# HP ProtectTools

## Passos Iniciais

Bluetooth é marca comercial de seu proprietário, utilizada sob licença pela Hewlett-Packard Company. Intel é uma marca comercial da Intel Corporation nos Estados Unidos e em outros países, utilizada sob licença. Microsoft e Windows são marcas registradas nos EUA da Microsoft Corporation.

As informações contidas neste documento estão sujeitas a alterações sem aviso. As únicas garantias para produtos e serviços da HP são as estabelecidas nas declarações de garantia expressa que acompanham tais produtos e serviços. Nenhuma informação contida neste documento deve ser interpretada como uma garantia adicional. A HP não será responsável por erros técnicos ou editoriais nem por omissões contidos neste documento.

Primeira edição: Agosto de 2012

Número de peça do documento: 702113-201

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

Os módulos de software disponíveis para o computador podem variar, dependendo do seu modelo.

Os módulos do software HP ProtectTools podem ser pré-instalados, pré-carregados, ou estar à disposição para download no site da HP. Consulte http://www.hp.com para obter mais informações.

**NOTA:** As instruções contidas neste guia pressupõem que os módulos aplicáveis do software HP ProtectTools já foram instalados.

## Recursos do HP ProtectTools

A tabela a seguir contém detalhes dos principais recursos dos módulos do HP ProtectTools.

| Módulo | Principais recursos |
|---|---|
| Console Administrativo do HP ProtectTools Security Manager | Os administradores podem executar as seguintes funções:<br>• Use o assistente de configuração do Security Manager para definir e configurar níveis de segurança e métodos de login de segurança.<br>• Configura opções ocultas de usuários.<br>• Ativar Drive Encryption e configurar acesso de usuário.<br>• Configurar políticas e acesso do usuário ao Device Access Manager.<br>• Usar ferramentas de administrador para adicionar e remover usuários do HP ProtectTools e ver status de usuários. |

| Módulo | Principais recursos |
| --- | --- |
| Console de usuário do HP ProtectTools Security Manager | Os usuários em geral podem executar as seguintes funções:<br>• Exibir configurações de status da criptografia e do Device Access Manager.<br>• Ativar o Computrace para o HP ProtectTools.<br>• Configurar preferências e opções de Backup e Restauração. |
| Gerenciador de Credenciais | Os usuários em geral podem executar as seguintes funções:<br>• Alterar nomes e senhas dos usuários.<br>• Configurar e alterar as credenciais dos usuários, tais como senha do Windows, impressão digital, imagens do rosto, smart card, cartão de proximidade, ou cartão sem contatos. |
| Gerenciador de Senhas | Os usuários em geral podem executar as seguintes funções:<br>• Organizar e configurar nomes de usuários e senhas.<br>• Cria senhas mais fortes para aumentar a segurança da conta. O Password Manager preenche e envia automaticamente as informações.<br>• Simplifique o processo de login com o recurso Single Sign On, que lembra e aplica as credenciais dos usuários. |
| Drive Encryption for HP ProtectTools (somente em determinados modelos) | • Oferece criptografia completa, de volumes inteiros, para unidades de disco rígido.<br>• Força a autenticação de pré-inicialização para decodificar e acessar dados.<br>• Oferece a opção de ativar unidades autocriptografadas (somente em determinados modelos). |
| 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.<br>• Impede que usuários não autorizados retirem dados usando uma mídia de armazenamento externa, além da introdução de vírus no sistema usando mídias externas.<br>• Permite aos administradores desativar o acesso de indivíduos específicos ou grupos de usuários a dispositivos de comunicação. |
| Recuperação em caso de roubo (Computrace for HP ProtectTools, vendido separadamente) | • Para ser ativado, requer a aquisição separada de assinaturas de rastreamento e acompanhamento.<br>• Fornece rastreamento seguro de ativo.<br>• Monitora a atividade do usuário, bem como as alterações de hardware e software.<br>• Permanece ativo ainda que o disco rígido seja reformatado ou substituído. |

# 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.

## Gerenciador de Senhas

O Password Manager armazena nomes de usuário e senhas e pode ser usado para:

- Salvar nomes e senhas de login para acesso à Internet ou ao 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 Password Manager para associar links da web a diferentes nomes de usuário e senhas. Quando ela acessa um site para fazer login, o Password Manager apresenta as credenciais automaticamente. Se ela quiser ver os nomes de usuário e senhas, o Password Manager pode ser configurado para exibi-los.

O Password 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 Password Manager. Ao concluir, o contador implementa o Password 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 (somente em determinados modelos)

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 exige 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 aumentar ainda mais a segurança da unidade optando por criptografar os dados com a opção de unidade autocriptografada.

O Drive Encryption for HP ProtectTools não permite 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.

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

O Device Access Manager for HP ProtectTools permite a um administrador restringir e gerenciar o acesso ao hardware. 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 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.

**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.

## Computrace for HP ProtectTools (anteriormente LoJack Pro) (comprado separadamente)

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

**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.

# Como alcançar os principais objetivos de segurança

Os módulos do HP ProtectTools trabalham juntos para oferecer soluções a uma série de questões de segurança, entre elas os seguintes objetivos principais de segurança:

- Proteção contra roubo direcionado
- Como restringir acesso a dados confidenciais
- Como evitar acesso não autorizado de locais internos ou externos
- Como criar políticas de senhas fortes

## Proteção contra roubo direcionado

Um exemplo de roubo direcionado seria o roubo de um computador que contivesse dados confidenciais e informações sobre clientes em um 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.
  - Security Manager for HP ProtectTools—Consulte HP ProtectTools Security Manager na página 26.
  - Drive Encryption for HP ProtectTools—Consulte Drive Encryption for HP ProtectTools (somente em determinados modelos) na página 42.
- A criptografia ajuda a garantir que não haverá acesso aos dados, mesmo que o disco rígido seja removido e instalado em um sistema desprotegido.
- O Computrace pode rastrear a localização do computador após um roubo.
  - Computrace for HP ProtectTools—Consulte Recuperação em caso de roubo (somente em determinados modelos) na página 62.

## Como restringir acesso a dados confidenciais

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 de comunicação, para que informações confidenciais não possam ser copiadas da unidade de disco rígido. Consulte Configuração de Classe de Dispositivo na página 53.

## Como evitar acesso não autorizado 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.
  - Security Manager for HP ProtectTools—Consulte HP ProtectTools Security Manager na página 26.
  - Drive Encryption for HP ProtectTools—Consulte Drive Encryption for HP ProtectTools (somente em determinados modelos) na página 42.
- O Security Manager ajuda a impedir que um usuário não autorizado obtenha senhas ou acesso a aplicativos protegidos por senha. Consulte HP ProtectTools Security Manager na página 26.
- 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. Consulte Device Access Manager for HP ProtectTools (somente em determinados modelos) na página 51.

## Como criar 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). Consulte HP ProtectTools Security Manager na página 26.

# Elementos de segurança adicional

## Atribuição de funções de segurança

No gerenciamento da segurança de computadores (principalmente para grandes organizações), um hábito importante é dividir responsabilidades e direitos entre diversos tipos de administradores e usuários.

**NOTA:** Em uma pequena organização ou para uso individual, essas funções podem ser atribuídas a uma só pessoa.

Para o HP ProtectTools, as obrigações e os privilégios de segurança podem ser distribuídos entre as 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.

  **NOTA:** Muitos dos recursos do HP ProtectTools podem ser personalizados pelo agente de segurança em colaboração com a HP. Para obter mais informações, consulte http://www.hp.com.
- 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:** O administradores são encorajados a seguir as “práticas recomendadas” ao restringir os privilégios do usuário final e o acesso de usuários.

Não se devem conceder privilégios administrativos a usuários não autorizados.

# Password Manager for HP ProtectTools

A maioria dos recursos do HP ProtectTools Security Manager são protegidos por senhas. A tabela a seguir enumera as senhas comumente usadas, o módulo do software onde a senha é configurada e a função da senha.

As senhas que são definidas e usadas somente pelos administradores de TI também são indicadas nesta tabela. Todas as outras senhas podem ser definidas pelos usuários normais ou pelos administradores.

| Senha do HP ProtectTools | Definida no seguinte módulo | Função |
|---|---|---|
| Senha de logon do Windows | Painel de controle do Windows ou HP ProtectTools Security Manager | Pode ser usada em login manual ou em autenticação para acesso a diversos recursos do Security Manager. |
| Senha do Security Manager Backup and Recovery | Security Manager, de usuário individual | Protege o acesso ao arquivo de backup e recuperação do Security Manager. |
| PIN do smart card | Gerenciador de Credenciais | Pode ser usado como autenticação multifatores.<br>Pode ser usado como autenticação do Windows.<br>Autentica usuários do Drive Encryption, se o smart card estiver selecionado. |

## Como criar uma senha segura

Ao criar senhas seguras, é preciso primeiro seguir todas as especificações definidas pelo programa. Geralmente, porém, pense em adotar as seguintes diretrizes para ajudá-lo a criar senhas fortes e reduzir as possibilidades de comprometimento da sua senha:

- 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 pontuações.
- Substitua letras por caracteres especiais ou números numa palavra-chave. Por exemplo, use o número 1 em vez das 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 esteja no 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.

- Troque de senha regularmente. Você pode trocar só alguns caracteres que incrementem.
- Caso anote a sua senha, não a guarde em local comumente visível que esteja muitoperto do computador.
- Não save a senha em um arquivo como, por exemplo, um email no computador.
- Não compartilhe contas nem revele a sua senha para ninguém.

## Backup de credenciais e configurações

Pode-se fazer backup de credenciais das seguintes maneiras:

- Use Drive Encryption for HP ProtectTools para selecionar e fazer o backup das credenciais do HP ProtectTools.
- Use a ferramenta Backup and Recovery no HP ProtectTools Security Manager como local central de onde fazer backup e recuperar credenciais de segurança de alguns dos módulos instalados do HP ProtectTools.

# 2 Passos Iniciais

Para configurar o HP ProtectTools, use o Assistente de Configuração do HP Client Security ou o Assistente de Configuração do HP ProtectTools Security Manager.

Após concluir o Assistente de Configuração do HP Client Security, o status do aplicativo será exibido no Painel de Controle do HP Client Security.

## Assistente de Configuração do HP Client Security

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

O Assistente de Configuração do HP Client Security ajuda você a configurar os recursos do Security Manager usados com mais frequência. Caso não tenha concluído o Assistente de Configuração do HP Client Security anteriormente, é possível iniciar o Assistente de Configuração do HP Client Security das seguintes maneiras:

▲ Na tela inicial, clique ou toque no apliacativo **HP Client Security**.

– ou –

Na área de trabalho do Windows, clique ou toque no gadget **HP ProtectTools**.

As páginas são exibidas na seguinte ordem:

1. **Senha do Windows**—Digite sua senha do Windows.

   Isto usará uma forte autenticação para proteger sua conta do Windows.

2. **SpareKey**—Para registrar a opção SpareKey, selecione três perguntas de segurança.

3. **Registrar impressões digitais**—Se um leitor de impressões digitais e o driver associado estiverem instalados, é possível registrar impressões digitais. É preciso selecionar e registrar pelo menos 2 impressões digitais.

4. **Criptografia da unidade**—Se o Drive Encryption for HP ProtectTools estiver instalado, é possível ativar a criptografia na unidade principal:

   - Criptografia de software para uma unidade de disco rígido tradicional
   - Criptografia de hardware se uma unidade autocriptografada for detectada.

   É preciso salvar uma chave de criptografia em pelo menos um dos itens a seguir antes de ativar a criptografia:

   **NOTA:** Se o assistente for cancelado, não será possível ativar o Windows nem a autenticação do Drive Encryption.

   - **Mídia removível**, como uma anidade USB flash no formato FAT32.
     - Essa opção é selecionada por padrão se uma única unidade removível for detectada antes da página do Drive Encryption ser exibida.
     - Se 2 ou mais dispositivos removíveis forem detectados, selecione uma das unidades exibidas.
   - **SkyDrive**—Essa opção fica disponível se uma conexão com a Internet for detectada.

É necessário um Live ID® do Windows. Insira seu ID e senha, ou registre-se.

5. A página Finalizar exibe uma notificação de sucesso, e solicita a reinicialização para que seja feita a ativação do Drive Encryption.

# Assistente de Configuração do HP ProtectTools Security Manager

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

Assistente de Configuração do HP ProtectTools Security Manager ajuda na configuração dos recursos do Security Manager. Além das configurações encontradas no assistente, os administradores podem configurar muitos recursos de segurança adicionais através do Console Administrativo. Essas configurações aplicam-se ao computador e a todos os usuários que o compartilham.

Para iniciar o Assistente de Configuração do HP ProtectTools Security Manager:

▲ Clique em **Assistente de configuração** no painel esquerdo do Console Administrativo e, então, siga as instruções na tela até que a configuração seja concluída.

Os administradores podem iniciar o console administrativo a partir do console de usuário do HP ProtectTools Security Manager. Para obter mais informações, consulte Console Administrativo do HP ProtectTools Security Manager na página 15.

O Security Manager e seus aplicativos estão disponíveis para todos os usuários que compartilham o computador.

# Painel de controle do HP Client Security

Para abrir o HP Client Security caso tenha concluído o Assistente de Configuração do HP Client Security:

▲ Na tela inicial, digite `hp` e selecione o **HP Client Security**.

O painel de controle exibirá uma visão geral dos recursos e status relacionados de cada aplicativo.

▲ Clique ou toque em uma linha de aplicativo para exibir mais informações sobre o aplicativo selecionado:

- O botão **Configurar agora** indica um aplicativo ainda não configurado. Clique ou toque no botão para abrir a página do aplicativo e configurá-lo.
- O botão **Configurações** indica um aplicativo com o status OK. Clique ou toque no botão para acessar as configurações do aplicativo.
- O **Console de usuário** é iniciado para uma configuração do usuário.
- O **Console administrativo** é iniciado para uma configuração que exija privilégios de administrador.
- O **Painel de status** fica aberto após o Console de usuário ou o Console administrativo for iniciado. Uma vez que as configurações tenham sido feitas e o console fechado, o status é atualizado.

# 3 Easy Setup Guide for Small Business

Este capítulo destina-se a demonstrar as etapas básicas para ativar as opções mais comuns e úteis dentro do HP ProtectTools for Small Business. Existem inúmeras ferramentas e opções disponíveis neste software que permitem fazer pequenos ajustes nas suas preferências e definir o seu controle de acesso. Este Easy Setup Guide se concentrará em fazer cada módulo funcionar com o mínimo possível de tempo e esforço na configuração. Para obter informações adicionais, selecione o módulo em que está interessado e clique em **?** ou no botão Ajuda no canto superior direito. Esse botão oferece automaticamente informações de ajuda a respeito da janela em exibição.

## Passos iniciais

1. Na área de trabalho do Windows, clique duas vezes no ícone do **HP ProtectTools** localizado na área de notificação, na extrema direita da barra de tarefas, para abrir o HP ProtectTools Security Manager.
2. Insira a sua senha do Windows, ou crie uma senha para o Windows.
3. Conclua o assistente de configuração.

**NOTA:** Por padrão, o HP ProtectTools Security Manager é definido como forte política de autenticação.

Essa configuração destina-se a impedir acesso não autorizado ao fazer login no Windows e deve ser usada quando houver necessidade de alta segurança, ou se os usuários se afastarem freqüentemente do sistema no decorrer do dia. Se quiser alterar essa configuração, clique na guia Política de Sessão e faça as suas seleções.

Para que o HP ProtectTools Security Manager exija autenticação apenas uma vez durante o logon do Windows, siga esses passos:

1. Na área de trabalho do Windows, clique duas vezes no ícone do **HP ProtectTools** localizado na área de notificação, na extrema direita da barra de tarefas, para abrir o HP ProtectTools Security Manager.
2. No painel esquerdo, clique em **Administração**, em seguida, clique em **Console Administrativo**.
3. No painel da esquerda em **Sistema**, selecione **Autenticação** no grupo **Segurança**.
4. Clique na guia **Política de sessão** e selecione os requisitos de combinação de logon para a sessão. Para restaurar as configurações, clique em **Restaurar padrões**.
5. Clique no botão **Aplicar** quando terminar.

## Password Manager

Senhas! Todos temos um grande número de senhas – principalmente se costumamos acessar sites ou usar aplicativos que exijam logon. O usuário normal ou usa a mesma senha para todos os aplicativos e sites, ou exagera na criatividade e acaba esquecendo a qual site cada senha pertence.

O Password Manager lembra suas senhas automaticamente ou oferece a opção de escolher para quais sites lembrar e para quais omitir. Após se conectar ao computador, o Password Manager fornecerá suas senhas ou credenciais aos sites e aplicativos participantes.

Ao acessar qualquer aplicativo ou siste que exija credenciais, o Password Manager reconhece o site automaticamente e pergunta se o usuário quer que o software se lembre das suas informações. Se quiser excluir certos siste, é possível declinar o pedido.

Para começar a salvar sites, nomes de usuários e senhas:

1. Por exemplo, navegue até um aplicativo ou site participante e clique no ícone do Password Manager no canto superior esquerdo da página para adicionar a autenticação web.
2. Dê nome ao link (opcional) e insira um nome de usuário e uma senha no Password Manager.

**NOTA:** As áreas que o Password Manager usará agora e nas visitas subsequentes estão realçadas.

3. Quando terminar, clique no botão **OK**.
4. O Password Manager também salva o nome de usuário e a senha de compartilhamentos na rede ou de unidades de rede.

## Exibir e gerenciar as autenticações salvas no Password Manager

O Password Manager permite ver, gerenciar, fazer backup e iniciar as autenticações num local central. O Password Manager também aceita iniciar sites salvos do Windows.

Para abrir o Password Manager, use um destes dois métodos:

- Use a combinação de teclas ctrl+tecla do logo do Windows+h para abrir o Password Manager, e depois clique em **Open** para iniciar e autenticar o atalho salvo.

  – ou –

- Selecione a guia **Gerenciar** no Password Manager para abrir o HP ProtectTools Security Manager e editar as credenciais.

A opção **Editar** do Password Manager permite visualizar e modificar o nome, o nome de logon, e até mesmo revelar as senhas.

HP ProtectTools para pequenas empresas permite que seja feito back-up de todas as credenciais e configurações, ou que estas sejam copiadas para outro computador.

# Device Access Manager for HP ProtectTools

Pode-se usar o Device Access Manager para restringir o uso de diversos dispositivos, internos e externos, de armazenamento para que os dados permaneçam seguros no disco rígido e não saiam de dentro da sua empresa. Um exemplo seria permitir a um usuário o acesso aos dados, porém impedi-lo de copiá-los em CD, reprodutor pessoal de música, ou dispositivo de memória USB. Abaixo há um modo fácil de configurar isso.

1. Na área de trabalho do Windows, clique duas vezes no ícone do **HP ProtectTools** localizado na área de notificação, na extrema direita da barra de tarefas, para abrir o console de usuário do HP ProtectTools Security Manager.
2. No painel esquerdo do HP ProtectTools Security Manager, clique em **Administração**, em seguida, clique em **Console Administrativo**.
3. Clique em **Device Access Manager** e, em seguida, clique em **Configuração de Classe de Dispositivo**.
4. O próximo passo é selecionar quem vai continuar a ter a acesso enquanto todos os outros estiverem bloqueados.
5. Selecione os dispositivos de hardware que quiser restringir e, então, clique no botão **Aplicar** para concluir o processo.
6. Selecione **Adicionar**, clique em **Avançado** e, então, clique em **Encontrar agora**.
7. Selecione o usuário desejado e clique em **OK > OK > Aplicar**.

   Sua escolha será exibida na caixa **Usuários/Grupos**.
8. Selecione a **Classe de dispositivo** que será usada pelo usuário, selecione **Permitir** ou **Negar**, e clique em **Aplicar**.

# Drive Encryption for HP ProtectTools

O Drive Encryption for HP ProtectTools é usado para proteger os dados por meio da criptografia de todo o disco rígido. Os dados contidos no disco rígido ficarão protegidos se o seu PC for roubado ou se o disco rígido for removido do computador original e instalado em outro computador.

Um outro benefício de segurança é que o Drive Encryption exige a autenticação imediata com nome de usuário e senha para que o sistema operacional seja inicializado. Esse processo é chamado de autenticação na pré-inicialização.

Para facilitar, diversos módulos de software sincronizam as senhas automaticamente, entre elas contas de usuário do Windows, domínios, Drive Encryption for HP ProtectTools, Password Manager e HP ProtectTools Security Manager.

Adote as seguintes etapas simples para ativar o Drive Encryption for HP ProtectTools:

1. Na área de trabalho do Windows, clique duas vezes no ícone do **HP ProtectTools** localizado na área de notificação, na extrema direita da barra de tarefas, para abrir o HP ProtectTools Security Manager.
2. No painel esquerdo, clique em **Administração**, em seguida, clique em **Console Administrativo**.
3. No painel esquerdo, clique em **Assistente de Configuração**.
4. Selecione **Avançar** na tela de boas-vindas.

5. Digite a sua senha do Windows para iniciar o assistente de ativação e, então, clique em **Avançar**.
6. Ignore o SpareKey se ele não for desejado.
7. Marque a caixa de seleção **Drive Encryption** e clique em **Avançar**.
8. Marque a unidade a criptografar e, então, clique em **Avançar**.
9. A janela de configuração do Drive Encryption requer uma unidade flash USB ou outro dispositivo externo para que a chave de recuperação de criptografia seja armazenada. Mantenha essa chave de recuperação segura e guardada, pois será usada para recuperar dados ou acessar a unidade caso a senha de pré-inicialização seja perdida ou esquecida.
10. Clique em **Avançar**, conclua o processo e, então, clique em **Concluir**. Remova a unidade flash USB e reinicie o computador quando estiver pronto.
11. Quando o sistema iniciar, o Drive Encryption vai pedir a sua senha do Windows. Digite a senha e, depois, clique em **OK**.

**NOTA:** O computador pode aparentar lentidão enquanto a unidade é criptografada. Após a conclusão da criptografia, o desempenho retornará ao normal. Conforme os dados da unidade forem acessados, estes serão criptografados e descriptografados de acordo com as solicitações do administrador.

A autenticação do Drive Encryption “passará” do logon do Windows diretamente para a área de trabalho do Windows. Dessa forma, não será necessário inserir a senha duas vezes.

# 4 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 console de usuário do Security Manager para auxiliar na recuperação do computador se ele for perdido ou roubado.

Usando o Console Administrativo, 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

## Passos iniciais

Para configurar o HP ProtectTools, use o Assistente de Configuração do HP Client Security ou o Assistente de Configuração do HP ProtectTools Security Manager.

Após concluir o Assistente de Configuração do HP Client Security, o status do aplicativo será exibido no Painel de Controle do HP Client Security.

### Assistente de Configuração do HP Client Security

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

O Assistente de Configuração do HP Client Security ajuda você a configurar os recursos do Security Manager usados com mais frequência. Caso não tenha concluído o Assistente de Configuração do HP Client Security anteriormente, é possível iniciar o Assistente de Configuração do HP Client Security das seguintes maneiras:

▲ Na tela inicial, clique ou toque no apliacativo **HP Client Security**.

– ou –

Na área de trabalho do Windows, clique ou toque no gadget **HP ProtectTools**.

As páginas são exibidas na seguinte ordem:

1. **Senha do Windows**—Digite sua senha do Windows.

   Isto usará uma forte autenticação para proteger sua conta do Windows.

2. **SpareKey**—Para registrar a opção SpareKey, selecione três perguntas de segurança.

3. **Registrar impressões digitais**—Se um leitor de impressões digitais e o driver associado estiverem instalados, é possível registrar impressões digitais. É preciso selecionar e registrar pelo menos 2 impressões digitais.

4. **Criptografia da unidade**—Se o Drive Encryption for HP ProtectTools estiver instalado, é possível ativar a criptografia na unidade principal:

   - Criptografia de software para uma unidade de disco rígido tradicional
   - Criptografia de hardware se uma unidade autocriptografada for detectada.

   É preciso salvar uma chave de criptografia em pelo menos um dos itens a seguir antes de ativar a criptografia:

   **NOTA:** Se o assistente for cancelado, não será possível ativar o Windows nem a autenticação do Drive Encryption.

   - **Mídia removível**, como uma anidade USB flash no formato FAT32.
     - Essa opção é selecionada por padrão se uma única unidade removível for detectada antes da página do Drive Encryption ser exibida.
     - Se 2 ou mais dispositivos removíveis forem detectados, selecione uma das unidades exibidas.
   - **SkyDrive**—Essa opção fica disponível se uma conexão com a Internet for detectada.

     É necessário um Live ID® do Windows. Insira seu ID e senha, ou registre-se.

5. A página Finalizar exibe uma notificação de sucesso, e solicita a reinicialização para que seja feita a ativação do Drive Encryption.

## Assistente de Configuração do HP ProtectTools Security Manager

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

Assistente de Configuração do HP ProtectTools Security Manager ajuda na configuração dos recursos do Security Manager. Além das configurações encontradas no assistente, os administradores podem configurar muitos recursos de segurança adicionais através do Console Administrativo. Essas configurações aplicam-se ao computador e a todos os usuários que o compartilham.

Para iniciar o Assistente de Configuração do HP ProtectTools Security Manager:

▲ Clique em **Assistente de configuração** no painel esquerdo do Console Administrativo e, então, siga as instruções na tela até que a configuração seja concluída.

Os administradores podem iniciar o console administrativo a partir do console de usuário do HP ProtectTools Security Manager. Para obter mais informações, consulte Console Administrativo do HP ProtectTools Security Manager na página 15.

O Security Manager e seus aplicativos estão disponíveis para todos os usuários que compartilham o computador.

## Painel de controle do HP Client Security

Para abrir o HP Client Security caso tenha concluído o Assistente de Configuração do HP Client Security:

▲ Na tela inicial, digite `hp` e selecione o **HP Client Security**.

O painel de controle exibirá uma visão geral dos recursos e status relacionados de cada aplicativo.

▲ Clique ou toque em uma linha de aplicativo para exibir mais informações sobre o aplicativo selecionado:

- O botão **Configurar agora** indica um aplicativo ainda não configurado. Clique ou toque no botão para abrir a página do aplicativo e configurá-lo.
- O botão **Configurações** indica um aplicativo com o status OK. Clique ou toque no botão para acessar as configurações do aplicativo.
- O **Console de usuário** é iniciado para uma configuração do usuário.
- O **Console administrativo** é iniciado para uma configuração que exija privilégios de administrador.
- O **Painel de status** fica aberto após o Console de usuário ou o Console administrativo for iniciado. Uma vez que as configurações tenham sido feitas e o console fechado, o status é atualizado.

# Abertura do Console Administrativo do HP ProtectTools

Use o Console Administrativo do HP ProtectTools para tarefas administrativas, tais como estabelecimento de políticas de sistema ou configurações de software. Abra o HP ProtectTools Security Manager para acessar o Console Administrativo:

1. Na área de trabalho do Windows, clique duas vezes no ícone do **HP ProtectTools** na área de notificação, à direita da barra de tarefas.

   – ou –

   No **Painel de controle**, selecione **Sistema e Segurança** e, então, selecione **HP ProtectTools Security Manager**.

2. No painel esquerdo do console de usuário 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.

1. Na área de trabalho do Windows, clique duas vezes no ícone do **HP ProtectTools** na área de notificação, à direita da barra de tarefas.

   – ou –

   No **Painel de controle**, selecione **Sistema e Segurança** e, então, selecione **HP ProtectTools Security Manager**.

2. No painel esquerdo do console de usuário do Security Manager, clique em **Administração**, em seguida, clique em **Console Administrativo**.

O Console Administrativo exibe as seguintes seleções na Página inicial no painel esquerdo:

- **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**—Permite que você configure o Drive Encryption (somente os modelos selecionados).
- **Computador**—Permite que você configure o Device Access Manager.
- **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 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 e especifique as configurações.

## 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 para 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**, selecione uma categoria de usuário, como Administradores ou Usuários comuns.
3. Clique em uma credencial para exibir a caixa de diálogo de edição.
4. Para exigir uma combinação de duas credenciais de autenticação, clique na seta para baixo para selecionar cada credencial e clique em **OK**.
5. Para remover uma credencial, clique no **X** ou clique com o botão direito do mouse na credencial e clique em **Excluir**.
6. Clique em **Sim** na caixa de diálogo de configuração.
7. Para confirmar se os usuários conseguem fazer login, clique em **Verifique se os usuários do HP ProtectTools podem fazer login**.
8. Para retornar às configurações originais, clique em **Restaurar padrões**.
9. Clique em **Aplicar**.

## Política de sessão

Para definir as políticas referentes às credenciais necessárias, com o objetivo de realizar uma autenticação 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**, selecione uma categoria de usuário, como Administradores ou Usuários comuns.
3. Clique em uma credencial para exibir a caixa de diálogo de edição.
4. Para exigir uma combinação de duas credenciais de autenticação, clique na seta para baixo para selecionar cada credencial e clique em **OK**.
5. Para remover uma credencial, clique no **X** ou clique com o botão direito do mouse na credencial e clique em **Excluir**.
6. Clique em **Sim** na caixa de diálogo de configuração.
7. Para confirmar se os usuários conseguem fazer login, clique em **Verifique se os usuários do HP ProtectTools podem fazer login**.
8. Para retornar às configurações originais, clique em **Restaurar padrões**.
9. Clique em **Aplicar**.

## Configurações

Para permitir que os usuários do computador ignorem o login do Windows se a autenticação já tiver sido realizada no nível do BIOS ou no nível do Drive Encryption:

1. No painel esquerdo do Console Administrativo, clique em **Segurança**, em seguida clique em **Configurações**.
2. **Permitir login único**—Marque a caixa de seleção para ativar o Login único ou desmarque a caixa de seleção para desativá-lo.
3. 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 quanto 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 para 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. 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.
2. Para permitir a recuperação do SpareKey para login no Windows, marque a caixa de seleção.
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 de seus dedos.

  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.

## Rosto

Se uma webcam estiver instalada ou conectada ao computador, e se o programa Face Recognition estiver instalado, os administradores poderão 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 **Credenciais** e, em seguida, clique em **Rosto**.
2. 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**.

3. Para retornar as configurações aos valores originais, clique em **Restaurar padrões**.
4. Clique em **Aplicar**.

## Smart card

É necessário que os administradores inicializem o smart card antes que ele possa ser usado para autenticação. A maioria dos smart cards padrão CSP e PKCS11 são suportados no Windows.

### 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 middleware do smart card precisa estar instalado.

1. Obtenha e instale o middleware para o smart card usado (como o ActivClient 6.x para um smart card ActivIdentity).
2. Insira o smart card no leitor.
3. Inicialize (formate) o smart card.
   a. Inicie a ferramenta de inicialização do smart card, ou ela pode ter sido exibida quando você inseriu o smart card no leitor.
   b. Siga as instruções na tela para configurar um PIN.
   c. Anote o código de desbloqueio para futura referência.
4. Crie um par de chaves e um certificado.
   a. Inicie o **Console Administrativo do HP ProtectTools**.
   b. Clique em **Credenciais**, em **Smart Card** e na guia **Administração**.
   c. Certifique-se de que a opção **Inicializar o smart card** esteja selecionada.
   d. Insira o PIN, clique em **Aplicar** e siga as instruções na tela.

      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. Clique no **Assistente de Configuração**.
2. Na tela **Bem-vindo!**, clique em **Avançar**.
3. Insira sua senha do Windows e, em seguida, clique em **Avançar**.
4. Na página **SpareKey**, clique em **Ignorar configuração do SpareKey**, a não ser que você queira atualizar suas informações do SpareKey e clique em **Avançar**.
5. Na página **Ativar recursos de segurança**, clique em **Avançar**.
6. Na página **Escolher suas credenciais**, certifique-se de que a opção **Smart card** esteja selecionada, e em seguida clique em **Avançar**.

7. Na página **Smart card**, insira o PIN e clique em **Avançar**.
8. Clique em **Concluir**.

Os usuários também podem registrar um smart card no console de usuário do Security Manager. Para obter mais informações, consulte a ajuda do software HP ProtectTools Security Manager clicando no ícone **?** azul no canto superior direito da página Smart card.

### Configuração do smart card

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

- **Configurações**—Marque a caixa de seleção **Bloquear computador ao remover smart card** para configurar o computador para ser bloqueado automaticamente quando um smart card for removido e clique em **Aplicar**.

**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**—Apaga 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 compatíveis com seu smart card ou middleware associado não estão disponíveis.

▲ Clique em **Aplicar**.

## Cartão sem contatos

Um cartão sem contatos é um pequeno cartão de plástico que contém um chip de computador. Se um leitor de cartão sem contatos estiver conectado ao computador, se o driver associado do fabricante tiver sido instalado e se um cartão sem contatos tiver sido selecionado como credencial de autenticação, você poderá usar o cartão sem contatos para autenticação. Os seguintes tipos de cartões sem contatos são suportados pelo HP ProtectTools:

- Cartões de memória Contactless HID iCLASS
- Contactless MiFare Classic 1k, 4k e mini cartões de memória

▲ Para configurar seu cartão sem contatos, coloque-o muito perto do leitor, siga as instruções na tela e clique em **Aplicar**.

### Cartão de proximidade

Um cartão de proximidade é um pequeno cartão de plástico que contém um chip de computador. Se um leitor de cartão de proximidade estiver conectado ao computador, se o driver associado do fabricante tiver sido instalado e se um cartão de proximidade tiver sido selecionado como uma credencial de autenticação, você poderá usar um cartão proximidade em conjunto com qualquer outra credencial para obter segurança adicional.

▲ Para configurar seu cartão de proximidade, coloque-o bem perto do leitor e clique em **Aplicar**.

### Bluetooth

Se o computador estiver equipado com a® funcionalidade Bluetooth, se Bluetooth tiver sido selecionado como uma credencial de autenticação e se um telefone Bluetooth estiver pareado com o computador, você poderá usar seu telefone Bluetooth com qualquer outra credencial para obter segurança adicional. Especificar as configurações Bluetooth:

▲ Para permitir a autenticação silenciosa, marque a caixa de seleção e clique em **Aplicar**.

### PIN

Se PIN tiver sido selecionado como uma credencial de autenticação, você poderá usar um PIN em conjunto com outras credenciais para obter segurança adicional. Especifique as configurações do PIN:

1. Clique na seta para cima ou para baixo para selecionar o comprimento mínimo do PIN.

   O número máximo de dígitos permitidos é 8.

2. Clique em **Aplicar**.

# Aplicativos

A página Configurações de Aplicativos no painel esquerdo do Console Administrativo contém duas guias que permitem a você personalizar o comportamento dos aplicativos do HP ProtectTools Security Manager recém-instalados.

▲ No painel esquerdo do Console Administrativo, em **Aplicativos**, clique em **Configurações**.

## 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.

1. Marque a caixa de seleção próxima a uma configuração específica para ativá-la, ou desmarque a caixa de seleção para desativar a configuração.
2. Clique em **Aplicar**.

## Guia Aplicativos

Os administradores podem ativar ou desativar os seguintes aplicativos:

- **Status**—Marque a caixa de seleção para ativar todos os aplicativos ou desmarque a caixa de seleção para desativá-los.
- **Password Manager**—Ativa o aplicativo Password Manager para todos os usuários do computador.

1. Marque a caixa de seleção próxima a uma configuração específica para ativá-la, ou desmarque a caixa de seleção para desativar a configuração.
2. Clique em **Aplicar**.

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

# Dados

A seção Dados do painel esquerdo do Console Administrativo permite que você configure o seguinte aplicativo:

- **Drive Encryption**—Configurar e exibir o status da unidade. Para obter mais informações, consulte a Ajuda do software Drive Encryption clicando no ícone **?** azul no canto superior direito da página Drive Encryption.

# Computador

A seção Computador do painel esquerdo do Console Administrativo permite que você configure o aplicativo Device Access Manager:

- Configuração Simples
- Configuração de Classe de Dispositivo
- Configuração da autenticação Just-In-Time (JITA)
- Configurações avançadas

Para obter mais informações, consulte a Ajuda do software Device Access Manager clicando no ícone **?** azul no canto superior direito da página Device Access Manager.

# 5 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:

▲ Na área de trabalho do Windows, clique duas vezes no ícone do **HP ProtectTools** na área de notificação, à direita da barra de tarefas.

– ou –

No **Painel de controle**, selecione **Sistema e Segurança** e, então, selecione **HP ProtectTools Security Manager**.

## Usando o Console de Usuário do Security Manager

O console de usuário do Security Manager é o ponto central para se ter acesso fácil aos recursos, aplicativos e configurações do HP ProtectTools Security Manager. O Console de Usuário exibe os seguintes componentes:

- **ID Card**—Exibe o nome de usuário do Windows e um ícone para identificar 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.
  - **Recuperação em caso de roubo**—Computrace for HP ProtectTools (vendido separadamente)
- **Meus Logins**—Gerencie suas credenciais de autenticação com o Password Manager e o Credential Manager.

- **Meus Dados**—Gerencie a segurança de seus dados com Drive Encryption.

**NOTA:** Este item não é exibido se o aplicativo não estiver instalado.

- **Meu Computador**—Gerencie a segurança de seu computador com Device Access Manager.

**NOTA:** Este item não é exibido se o aplicativo não estiver instalado.

- **Administratção**—Permite que os administradores acessem o **Console Administrativo** para gerenciar a segurança e os usuários.
- **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 Console de Usuário do Security Manager. Este ícone se encontra na parte superior direita do quadro da janela, próximo aos ícones minimizar e maximizar.

# Seu ID card pessoal

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

Você pode alterar 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 console de usuário do Security Manager. Para obter mais informações, consulte Abertura do Security Manager na página 26.
2. Clique em ID Card no canto superior esquerdo do console de usuário.
3. Clique na caixa que exibe o nome de usuário do Windows para esta conta, digite o novo nome e clique em **Salvar**.

# 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, seu rosto, smart card, cartão de proximidade, cartão sem contatos, telefone Bluetooth ou PIN.
- **Credential Manager**—Fornece um meio de alterar sua senha do Windows, registrar impressões digitais, registrar rostos ou configurar um smart card, cartão sem contatos, cartão de proximidade, telefone Bluetooth ou PIN com facilidade.

Os administradores podem acessar informações sobre aplicativos de segurança adicionais disponíveis 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, rosto, smart card, cartão de proximidade, cartão sem contatos, PIN ou da senha do Windows.

O Password Manager oferece as seguintes opções:

### Guia Gerenciar

- Adicionar, editar ou excluir logins.
- 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.

### Guia Força da senha

- Verificar a força de senhas individuais usadas em sites da web e aplicativos, além da força da senha geral.
- A força da senha é ilustrada por indicadores de status vermelhos, amarelos ou verdes.

O ícone do **Password Manager** 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, será exibido um sinal de adição (+) no ícone.

▲ Clique no ícone do **Password Manager** para exibir um menu de contexto em que você pode escolher entre as opções a seguir.

- Adicionar [domínio.com] ao Password Manager
- Abrir o Password Manager
- Configurações de ícones
- Ajuda

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

As opções abaixo são exibidas no menu de contexto:

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

- **Preencha os dados de login**—Exibe uma página Verificar sua identidade. Se autenticados com sucesso, seus dados de login serão colocados automaticamente nos campos de login e a página será enviada (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 ao Gerenciador de Senhas.
- **Abrir Gerenciador de Senhas**—Abre o Gerenciador de Senhas.
- **Ajuda**—Exibe a Ajuda do 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. É possível usar esses logins após navegar até o site da Web ou programa ou clicar em um login do menu **Links Rápidos do Password Manager** para que o Password Manager abra o site da Web ou programa e faça o seu login.

Para adicionar um login:

1. Abra a tela de login de um site da Web ou programa.
2. Clique na seta do ícone do **Password Manager** e, a seguir, clique em uma das seguintes opções, dependendo de pertencer a tela de login a um site da Web ou 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. Também é possível ver essa caixa de diálogo clicando em **Adicionar login** na guia **Gerenciar Password Manager**, usando o atalho ctrl+tecla do logotipo do Windows+h ou deslizando o(s) dedo(s).
   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. Clique em **OK** para selecionar o método de autenticação que deseja usar (impressões digitais, rosto, smart card, cartão de proximidade, cartão sem contatos, telefone Bluetooth, PIN ou senha) e, em seguida, faça login com 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.

e. 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.
   - Clique em **Fechar**.

Toda vez em que você acessar esse site da Web ou abrir esse programa, o ícone do **Gerenciador de Senhas** 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 fazer o login.

## Edição de logins

Para editar um login, siga as etapas abaixo:

1. Abra a tela de login de 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 em **Editar 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 **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 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**.

## Uso do menu Links Rápidos do Password Manager

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 **Links Rápidos do Password Manager**, 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 **Links Rápidos** do Password Manager.

Para exibir o menu **Links Rápidos**:

1. Pressione a combinação de teclas de atalho do **Gerenciador de Senhas** (ctrl+tecla de logo do Windows+h é a configuração de fábrica). Para alterar a combinação de tecla de atalho, no console de usuário do Security Manager, clique em **Password Manager** e depois em **Configurações**.
2. Forneça 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 Console de Usuário do Security Manager, clique em **Security 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 console de usuário do Security Manager, clique em **Gerenciador de Senhas** e, a seguir, na guia **Gerenciar**.

- **Adicionar um login**—Clique em **Adicionar login** e siga as instruções na tela.
- **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 29.

- **Editar**—Edite um login. Para obter mais informações, consulte Edição de logins na página 30.
- **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 31.

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

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

Na guia **Força da senha**, indicadores de status vermelhos, amarelos ou verdes ilustram a força das senhas individuais usadas em sites da web e aplicativos, além da força da senha geral.

## Configurações do ícone do Password Manager

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

1. Clique no ícone e, em seguida, clique em **Configurações do Ícone** para personalizar a forma como o Gerenciador de Senhas trata possíveis sites de login.
   - **Sugerir a adição de logins para telas de login**—Clique nesta opção para que o Gerenciador de Senhas solicite que você adicione um login quando for exibida uma tela de login para a qual ainda não exista um login configurado.
   - **Excluir esta tela**—Marque essa caixa de seleção para que o Gerenciador de Senhas 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 console de usuário do Security Manager e clique em **Gerenciador de Senhas**.
     - 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 29.
- O ícone do **Password Manager** será exibido sempre que a tela de login desse site da Web ou programa se abrir.

**Não solicitar para adicionar logins para telas de login**—Selecione o botão de opção.

2. Para acessar configurações adicionais do Gerenciador de Senhas, clique em **Gerenciador de Senhas** e depois em **Configurações** no console de usuário do Security Manager.

### Configurações

É possível especificar configurações para personalizar o Password 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 ao menu **Logins**. Para desativar esse recurso, desmarque a caixa de seleção ao lado de **Sugerir a adição de logins para telas de login**.
2. **Abrir o Gerenciador de Senhas com ctrl+win+h**—O atalho padrão que abre o menu de **Links Rápidos do Gerenciador de Senhas** 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 verificar sua identidade. 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
- Rosto
- Smart Card
- Cartão sem Contatos
- Cartão de Proximidade
- Bluetooth
- PIN

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 console de usuário 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.

HP ProtectTools Security Manager solicita a definição de sua SpareKey durante a configuração inicial no Assistente de Configuração do HP ProtectTools Security Manager.

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 **Criar**.

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 de boas-vindas do Windows.

## Registro de impressões digitais

Se o administrador selecionou Impressões digitais na tela **Escolher suas credenciais** e o computador tiver um leitor de impressões digitais integrado ou conectado a ele, o Assistente de Configuração do HP ProtectTools Security Manager guiará você pelo processo de configuração ou registro de impressões digitais. Também é possível registrar suas impressões digitais na página Impressão digital em **Credential Manager** no console de usuário do Security Manager.

1. Na página de impressões digitais do assistente, um desenho de duas mãos é exibido. 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. Será solicitado que você deslize o dedo até que sua impressão digital seja registrada com sucesso. O dedo registrado será realçado 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 assistente, 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.

## Registro de cenas para login com rosto

Se você escolher login com rosto, e se uma webcam estiver integrada ou conectada ao seu computador, o Assistente de Configuração do HP ProtectTools Security Manager solicitará que você registre cenas. Também é possível registrar cenas na página de login Rosto em **Credential Manager** no console de usuário 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 com o assistente de instalação do HP ProtectTools Security Manager:

1. Na página de login de rosto do assistente, clique em **Avançado** e configure opções adicionais. Para obter mais informações, consulte Configurações avançadas do usuário na página 37.
2. Clique em **OK**.
3. Clique em **Iniciar**, ou se tiver registrado cenas anteriormente, clique em **Registrar nova cena**.
4. Durante o registro da cena, você poderá assistir uma demonstração clicando em **Reproduzir vídeo**.

   Se este for o primeiro registro, será exibida uma caixa de diálogo perguntando se você deseja ver um vídeo de demonstração. Clique em **Sim** ou em **Não**.
5. Com pouca luz, o software pode iluminar a tela automaticamente ou, para alterar a luz de fundo, clique no ícone **Lâmpada**.
6. Clique no ícone **Câmera** e siga as instruções na tela para registrar sua cena.

   **NOTA:** Observe sua imagem, virando sua cabeça adequadamente, enquanto as cenas estiverem sendo capturadas.
7. Clique em **Avançar**.

Também é possível registrar cenas a partir do console de usuário do Security Manager:

1. Abra o console de usuário do Security Manager. Para obter mais informações, consulte Abertura do Security Manager na página 26.
2. Em **Meus Logins**, clique em **Credential Manager** e clique em **Rosto**.
3. Clique em **Avançado** para configurar as opções adicionais. Para obter mais informações, consulte Configurações avançadas do usuário na página 37.
4. Clique em **OK**.
5. Clique em **Iniciar**, ou se tiver registrado cenas anteriormente, clique em **Registrar nova cena**.
6. Caso você seja solicitado a inserir sua senha do Windows, insira-a e, em seguida, clique em **Avançar**.

7. Durante o registro da cena, você poderá assistir uma demonstração clicando em **Reproduzir vídeo**.

   Se este for o primeiro registro, será exibida uma caixa de diálogo perguntando se você deseja ver um vídeo de demonstração. Clique em **Sim** ou em **Não**.

8. Com pouca luz, o software pode iluminar a tela automaticamente ou, para alterar a luz de fundo, clique no ícone **Lâmpada**.

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

**NOTA:** Observe sua imagem, virando sua cabeça adequadamente, enquanto as cenas estiverem sendo capturadas.

Para obter mais informações, consulte a Ajuda do software Face Recognition clicando no ícone **?** azul no canto superior direito da página de registro.

### Autenticação

Após o registro de uma ou mais cenas, você pode usar seu rosto para a autenticação quando fizer login no computador ou quando iniciar uma nova sessão do Windows.

1. Quando a tela de autenticação for iniciada e a câmera detectar seu rosto, você terá 5 segundos para iniciar o processo de login. Se o seu rosto for autenticado com sucesso, será possível acessar o computador.

2. Se o limite de tempo do login com rosto for excedido, o Face Recognition pausará. Clique no ícone **Câmera** para retornar ao processo de autenticação.

**NOTA:** Se a iluminação for insuficiente, e se você não puder fazer login usando o Face Recognition, digite sua senha do Windows para fazer login no computador.

3. Depois de fazer login no computador, se o Face Recognition solicitar a inclusão de cenas adicionais para aprimorar sua capacidade de fazer login em futuras sessões, clique em **Sim**.

### Modo escuro

Se a iluminação estiver muito fraca durante o processo de login com rosto, a cor do plano de fundo da tela de login com rosto se torna automaticamente branca a fim de fornecer uma melhor iluminação do rosto.

Para alterar manualmente a cor do plano de fundo da tela de login com rosto, clique no ícone **Lâmpada**.

### Aprendizado

Se você não conseguir fazer login com rosto mas tiver sucesso ao inserir sua senha, talvez lhe seja solicitado salvar uma série de imagens para aumentar as chances de fazer login com rosto bem-sucedido no futuro.

### Exclusão de uma cena

Para excluir uma cena atualmente registrada:

1. Abra o console de usuário do Security Manager. Para obter mais informações, consulte Abertura do Security Manager na página 26.

2. Em **Meus Logins**, clique em **Credential Manager**, em seguida, clique em **Rosto**.

3. Clique na cena a ser excluída e, em seguida, clique no ícone **Lixeira**.

4. Clique em **OK** na caixa de diálogo de confirmação.

### Configurações avançadas do usuário

1. Abra o console de usuário do Security Manager. Para obter mais informações, consulte Abertura do Security Manager na página 26.
2. Em **Meus Logins**, clique em **Credential Manager** e clique em **Rosto**.
3. Clique em **Avançado** para configurar as seguintes opções:

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

   - **Reproduzir som nos eventos de reconhecimento de rosto**—Toca um som quando o login de rosto é bem-sucedido ou falha
   - **Solicitar atualização de cenas quando houver falha no login**—Se o login de rosto não for bem-sucedido, mas você inserir sua senha com sucesso, talvez seja solicitado o salvamento da série de imagens capturadas para aumentar a chance de um login de rosto bem-sucedido no futuro.
   - **Solicitar registro de uma nova cena quando houver falha no login**—Se o login de rosto não for bem-sucedido, mas você inserir sua senha com sucesso, talvez seja solicitado o registro de uma nova cena para aumentar a chance de um login de rosto bem-sucedido no futuro
4. Para retornar as configurações aos valores originais, clique em **Restaurar padrões**.
5. Clique em **OK**.

## Configuração de um smart card

Se o leitor de smart card for interno ou se estiver conectado ao computador e se o administrador tiver ativado um smart card como uma credencial de autenticação e executado as etapas descritas na Ajuda do software Console Administrativo do HP ProtectTools, o Assistente de Configuração do HP ProtectTools Security Manager solicitará a inserção e a configuração de um smart card. Você também pode configurar seu smart card na página Smart Card em **Credential Manager**, no console de usuário do Security Manager.

**NOTA:** É necessário que os administradores inicializem o smart card antes que ele possa ser usado.

### 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 gerenciamento de PIN que o HP ProtectTools usará em seu algoritmo de segurança.

Os administradores também podem inicializar o smart card usando o software do fabricante e o Console Administrativo do HP ProtectTools.' Para obter mais informações, consulte a ajuda do software Console Administrativo do HP ProtectTools.

### Registro do smart card

Após o smart card ser inicializado, os usuários podem registrá-lo no Security Manager:

1. Abra o console de usuário do Security Manager. Para obter mais informações, consulte Abertura do Security Manager na página 26.
2. Clique em **Credential Manager** e em **Smart card**.

3. Certifique-se de que a opção **Configurar** esteja selecionada.
4. Insira sua senha do Windows e seu PIN, em seguida clique em **Salvar**.

Os administradores também podem registrar o smart card no Console Administrativo do HP ProtectTools. Para obter mais informações, consulte a ajuda do software Console Administrativo do HP ProtectTools.

### Alteração do PIN do smart card

Para alterar o PIN do smart card:

1. Insira um smart card que tenha sido anteriormente formatado e inicializado.
2. Selecione **Alterar PIN do smart card**.
3. Insira seu PIN antigo e, em seguida, insira e confirme um novo PIN.

## Cartão sem contatos

Um cartão sem contatos é um pequeno cartão de plástico que contém um chip de computador. Se um leitor de cartão sem contatos estiver conectado ao computador, se o administrador tiver instalado o driver associado do fabricante e se o administrador tiver ativado um cartão sem contatos como uma credencial de autenticação, você poderá usar um cartão sem contatos como uma credencial de autenticação. Os seguintes tipos de cartões sem contatos são suportados pelo HP ProtectTools:

- Cartões de memória Contactless HID iCLASS
- Contactless MiFare Classic 1k, 4k e mini cartões de memória

▲ Para configurar seu cartão sem contatos, coloque-o muito perto do leitor, siga as instruções na tela e clique em **Aplicar**.

## Cartão de proximidade

Um cartão de proximidade é um pequeno cartão de plástico que contém um chip de computador. Se um leitor de cartão de proximidade estiver conectado ao computador, se o administrador tiver instalado o driver associado do fabricante e se o administrador tiver ativado um cartão de proximidade como uma credencial de autenticação, você poderá usar um cartão de proximidade em conjunto com qualquer outra credencial para obter segurança adicional.

▲ Para configurar seu cartão de proximidade, coloque-o muito perto do leitor, siga as instruções na tela e clique em **Aplicar**.

## Bluetooth

Se o administrador tiver ativado o Bluetooth como uma credencial de autenticação, você poderá configurar um telefone Bluetooth em conjunto com outras credenciais para obter segurança adicional.

**NOTA:** Somente dispositivos de telefone Bluetooth são suportados.

1. Certifique-se de que a funcionalidade Bluetooth esteja ativada no computador e que o telefone Bluetooth esteja definido em modo de descoberta. Para conectar o telefone, talvez seja necessário digitar um código gerado automaticamente no dispositivo Bluetooth. Dependendo das configurações do dispositivo Bluetooth, talvez seja necessária uma comparação dos códigos de pareamento entre o computador e o telefone.
2. Para registrar o telefone, selecione-o e clique em **Registrar**.
3. Clique em **OK** na caixa de diálogo de confirmação.

### PIN

Se o administrador tiver ativado um PIN como uma credencial de autenticação, você poderá configurar um PIN em conjunto com outras credenciais para obter segurança adicional.

▲ Para configurar um novo PIN, insira o PIN e insira-o novamente para confirmá-lo.

## Administração

Os administradores podem acessar o Console Administrativo e o Gerenciamento Central clicando em **Administração** e, então, selecionando **Console Administrativo** no painel inferior esquerdo do console de usuário do HP ProtectTools Security Manager.

Para obter mais informações, consulte a ajuda do software Console Administrativo do HP ProtectTools.

## Avançado

As seguintes opções podem ser acessadas clicando-se em **Avançado** no painel inferior esquerdo do console de usuário:

- **Preferências**—Permite que você personalize as configurações do Security Manager.
- **Backup e Restauração**—Permite que você faça backup ou restaure dados do Security Manager.
- **Sobre**—Exibe informações da versão do Security Manager.

### Configuração de preferências

É possível personalizar as configurações do HP ProtectTools Security Manager. No console de usuário 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**, na configuração Som do 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:** Somente as informações do Password Manager e do Face Recognition são incluídas no back-up feito por este recurso. O Drive Encryption possui um método de back-up independente. Não é feito backup das informações de autenticação por impressão digital e do Device Access Manager.

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 console de usuário do Security Manager. Para obter mais informações, consulte Abertura do Security Manager na página 26.
2. No painel esquerdo do console de usuário, 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 console de usuário do Security Manager. Para obter mais informações, consulte Abertura do Security Manager na página 26.
2. No painel esquerdo do console de usuário, 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**.

# 6 Drive Encryption for HP ProtectTools (somente em determinados modelos)

O Drive Encryption for HP ProtectTools oferece proteção de dados completa, criptografando os dados 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 Windows.

O HP ProtectTools Security Manager (Assistente de Configuração do HP Client Security, Assistente de Configuração Avançada, ou o Console Administrativo) permite que os administradores do Windows ativem o Drive Encryption, efetuem backup da chave de criptografia e marquem ou desmarquem unidade(s) ou partição(ões) para criptografia. Para obter mais informações, consulte a Ajuda do software HP ProtectTools Security Manager.

As seguintes tarefas podem ser executadas com o Drive Encryption:

- Selecionando configurações do Drive Encryption:
  - Ativando uma senha protegida por TPM
  - Criptografando ou descriptografando partições ou unidades usando criptografia por software
  - Criptografando ou descriptografando unidades de criptografia automática individuais usando criptografia por hardware
  - Adicionando mais segurança pela desativação da Suspensão ou do Modo de espera para garantir que a autenticação na pré-inicialização do Drive Encryption seja sempre exigida

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

- Criando chaves de backup
- Recuperação de acesso a um computador criptografado usando chaves de backup e o HP SpareKey
- Ativação da autenticação pré-inicialização do Drive Encryption usando uma senha, impressão digital registrada ou PIN para os smart cards selecionados.

# Início do Drive Encryption

Os administradores podem acessar o Drive Encryption pelo Console de Usuário do HP ProtectTools Security Manager.

1. Na área de trabalho do Windows, clique duas vezes no ícone do **HP ProtectTools** na área de notificação, à direita da barra de tarefas.

   – ou –

   No **Painel de controle**, selecione **Sistema e Segurança** e, então, selecione **HP ProtectTools Security Manager**.

2. No painel esquerdo do HP ProtectTools Security Manager, selecione **Administração**. Em seguida, selecione **Console Administrativo**.

3. No painel esquerdo do Console Administrativo do HP ProtectTools, selecione **Device Encryption**.

# Tarefas básicas

## Ativando o Drive Encryption para discos rígidos padrão

Discos rígidos padrão são criptografados usando a criptografia por software. Para ativar o Drive Encryption, siga estas etapas:

1. Inicie o **Console Administrativo do HP ProtectTools**. Para obter mais informações, consulte Abertura do Console Administrativo do HP ProtectTools na página 17.

2. No painel esquerdo, clique em **Assistente de Configuração**.

3. Marque a caixa de seleção **Drive Encryption** e clique em **Avançar**.

4. Para realizar um back-up da chave de criptografia, conecte um dispositivo externo para que a chave seja gravada. Essa chave deve ser usada para acessar os dados, caso não seja possível fazê-lo por outro métodos.

5. Em **Fazer backup de chaves do Drive Encryption**, marque a caixa de seleção do dispositivo de armazenamento onde a chave de criptografia será salva.

6. Clique em **Avançar**.

**NOTA:** Será solicitado que você reinicie o computador. Após a reinicialização, a pré--inicialização do Drive Encryption é exibida, exigindo autenticação antes de iniciar o Windows.

O Drive Encryption foi ativado. A criptografia da(s) partição(ões) da unidade selecionada pode levar algumas horas, dependendo do número e do tamanho da(s) partição(ões).

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

## Ativando o Drive Encryption para unidades de criptografia automática

Unidades de criptografia automática que atendem à especificação OPAL do Trusted Computing Group para gerenciamento desse tipo de unidade podem ser criptografadas usando criptografia por software ou hardware. Para ativar o Drive Encryption para unidades de criptografia automática, siga estas etapas:

**NOTA:** A criptografia por hardware só estará disponível se TODAS as unidades de seu computador forem unidades autocriptografadas que atendam à especificação OPAL do Trusted Computing Group para gerenciamento de unidade autocriptografada. Neste caso, a opção **Usar criptografia de unidade de hardware** está disponível, e a criptografia por hardware ou de software poderá ser usada.

Se houver uma mistura de unidades autocriptografadas e unidades de disco rígido padrão, a opção **Usar criptografia de unidade hardware** não estará disponível, e somente a criptografia por software poderá ser utilizada. Para obter mais informações, consulte Ativando o Drive Encryption para discos rígidos padrão na página 43.

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

– ou –

### Criptografia por software

1. Inicie o **Console Administrativo do HP ProtectTools**. Para obter mais informações, consulte Abertura do Console Administrativo do HP ProtectTools na página 17.
2. No painel esquerdo, clique em **Assistente de Configuração**.
3. Marque a caixa de seleção **Drive Encryption** e clique em **Avançar**.

   **NOTA:** Se a opção **Usar criptografia de unidade de hardware** estiver disponível na parte inferior da tela, desmarque a caixa de seleção.
4. Em **Unidades para criptografar**, marque a caixa de seleção da unidade de disco rígido que deseja criptografar e clique em **Avançar**.
5. Para fazer backup da chave de criptografia, insira o dispositivo de armazenamento no slot apropriado.
6. Em **Fazer backup de chaves do Drive Encryption**, marque a caixa de seleção do dispositivo de armazenamento onde a chave de criptografia será salva.
7. 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. Inicie o **Console Administrativo do HP ProtectTools**. Para obter mais informações, consulte Abertura do Console Administrativo do HP ProtectTools na página 17.
2. No painel esquerdo, clique em **Assistente de Configuração**.
3. Marque a caixa de seleção **Drive Encryption** e clique em **Avançar**.
4. Se a caixa de seleção **Usar criptografia de unidade de hardware** estiver disponível na parte inferior da tela, certifique-se de que esteja marcada.

   Se a caixa de seleção estiver desmarcada ou se não estiver disponível, a criptografia por software será aplicada. Para obter mais informações, consulte Ativando o Drive Encryption para discos rígidos padrão na página 43.

5. Em **Unidades para criptografar**, marque a caixa de seleção da unidade de disco rígido que deseja criptografar e clique em **Avançar**.

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

Se mais de uma unidade for mostrada, o disco 0 também estará automaticamente selecionado e esmaecido, mas a opção para selecionar outros discos rígidos para criptografia por hardware será disponibilizada.

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

6. Para fazer backup da chave de criptografia, insira o dispositivo de armazenamento no slot apropriado.
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:** Será solicitado que você reinicie o computador. A pré-inicialização do Drive Encryption será exibida, exigindo autenticação antes do início do Windows.

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

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

## Desativando o 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.

1. Inicie o **Console Administrativo do HP ProtectTools**. Para obter mais informações, consulte Abertura do Console Administrativo do HP ProtectTools na página 17.
2. No painel esquerdo, clique em **Assistente de Configuração**.
3. 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. Poderá levar algumas horas, dependendo do tamanho da(s) partição(ões) do disco rígido criptografado. Quando a decodificação for concluída, o Drive Encryption será desativado.

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

Assim que o Drive Encryption for desativado, o computador deverá ser desligado (se tiver sido criptografado por hardware) ou reiniciado (se tiver sido criptografado por software).

## Login após o Drive Encryption ser ativado

Quando o computador for ligado, o Drive Encryption ativado e a conta de usuário registrada, será necessário fazer logon na tela de logon no Drive Encryption:

**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 criptografia por hardware oferece a opção **Desativar o modo de suspensão para garantir mais segurança**, que impede que o modo de suspensão ou o modo de espera ocorram quando desativados.

Ao sair do modo de hibernação, a autenticação pré-inicialização do Drive Encryption não é exibida para criptografia por software ou por hardware.

**NOTA:** Se o administrador do Windows tiver ativado o Pre-boot Security do BIOS no HP ProtectTools Security Manager e se o Login de uma etapa estiver desativado (por padrão), será possível fazer o login no computador imediatamente após a autenticação na pré-inicialização do BIOS, sem a necessidade de nova autenticação na tela de login do Drive Encryption.

### Login de usuário único:

- ▲ Na página **Login**, insira sua senha do Windows. PIN do smart card, SpareKey, rosto ou forneça uma impressão digital registrada.

### Login de vários usuários:

1. Na página **Selecione um usuário para logon**, selecione o usuário para logon na lista suspensa e clique em **Avançar**.
2. Na página **Login**, 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 suportados

- ActivIdentity Oberthur Cosmopol IC 64k V5.2
- Gemalto Cyberflex Access 64k V2c
- ActivIdentity Activkey SIM (Gemalto Cyberflex Access 64k V2c)

**NOTA:** Se a chave de recuperação for usada na tela de login do Drive Encryption, serão necessárias credenciais adicionais no login do Windows para o acesso a contas de usuário.

## 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. Após a ativação, qualquer disco rígido adicionado ou partição criados poderão ser criptografados segundo estas etapas:

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 com diferentes unidades, onde estão presentes uma ou mais unidades de disco rígido padrão e uma ou mais unidades de criptografia automática.

– ou –

▲ Para unidades criptografadas por hardware, selecione as unidades adicionais a serem criptografadas.

# 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, desativado ou a criptografia por hardware foi ativada) e visualizar o status da criptografia de todas as unidades de disco rígido do computador.

**NOTA:** Somente os discos rígidos adicionais podem ser marcados ou desmarcados para criptografia por hardware na página Configurações do Drive Encryption.

- 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 está em um dos seguintes estados:

### Criptografia por software

- Não criptografado
- Criptografado
- Criptografando
- Descriptografando

### Criptografia por hardware

- Criptografado
- Não criptografado (para unidades adicionais)

## Utilização de segurança aprimorada com TPM (somente modelos selecionados)

Se o Trusted Platform Module (TPM) estiver ativado e a funcionalidade Segurança aprimorada com TPM do Drive Encryption estiver selecionada, a senha do Drive Encryption estará protegida pelo chip de segurança TPM. Se o disco rígido for removido e instalado em outro computador, o acesso à unidade será negado.

**CUIDADO:** Não é possível compartilhar a propriedade do TPM com o TPM.msc do Windows.

**NOTA:** Como a senha é protegida por um chip de segurança TPM, se a unidade de disco rígido for movida para outro computador, os dados não poderão ser acessados, a menos que as configurações do TPM sejam migradas para esse computador.

**NOTA:** A opção TPM deve ser ativada na configuração do BIOS.

### Criptografia ou decodificação de partições de unidade individual (somente criptografia por software)

Os administradores podem usar a página Configurações do Drive Encryption para criptografar uma ou mais partições de disco rígido no computador ou decodificar qualquer partição de unidade que já tenha sido criptografada.

1. Inicie o **Console Administrativo do HP ProtectTools**. Para obter mais informações, consulte Abertura do Console Administrativo do HP ProtectTools na página 17.
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 de cada unidade de disco rígido que deseja criptografar ou descriptografar e clique em **Aplicar**.

**NOTA:** Quando uma partição estiver sendo criptografada ou descriptografada, a barra de progresso exibirá a porcentagem da partição criptografada e o tempo restante para a conclusão do processo.

**NOTA:** Partições dinâmicas não são suportadas. Se uma partição for exibida como disponível, mas não puder ser criptografada quando selecionada, significa que ela é dinâmica. Uma partição dinâmica resulta da redução de uma partição para criar uma nova partição dentro do Gerenciamento de Disco.

Será exibido um aviso se uma partição for convertida em uma partição dinâmica.

## Backup e Restauração (tarefa do administrador)

Quando o Drive Encryption é ativado, os administradores podem usar a página de backup de chave de criptografia para fazer backup de chaves de criptografia em mídias removíveis e realizar uma recuperação.

### Fazer backup de chaves de criptografia

Os administradores podem fazer backup da chave de criptografia para 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 ao computador. O local de armazenamento também deve estar seguro, uma vez que dispositivo de armazenamento permite o acesso ao Windows.

**NOTA:** Para salvar a chave de criptografia, é preciso utilizar um dispositivo de armazenamento USB com formato FAT32 ou FAT16. Um disquete, um memory stick USB, um cartão de memória Secure Digital (SD) ou um MultiMedia Card (MMC) pode ser usado para backup.

1. Inicie o **Console Administrativo do HP ProtectTools**. Para obter mais informações, consulte Abertura do Console Administrativo do HP ProtectTools na página 17.
2. No painel esquerdo, clique no ícone **+** à esquerda de **Drive Encryption** para exibir as opções disponíveis.
3. Clique em **Fazer backup de chaves de criptografia**.

4. Insira o dispositivo de armazenamento que está sendo usado para fazer backup da chave de criptografia.

**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 MultiMedia Card (MMC) pode ser usado para backup. Em alguns casos, o SkyDrive pode ser usado.

5. Em **Unidade**, marque a caixa de seleção do dispositivo onde deseja fazer o backup da chave de criptografia.
6. Clique em **Backup das chaves**.
7. Leia as informações na página exibida, em seguida clique em **OK**. A chave de criptografia é salva no dispositivo de armazenamento selecionado.

### Recuperação de acesso a um computador ativado usando chaves de backup

Os administradores podem realizar uma recuperação usando a chave do Drive Encryption gravada no backup feito em um dispositivo de armazenamento removível na ativação ou selecionando a opção **Backup de chaves do Drive Encryption Keys** no Security Manager.

1. Insira o dispositivo de armazenamento removível que contém sua chave de backup.
2. Ligue o computador.
3. Quando a caixa de diálogo de login do Drive Encryption for HP ProtectTools for exibida, clique em **Opções**.
4. Clique em **Recuperação**.
5. Insira o caminho ou o nome do arquivo que contém sua chave de backup e clique em **Recuperar**.

   – ou –

   Clique em **Procurar** para pesquisar o arquivo de backup necessário, clique em **OK** e então clique em **Recuperar**.
6. Quando a caixa de diálogo de confirmação for exibida, clique em **OK**.

   A tela de logon do Windows é exibida.

**NOTA:** Se a chave de recuperação for usada na tela de login do Drive Encryption, serão necessárias credenciais adicionais no login do Windows para o acesso a contas de usuário. É altamente recomendável que você redefina sua senha após a execução de uma recuperação.

## Execução de uma recuperação do HP SpareKey

A recuperação do SpareKey na Pré-inicialização de criptografia da unidade exige que você responda perguntas de segurança corretamente antes de poder acessar o computador. Para obter mais informações sobre a configuração da Recuperação do SpareKey, consulte a Ajuda do software Security Manager.

Para executar uma Recuperação do HP SpareKey caso tenha esquecido sua senha:

1. Ligue o computador.
2. Quando a página Drive Encryption for HP ProtectTools for exibida, navegue até a página de login do usuário.

3. Clique em **SpareKey**.

**NOTA:** Se seu SpareKey não tiver sido inicializado no Security Manager, o botão **SpareKey** não estará disponível.

4. Digite as respostas corretas para as perguntas exibidas e clique em **Login**.

   A tela de logon do Windows é exibida.

**NOTA:** Se o SpareKey for usado na tela de login do Drive Encryption, serão necessárias credenciais adicionais no login do Windows para o acesso a contas de usuário. É altamente recomendável que você redefina sua senha após a execução de uma recuperação.

# Exibição do status da criptografia

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

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

1. Inicie o **Console de Usuário do HP ProtectTools**. Para obter mais informações, consulte Abertura do Security Manager na página 26.
2. Em **Meus dados**, clique em **Drive Encryption**.

   Em um cenário de criptografia por software ou por hardware, o status de criptografia da unidade é exibido como um dos seguintes:

   - Ativado
   - Desativado

   Em um cenário de criptografia por software, o status de criptografia da unidade é exibido como um dos seguintes para cada disco rígido ou partição de disco rígido:

   - Não criptografado
   - Criptografado
   - Criptografar
   - Descriptografar

   Em um cenário de criptografia por hardware, o status de criptografia da unidade é exibido como um dos seguintes:

   - Não criptografado
   - 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.

# 7 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 60.

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 logon como administrador.
2. Inicie o **HP ProtectTools Security Manager** a partir do **Painel de Controle do HP Client Security**.

   – ou –

   Na área de trabalho do Windows, clique duas vezes no ícone do **HP ProtectTools** na área de notificação, à direita da barra de tarefas.

   – ou –

   No **Painel de controle**, selecione **Sistema e Segurança** e, então, selecione **HP ProtectTools Security Manager**.
3. No painel esquerdo do Security Manager, clique em **Administração**. Em seguida, selecione **Console Administrativo**.
4. No painel esquerdo do Console Administrativo, clique em **Device Access Manager**.

Usuários padrão 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

**NOTA:** Se forem usados dispositivos Bluetooth como credenciais de autenticação, o acesso do dispositivo Bluetooth não deverá ser restrito na política do Device Access Manager.

- 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 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:

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 dispositivos:

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 dispositivos:

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 dispositivos:

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 dispositivos:

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 dispositivos:

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 dispositivos:

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 a 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 a 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** é 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 a ter 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.

**NOTA:** A página Configurações avançadas não será redefinida.

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 a todos os que não sejam do grupo 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 de 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 59 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, como por exemplo negar acesso a mídias removíveis a 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 a dispositivos automaticamente ao usuário. Na visualização **Configuração de Classe de Dispositivo**, se o grupo Usuários não tiver acesso a um dispositivo, o grupo Administradores de dispositivos terá que 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 a 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**.

## Suporte a dispositivo 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

# 8 Recuperação em caso de roubo (somente em determinados modelos)

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. Abra o console de usuário do Security Manager. Para obter mais informações, consulte Abertura do Security Manager na página 26.
3. No painel esquerdo do Security Manager, clique em **Recuperação em caso de roubo**.
4. Para iniciar o assistente para ativação do Computrace, clique em **Iniciar**.
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 da 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 logon no Centro de Atendimento ao Cliente:

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

# 9 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.

## 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. Usando o **Painel de Controle**, adicione um layout de teclado compatível (adicione os teclados US/English no idioma de entrada chinês).
  2. Defina o teclado suportado para entrada padrão.
  3. 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. Para obter mais informações sobre caracteres não compatíveis, consulte a ajuda do software Console Administrativo do HP ProtectTools.
  2. Execute o Assistente de Configuração do HP ProtectTools Security Manager novamente e reinsira a nova senha do Windows.

## 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.

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. |

| Idioma | Windows | BIOS | Criptografia da unidade |
|---|---|---|---|
| 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.<br>◦ As teclas å, ®, e Þ na segunda fileira são rejeitadas.<br>◦ As teclas á, ð, e ø na terceira fileira são rejeitadas.<br>◦ A tecla æ na fileira inferior é rejeitada. | n/d | n/d |
| Tcheco | ◦ A tecla ğ é rejeitada.<br>◦ A tecla į é rejeitada.<br>◦ A tecla ų é rejeitada.<br>◦ As teclas ė, ı, e ż são rejeitadas.<br>◦ As teclas ģ, ķ, ļ, ņ, e ţ 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.<br>◦ 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 | 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 |

# 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.

**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.

**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.

**cena**
Imagem de um usuário registrado a ser usada para autenticação.

**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.

**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 Administrativo**
Um local central onde os administradores podem acessar e gerenciar os recursos e as configurações no 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.

**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.

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

**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.

**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.

**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.

**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.

**login**

Um objeto dentro do Security Manager que consiste em um nome de usuário e uma senha (e, possivelmente, outras determinadas informações), que pode ser usado para fazer login em sites da Web ou em outros programas.

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

**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.

**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.

**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.

**Recuperação do HP SpareKey**
A capacidade de acessar o computador respondendo corretamente a perguntas de segurança.

**reinicializar**
O processo de reinicialização do computador.

**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.

**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.

**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.

**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

## T



## U