de confirmação antes de fragmentar o item ou desmarque-a para fragmentar o item sem exibir uma mensagem de confirmação.

   NOTA: Um ativo será fragmentado ainda que a caixa de seleção referente a ele esteja desmarcada.

   Para remover um ativo da lista de exclusão, clique no ativo e, em seguida, clique em **Remover**.
4. Para proteger ativos contra a exclusão automática:
   a. Em **Não excluir o seguinte**, clique em **Adicionar**, em seguida navegue até o arquivo ou pasta ou digite o respectivo caminho.
   b. Clique em **Abrir**, em seguida clique em **OK**.

   Para remover um ativo da lista de exclusões, clique no ativo e, em seguida, clique em **Excluir**.
5. Clique em **Aplicar**.

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 Utilização de uma sequência de teclas para iniciar a fragmentação na página 81.
- 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 Utilização do ícone do File Sanitizer na página 82.
- 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 82 ou Fragmentação manual de todos os itens selecionados na página 83.
- Ativar manualmente a purificação de espaço livre — Este recurso permite que você ative manualmente a purificação de espaço livre. Para detalhes, consulte Ativação manual de uma limpeza do espaço livre na página 83.
- Interromper uma operação de purificação de espaço livre ou fragmentação — Este recurso permite que você interrompa uma operação de fragmentação ou de purificação de espaço livre. Para detalhes, consulte Interrupção de uma operação de fragmentação ou purificação de espaço livre na página 83.
- Visualizar arquivos de registro — Este recurso permite que você visualize os arquivos de registro da purificação de espaço livre e da fragmentação, os quais contêm os erros e falhas da última operação de fragmentação ou purificação de espaço livre. Para detalhes, consulte Visualização de arquivos de log na página 83.

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

Utilização de uma sequência de teclas para iniciar a fragmentação

1. Abra o File Sanitizer e clique em **Fragmentar**.
2. Marque a caixa de seleção **Sequência de teclas**.
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 sequência de teclas diferente das outras sequências de teclas que você configurou.

Para iniciar a fragmentação usando uma sequência 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**.

Utilização 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** em sua 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 itens 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 de uma limpeza do 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 purificação de espaço livre

Quando uma operação de fragmentação ou purificação de espaço livre estiver em andamento, uma mensagem será exibida acima do ícone do HP ProtectTools Security Manager na área de notificação, no lado direito da barra de tarefas. A mensagem fornece detalhes sobre o processo de fragmentação ou purificação de espaço livre (porcentagem concluída) e apresenta a opção de cancelar a operação.

- ▲ Para cancelar a operação, clique na mensagem e clique em **Parar**.

Visualização de arquivos de log

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.

É criado um arquivo de log para operações de fragmentação e outro para operações de purificação de espaço livre, separadamente. Ambos ficam localizados na unidade de disco rígido:

- 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

Para sistemas de 64 bits, os arquivos de log ficam localizados na unidade de disco rígido:

- C:\Program Files (x86)\Hewlett-Packard\File Sanitizer*[Nome do usuário]*_ShredderLog.txt
- C:\Program Files (x86)\Hewlett-Packard\File Sanitizer*[Nome do usuário]*_DiskBleachLog.txt

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

O HP ProtectTools Device Access Manager controla o acesso a dados desativando dispositivos de transferência de dados.

NOTA: Alguns dispositivos de interface humana/entrada de dados, como mouse, teclado, TouchPad e leitor de impressão digital, não são controlados pelo Device Access Manager. Para obter mais informações, consulte Classes de dispositivos não gerenciadas na página 96.

Os administradores do sistema operacional Windows® usam o HP ProtectTools Device Access Manager para controlar o acesso aos dispositivos de um sistema e oferecer proteção contra acessos não autorizados:

- Perfis de dispositivo são criados para cada usuário, de forma a definir os dispositivos para os quais o usuário possui ou não permissão de acesso.
- A autenticação Just-in-time (JITA) permite que usuários predefinidos autentiquem a si próprios para acessar dispositivos aos quais, de outra forma, não teriam acesso.
- É possível excluir administradores e usuários confiáveis das restrições de acesso a dispositivos impostas pelo Device Access Manager adicionando-os ao grupo Administradores de dispositivos. A inscrição nesse grupo é gerenciada com o uso das Configurações avançadas.
- O acesso a dispositivos pode ser concedido ou negado com base na associação a um grupo ou para usuários individuais.
- Para classes de dispositivos como unidades de CD-ROM e de DVD, o acesso de leitura e gravação pode ser permitido ou negado separadamente.

Abertura do Device Access Manager

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

Usuários com privilégios limitados podem visualizar a política do HP ProtectTools Device Access Manager utilizando o HP ProtectTools Security Manager. Esse console oferece visualização somente leitura.

Procedimentos de configuração

Configuração do acesso a dispositivos

O HP ProtectTools Device Access Manager oferece quatro visualizações:

- **Configuração simples**: concede ou nega acesso a classes de dispositivos, com base na associação com o grupo Administradores de dispositivos.
- **Configuração de classe de dispositivo**: concede ou nega acesso a tipos de dispositivos ou a dispositivos específicos para usuários ou grupos específicos.
- **Configuração JITA**: configura a autenticação Just-in-time (JITA), permitindo que determinados usuários acessem unidades de DVD/CD-ROM ou mídias removíveis autenticando a si próprios.
- **Configurações avançadas**: configuram uma lista de letras de unidades às quais o Device Access Manager não irá restringir acesso, tais como a unidade C ou a unidade do sistema. A associação com o grupo Administradores de dispositivos também pode ser gerenciada a partir dessa visualização.

Configuração simples

Os administradores podem usar a visualização **Configuração simples** para conceder ou negar acesso às seguintes classes de dispositivos para todos que não sejam do grupo de administradores de dispositivos:

- Todas as mídias removíveis (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 modem
- Todos os dispositivos PCMCIA/ExpressCard
- Todos os dispositivos 1394

Para permitir ou negar o acesso a uma classe de dispositivos para todos que não sejam do grupo de administradores de dispositivos, siga estas etapas:

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

   Se a caixa de seleção estiver esmaecida, valores que afetam o cenário de acesso foram alterados na visualização **Configuração de classe de dispositivo**. Para redefinir as configurações com os valores de fábrica, clique em **Redefinir** na visualização **Configuração de classe de dispositivo**.
3. Clique em **Aplicar**.

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

4. Clique em **OK**.

Iniciando o serviço em segundo plano

Na primeira vez em que uma nova política é definida e aplicada, o serviço em segundo plano Bloqueio de dispositivos/auditoria do HP ProtectTools é iniciado automaticamente e é configurado para ser iniciado automaticamente sempre que o sistema for iniciado.

NOTA: Um perfil de dispositivo deve estar definido para que o aviso do serviço em segundo plano seja exibido.

Os administradores também podem iniciar ou interromper esse serviço da seguinte maneira:

1. No Windows® 7, clique em **Iniciar**, **Painel de controle**, em seguida clique em **Sistema e segurança**.

   – ou –

   No Windows Vista®, clique em **Iniciar**, **Painel de controle** e em seguida clique em **Sistema e manutenção**.

   – ou –

   No Windows XP, clique em **Iniciar**, **Painel de controle** e em seguida clique em **Desempenho e manutenção**.

2. Clique em **Ferramentas administrativas** e, em seguida, em **Serviços**.
3. Selecione o serviço **Bloqueio de dispositivos/auditoria do HP ProtectTools**.
4. Para iniciar o serviço, clique em **Iniciar**.

   – ou –

   Para interromper o serviço se ele estiver sendo executado, clique em **Parar**.

A interrupção do serviço Bloqueio de dispositivos/auditoria não interrompe o bloqueio de dispositivos. Dois componentes reforçam o bloqueio de dispositivos:

- Serviço Bloqueio de dispositivos/auditoria
- Driver DAMDrv.sys

Iniciar o serviço inicia o driver do dispositivo, mas interromper o serviço não interrompe o driver.

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

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

Configuração de classe de dispositivo

Administradores podem visualizar e modificar listas de usuários e grupos que possuem ou não permissão para acessar classes de dispositivos ou dispositivos específicos.

A visualização **Configuração de classe de dispositivo** possui as seguintes seções:

- **Lista de dispositivos**: Exibe todas as classes de dispositivos e dispositivos que estão instalados no sistema ou que podem ter sido instalados anteriormente no sistema.
  - A proteção é geralmente aplicada a uma classe de dispositivos. Um usuário ou grupo selecionado será capaz de acessar qualquer dispositivo da classe de dispositivos.
  - A proteção também pode ser aplicada a dispositivos específicos.
- **Lista de usuários**: exibe todos os usuários e grupos que possuem acesso permitido ou negado à classe de dispositivos selecionada ou a um dispositivo específico.
  - A entrada na Lista de usuários pode ser feita para um usuário específico ou para um grupo do qual o usuário seja membro.
  - Se uma entrada de usuário ou grupo na Lista de usuários não estiver disponível, a configuração foi herdada da classe de dispositivo na Lista de dispositivos ou da pasta Classe.
  - Algumas classes de dispositivos, como DVD e CD-ROM, podem ser controladas ainda mais permitindo-se ou negando o acesso separadamente para operações de leitura e gravação.

    Para outros dispositivos e classes, os direitos de acesso de leitura e gravação podem ser herdados. Por exemplo, o acesso de leitura pode ser herdado de uma classe superior, mas o acesso de gravação pode ser especificamente negado para um usuário ou grupo.

    NOTA: Se a caixa de seleção **Leitura** estiver desmarcada, a entrada no controle de acesso não terá efeito sobre o acesso de leitura para o dispositivo, mas o acesso de leitura não será negado.

    NOTA: O grupo Administradores não pode ser adicionado à Lista de usuários. Ao invés disso, utilize o grupo Administradores de dispositivos.

    Exemplo 1 — Se um usuário ou grupo tiver o acesso de gravação negado para um dispositivo ou classe de dispositivo:

    O mesmo usuário, o mesmo grupo ou um membro do mesmo grupo pode ter o acesso de gravação ou de leitura+gravação concedido somente para um dispositivo que esteja abaixo desse dispositivo na hierarquia de dispositivos.

    Exemplo 2 — Se um usuário ou grupo tiver o acesso de gravação permitido para um dispositivo ou classe de dispositivo:

    O mesmo usuário, o mesmo grupo ou um membro do mesmo grupo pode ter o acesso de gravação ou de leitura+gravação negado somente para o mesmo dispositivo ou para um dispositivo abaixo desse dispositivo na hierarquia de dispositivos.

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

    O mesmo usuário, o mesmo grupo ou um membro do mesmo grupo pode ter o acesso de leitura ou de leitura+gravação negado somente para o mesmo dispositivo ou para um dispositivo abaixo desse dispositivo na hierarquia de dispositivos.

    Exemplo 4 — Se um usuário ou grupo tiver o acesso de leitura negado para um dispositivo ou classe de dispositivo:

O mesmo usuário, o mesmo grupo ou um membro do mesmo grupo pode ter o acesso de leitura ou de leitura+gravação concedido somente para um dispositivo abaixo desse dispositivo na hierarquia de dispositivos.

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

O mesmo usuário, o mesmo grupo ou um membro do mesmo grupo pode ter o acesso de gravação ou de leitura+gravação negado somente para o mesmo dispositivo ou para um dispositivo abaixo desse dispositivo na hierarquia de dispositivos.

Exemplo 6 — Se um usuário ou grupo tiver o acesso de leitura+gravação negado para um dispositivo ou classe de dispositivo:

O mesmo usuário, o mesmo grupo ou um membro do mesmo grupo pode ter o acesso de leitura ou de leitura+gravação concedido somente para um dispositivo abaixo desse dispositivo na hierarquia de dispositivos.

Negação de acesso para um usuário ou grupo

Para evitar que um usuário ou grupo acesse um dispositivo ou classe de dispositivos:

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

NOTA: Quando configurações de negação e permissão são definidas no mesmo nível de dispositivo para um usuário, a negação do acesso tem precedência sobre a permissão de acesso.

Permissão de acesso para um usuário ou grupo

Para conceder permissão a um usuário ou grupo para acessar um dispositivo ou classe de dispositivos:

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

   A caixa de diálogo Selecionar usuários ou grupos será exibida.

4. Clique em **Avançado** e, em seguida, clique em **Localizar agora** para pesquisar usuários ou grupos para adicionar.
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** novamente.
7. Clique em **Permitir** para conceder o acesso a este usuário.
8. Clique em **Aplicar**.

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

Para permitir o acesso a uma classe de dispositivos para um usuário e negar o acesso para todos os demais membros do grupo desse usuário:

1. No painel esquerdo do Console Administrativo do HP ProtectTools, clique em **Device Access Manager** e, em seguida, clique em **Configuração de classe de dispositivo**.
2. Na lista de dispositivos, clique na classe de dispositivo que deseja configurar.
   - **Classe de dispositivo**
   - **Todos os dispositivos**
   - **Dispositivo individual**
3. Em **Usuário/Grupos**, selecione o grupo ao qual negar o acesso e clique em **Negar**.
4. Navegue até a pasta abaixo da classe desejada e adicione o usuário específico.
5. Clique em **Permitir** para conceder o acesso a esse usuário.
6. Clique em **Aplicar**.

Permissão de acesso a um dispositivo específico para um usuário de um grupo

Os administradores podem permitir o acesso a um dispositivo específico e negar o acesso a todos os dispositivos da classe para todos os demais membros do grupo desse usuário:

1. No painel esquerdo do Console Administrativo do HP ProtectTools, clique em **Device Access Manager** e, em seguida, clique em **Configuração de classe de dispositivo**.
2. Na lista de dispositivos, clique na classe de dispositivo que deseja configurar e navegue para a pasta abaixo dela.
3. Em **Usuário/Grupos**, clique em **Permitir** próximo ao grupo ao qual o acesso será concedido.
4. Clique em **Negar** próximo ao grupo ao qual o acesso será negado.
5. Na lista de dispositivos, navegue até o dispositivo específico ao qual deverá ser permitido o acesso para o usuário.
6. Clique em **Adicionar**.

   A caixa de diálogo Selecionar usuários ou grupos será exibida.
7. Clique em **Avançado** e, em seguida, clique em **Localizar agora** para pesquisar usuários ou grupos para adicionar.

8. Clique em um usuário que terá o acesso permitido e, em seguida, clique em **OK**.
9. Clique em **Permitir** para conceder o acesso a este usuário.
10. Clique em **Aplicar**.

Remoção de configurações para um usuário ou grupo

Para retirar a permissão de um usuário ou grupo para acessar um dispositivo ou classe de dispositivo, siga estas etapas:

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

Redefinição da configuração

⚠ **CUIDADO:** A redefinição da configuração descarta todas as alterações de configuração do dispositivo realizadas e retorna todas as configurações aos valores definidos na fábrica.

Para redefinir as configurações com os valores de fábrica:

1. No painel esquerdo do Console Administrativo do HP ProtectTools, clique em **Device Access Manager** e, em seguida, clique em **Configuração de classe de dispositivo**.
2. Clique em **Redefinir**.
3. Clique em **Sim** na solicitação de confirmação.
4. Clique em **Aplicar**.

Configuração JITA

A Configuração JITA permite ao administrador visualizar e modificar listas de usuários e grupos que possuem permissão para acessar dispositivos usando a autenticação Just-in-Time (JITA).

Os usuários com permissão JITA poderão acessar alguns dispositivos para os quais políticas criadas nas visualizações **Configuração simples** ou **Configuração de classe de dispositivo** sofreram limitações.

- **Cenário**: uma política de Configuração simples é definida para negar acesso à unidade de DVD/CD-ROM para todos os que não sejam do grupo de administradores de dispositivos.
- **Resultado**: um usuário com permissão JITA que tente acessar a unidade de DVD/CD-ROM recebe a mesma mensagem de “Acesso negado” que um usuário sem permissão JITA. Em seguida, será exibida uma mensagem em balão perguntando se o usuário gostaria de obter acesso JITA. Se o balão for clicado, a caixa de diálogo Autenticação de usuário será exibida.

Quando o usuário inserir suas credenciais com sucesso, será concedido acesso à unidade de DVD/CD-ROM.

O período da autorização JITA pode ser definido com um número determinado de minutos ou 0 minuto. O período JITA de 0 minuto não expira. Os usuários terão acesso ao dispositivo do momento da autenticação até o momento em que realizarem logout do sistema.

O período JITA também pode ser estendido, se for configurado para isso. Nesse cenário, 1 minuto antes da expiração do período JITA, os usuários poderão clicar na solicitação para estender seu acesso sem precisar fazer nova autenticação.

Independentemente de o usuário receber um período JITA limitado ou ilimitado, assim que ele fizer logout do sistema ou que outro usuário fizer login, o período JITA vai expirar. Na próxima vez em que o usuário fizer login e tentar acessar um dispositivo com permissão JITA, ele será solicitado a inserir suas credenciais.

A JITA está disponível para as seguintes classes de dispositivos:

- Unidades de DVD/CD-ROM
- Mídias removíveis

Criação de uma JITA para um usuário ou grupo

Administradores podem permitir acesso a dispositivos para usuários ou grupos utilizando a autenticação Just-in-Time.

1. No painel esquerdo do Console Administrativo do HP ProtectTools, clique em **Device Access Manager** e, em seguida, clique em **Configuração JITA**.
2. A partir do menu suspenso do dispositivo, selecione **Mídia removível** ou **Unidades de DVD/CD-ROM**.
3. Clique em **+** para adicionar um usuário ou grupo à configuração JITA.
4. Marque a caixa de seleção **Ativado**.
5. Defina o período JITA com o tempo desejado.
6. Clique em **Aplicar**.

O usuário precisar fazer logout e, em seguida, login novamente para que a nova configuração JITA seja aplicada.

Criação de uma JITA extensível para um usuário ou grupo

Administradores podem permitir acesso a dispositivos para usuários ou grupos utilizando a autenticação Just-in-Time, que pode ser estendida antes de expirar.

1. No painel esquerdo do Console Administrativo do HP ProtectTools, clique em **Device Access Manager** e, em seguida, clique em **Configuração JITA**.
2. A partir do menu suspenso do dispositivo, selecione **Mídia removível** ou **Unidades de DVD/CD-ROM**.
3. Clique em **+** para adicionar um usuário ou grupo à configuração JITA.
4. Marque a caixa de seleção **Ativado**.
5. Defina o período JITA com o tempo desejado.

6. Marque a caixa de seleção **Extensível**.
7. Clique em **Aplicar**.

O usuário precisar fazer logout e, em seguida, login novamente para que a nova configuração JITA seja aplicada.

Desativação de uma JITA para um usuário ou grupo

Os administradores podem desativar o acesso a dispositivos para usuários ou grupos utilizando a autenticação Just-in-Time.

1. No painel esquerdo do Console Administrativo do HP ProtectTools, clique em **Device Access Manager** e, em seguida, clique em **Configuração JITA**.
2. A partir do menu suspenso do dispositivo, selecione **Mídia removível** ou **Unidades de DVD/CD-ROM**.
3. Selecione o usuário ou grupo para o qual deseja desativar a JITA.
4. Desmarque a caixa de seleção **Ativado**.
5. Clique em **Aplicar**.

Quando o usuário fizer login e tentar acessar o dispositivo, o acesso será negado.

Configurações avançadas

As Configurações avançadas fornecem as seguintes funções:

- Gerenciamento do grupo Administradores de dispositivos
- Gerenciamento das letras de unidades às quais o Device Access Manager nunca nega acesso.

O grupo Administradores de dispositivos é usado para excluir usuários confiáveis (confiáveis em termos de acesso a dispositivos) das restrições de acesso a dispositivos impostas por uma política do Device Access Manager. O conceito de usuários confiáveis normalmente inclui os administradores do sistema. Consulte Grupo Administradores de dispositivos na página 95 para obter mais informações.

A visualização **Configurações avançadas** também permite que o administrador configure uma lista de letras de unidades às quais o Device Access Manager não restringirá o acesso a usuário algum.

NOTA: É preciso que os serviços em segundo plano do Device Access Manager estejam em execução quando a lista de letras de unidades for configurada.

Para iniciar esses serviços:

1. Aplique uma política de Configuração simples, por exemplo, negar acesso a mídias removíveis para todos os que não sejam administradores de dispositivos.

   – ou –

   Abra uma janela de prompt de comando com privilégios de Administrador e em seguida digite:

   ```
   sc start flcdlock
   ```

   Pressione enter.

2. Quando os serviços forem iniciados, a lista de unidades poderá ser editada. Insira as letras de unidade dos dispositivos que você não deseja que o Device Access Manager controle.

   As letras de unidades são exibidas para unidades de disco rígido físicas ou partições.

   NOTA: Independentemente de a unidade do sistema (normalmente a C) estar nessa lista, o acesso a ela jamais será negado a qualquer usuário.

Grupo Administradores de dispositivos

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

O grupo Administradores de dispositivos é usado para excluir usuários confiáveis (confiáveis em termos de acesso a dispositivos) das restrições de acesso a dispositivos impostas por uma política do Device Access Manager. O conceito de usuários confiáveis normalmente inclui os administradores do sistema.

NOTA: Adicionar um usuário ao grupo Administradores de dispositivos não concede permissão de acesso automaticamente a dispositivos para o usuário. Na visualização **Configuração de classe de dispositivo**, se o grupo Usuários não tiver acesso a um dispositivo, o grupo Administradores de dispositivos terá de ter acesso para que seus membros possam acessar o dispositivo. No entanto, a visualização **Configuração simples** pode ser usada para negar acesso a classes de dispositivos para todos os usuários que não forem membros do grupo Administradores de dispositivos.

Para adicionar usuários ao grupo Administradores de dispositivos:

1. Na visualização **Configurações avançadas**, clique em **+**.
2. Insira o nome de usuário do usuário confiável.
3. Clique em **OK**.
4. Clique em **Aplicar**.

Os métodos alternativos para gerenciar a associação com este grupo incluem:

- Para o Windows 7 Professional ou Windows Vista, é possível adicionar usuários usando o snap-in padrão “Usuários e Grupos Locais” do Microsoft Management Console (MMC).
- Para versões domésticas do Windows 7, Vista ou XP, a partir de uma conta com privilégios de administrador, digite o seguinte em uma janela de prompt de comando:

  ```
  net localgroup "Administradores de dispositivos" username /add
  ```

  Neste comando, “username” é o nome de usuário do usuário que você deseja adicionar a esse grupo.

Suporte a eSATA

Para que o Device Access Manager controle dispositivos eSATA, é necessário realizar as seguintes configurações:

1. A unidade precisa estar conectada quando o sistema for inicializado.
2. Utilizando a visualização **Configurações avançadas**, assegure-se de que a unidade eSATA não esteja na lista de letras de unidades às quais o Device Access Manager não negará acesso. Se a letra da unidade eSATA estiver listada, exclua a letra e em seguida clique em **Aplicar**.
3. O dispositivo pode ser controlado usando a classe de dispositivo Mídia removível, tanto na visualização **Configuração simples** quanto na **Configuração de classe de dispositivo**.

Classes de dispositivos não gerenciadas

O HP ProtectTools Device Access Manager não gerencia as seguintes classes de dispositivos:

- Dispositivos de entrada/saída
  - Biométricos
  - Mouse
  - Teclado
  - Impressora
  - Impressoras Plug and Play (PnP)
  - Upgrade de impressora
  - Dispositivos infravermelhos de interface humana
  - Leitor de smart card

- Multiporta serial
- Unidade de disco
- Controlador de disquete (FDC)
- Controlador de disco rígido (HDC)
- Classe de dispositivos de interface humana (HID)

- Energia
  - Bateria
  - Suporte a gerenciamento de energia avançado (APM)
- Diversos
  - Computador
  - Decodificador
  - Tela
  - Processador
  - Sistema
  - Desconhecido
  - Volume
  - Instantâneo de volume
  - Dispositivos de segurança
  - Acelerador de segurança
  - Driver unificado de tela Intel®
  - Driver de mídia
  - Alternador de mídia
  - Multifunção
  - Legacard
  - Cliente de rede
  - Serviço de rede
  - Transporte de rede
  - Adaptador SCSI

9 Recuperação em caso de roubo

O Computrace for HP ProtectTools (adquirido separadamente) permite monitorar, gerenciar e rastrear remotamente seu computador.

Quando ativado, o Computrace for HP ProtectTools é configurado a partir do Centro de Atendimento ao Cliente da Absolute Software. No Centro de Atendimento ao Cliente, o administrador pode configurar o Computrace for HP ProtectTools para monitorar ou gerenciar o computador. Se o sistema estiver em local indevido ou for roubado, o Centro de Atendimento ao Cliente pode auxiliar as autoridades locais na localização e recuperação do computador. Se configurado, o Computrace pode continuar a funcionar ainda que a unidade de disco rígido seja apagada ou substituída.

Para ativar o Computrace for HP ProtectTools:

1. Conecte-se à Internet.
2. Clique em **Iniciar**, **Todos os Programas**, **HP** e, em seguida, clique em **HP ProtectTools Security Manager**.
3. No painel esquerdo do Security Manager, clique em **Recuperação em caso de roubo**.
4. Para iniciar o assistente de ativação do Computrace, clique em **Ativar agora**.
5. Insira suas informações de contato e as informações do seu cartão de crédito ou insira a chave de produto pré-adquirida.

O assistente de ativação processará a transação com segurança e configurará sua conta de usuário no site do Centro de Atendimento ao Cliente da Absolute Software. Uma vez concluída a operação, você receberá uma confirmação por e-mail contendo as informações de sua conta no Centro de Atendimento ao Cliente.

Se você já tiver executado o assistente de ativação do Computrace e sua conta de usuário do Centro de Atendimento ao Cliente já existir, você poderá comprar licenças adicionais contatando seu representante de conta HP.

Para fazer login no Centro de Atendimento ao Cliente:

1. Acesse https://cc.absolute.com/.
2. Nos campos **Nome de usuário** e **Senha**, insira as credenciais que você recebeu no e-mail de confirmação e clique no botão **Login**.

Usando o Centro de Atendimento ao Cliente, você pode:

- Monitorar seus computadores.
- Proteger seus dados remotamente.
- Relatar o roubo de qualquer computador protegido pelo Computrace.

▲ Clique em **Saiba mais** para obter mais informações sobre o Computrace for HP ProtectTools.

10 Embedded Security for HP ProtectTools (somente em determinados modelos)

NOTA: O chip de segurança integrada do módulo de plataforma confiável (TPM) deve estar instalado no computador para que se possa utilizar o Embedded Security for ProtectTools.

Embedded Security for ProtectTools oferece proteção contra o acesso não autorizado a dados ou credenciais do usuário. Esse módulo de software fornece os seguintes recursos de segurança:

- Criptografia de pastas e arquivos Enhanced Microsoft® Encryption File System (EFS - Sistema de criptografia de arquivos aprimorado da Microsoft)
- Criação de uma unidade pessoal protegida (PSD) para proteção de dados do usuário
- Funções de gerenciamento de dados, como backup e restauração da hierarquia principal
- Suporte a aplicativos de terceiros (como Microsoft Outlook e Internet Explorer) para operações de certificado digital protegidas durante a utilização do software Embedded Security

O chip de segurança integrado TPM aprimora e ativa outros recursos de segurança do HP ProtectTools Security Manager. Por exemplo, o Credential Manager for HP ProtectTools pode usar o chip integrado como um fator de autenticação quando o usuário faz login no Windows.

Procedimentos de configuração

⚠ **CUIDADO:** Para reduzir o risco à segurança, é altamente recomendado que seu administrador de TI inicialize imediatamente o chip de segurança integrado. Não inicializar o chip de segurança integrado pode fazer com que um usuário não autorizado, um invasor de computador ou um vírus tome conta do computador e obtenha controle sobre as tarefas do proprietário, como o manuseio do arquivo de recuperação de emergência e a definição de configurações de acesso do usuário.

Siga as etapas nas duas seções adiante para ativar e inicializar o chip de segurança integrado.

Ativação do chip de segurança integrado no utilitário de configuração do computador

O chip de segurança integrado deve ser ativado no assistente de inicialização rápida ou no utilitário de configuração do computador.

Para ativar o chip de segurança integrado no utilitário de configuração do computador:

1. Abra o utilitário de configuração ligando ou reiniciando o computador e, em seguida, pressione f10 enquanto a mensagem “f10 = ROM Based Setup” (f10 = Configuração baseada na ROM) estiver sendo exibida no canto inferior esquerdo da tela.
2. Se uma senha de administrador não tiver sido definida, use as teclas de seta para selecionar **Security** (Segurança), selecione **Setup password** (Configurar senha) e, em seguida, pressione enter.
3. Digite a senha nas caixas **New password** (Nova senha) e **Verify new password** (Verificar nova senha) e, em seguida, pressione f10.
4. No menu **Security** (Segurança), use as teclas de chave para selecionar **TPM Embedded Security** (Segurança integrada com TPM), em seguida, pressione enter.
5. Em **Embedded Security** (Segurança integrada), se o dispositivo estiver oculto, selecione **Available** (Disponível).
6. Selecione **Embedded security device state** (Estado do dispositivo de segurança integrado) e altere a configuração para **Enable** (Ativar).
7. Pressione f10 para aceitar as alterações na configuração do Embedded Security.
8. Para salvar suas preferências e sair do utilitário de configuração do computador, use as teclas de seta para selecionar **File** (Arquivo), selecione **Save Changes and Exit** (Salvar alterações e sair) e siga as instruções na tela.

Inicialização do chip de segurança integrado

No processo de inicialização do Embedded Security, você irá executar as seguintes tarefas:

- Definir uma senha de proprietário para o chip embedded security que protege o acesso a todas as funções do proprietário do chip embedded security.
- Configurar o arquivo de recuperação de emergência, que é uma área de armazenamento protegida que permite nova criptografia das chaves de usuário básico para todos os usuários.

Para inicializar o chip embedded security:

1. Clique com o botão direito no ícone **HP ProtectTools Security Manager** na área de notificação, à direita da barra de tarefas e, em seguida, selecione **Inicialização do Embedded Security**.

   O assistente de inicialização do ProtectTools Embedded Security é aberto.

2. Siga as instruções na tela.

Configuração da conta de usuário básico

A configuração de uma conta de usuário básico no Embedded Security executa as seguintes tarefas:

- Produz uma chave de usuário básico que protege as informações criptografadas, e define uma senha de chave de usuário básico para proteger a chave de usuário básico.
- Configura uma unidade pessoal protegida (PSD) para armazenamento de pastas e arquivos criptografados.

CUIDADO: Proteja a senha de chave de usuário básico. As informações criptografadas não podem ser acessadas nem recuperadas sem essa senha.

Para configurar uma conta de usuário básico e ativar os recursos de segurança do usuário:

1. Se o Assistente de Inicialização do Usuário do Embedded Security não estiver aberto, clique em **Iniciar**, **Todos os Programas**, **HP** e, em seguida, clique em **HP ProtectTools Security Manager**.
2. No painel esquerdo, clique em **Embedded Security** e, em seguida, clique em **Configurações de usuários**.
3. No painel direito, em **Funções do Embedded Security**, clique em **Configurar**.

   O assistente de inicialização do usuário do Embedded Security é aberto.
4. Siga as instruções na tela.

NOTA: Para usar e-mail protegido, é preciso primeiro configurar o cliente de e-mail para usar um certificado digital criado com o Embedded Security. Se não houver um certificado digital disponível, é preciso obter um de uma autoridade de certificação. Para obter instruções sobre a configuração de seu e-mail e a obtenção de um certificado digital, consulte a Ajuda do software cliente de e-mail.

Tarefas básicas

Após a configuração da conta de usuário básico, é possível executar as seguintes tarefas:

- Criptografar arquivos e pastas
- Enviar e receber e-mail criptografado

Utilização da unidade pessoal protegida (PSD)

Após configurar a PSD, você será solicitado a digitar a senha da chave de usuário básico no próximo login. Se a senha de chave de usuário básico for inserida corretamente, é possível acessar a PSD diretamente do Windows Explorer.

Criptografar arquivos e pastas

Quando trabalhar com arquivos criptografados, observe as seguintes regras:

- Somente arquivos e pastas em partições NTFS podem ser criptografados. Arquivos e pastas em partições FAT não podem ser criptografados.
- Arquivos de sistema e arquivos compactados não podem ser criptografados, e arquivos criptografados não podem ser compactados.
- Pastas temporárias devem ser criptografadas, porque interessam particularmente aos hackers.
- Uma política de recuperação é automaticamente configurada quando um arquivo ou pasta é criptografado pela primeira vez. Essa política garante que se os certificados de criptografia e as chaves de privacidade forem perdidos, será possível usar um agente de recuperação para decodificar as informações.

Para criptografar arquivos e pastas:

1. Clique com o botão direito no arquivo ou pasta que deseja criptografar.
2. Clique em **Criptografar**.
3. Clique em uma das seguintes opções:
    - **Aplicar alterações a esta pasta somente.**
    - **Aplicar alterações a esta pasta, subpastas e arquivos.**
4. Clique em **OK**.

Enviar e receber e-mail criptografado

O Embedded Security permite o envio e o recebimento de e-mail criptografado, mas os procedimentos variam de acordo com o programa utilizado para acessar e-mail. Para obter mais informações, consulte a Ajuda de software do Embedded Security e a ajuda de software do seu programa de e-mail.

Alteração da senha de chave de usuário básico

Para alterar da senha de chave de usuário básico:

1. Clique em **Iniciar**, **Todos os Programas**, **HP** e, em seguida, clique em **HP ProtectTools Security Manager**.
2. No painel esquerdo, clique em **Embedded Security** e, em seguida, clique em **Configurações de usuários**.
3. No painel direito, em **Senha de usuário básico**, clique em **Alterar**.
4. Digite a senha antiga e, em seguida, defina e confirme a nova senha.
5. Clique em **OK**.

Tarefas avançadas

Os administradores podem executar as seguintes tarefas no Embedded Security:

- Backup e restauração de credenciais do Embedded Security, configurações do Embedded Security e Unidades Pessoais Protegidas
- Alterando a senha de proprietário
- Redefinição da senha de usuário
- Migração segura das credenciais de segurança do usuário de uma plataforma de origem para uma plataforma de destino

Backup e restauração

O recurso de backup do Embedded Security cria um arquivo que contém informações de certificação a serem restauradas em caso de emergência.

Criação de um arquivo de backup

Para criar um arquivo de backup:

1. Clique em **Iniciar**, **Todos os Programas**, **HP** e, em seguida, clique em **Console Administrativo do HP ProtectTools**.
2. No painel esquerdo, clique em **Embedded Security** e, em seguida, clique em **Backup**.
3. No painel direito, clique em **Configurar**. O Embedded Security for HP ProtectTools Backup Wizard é aberto.
4. Siga as instruções na tela.

Restauração dos dados de certificação do arquivo de backup

Para restaurar dados do arquivo de backup:

1. Clique em **Iniciar**, **Todos os Programas**, **HP** e, em seguida, clique em **Console Administrativo do HP ProtectTools**.
2. No painel esquerdo, clique em **Embedded Security** e, em seguida, clique em **Backup**.
3. No painel direito, clique em **Configurar**. O Embedded Security for HP ProtectTools Backup Wizard é aberto.
4. Siga as instruções na tela.

Alteração da senha de proprietário

Os administradores podem alterar a senha de proprietário:

1. Clique em **Iniciar**, **Todos os Programas**, **HP** e, em seguida, clique em **Console Administrativo do HP ProtectTools**.
2. No painel esquerdo, clique em **Embedded Security** e, em seguida, clique em **Avançado**.
3. No painel direito, em **Senha de proprietário**, clique em **Alterar**.
4. Digite a senha de proprietário antiga e, em seguida, defina e confirme a nova senha de proprietário.
5. Clique em **OK**.

Redefinição da senha de usuário

Um administrador pode ajudar o usuário a redefinir uma senha esquecida. Para obter mais informações, consulte a Ajuda do software.

Migração de chaves com o assistente de migração

A migração é uma tarefa avançada de administrador que permite o gerenciamento, a restauração e a transferência de chaves e certificados.

Para obter detalhes sobre a migração, consulte a Ajuda de software do Embedded Security.

11 Exceções da senha localizada

No nível de Segurança do Pre-boot e no nível do HP Drive Encryption, o suporte à localização de senha é limitado, conforme descrito nas seções seguintes.

Os IMEs do Windows não são suportados no nível de Segurança do Pre-boot ou no nível do HP Drive Encryption.

No Windows, o usuário pode escolher um IME (editor de método de entrada) para inserir caracteres e símbolos complexos, como caracteres japoneses ou chineses, ao utilizar um teclado ocidental padrão.

Os IMEs não são suportados no nível de Segurança do Pre-boot ou no nível do HP Drive Encryption. Uma senha do Windows não pode ser inserida com um IME na tela de login da Segurança do Pre--boot ou do HP Drive Encryption, podendo ocasionar uma situação de travamento. Em alguns casos, o Microsoft® Windows não exibe o IME quando o usuário insere a senha.

Por exemplo, em algumas instalações japonesas do Windows XP, o IME padrão é chamado de Microsoft IME Standard 2002 for Japanese, que, na verdade, converte para o layout de teclado E0010411. No entanto, isso é um IME, não um layout de teclado. (O esquema de codificação de layout de teclado é reservado pela Microsoft para os IMEs, que estendem o conceito de um layout de teclado.) Levando em conta que esse não é um layout de teclado que pode ser representado no ambiente de digitação para o prompt de senha de Segurança do Pre-boot do BIOS ou para o prompt de senha do HP Drive Encryption, qualquer senha digitada com esse IME é rejeitada pelo HP ProtectTools. O Microsoft IME Standard 2002 for Japanese também é diferente do “Nome Comum” no Microsoft Windows Vista®. O Windows mapeia alguns IMEs para um layout de teclado. Nesses casos, o IME é suportado pelo HP ProtectTools, visto que a definição subjacente do layout de teclado (o código hexadecimal) está sendo usada.

A solução é mudar para um dos seguintes layouts de teclado suportados que convertem para o layout de teclado 00000411:

- Microsoft IME for Japanese
- O layout de teclado japonês
- Office 2007 IME for Japanese—Se a Microsoft ou uma empresa terceira utilizar o termo IME ou editor de método de entrada, o método de entrada pode não ser, na verdade, um IME. Isso pode causar confusão, mas o software lê a representação do código hexadecimal. Assim, se um IME se equiparar a um layout de teclado suportado, então, o HP ProtectTools pode suportar a configuração.

⚠ **AVISO!** Quando o HP ProtectTools é implementado, as senhas inseridas com um IME do Windows serão rejeitadas.

Alterações de senha usando um layout de teclado que também é suportado

Se a senha for inicialmente definida com um layout de teclado, como o Inglês EUA (409), e, em seguida, o usuário mudar a senha usando um layout de teclado diferente que também é suportado, como América Latina (080A), a alteração da senha funcionará no HP Drive Encryption, mas falhará no BIOS caso o usuário utilize caracteres que existam no segundo, mas não no primeiro (por exemplo, ē).

NOTA: Os administradores podem resolver esse problema usando o recurso HP ProtectTools Manage Users para remover o usuário do HP ProtectTools, selecionando o layout de teclado desejado no sistema operacional, e, em seguida, executando o Assistente de Configuração do Security Manager novamente para o mesmo usuário. O BIOS armazena o layout de teclado desejado, e as senhas que podem ser digitadas nesse layout de teclado serão apropriadamente definidas no BIOS.

Outro problema potencial é a utilização de layouts de teclado diferentes que podem produzir os mesmos caracteres. Por exemplo, tanto o layout de teclado internacional dos EUA (20409) quanto o layout de teclado da América Latina (080A) podem produzir o caractere é, embora sequências de teclas diferentes possam ser necessárias. Se uma senha é definida inicialmente com o layout de teclado da América Latina, então, esse layout é definido no BIOS, mesmo que a senha seja alterada posteriormente usando o layout de teclado internacional dos EUA.

Manuseio especial de teclas

- Chinês, Eslovaco, Francês Canadense e Tcheco

  Quando um usuário seleciona um dos layouts de teclado anteriores e, em seguida, reinsere a senha (por exemplo, abcdef), a mesma senha deve ser inserida enquanto a tecla shift é pressionada para letra minúscula e a tecla shift e a tecla caps lock para letra maiúscula na Segurança do Pre-boot do BIOS e no HP Drive Encryption. As senhas numéricas devem ser inseridas usando o teclado numérico.

- Coreano

  Quando um usuário seleciona um layout de teclado coreano suportado e, em seguida, insere uma senha, a mesma senha deve ser inserida enquanto a tecla alt à direta é pressionada para letra minúscula e a tecla alt e a tecla caps lock à direta para letra maiúscula na Segurança do Pre-boot do BIOS e no HP Drive Encryption.

- Os caracteres não suportados estão listados na seguinte tabela:

Idioma	Windows	BIOS	Criptografia da unidade
Árabe	As teclas ﻯ ,ﻰ e ﻯ geram dois caracteres.	As teclas ﻯ ,ﻰ e ﻯ geram um caractere.	As teclas ﻯ ,ﻰ e ﻯ geram um caractere.
Francês Canadense	ç, è, à e é com caps lock são Ç, È, À e É no Windows.	ç, è, à e é com caps lock são ç, è, à e é na Segurança do Pre-boot do BIOS.	ç, è, à e é com caps lock são ç, è, à e é no HP Drive Encryption.
Espanhol	40a não é suportado. Ele, todavia, funciona visto que o software o converte para c0a. No entanto, devido a diferenças sutis entre os layouts de teclado, recomenda-se que os usuários que falam espanhol alterem seu layout de teclado do Windows para 1040a (Variação do espanhol) ou 080a (América Latina).	n/d	n/d
EUA internacional	◦ As teclas ¡, ¤, ‘, ’, ¥ e × na fileira superior são rejeitadas. ◦ As teclas å, ® e Þ na segunda fileira são rejeitadas. ◦ As teclas á, ð e ø na terceira fileira são rejeitadas. ◦ A tecla æ na fileira inferior é rejeitada.	n/d	n/d

Idioma	Windows	BIOS	Criptografia da unidade
Tcheco	◦ A tecla ğ é rejeitada. ◦ A tecla į é rejeitada. ◦ A tecla ų é rejeitada. ◦ As teclas ė, ı e ż são rejeitadas. ◦ As teclas ģ, ķ, ļ, ņ e ŗ são rejeitadas.	n/d	n/d
Eslovaco	A tecla ż é rejeitada.	◦ As teclas š, ś e ş são rejeitadas quando digitadas, mas são aceitas quando inseridas com o teclado via software. ◦ A tecla morta (dead key) ţ gera dois caracteres.	n/d
Húngaro	A tecla ż é rejeitada.	A tecla ţ gera dois caracteres.	n/d
Esloveno	A tecla żŻ é rejeitada no Windows, e a tecla alt gera uma tecla morta no BIOS.	As teclas ú, Ú, ů, Ů, ş, Ş, ś, Ś, š e Š são rejeitadas no BIOS.	n/d
Japonês	Para o Windows XP, o layout de teclado padrão japonês, 411, é totalmente suportado. Um IME, em geral representado no Windows XP como Microsoft Standard IME 2002, normalmente não seria suportado. No entanto, testes empíricos demonstraram que esse IME é uma quase duplicação do layout de teclado 411 ao digitar caracteres simples. O software, portanto, altera esse IME para o layout de teclado 411 ao proteger o BIOS e o HP Drive Encryption com senhas japonesas localizadas. Quando disponível, o IME do Microsoft Office 2007 é uma opção melhor. Apesar do nome IME, na verdade é o layout de teclado 411 que é suportado.	n/d	n/d

O que fazer quando uma senha é rejeitada

As senhas podem ser rejeitadas devido às seguintes razões:

- O usuário está usando um IME que não é suportado. Esse é um problema comum em idiomas de dois bytes (Coreano, Japonês, Chinês). Para solucionar esse problema:

  1. clique em **Iniciar**, **Painel de Controle**, em seguida clique em **Opções regionais e de idioma**.
  2. Clique na guia **Idiomas**.
  3. Clique no botão **Detalhes**.
  4. Na guia **Configurações** , clique no botão **Adicionar** para adicionar um teclado suportado (adicione teclados dos EUA sob o idioma de entrada chinês).
  5. Defina o teclado suportado para entrada padrão.
  6. Reinicie o HP ProtectTools, e insira a senha novamente.

- O usuário está usando um caractere que não é suportado. Para solucionar esse problema:

  1. Altere a senha do Windows de maneira a utilizar apenas caracteres suportados. Os caracteres não suportados estão listados em Manuseio especial de teclas na página 112.
  2. Execute o Assistente de Configuração do Security Manager novamente e reinsira a nova senha do Windows.

Glossário

administrador
Consulte *Administrador do Windows*.

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

arquivo de recuperação de emergência
Uma área de armazenamento protegida que permite a recriptografia de chaves de usuário básico 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 se 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
O processo de verificar se um usuário está autorizado a executar uma tarefa como acessar um computador, modificar configurações de um programa específico ou visualizar dados protegidos.

autenticação na inicialização
Um recurso de segurança que requer alguma forma de autenticação, como um smart card, chip de segurança ou senha, quando o computador é ligado.

autoridade de certificação (CA)
Um serviço que emite os certificados necessários para a execução de uma infraestrutura 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 que você assine, criptografe ou remova 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.

cena
Uma foto de um usuário registrado a ser usada para autenticação.

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.

chip de segurança integrado Trusted Platform Module (TPM)
Termo genérico para o HP ProtectTools Embedded Security Chip. Um módulo TPM autentica um computador, e não um usuário, armazenando informações específicas do sistema anfitrião (host), como chaves de criptografia, certificados digitais e senhas. O módulo TPM minimiza o risco de comprometimento das informações armazenadas no computador por roubo físico ou invasão por hackers externos.

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
Um procedimento, como o uso de um algoritmo, empregado em criptografias para converter texto plano em texto cifrado a fim de evitar que destinatários não autorizados leiam os dados. Há vários tipos de criptografia de dados, e eles são a base para a segurança na rede. Os tipos comuns incluem o Data Encryption Standard e a criptografia de chave privada.

console
Um local central onde é possível acessar e gerenciar os recursos e configurações no Console Administrativo do HP ProtectTools.

conta de rede
Uma conta de usuário ou administrador do Windows, no computador local, em um grupo de trabalho ou em um domínio.

conta de usuário do Windows
O perfil de uma pessoa autorizada a fazer login em uma rede ou computador específico.

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
O meio pelo qual o usuário comprova a elegibilidade de uma tarefa em particular no processo de autenticação.

criptografia
A prática de criptografia e decodificação de dados de modo que eles possam ser decodificados apenas por indivíduos específicos.

decodificação
Um procedimento usado em criptografia para converter dados criptografados em texto comum.

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 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
Um recurso de segurança que vincula a unidade de disco rígido a um usuário e requer que o usuário digite corretamente a senha do DriveLock quando o computador for inicializado.

EFS (Encryption File System, sistema de criptografia de arquivo)
Sistema que criptografa todos os arquivos e subpastas na pasta selecionada.

exclusão simples
Exclusão da referência do Windows para um ativo. O conteúdo do ativo permanece no disco rígido até que os dados ocultos sejam sobrescritos 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
Uma cópia de backup da chave de criptografia da unidade.

ID card
Um gadget de área de trabalho do 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 uma 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.

JITA
Autenticação Just-In-Time.

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 onde é possível acessar e gerenciar os recursos e configurações no Security Manager for HP ProtectTools.

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

PIN
Personal Identification Number (número de identificação pessoal).

PKI
O padrão da infraestrutura de chave pública 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)
Um provedor ou biblioteca de algoritmos criptográficos que pode ser usado em uma interface bem definida para executar funções criptográficas específicas.

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
O 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.

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

selo 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.

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

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

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, semelhante em tamanho e formato a um cartão de crédito, que armazena informações de identificação sobre o usuário. Usado para autenticar o proprietário de um computador.

tela de login do Drive Encryption
É a tela de login exibida antes de o Windows ser iniciado. Os usuários devem inserir seu nome de usuário e sua senha do Windows ou PIN do smart card. Na maioria das vezes, a inserção da informação correta na tela de login do Drive Encryption permite o acesso direto ao Windows, sem que seja necessário efetuar login novamente na tela de login do Windows.

token
Consulte *método de login de segurança*.

token USB

Um dispositivo de segurança que armazena informações de identificação sobre um usuário. Como um smart 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 smart card e leitor de cartão. O token é salvo na unidade de disco rígido do computador ou no registro do Windows. Ao fazer login com um token virtual, você é solicitado a informar um PIN de usuário para concluir 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.

Índice

D

E