HP Client Security

Passos Iniciais

Primeira edição: agosto de 2013

Número de peça: 735339-201

Conteúdo

1 Introdução ao HP Client Security Manager

O HP Client Security permite que você proteja seus dados, dispositivo e identidade, aumentando, assim, a segurança de seu computador.

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

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

NOTA: As instruções neste guia estão escritas supondo que você já instalou os módulos de software do HP Client Security.

Recursos do HP Client Security

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

Módulo	Principais recursos
HP Client Security Manager	Os administradores podem executar as seguintes funções: • Proteger seu computador antes do Windows® ser iniciado • Proteger sua conta do Windows usando a autenticação forte • Administrar suas informações de login e senhas de websites e aplicativos • Alterar facilmente sua senha do sistema operacional Windows. • Usar impressões digitais para segurança e a conveniência extras • Configurar um smart card, cartão sem contato, ou um cartão de proximidade para autenticação • Usar seu telefone Bluetooth como um método de identificação • Definir um PIN para expandir suas escolhas de autenticação • Configurar as políticas de login e da sessão • Fazer backup e restaure os dados de programa • Adicionar mais aplicativos, como o HP Drive Encryption, HP File Sanitizer, HP Trust Circles, HP Device Access Manager, e HP Computrace Os usuários em geral podem executar as seguintes funções: • Visualizar as configurações do Encryption Status e do Device Access Manager. • Ativar o Computrace. • Configurar as Preferências e as opções de Backup e Restauração.

Módulo	Principais recursos
Gerenciador de Senhas	Os usuários em geral podem executar as seguintes funções: • Organizar e configurar nomes de usuários e senhas. • Criar senhas mais fortes para maior segurança das contas de e--mail e de sites da Web. O Password Manager preenche e envia as informações automaticamente. • Simplifique o processo de login com o recurso Single Sign On, que lembra e aplica as credenciais dos usuários. • Marcar uma conta como comprometida, para que você seja alertado sobre outra(s) conta(s) com credenciais similares. • Importar dados de login de um navegador compatível.
HP Drive Encryption (somente em determinados modelos)	• Oferece criptografia completa, de volumes inteiros, para unidades de disco rígido. • Força a autenticação de pré-inicialização para decodificar e acessar dados. • Oferece a opção de ativar unidades autocriptografadas (somente em determinados modelos).
HP Device Access Manager	• Permite que os gerentes de TI controlem o acesso a dispositivos com base em perfis de usuários. • Impede que usuários não autorizados retirem dados usando uma mídia de armazenamento externa, além da introdução de vírus no sistema usando mídias externas. • Permite aos administradores desativar o acesso de indivíduos específicos ou grupos de usuários a dispositivos de comunicação.
HP Trust Circles	• Fornece segurança a arquivos e documentos. • Criptografa arquivos colocados em pastas especificadas pelo usuário e as protege dentro de um trust circle. • Permite que os arquivos sejam utilizados e compartilhados apenas pelos membros do trust circle.
Recuperação em caso de roubo (Computrace, comprado separadamente)	• Para ser ativado, requer a aquisição separada de assinaturas de rastreamento e acompanhamento. • Fornece rastreamento seguro de ativo. • Monitora a atividade do usuário, bem como as alterações de hardware e software. • Permanece ativo ainda que o disco rígido seja reformatado ou substituído.

Descrição do produto e exemplos de uso comuns do HP Client Security

A maioria dos produtos do HP Client Security possui tanto a autenticação de usuário (normalmente uma senha) e um backup administrativo para obter acesso se as senhas forem perdidas, indisponíveis, esquecidas ou a qualquer momento em que a segurança corporativa requeira acesso.

NOTA: Alguns dos produtos do HP Client Security são desenvolvidos para restringir o acesso aos dados. Os dados devem ser criptografados quando é importante que o usuário poderia perder as informações comprometidas. Recomenda-se efetuar um backup de todos os dados 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.
- Marcar uma conta como comprometida, para que você seja alertado sobre outra(s) conta(s) com credenciais similares.
- Importar dados de login de um navegador compatível.

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 funcionário dedicado foi promovido e agora irá gerenciar todo o departamento de contabilidade. A equipe deve fazer login em um grande número de contas de clientes Web, e cada uma usa diferentes informações de login. Esta informação de login precisa ser compartilhada com outros colegas,, portanto confidencialidade é um problema. O funcionário decide organizar todos os links da Web, nomes de usuários e senhas da empresa, com o Password Manager. Uma vez concluído, o funcionário implanta o Password Manager para os funcionários para que eles possam trabalhar com as contas da Web e nunca saibam as credenciais de login que estão usando.

HP Drive Encryption (somente em determinados modelos)

O HP Drive Encryption é utilizado para restringir o acesso aos dados na unidade de disco rígido inteira ou um disco secundário do computador. O Drive Encryption também pode gerenciar discos de autocriptografia.

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.

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.

HP Device Access Manager (somente em determinados modelos)

O HP Device Access Manager permite a um administrador restringir e gerenciar o acesso ao hardware. O Device Access Manager pode ser usado para bloquear o acesso não autorizado a unidades Flash USB onde os dados poderiam ser copiados. Ele também pode restringir o acesso a unidades de CD/DVD, controle de dispositivos USB, conexões de rede e assim por diante. Um exemplo seria uma situação onde fornecedores externos precisam de acesso aos computadores de uma empresa, mas não conseguem copiar os dados para uma unidade USB.

Exemplo 1: Um gerente de uma empresa de fornecimento de dispositivos médicos normalmente trabalha com registros médicos pessoais junto com as informações de sua empresa. Os funcionários precisam de acesso a esses dados, no entanto, é extremamente importante que os dados não sejam removidos do computador por uma unidade USB ou qualquer outro meio de armazenamento externo. A rede é segura, 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 desabilitar as portas USB e gravadores de CD para que eles não possam ser usados. Apesar de as portas USB estarem bloqueadas, o mouse e o teclado continuam funcionando.

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 (comprado separadamente)

O Computrace (comprado separadamente) é um serviço que pode rastrear a localização de um computador roubado sempre que o usuário acessar a Internet. O Computrace também pode ajudar a gerenciar e localizar computadores remotamente, bem como monitorar o uso e 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 Client Security podem trabalhar juntos para oferecer soluções para uma variedade de problemas de segurança, incluindo 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.
  - HP Client Security—Consulte HP Client Security na página 13.
  - HP Drive Encryption—Consulte HP Drive Encryption (somente em determinados modelos) na página 30.
- 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: Consulte Recuperação em caso de roubo (somente em determinados modelos) na página 54.

Como restringir acesso a dados confidenciais

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

- O Device Access Manager permite que os gerentes de TI restrinjam o acesso a dispositivos de comunicação de modo que informações confidenciais não possam ser copiadas da unidade de disco rígido. Consulte Visualização do sistema na página 44.

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 para recursos de redes corporativas, como informações de serviços financeiros, de um executivo, ou da Equipe de Pesquisa e Desenvolvimento, e para informações privadas, como registros médicos de pacientes ou registros financeiros pessoais. Os seguintes recursos ajudam a evitar o acesso não autorizado:

- O recurso de autenticação de pré-inicialização, se ativado, ajuda a evitar o acesso ao sistema operacional. (consulte HP Drive Encryption (somente em determinados modelos) na página 30.
- O HP Client Security ajuda a garantir que um usuário não autorizado não consiga obter senhas ou acesso a aplicativos protegidos por senha. Consulte HP Client Security na página 13.
- O Device Access Manager permite que os gerentes de TI restrinjam o acesso a dispositivos de gravação de modo que informações confidenciais não possam ser copiadas da unidade de disco rígido. Consulte HP Device Access Manager (somente em determinados modelos) na página 43.

Como criar políticas de senhas fortes

Se uma política da empresa que requer o uso de uma política de senha forte para dezenas de aplicativos e bancos de dados baseados na Internet entrar em vigor, o Password Manager fornece um repositório protegido para senhas e serviço de Single Sign On. Consulte Password Manager na página 19.

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 Client Security, os deveres e privilégios de segurança podem ser divididos nas seguintes funções:

- Agente de segurança: define o nível de segurança para a empresa ou rede e determina os recursos de segurança a serem implantados, como o Drive Encryption.

  NOTA: Muitos dos recursos no HP Client Security podem ser personalizados pelo agente de segurança em cooperação 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 pelo agente de segurança. Também pode ativar ou desativar alguns recursos. Por exemplo, se o agente de segurança tiver decidido implementar smart cards, o administrador de TI pode ativar a senha e o modo smart card.
- Usuário: utiliza os recursos de segurança. Por exemplo, se o agente de segurança e o administrador de TI ativaram smart cards para o sistema, o usuário pode definir o PIN do smart card e usar o cartão para autenticação.

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

Não se devem conceder privilégios administrativos a usuários não autorizados.

Gerenciamento de senhas do HP Client Security

A maioria dos recursos do HP Client Security é protegida por senhas. A tabela a seguir relaciona as senhas que são usadas geralmente, o módulo de software onde as senhas são definidas e a função das senhas.

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 Client Security	Definida no seguinte módulo	Função
Senha de logon do Windows	Painel de Controle do Windows ou HP Client Security	Pode ser usada para efetuar login manual e autenticação para acesso a vários recursos do HP Client Security.

Senha do HP Client Security	Definida no seguinte módulo	Função
Senha de Backup and Recovery do HP Client Security	HP Client Security, por usuário individual	Protege o acesso ao arquivo do HP Client Security Backup and Recovery.
PIN do smart card	Gerenciador de Credenciais	Pode ser usado como autenticação multifatores. Pode ser usado como autenticação do Windows. 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

Você pode usar a ferramenta Backup e Recuperação no HP Client Security como um local central onde é possível fazer backup e restaurar credenciais de segurança de alguns dos módulos do HP Client Security.

2 Passos iniciais

Para configurar o HP Client Security para uso com suas credenciais, inicie o HP Client Security de uma das seguintes formas: Uma vez que o assistente tenha sido concluído por um usuário, ele não pode ser iniciado novamente por esse mesmo usuário.

1. Na tela Iniciar ou Aplicativos, clique ou toque no aplicativo **HP Client Security** (Windows 8).

   – ou –

   Na área de trabalho do Windows, clique ou toque no **HP Client Security Gadget** (Windows 7).

   – ou –

   Na área de trabalho do Windows, clique ou toque duas vezes no ícone do **HP Client Security** na área de notificações, localizado no lado direito da barra de tarefas.

   – ou –

   Na área de trabalho do Windows, clique em ou toque no ícone **HP Client Security** na área de notificação e, em seguida, selecione **Abrir HP Client Security**.

2. O assistente de configuração do HP Client Security é iniciado com a exibição da página de Boas-vindas.

3. Leia a tela de Boas-vindas, verifique sua identidade digitando seu senha do Windows e, em seguida, clique ou toque em **Avançar**.

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

4. Na página HP SpareKey, selecione três perguntas de segurança. Insira uma resposta para cada pergunta e, em seguida, clique em **Avançar**. Perguntas personalizadas também são permitidas. Para obter mais informações, consulte HP SpareKey—Recuperação de senha na página 15.

5. Na página Impressões Digitais, registre pelo menos o número mínimo de impressões digitais, e em seguida, clique ou toque em **Avançar**. Para obter mais informações, consulte Impressões digitais na página 13.

6. Na página Drive Encryption, ative criptografia, faça backup da chave de criptografia e, em seguida, clique ou toque em **Avançar**. Para obter mais informações, consulte a Ajuda do software HP Drive Encryption.

   NOTA: Isso se aplica a um cenário onde o usuário é um administrador, e o assistente de configuração do HP Client Security não foi configurado anteriormente por um administrador.

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

   Essa página fornece o status dos recursos e credenciais.

8. O assistente de configuração do HP Client Security garante a ativação dos recursos da Autenticação Just In Time e File Sanitizer. Para obter mais informações, consulte a Ajuda do software HP Device Access Manager e a Ajuda do software HP File Sanitizer.

   NOTA: Isso se aplica a um cenário onde o usuário é um administrador, e o assistente de configuração do HP Client Security não foi configurado anteriormente por um administrador.

Abertura do HP Client Security

Você pode abrir o aplicativo HP Client Security de uma das seguintes formas:

NOTA: O assistente de configuração do HP Client Security deve ser completado antes que o aplicativo HP Client Security possa ser aberto.

- Na Tela Iniciar ou na Tela Aplicativos, clique ou toque no aplicativo **HP Client Security**.

  – ou –

  Na Área de trabalho do Windows, clique ou toque no **HP Client Security** Gadget (Windows 7).

  – ou –

  Na área de trabalho do Windows, clique ou toque duas vezes no ícone do **HP Client Security** na área de notificação, localizado no lado direito na barra de tarefas.

  – ou –

  Na área de trabalho do Windows, clique em ou toque no ícone **HP Client Security** na área de notificação e, em seguida, selecione **Abrir HP Client Security**.

3 Guia de configuração fácil para pequenas empresas

Este capítulo foi desenvolvido para demonstrar as etapas básicas para ativar as opções mais comuns e úteis do HP Client Security para pequenas empresas. Várias ferramentas e opções neste software permitem ajustar suas preferências e definir seu controle de acesso. O foco deste Guia de configuração fácil é fazer com que cada módulo seja executado com o mínimo de esforço e tempo de configuração Para outras informações, selecione o módulo no qual está interessado e, em seguida, clique em **?** ou no botão Ajuda no canto superior direito. Esse botão exibirá automaticamente informações para ajudá-lo com a janela atual exibida.

Passos iniciais

1. Na área de trabalho do Windows, abra o HP Client Security clicando duas vezes no ícone **HP Client Security** na área de notificação, localizada no lado direito da barra de tarefas.
2. Insira a sua senha do Windows, ou crie uma senha para o Windows.
3. Conclua a Configuração do HP Client Security.

Para fazer com que o HP Client Security requeira autenticação somente uma vez durante o login no Windows, consulte Recursos de segurança na página 27.

Password Manager

Todo mundo tem muitas senhas, especialmente se acessa regularmente sites ou usa aplicativos que requerem login. O usuário normal usa a mesma senha para cada aplicativo e site ou se torna criativo e rapidamente se esquece qual senha corresponde a cada aplicativo.

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.
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 a combinação de teclas Ctrl+tecla Windows+h para abrir o Password Manager e, em seguida, clique em **Login** para iniciar e autenticar a atalho salvo.

A opção **Editar** do Gerenciador de Senhas permite visualizar e modificar o nome, nome de login e até mesmo revelar as senhas.

O HP Client Security para pequenas empresas permite o backup e/ou cópia para outro computador de todas as credenciais e configurações.

HP Device Access Manager

O Device Access Manager pode ser usado para restringir o uso de vários dispositivos de armazenamento interno e externo de modo que seus dados permaneçam protegidos na unidade de disco rígido e não sejam roubados de sua empresa. Um exemplo poderia ser permitir a um usuário acessar seus dados, mas bloquear sua cópia a um CD, reprodutor de música ou dispositivo de memória USB.

1. Abrir **Device Access Manager** (consulte Inicialização do Device Access Manager na página 43).

   Acesso para o usuário atual é exibido.

2. Para alterar o acesso dos usuários, grupos ou dispositivos, clique ou toque em **Alterar**. Para obter mais informações, consulte Visualização do sistema na página 44.

HP Drive Encryption

O HP Drive Encryption é usado para proteger seus dados ao criptografar toda a unidade de disco rígido. Os dados em sua unidade de disco rígido permanecerão protegidos se seu PC for roubado e/ou se a unidade de disco rígido for removida do computador original e colocada em um computador diferente.

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 o trabalho, vários módulos de software sincronizam as senhas automaticamente, incluindo contas de usuário e domínios de autenticação do Windows, HP Drive Encryption, Password Manager e HP Client Security.

Para configurar o HP Drive Encryption durante a configuração inicial com o assistente de configuração do HP Client Security, consulte Passos iniciais na página 8.

4 HP Client Security

A Página Inicial do HP Client Security é o ponto central para se ter acesso fácil aos recursos, aplicativos e configurações do HP Client Security. A Página Inicial é dividida em três seções:

- **DADOS**—Oferece acesso a aplicativos usados para o gerenciamento da segurança de dados.
- **DISPOSITIVO**—Oferece acesso a aplicativos usados para o gerenciamento de dispositivos.
- **IDENTIDADE**—Oferece inscrição e gerenciamento de credenciais de autenticação.

Mova o cursor sobre o bloco de um aplicativo para exibir a descrição desse aplicativo.

O HP Client Security pode oferecer links para as configurações administrativas e do usuário na parte inferior da página. O HP Client Security oferece acesso às Configurações Avançadas e aos recursos tocando ou clicando no ícone da **Engrenagem** (configurações).

Recursos de identidade, aplicativos e configurações.

Os recursos, aplicativos e configurações de Identidade oferecidos pelo HP Client Security podem auxiliá-lo a gerenciar vários aspectos da sua identidade digital. Clique ou toque em um dos seguintes blocos na Página Inicial do HP Client Security, e então digite a sua senha do Windows:

- **Impressões Digitais**—Registra e gerencia as suas credenciais de impressão digital.
- **SpareKey**—Configura e gerencia as credenciais da sua HP SpareKey, que podem ser usadas para fazer o login no seu computador, caso outras credenciais tenham sido perdidas ou extraviadas. Também permite que você restaure as suas senhas perdidas.
- **Senha do Windows**—Oferece acesso rápido para modificar a sua senha do Windows.
- **Dispositivos com Bluetooth**—Permite que você registre e gerencie os seus dispositivos com Bluetooth.
- **Cartões**—Permite que você registre e gerencie os seus smart cards, cartões sem contatos e cartões de aproximação.
- **PIN**—Permite que você registre e gerencie as suas credenciais de PIN.
- **RSA SecurID**—Permite registrar e gerenciar as credenciais do seu RSA SecurID (se a configuração estiver correta).
- **Password Manager**—Permite que você gerencie senhas para as suas contas online e seus aplicativos.

Impressões digitais

O assistente de configuração do HP Client Security orientará você durante o processo de configuração ou de "registro" das suas impressões digitais.

Também é possível registrar ou excluir suas impressões digitais na página Impressões Digitais, que você pode acessar clicando ou tocando no ícone Impressões Digitais, na Página Inicial do HP Client Security.

1. Na página Impressões Digitais, faça a leitura de um dedo até que ele seja registrado com êxito.

   O número de dedos que devem ser registrados é indicado na página. São preferíveis os dedos indicador e médio.

2. Para excluir as impressões digitais registradas anteriormente, clique ou toque em **Excluir**.
3. Para registrar dedos adicionais, clique ou toque **Registrar impressão digital adicional**.
4. Clique ou toque em **Salvar** antes de sair da página.

⚠ **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.

- ▲ Para ter acesso às Configurações Administrativas de Impressões Digitais, onde os administradores podem especificar o registro, exatidão e outras configurações, clique ou toque em **Configurações Administrativas** (é necessário ter privilégios administrativos).
- ▲ Para ter acesso às Configurações de Usuário de Impressões Digitais, onde você pode especificar as configurações que controlam o comportamento e aparência do reconhecimento de impressão digital, clique ou toque em **Configurações de Usuário**.

Configurações Administrativas de Impressões Digitais

Os administradores podem especificar o registro, a exatidão e outras configurações de um Leitor de impressão digital. É necessário ter privilégios administrativos.

- ▲ Para ter acesso às Configurações Administrativas para a credencial de impressão digital, clique ou toque em **Configurações Administrativas**, na página de Impressões Digitais.

- **Registro de Usuário**—Escolha o número mínimo e máximo de impressões digitais que um usuário pode registrar.
- **Reconhecimento**—Mova a barra deslizante para ajustar a sensibilidade do leitor de impressão digital durante a leitura de seus dedos.

  Se as impressões digitais não forem reconhecidas com consistência, 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.

Configurações de Usuário de Impressões Digitais

Na página das Configurações de Usuário de Impressões Digitais, é possível especificar as configurações que controlam a aparência e comportamento do reconhecimento de impressões Digitais.

▲ Para ter acesso às Configurações de Usuários para a credencial de impressão digital, clique ou toque em **Configurações de Usuário**, na página de Impressões Digitais.

- **Ativar resposta sonora**—Por padrão, o HP Client Security 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 a caixa de seleção.
- **Mostrar resposta de qualidade de verificação**—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.

HP SpareKey—Recuperação de senha

O HP SpareKey permite acessar o computador (em plataformas suportadas) respondendo a três perguntas de segurança.

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

Para configurar sua HP SpareKey:

1. Na página da HP SpareKey do assistente, selecione três perguntas e, em seguida, insira uma resposta para cada pergunta.

   É possível selecionar as perguntas de uma lista predefinida ou formular as suas próprias perguntas.

2. Clique ou toque em **Registrar**.

Para excluir a sua HP SpareKey:

▲ Clique ou toque em **Excluir SpareKey**.

Após a definição de sua SpareKey, você pode acessar seu computador usando sua SpareKey a partir de uma tela de login de autenticação na inicialização ou da tela de Boas-Vindas do Windows.

É possível selecionar perguntas diferentes ou alterar as suas perguntas na página do SpareKey, que você pode acessar a partir do bloco de Recuperação de Senha na Página Inicial do HP Client Security.

Para acessar as Configurações do HP SpareKey, onde o administrador pode especificar as configurações referentes à credencial do HP SpareKey, clique em **Configurações** (é necessário ter privilégios administrativos).

HP SpareKey Settings

Na página de Configurações do HP SpareKey, é possível especificar as configurações que controlam o comportamento e o uso das credenciais do HP SpareKey.

▲ Para abrir a página de Configurações do HP SpareKey, clique ou toque em **Configurações**, na página do HP SpareKey (é necessário ter privilégios administrativos).

Os administradores podem selecionar as seguintes configurações:

- Especificar as perguntas que são apresentadas a cada usuário durante a configuração do HP SpareKey.
- Adicionar até três perguntas de segurança personalizadas à lista apresentada aos usuários.
- Decidir se os usuários terão ou não permissão para redigir suas próprias perguntas de segurança.
- Especificar quais ambientes de autenticação (Windows ou autenticação na inicialização) permitem o uso do HP SpareKey para recuperação de senha.

Senha do Windows

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

Para alterar a sua senha do Windows:

1. Na página Inicial do HP Client Security, clique ou toque em **Senha do Windows**.
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 ou toque em **Alterar** para mudar imediatamente sua senha atual para a nova senha digitada.

Dispositivos com 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 ou toque em **Registrar**.

Para ter acesso à Configurações dos Dispositivos com Bluetooth na página 16 página onde o administrador pode especificar as configurações para dispositivos com Bluetooth, clique em **Configurações** (é necessário ter privilégios administrativos).

Configurações dos Dispositivos com Bluetooth

Os administradores podem especificar as seguintes configurações que controlam o comportamento e o uso das credenciais dos dispositivos com Bluetooth:

Autenticação silenciosa

- **Use automaticamente o seu dispositivo com Bluetooth registrado conectado durante a verificação da sua identidade**—Marque a caixa de seleção para permitir que os usuários

usem as credenciais de Bluetooth para a autenticação sem exigir ação do usuário, ou desmarque a caixa de seleção para desativar esta opção.

Proximidade do Bluetooth

- **Bloqueie o computador quando o seu dispositivo Bluetooth registrado sair do alcance do seu computador**—Marque a caixa de seleção para travar o computador quando o dispositivo com Bluetooth conectado durante o login sair do alcance, ou desmarque a caixa de seleção para desativar esta opção.

NOTA: O módulo Bluetooth do seu computador deve suportar a capacidade para utilizar este recurso.

Cartões

O HP Client Security pode suportar diferentes tipos de cartões de identificação, que são pequenos cartões de plástico contendo um chip de computador, como smart cards, cartões sem contatos e cartões de proximidade. Se um desses cartões e um leitor de cartão apropriado estiverem conectados ao computador, se o administrador tiver instalado o driver associado do fabricante e se o administrador tiver ativado o cartão como uma credencial de autenticação, será possível usar o cartão como uma credencial de autenticação.

O fabricante do smart card deve fornecer ferramentas para instalar um certificado de segurança e um gerenciamento de PIN que o HP Client Security usará em seu algoritmo de segurança. O número e o tipo de caracteres usados como PIN podem variar. É necessário que os administradores inicializem o smart card antes que ele possa ser usado.

Os seguintes formatos de Smart Card são suportados pelo HP Client Security:

- CSP
- PKCS11

Os seguintes tipos de cartões sem contatos são suportados pelo HP Client Security:

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

Os seguintes cartões de proximidade são suportados pelo HP Client Security:

- HID Proximity Cards

Para registrar um smart card:

1. Insira o cartão em um leitor de smart card anexo.
2. Quando o cartão for reconhecido, digite o PIN do cartão e clique ou toque em **Registrar**.

Para alterar um PIN de smart card:

1. Insira o cartão em um leitor de smart card anexo.
2. Quando o cartão for reconhecido, digite o PIN do cartão e clique ou toque em **Autenticar**.
3. Clique ou toque em **Mudar PIN** e, em seguida, digite o novo PIN.

Para registrar um cartão de proximidade ou um cartão sem contato:

1. Posicione o cartão sobre o leitor apropriado ou muito próximo dele.
2. Quando o cartão for reconhecido, clique ou toque em **Registrar**.

Para excluir um cartão registrado:

1. Apresente o cartão ao leitor.
2. Somente no caso dos Smart Card, digite o PIN atribuído ao cartão e clique ou toque em **Autenticar**.
3. Clique ou toque em **Excluir**.

Uma vez que o cartão tenha sido registrado, os detalhes do cartão serão exibidos em **Cartões Registrados**. Quando um cartão for excluído, ele será removido da lista.

Para acessar as Configurações do Smart Card, dos cartões de proximidade e dos cartões sem contato, onde os administradores podem especificar as configurações referentes às credenciais dos cartões, clique ou toque em **Configurações** (é necessário ter privilégios administrativos).

Configurações do Smart Card, cartões de proximidade e cartões sem contato

Para acessar as configurações de um cartão, clique ou toque no cartão na lista, e em seguida clique e toque a seta que é exibida.

Para alterar um PIN de smart card:

1. Apresente o cartão ao leitor
2. Digite o PIN atribuído ao cartão e clique ou toque em **Continuar**.
3. Digite e confirme o novo PIN, e então clique ou toque em **Continuar**.

Para inicializar um PIN de smart card:

1. Apresente o cartão ao leitor
2. Digite o PIN atribuído ao cartão e clique ou toque em **Continuar**.
3. Digite e confirme o novo PIN, e então clique ou toque em **Continuar**.
4. Clique ou toque em **Sim** para confirmar a inicialização.

Para limpar os dados do cartão:

1. Apresente o cartão ao leitor
2. Digite o PIN atribuído ao cartão (somente no caso de Smart Cards) e clique ou toque em **Continuar**.
3. Clique ou toque em **Sim** para confirmar a exclusão.

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:

▲ Digite o PIN, digite-o novamente para confirmá-lo e, em seguida, clique ou toque em **Aplicar**.

Para excluir um PIN:

▲ Clique ou toque em **Excluir** e clique ou toque em **Sim** para confirmar.

Para acessar as Configurações de PIN, onde os administradores podem especificar as configurações referentes às credenciais de PIN, clique ou toque em **Configurações** (é necessário ter privilégios administrativos).

Configurações do PIN

Na página de Configurações do PIN, é possível especificar o comprimento mínimo e máximo aceitável para a credencial do PIN.

RSA SecurID

Se o administrador tiver ativado o RSA como credencial de autenticação, e se as condições abaixo forem verdadeiras, é possível registrar ou excluir uma credencial de RSA SecurID.

NOTA: É necessária configuração apropriada.

- O usuário deve ter sido criado em um Servidor de RSA.
- O token do RSA SecurID atribuído ao usuário e ao computador devem ter sido adicionados ao domínio do Servidor RSA.
- O software SecurID deve estar instalado no computador.
- Deve haver uma conexão disponível para o Servidor RSA configurado apropriadamente.

Para registrar uma credencial do RSA SecurID:

▲ Digite o seu nome de usuário e o código de acesso do RSA SecurID (o código do token do RSA SecurID ou o PIN+código do token, dependendo de qual é o seu ambiente), e então clique ou toque em **Aplicar**.

Após o registro ter sido feito com sucesso, a mensagem de "A sua credencial de RSA SecurID foi registrada com sucesso" será exibida, e o botão Excluir é ativado.

Para excluir uma credencial de RSA SecurID:

▲ Clique em **Excluir** e então selecione **Sim** no popup que perguntará “Tem certeza de que quer excluir as suas credenciais de RSA SecurID?"

Password Manager

Fazer login em sites da web e aplicativos é mais fácil e seguro com o Password Manager. É possível criar senhas mais fortes, que você não precisa anotar ou memorizar, e então fazer login fácil e rapidamente por meio de impressão digital, smart card, cartão de proximidade, cartão sem contatos, telefone Bluetooth, PIN, credenciais de RSA ou da senha do Windows.

NOTA: Devido à estrutura em constante mudança das telas de login da Web, o Password Manager pode não conseguir suportar todos os sites da web o tempo todo.

O Gerenciador de Senhas oferece as seguintes opções:

Página do Password Manager

- Clique o toque em uma conta para abrir automaticamente uma página da web ou um aplicativo e fazer o login.
- Use as categorias para organizar as suas contas.

Força de senha

- Saber rapidamente se alguma de suas senhas é um risco à segurança.
- Quando adicionar dados de login, verifique a força de senhas individuais usadas para sites da Web e aplicativos.
- 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, um sinal de adição (+) será exibido no ícone.

▲ Clique ou toque 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 Password Manager**—Permite que você adicione um login para a tela de login atual.
- **Abrir Password Manager**—Abre o Password Manager.
- **Configurações do Ícone**—Permite que você especifique as condições em que o ícone do **Password Manager** é exibido.
- **Ajuda**—Exibe a Ajuda do HP Client Security.

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 para **Verificar sua identidade**. Se autenticados com sucesso, seus dados de login serão colocados nos campos de login e a página será enviada (se o envio foi especificado quando o login foi criado ou editado pela 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 Password Manager.
- **Abrir Password Manager**—Abre o Password Manager.
- **Ajuda**—Exibe a Ajuda do HP Client Security.

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

Adição de logins

Você pode adicionar facilmente um login para um site da Web ou programa digitando as informações de login uma única vez. Feito isso, o Password Manager passa a inserir automaticamente as informações para você. Após navegar até o site da Web ou programa, você pode usar estes logins:

Para adicionar um login:

1. Abra a tela de login de um site da Web ou programa.
2. Clique ou toque no ícone do **Password Manager** e, a seguir, clique ou toque em uma das seguintes opções, dependendo de a tela de login ser de um site da Web ou programa:
   - Para um site da Web, clique ou toque em **Adicionar [nome do domínio] ao Password Manager**.
   - Para um programa, clique ou toque 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.
   a. Para preencher um campo de login com uma das escolhas pré-formatadas, clique ou toque nas setas à direita do campo.
   b. Para visualizar a senha para este login, clique ou toque 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 ou toque em **OK** para selecionar o método de autenticação que deseja usar (impressões digitais, 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 **Gerenciador de Senhas** a fim de avisar que o login foi criado.
   e. Se o Password Manager não detectar os campos de login, clique ou toque 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 ou toque em **Fechar**.

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

Edição de logins

Para editar um login:

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 ou toque no ícone do **Password Manager** e, em seguida, 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.

   Também é possível editar informações da conta a partir da página do Password Manager clicando ou tocando no login para exibir as opções de edição e, em seguida, selecionando **Editar**.

3. Edite suas informações de login.

   - Para editar o **Nome da conta**, digite um novo nome no campo.
   - Para adicionar ou editar o nome de uma **Categoria**, digite ou modifique o nome no campo **Categoria**.
   - Para selecionar um campo de login de **Nome de usuário** com uma das escolhas pré--formatadas, clique ou toque na seta para baixo à direita do campo.

     As escolhas pré-formatadas estão disponíveis somente no caso da edição de login a partir do comando Editar no menu de contexto do ícone do Password Manager.
   - Para selecionar um campo de login de **Senha** com uma das escolhas pré-formatadas, clique ou toque na seta para baixo à direita do campo.

     As escolhas pré-formatadas estão disponíveis somente no caso da edição de login a partir do comando Editar no menu de contexto do ícone do Password Manager.
   - Para adicionar outros campos a partir da tela do seu login, clique ou toque em **Mais campos**.
   - Para visualizar a senha para este login, clique ou toque no ícone **Exibir senha**.
   - Para que os campos de login sejam preenchidos, mas não enviados, desmarque a caixa de seleção **Enviar dados de login automaticamente**.
   - Para advertir que este login tem uma senha comprometida, selecione a caixa de seleção **Esta senha está comprometida**.

     Depois que as alterações forem salvas, todos os outros logins que compartilhem a mesma senha também serão marcados como comprometidos. É possível visitar cada conta afetada e alterar as senhas como for necessário.

4. Clique ou toque em **OK**.

Uso do menu Links Rápidos do Password Manager

O Password Manager oferece uma maneira rápida e fácil para abrir sites da Web e programas para os quais você criou logins. Clique duas vezes ou toque duas vezes no login de um programa ou site da Web a partir do menu **Links Rápidos do Password Manager**, ou da página do Password Manager no HP Client Security, 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**:

▲ Pressione a combinação de teclas **Password Manager** (Ctrl+tecla Windows +h é a configuração de fábrica). Para alterar a combinação de teclas de acesso rápido, na página Inicial do HP Client Security, clique em **Password Manager** e clique ou toque em **Configurações**.

Organização de logins em categorias

Crie uma ou mais categorias para manter seus logins em ordem.

Para atribuir um login a uma categoria:

1. Na Página Inicial do HP Client Security, clique ou toque em **Password Manager**.
2. Clique ou toque em uma entrada de conta e, em seguida, clique ou toque em **Editar**.

3. No campo**Categoria**, digite o nome de uma categoria.
4. Clique ou toque em **Salvar**.

Para remover uma conta de uma categoria:

1. Na Página Inicial do HP Client Security, clique ou toque em **Password Manager**.
2. Clique ou toque em uma entrada de conta e, em seguida, clique ou toque em **Editar**.
3. No campo**Categoria**, apague o nome da categoria.
4. Clique ou toque em **Salvar**.

Para dar um novo nome a uma categoria:

1. Na Página Inicial do HP Client Security, clique ou toque em **Password Manager**.
2. Clique ou toque em uma entrada de conta e, em seguida, clique ou toque em **Editar**.
3. No campo **Categoria**, altere o nome de uma categoria.
4. Clique ou toque em **Salvar**.

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 página do Password Manager.

Para gerenciar seus logins:

1. Na Página Inicial do HP Client Security, clique ou toque em **Password Manager**.
2. Clique ou toque em um login existente, selecione uma das opções a seguir e, então, siga as instruções na tela:
   - **Editar**: edite um login. Para obter mais informações, consulte Edição de logins na página 21.
   - **Log in**—Faz o login na conta selecionada.
   - **Excluir**—Exclui o login da conta selecionada.

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

1. Abra a tela de login para o site da Web ou programa.
2. Clique ou toque no ícone do **Password Manager** para exibir seu menu de contexto.
3. Clique ou toque em **Adicionar Login** e siga as instruções na tela.

Avaliação da força de sua senha

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

O Password Manager facilita o monitoramento e aperfeiçoamento de sua segurança, com análises instantâneas e automatizadas da força de cada uma das senhas usadas para fazer login em seus sites da Web e programas.

À medida que você digita uma senha durante a criação de um login do Password Manager para uma conta, uma barra colorida é exibida sob a senha para indicar a sua força. As cores indicam os seguintes valores:

- **Vermelho**—Fraco
- **Amarelo**—Regular
- **Verde**—Forte

Configurações do ícone do Gerenciador de Senhas

O Password Manager tenta identificar as telas de login de 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 ou toque no ícone e, em seguida, em **Configurações do Ícone** para personalizar a forma como o Password Manager trata possíveis sites de login.
   - **Solicitar a adição de logins para telas de login**—Clique ou toque nesta opção para que o Password Manager solicite que você adicione um login quando for exibida uma tela de login para a qual ainda não exista um login configurado.
   - **Excluir esta tela**: marque essa caixa de seleção para que o Password Manager não solicite novamente que você adicione um login para esta tela de login.
   - **Não solicitar para adicionar logins para telas de login** — selecione o botão de opção.
2. Para adicionar um login para uma tela que foi excluída anteriormente:
   a. Faça o login no site da web excluído anteriormente.
   b. Para que o Password Manager se lembre da senha deste site, clique ou toque em **Lembre-se** no pop-up para salvar a senha e criar um logon para a tela.
3. Para ter acesso a configurações adicionais do Password Manager, clique ou toque no ícone do Password Manager, em **Abrir o Password Manager** e em **Configurações**, na página do Password Manager.

Importação e exportação de logins

Na página de Importação e Exportação do HP Password Manager, é possível importar logins salvos por navegadores da Web no seu computador. Também é possível importar dados de um arquivo de backup do HP Client Security e exportar dados para um arquivo de backup do HP Client Security.

▲ Para abrir a página de importação e exportação, clique ou toque em **Importar e exportar** na página do Password Manager.

Para importar senhas de um navegador:

1. Clique ou toque no navegador do qual você quer importar senhas (são exibidos somente navegadores instalados).
2. Desmarque a caixa de seleção de qualquer conta para a qual você não queira importar senhas.
3. Clique ou toque em **Importar**.

As ações de importar dados de um arquivo de backup do HP Client Security e de exportar dados para ele podem ser realizadas por meio de links associados (em **Outras Opções**) na página de Importação e Exportação.

NOTA: Este recurso importa e exporta somente dados do Password Manager. Para obter mais informações sobre como fazer backup e como restaurar dados adicionais do HP Client Security, consulte Backup e restauração de dados na página 29.

Para importar dados de um arquivo de backup de HP Client Security:

1. Na página de Importação e Exportação do HP Password Manager, clique ou toque em **Importar dados de um arquivo de backup do HP Client Security**.
2. Verifique sua identidade.
3. Selecione o arquivo de backup previamente criado ou digite o caminho no campo fornecido e, em seguida, clique ou toque em **Navegar**.
4. Digite a senha usada para proteger o arquivo e clique ou toque em **Avançar**.
5. Clique ou toque em **Restaurar**.

Para exportar dados para um arquivo de backup do HP Client Security:

1. Na página de Importação e Exportação do HP Password Manager, clique ou toque em **Exportar dados para um arquivo de backup do HP Client Security**.
2. Verifique a sua identidade e clique ou toque em **Avançar**.
3. Digite um nome para o arquivo de backup. Por padrão, o arquivo será salvo na pasta Documentos. Para especificar um local diferente, clique ou toque em **Navegar**.
4. Digite e confirme uma senha para proteger o arquivo e, em seguida, clique ou toque em **Salvar**.

Configurações

É possível especificar configurações para personalizar o Password Manager:

- **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**.

- **Abrir o Password Manager com Ctrl+Win+h**: a tecla de acesso rápido padrão que abre o menu de **Links Rápidos do Password Manager** é Ctrl+tecla do Windows+h.

  Para alterar a tecla de acesso rápido, clique ou toque 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.

  As combinações reservadas para o Windows ou para aplicativos do Windows não podem ser usadas.

- Para retornar as configurações aos padrões de fábrica originais, clique ou toque em **Restaurar padrões**.

Configurações avançadas

Os administradores podem ter acesso às seguintes opções, selecionando o ícone da **Engrenagem** (configurações) na Tela Inicial do HP Client Security.

- **Políticas do Administrador**—Permite que você configure políticas de login e de sessão para os administradores.
- **Políticas de Usuário Padrão**—Permite que você configure políticas de login e de sessão para os usuários padrão.
- **Recursos de Segurança**—Permite que você aumente a segurança do seu computador protegendo sua conta de Windows pelo uso de autenticações fortes e/ou pela ativação de autenticações antes da inicialização do Windows.
- **Usuários**—Permite gerenciar os usuários e suas credenciais.
- **Minhas Políticas**—Permite que você reveja as usas políticas de autenticação e status de inscrição.
- **Backup e Restauração**—Permite que você faça backup ou restaure dados do HP Client Security.
- **Sobre o HP Client Security**—Exibe informações de versão sobre o HP Client Security.

Políticas de Administrador

É possível configurar políticas de login e de sessão para administradores do computador. As políticas de login estabelecidas aqui controlam as credenciais exigidas para que um administrador local faça o login no Windows. As políticas de sessão estabelecidas aqui controlam as credenciais exigidas para que um administrador local verifique a identidade em uma sessão do Windows.

Por padrão, todas as políticas novas ou modificadas são imediatamente impostas depois de clicar ou tocar na opção **Aplicar**.

Para adicionar uma nova política:

1. Na Página Inicial do HP Client Security, clique ou toque no ícone da **Engrenagem**.
2. Na página de Configurações Avançadas, clique ou toque em **Políticas de Administrador**.
3. Clique ou toque em **Adicionar nova política**.
4. Clique nas setas para baixo para selecionar as credenciais primárias e secundárias (opcionais) para a nova política e, em seguida, clique ou toque em **Adicionar**.
5. Clique em **Aplicar**.

Para retardar a imposição de uma política nova ou modificada:

1. Clique ou toque em **Impor esta política imediatamente**.
2. Selecione **Impor esta política na data específica**.
3. Digite a data ou use o calendário popup para selecionar a data em que essa política deverá ser imposta.
4. Se desejar, selecione um momento para lembrar os usuários sobre esta nova política.
5. Clique em **Aplicar**.

Políticas para Usuários Padrão

É possível configurar políticas de login e de sessão para usuários padrão do computador. As políticas de login estabelecidas aqui controlam as credenciais exigidas para que um usuário padrão faça o login no Windows. As políticas de sessão estabelecidas aqui controlam as credenciais exigidas para que um usuário padrão verifique a identidade em uma sessão do Windows.

Por padrão, todas as políticas novas ou modificadas são imediatamente impostas depois de clicar ou tocar na opção **Aplicar**.

Para adicionar uma nova política:

1. Na Página Inicial do HP Client Security, clique ou toque no ícone da **Engrenagem**.
2. Na página de Configurações Avançadas, clique ou toque em **Políticas de Usuário Padrão**.
3. Clique ou toque em **Adicionar nova política**.
4. Clique nas setas para baixo para selecionar as credenciais primárias e secundárias (opcionais) para a nova política e, em seguida, clique ou toque em **Adicionar**.
5. Clique em **Aplicar**.

Para retardar a imposição de uma política nova ou modificada:

1. Clique ou toque em **Impor esta política imediatamente**.
2. Selecione **Impor esta política na data específica**.
3. Digite a data ou use o calendário popup para selecionar a data em que essa política deverá ser imposta.
4. Se desejar, selecione um momento para lembrar os usuários sobre esta nova política.
5. Clique em **Aplicar**.

Recursos de segurança

É possível ativar recursos de segurança do HP Client Security que ajudam a proteger contra o acesso não autorizado ao computador.

Para definir os recursos de segurança:

1. Na Página Inicial do HP Client Security, clique ou toque no ícone da **Engrenagem**.
2. Na página de Configurações Avançadas, clique ou toque em **Recurso de segurança**.

3. Ative os recursos de segurança selecionando as caixas de seleção e, em seguida, clique ou toque em **Avançar**. Quanto mais recursos marcar, mais seguro estará o seu computador.

   As configurações a seguir se aplicam a todos os usuários.

   - **Segurança de login do Windows**— Protege suas contas do Windows solicitando o uso das credenciais do HP Client Security para o acesso.
   - **Segurança de pré-inicialização (Autenticação na inicialização)**— Protege o computador antes da inicialização do Windows. Essa seleção não estará disponível se o BIOS não suportá-la.
   - **Permitir o login ao One Step**—Esta configuração permite pular o login no Windows se a autenticação já tiver sido feita anteriormente, na Autenticação na inicialização ou no nível Drive Encryption.

4. Clique ou toque em **Usuários**, e, em seguida, clique ou toque no bloco do usuário.

Usuários

É possível monitorar e gerenciar os usuários do HP Client Security do computador.

Para adicionar um usuário do Windows no HP Client Security:

1. Na Página Inicial do HP Client Security, clique ou toque no ícone da **Engrenagem**.
2. Na página de Configurações Avançadas, clique ou toque em **Usuários**.
3. Clique ou toque em **Adicionar usuário de Windows no HP Client Security**.
4. Digite o nome do usuário que você deseja adicionar e clique ou toque em **OK**.
5. Digite a senha do usuário do Windows.

   Será exibido um bloco na página de Usuários para o usuário adicionado.

Para excluir um usuário do Windows do HP Client Security:

1. Na Página Inicial do HP Client Security, clique ou toque no ícone da **Engrenagem**.
2. Na página de Configurações Avançadas, clique ou toque em **Usuários**.
3. Clique ou toque no nome do usuário que deseja excluir.
4. Clique ou toque em **Excluir usuário**, e, em seguida, clique ou toque em **Sim** para confirmar.

Para exibir um resumo de políticas de login e de sessão impostas para um usuário:

▲ Clique ou toque em **Usuários**, e, em seguida, clique ou toque no bloco do usuário.

Minhas Políticas

É possível exibir as suas políticas de autenticação e status de inscrição. A página Minhas Políticas também oferece links para as páginas de Políticas de Administradores e Políticas de Usuário Padrão.

1. Na Página Inicial do HP Client Security, clique ou toque no ícone da **Engrenagem**.
2. Na página de Configurações Avançadas, clique ou toque em **Minhas Políticas**.

   Serão exibidas as políticas de login e de sessão impostas para os usuários que estão com login feito no momento.

A página Minhas Políticas também oferece links para Políticas de Administrador na página 26 e Políticas para Usuários Padrão na página 27.

Backup e restauração de dados

É recomendável que você faça backup de seus dados do HP Client Security 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 faça backup todos os dias.

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

NOTA: Esse recurso faz backup somente do Password Manager. O Drive Encryption possui um método de backup independente. Não é feito backup das informações de autenticação por impressão digital e do Device Access Manager.

Para que os dados possam ser restaurados a partir dos arquivos de backup, o HP Client Security deve estar instalado no computador que receberá o backup desses dados.

Para fazer backup de seus dados:

1. Na Página Inicial do HP Client Security, clique ou toque no ícone da **Engrenagem**.
2. Na página de Configurações Avançadas, clique ou toque em **Políticas de Administrador**.
3. Clique ou toque em **Backup e Restauração**.
4. Clique ou toque em **Backup** e, em seguida, verifique a sua identidade.
5. Selecione o módulo que deseja incluir no backup e clique ou toque em **Avançar**.
6. Insira um nome para o arquivo de armazenamento. Por padrão, o arquivo será salvo na pasta Documentos. Para especificar um local diferente, clique ou toque em **Navegar**.
7. Digite uma senha e confirme-a para proteger o arquivo.
8. Clique ou toque em **Salvar**.

Para restaurar seus dados:

1. Na Página Inicial do HP Client Security, clique ou toque no ícone da **Engrenagem**.
2. Na página de Configurações Avançadas, clique ou toque em **Políticas de Administrador**.
3. Clique ou toque em **Backup e Restauração**.
4. Selecione **Restaurar** e, em seguida, verifique a sua identidade.
5. Selecione o arquivo de armazenamento criado anteriormente. Insira o caminho no campo fornecido. Para especificar um local diferente, clique ou toque em **Navegar**.
6. Digite a senha usada para proteger o arquivo e clique ou toque em **Avançar**.
7. Selecione os módulos para os quais você quer restaurar dados.
8. Clique ou toque em **Restaurar**.

5 HP Drive Encryption (somente em determinados modelos)

O HP Drive Encryption fornece uma proteção de dados completa para criptografar os dados do computador. Quando o Drive Encryption está ativado, é necessário efetuar login na tela de login do Drive Encryption, exibida antes da inicialização do sistema operacional Windows®.

A Tela Inicial do HP Client Security 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 Client Security.

As seguintes tarefas podem ser executadas com o Drive Encryption:

- Selecionando configurações do Drive Encryption:
  - 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 smart cards selecionados

Início do Drive Encryption

Os administradores podem acessar o Drive Encryption pelo HP Client Security:

1. Na tela Iniciar, clique ou toque no aplicativo **HP Client Security** (Windows 8).

   – ou –

   Na área de trabalho do Windows, clique ou toque duas vezes no ícone do **HP Client Security** na área de notificação, localizado no lado direito na barra de tarefas.

2. Clique ou toque no ícone do **Drive Encryption**.

Tarefas gerais

Ativando o Drive Encryption para discos rígidos padrão

Unidades de disco rígido padrão são criptografadas utilizando criptografia por software. Siga estas etapas para criptografar uma unidade ou uma partição de disco:

1. Abra o **Drive Encryption**. Para obter mais informações, consulte Início do Drive Encryption na página 30.
2. Marque a caixa de seleção para a unidade ou partição que deseja criptografar e clique ou toque em **Chave de Backup**.

NOTA: Para melhorar os níveis de segurança, selecione a caixa de seleção **Desativar modo de suspensão para aumentar segurança** Ao desativar o modo de suspensão, não há qualquer risco das credenciais utilizadas para desbloquear a unidade sejam armazenadas na memória.

3. Selecione uma ou mais das opções de backup e clique ou toque em **Backup**. Para obter mais informações, consulte Fazendo backup de chaves de criptografia na página 34.
4. É possível continuar trabalhando enquanto o backup da chave de criptografia é executado. Não reinicialize o computador.

NOTA: Será solicitada a reinicialização do computador. Após a reinicialização, a tela de pré-inicialização de criptografia da unidade será exibida, solicitando uma autenticação antes do Windows iniciar.

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 Client Security.

Ativando o Drive Encryption para unidades de criptografia automática

Unidades autocriptografadas que atendem à especificação OPAL do Trusted Computing Group's OPAL para o gerenciamento de unidades autocriptografadas podem ser criptografadas usando a criptografia por software ou hardware. A criptografia por hardware é muito mais rápida que a criptografia por software. No entanto, não é possível selecionar quais partições de disco criptografar. Todo o disco, incluindo quaisquer partições, é criptografado.

Para criptografar partições específicas, é necessário usar a criptografia por software. Verifique se a caixa de seleção **Permitir somente criptografia por hardware para Unidades Autocriptografadas (SED)** está desmarcada.

Para ativar o Drive Encryption em unidades autocriptografadas, siga estas etapas:

1. Abra o **Drive Encryption**. Para obter mais informações, consulte Início do Drive Encryption na página 30.
2. Marque a caixa de seleção para a unidade que deseja criptografar e clique ou toque em **Chave de Backup**.

NOTA: Para melhorar os níveis de segurança, selecione a caixa de seleção **Desativar modo de suspensão para aumentar a segurança**. Ao desativar o modo de suspensão, não há qualquer risco das credenciais utilizadas para desbloquear a unidade sejam armazenadas na memória.

3. Selecione uma ou mais das opções de backup e clique ou toque em **Backup**. Para obter mais informações, consulte Fazendo backup de chaves de criptografia na página 34.
4. É possível continuar trabalhando enquanto o backup da chave de criptografia é executado. Não reinicialize o computador.

NOTA: Para autocriptografar unidades, será solicitado que você desligue o computador

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

Desativando o Drive Encryption

1. Abra o **Drive Encryption**. Para obter mais informações, consulte Início do Drive Encryption na página 30.
2. Desmarque a caixa de seleção de todas as Unidades criptografadas e clique ou toque em **Aplicar**.

   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

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

NOTA: 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 espera ocorram quando ativados.

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 Client Security, e se o One-Step Logon estiver ativado (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 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 ou toque 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

- 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.

Criptografia de unidades de disco rígido adicionais

É altamente recomendado a utilização do Assistente de Configuração do HP Drive Encryption para proteger seus dados criptografando a unidade de disco rígido. Após a ativação, qualquer disco rígido adicionado ou partição criada poderá ser criptografada segundo estas etapas:

1. Abra o **Drive Encryption**. Para obter mais informações, consulte Início do Drive Encryption na página 30.
2. 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 o Drive Encryption para visualizar e modificar o status de criptografia (Não Criptografado ou Criptografado) de todas as unidades de disco rígido no computador.

- 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)

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

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

1. Abra o **Drive Encryption**. Para obter mais informações, consulte Início do Drive Encryption na página 30.
2. Em **Status da unidade**, marque ou desmarque a caixa de seleção de cada partição de unidade de disco rígido que deseja criptografar ou decodificar, em seguida clique ou toque em **Aplicar**.

NOTA: Quando uma partição estiver sendo criptografada ou decodificada, a barra de progresso exibirá a porcentagem da partição criptografada.

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.

Gerenciamento de Disco

- **Apelido**—É possível dar nomes às suas unidades ou partições para facilitar a identificação.
- **Unidades desconectadas**—O Drive Encryption pode rastrear discos que são removidos do computador. Um disco removido do computador é automaticamente movido para a lista Desconectado. Se o disco é recolocado no sistema, ele aparecerá novamente na lista Conectado.
- Se não for mais necessário rastrear ou gerenciar a unidade desconectada, é possível removê-la da lista Desconectado.
- O Drive Encryption permanece ativado até que as caixas de seleção de todas as unidades conectadas sejam desmarcadas e a lista Desconectado esteja vazia.

Backup e recuperação (tarefa de 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.

Fazendo 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.

1. Abra o **Drive Encryption**. Para obter mais informações, consulte Início do Drive Encryption na página 30.
2. Selecione a caixa de seleção para uma unidade, e em seguida clique ou toque em **Chave de Backup**.

3. Em **Criar chave de recuperação do HP Drive Encryption** , selecione uma ou mais da opções seguintes:

   - **Armazenamento Removível**—Selecione a caixa de seleção, e em seguida selecione o dispositivo de armazenamento onde a chave de criptografia será salva.
   - **SkyDrive**—Selecione a caixa de seleção. É preciso estar conectado à Internet. Faça log in no Microsoft SkyDrive e clique ou toque em **Sim**.

   NOTA: Para usar a chave de backup do HP Drive Encryption que está armazenada no SkyDrive, é preciso fazer o seu download do SkyDrive para um dispositivo de armazenamento removível, e então inserir o dispositivo de armazenamento neste computador.

   - **TPM** (somente em alguns modelos)—Permite que você recupere os seus dados usando uma senha do TPM.

   CUIDADO: Se o TPM estiver desmarcado ou o se computador estiver danificado, você perderá o acesso ao backup. Se esse método for selecionado, é aconselhável selecionar também outro método.

4. Clique ou toque em **Backup**.

   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 **Chave de Backup** no Drive Encryption.

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 HP Drive Encryption for exibida, clique ou toque em **Recuperação**.
4. Insira o caminho ou o nome do arquivo que contém sua chave de backup e clique ou toque em **Recuperar**.
5. Quando a caixa de diálogo de confirmação for exibida, clique ou toque em **OK**.

   A tela de login 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 Client Security.

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

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

3. Clique em **SpareKey**.

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

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

   A tela de login 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.

6 HP File Sanitizer (somente em determinados modelos)

O File Sanitizer permite fragmentar ativos (por exemplo: informações pessoais ou arquivos, dados históricos ou da web ou outros componentes de dados) existentes no disco rígido do computador com segurança e limpar o disco rígido interno periodicamente.

O File Sanitizer não pode ser usado para limpar os tipos de unidades a seguir:

- Unidades Solid State (SSD), incluindo volumes de RAID que abrangem um dispositivo SSD
- Unidades externas conectadas por USB, Firewire ou interface eSATA

Se houver uma tentativa de fragmentação ou limpeza em um SSD, será exibida uma mensagem de aviso e a operação não será executada.

Fragmentação

A fragmentação é diferente de uma ação padrão de exclusão do Windows®. Quando você fragmenta um ativo usando o File Sanitizer, os arquivos são substituídos por dados insignificantes, o que torna praticamente impossível recuperar o ativo original. Uma ação de exclusão simples do Windows pode deixar o arquivo (ou ativo) intacto na unidade de disco rígido ou em um estado em que métodos periciais poderiam ser usados para recuperá-lo.

É possível programar um horário para fragmentação futuro ou ativar manualmente a fragmentação, selecionando o ícone do **File Sanitizer** na Tela Inicial do HP Client Security, ou usando o ícone do **File Sanitizer** na área de trabalho do Windows. Para obter mais informações, consulte Configuração de uma programação de fragmentação na página 39, Fragmentação com o botão direito do mouse na página 41 ou Ativação manual da operação de fragmentação na página 41.

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

Purificação de espaço livre

Excluir um ativo no Windows não remove completamente o seu conteúdo no disco rígido. O Windows exclui apenas a referência ao ativo ou o seu local no disco rígido. O conteúdo do ativo permanecerá no disco rígido até que outro ativo substitua essa área com novas informações.

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

NOTA: A purificação de espaço livre não oferece segurança adicional a ativos fragmentados.

Você pode programar um horário futuro para a purificação de espaço livre de ativos previamente fragmentados ou pode ativá-la manualmente, selecionando o ícone do **File Sanitizer** na Tela Inicial do HP Client Security, ou usando o ícone do **File Sanitizer** na área de trabalho do Windows. Para obter mais informações, consulte Programação de uma purificação de espaço livre na página 40, Ativação manual de purificação de espaço livre na página 42 ou Utilização do ícone do File Sanitizer na página 41.

Inicialização do File Sanitizer

1. Na tela Iniciar, clique ou toque no aplicativo **HP Client Security** (Windows 8).

   – ou –

   Na área de trabalho do Windows, clique ou toque duas vezes no ícone do **HP Client Security** na área de notificação, localizado no lado direito na barra de tarefas.

2. Em **Dados**, clique ou toque em **File Sanitizer**.

– ou –

▲ Clique duas vezes ou toque duas vezes no ícone do **File Sanitizer** na área de trabalho do Windows.

– ou –

▲ Clique com o botão direito ou toque e segure o ícone do **File Sanitizer** na área de trabalho do Windows, e depois selecione **Abrir File Sanitizer**.

Procedimentos de configuração

Fragmentação— o File Sanitizer exclui ou fragmenta categorias selecionadas de ativos com segurança.

1. Em **Fragmentação**, marque a caixa de seleção para cada tipo de arquivo a ser fragmentado, ou desmarque a caixa de seleção se não deseja fragmentar esses arquivos.
   - **Lixeira**: Fragmenta todos os itens na Lixeira.
   - **Arquivos temporários do sistema**: Fragmenta todos os arquivos existentes na pasta de temporários do sistema. As seguintes variáveis de ambiente são pesquisadas na ordem a seguir, e o primeiro caminho encontrado é considerado como a pasta do sistema:
     - TMP
     - TEMP
   - **Arquivos temporários da Internet**: Fragmenta cópias de páginas da Web, imagens e mídia salvas por navegadores da Web para visualização mais rápida.
   - **Cookies**: Fragmenta todos os arquivos armazenados no computador por sites da Web para salvar preferências, como informações de login.
2. Para iniciar a fragmentação, clique ou toque em **Fragmentar**

Purificação— Escreve dados aleatórios no espaço livre e evita a recuperação de itens excluídos.

▲ Para iniciar a purificação, clique ou toque em **Purificar**

Opções do File Sanitizer—Marque as caixas de seleção para cada uma das opções a seguir, ou desmarque as caixas de seleção para desativar uma opção.

- **Ativar ícone na Área de Trabalho**—Exibe o ícone do File Sanitizer na Área de Trabalho do Windows.
- **Ativar botão direito do mouse**—Permite que você clique com o botão direito ou toque e segure um ativo, e então selecionar **HP File Sanitizer – Fragmentar**.

- **Pedir senha do Windows antes da fragmentação manual**—Exige autenticação com a senha do Windows antes de fragmentar manualmente um item.
- **Fragmentar Cookies e Arquivos Temporários da Internet ao fechar navegador**—Fragmenta todos os ativos relacionados à Web selecionados, como o histórico de URL do navegador, quando você fechar um navegador da Web.

Configuração de uma programação de fragmentação

Você pode programar um horário para executar a fragmentação automaticamente, ou pode também fragmentar ativos manualmente a qualquer momento. Para obter mais informações, consulte Procedimentos de configuração na página 38.

1. Abra o File Sanitizer e clique ou toque em **Configurações**.
2. Para programar um horário para fragmentar ativos selecionados, vá a **Programação de fragmentação**, selecione **Nunca**, **Uma vez**, **Diariamente**, **Semanalmente** ou **Mensalmente**, e então selecione dia e hora:
   a. Clique ou toque na hora, minuto ou campo AM/PM.
   b. Role até que o número desejado seja exibido no mesmo nível dos outros campos.
   c. Clique ou toque no espaço em branco ao redor do campo de configuração de hora.
   d. Repita a mesma ação para cada campo até que a programação correta tenha sido selecionada.
3. São listados os quatro tipos de ativos abaixo:
   - **Lixeira**: Fragmenta todos os itens na Lixeira.
   - **Arquivos temporários do sistema**: Fragmenta todos os arquivos existentes na pasta de temporários do sistema. As seguintes variáveis de ambiente são pesquisadas na ordem a seguir, e o primeiro caminho encontrado é considerado como a pasta do sistema:
     - TMP
     - TEMP
   - **Arquivos temporários da Internet**: Fragmenta cópias de páginas da Web, imagens e mídia salvas por navegadores da Web para visualização mais rápida.
   - **Cookies**: Fragmenta todos os arquivos armazenados no computador por sites da Web para salvar preferências, como informações de login.

   Se tiverem sido marcados, esses ativos são fragmentados no horário programado.
4. Para selecionar ativos adicionais personalizados a serem fragmentados:
   a. Em **Lista de Fragmentação Programada**, clique ou toque em **Adicionar pasta** e navegue até o arquivo ou pasta.
   b. Clique ou toque em **Abrir** e clique ou toque em **OK**.

   Para remover um ativo da Lista de Fragmentação Programada, desmarque a caixa de seleção do ativo.

Programação de uma purificação de espaço livre

A purificação de espaço livre não oferece segurança adicional a ativos fragmentados.

1. Abra o File Sanitizer e clique ou toque em **Configurações**.
2. Para programar um horário para purificar a sua unidade de disco rígido, vá a **Programação de Purificação**, selecione **Nunca**, **Uma Vez**, **Diariamente**, **Semanalmente**, ou **Mensalmente**, e, em seguida, selecione dia e hora.
   a. Clique ou toque na hora, minuto ou campo AM/PM.
   b. Role até que o horário desejado seja exibido no mesmo nível dos outros campos.
   c. Clique ou toque no espaço em branco ao redor do campo de configuração de hora.
   d. Repita a mesma ação até que a programação correta tenha sido selecionada.

NOTA: A operação de purificação de espaço livre pode levar um tempo significativo. Verifique se o computador está ligado à alimentação de CA. Embora a purificação de espaço livre seja executada em segundo plano, o aumento da utilização do processador pode afetar o desempenho do computador. A purificação de espaço livre poderá ser realizada após algumas horas ou quando o computador não estiver em uso.

Proteção de arquivos contra a fragmentação

Para proteger arquivos ou pastas contra a fragmentação:

1. Abra o File Sanitizer e clique ou toque em **Configurações**.
2. Em **Lista Não Fragmentar Nunca**, clique ou toque em **Adicionar pasta**, e então navegue até o arquivo ou pasta.
3. Clique ou toque em **Abrir** e clique ou toque em **OK**.

NOTA: Os arquivos desta lista estarão protegidos enquanto permanecerem nela.

Para remover um ativo da lista de exclusões, desmarque a caixa de seleção do ativo.

Cálculos gerais

Use o File Sanitizer para executar as seguintes tarefas:

- **Usar o ícone File Sanitizer para iniciar a fragmentação**—Arraste os arquivos para o ícone do **File Sanitizer** na área de trabalho do Windows. Para obter detalhes, consulte Utilização do ícone do File Sanitizer na página 41.
- **Fragmentar manualmente um ativo específico ou todos os ativos selecionados**—Fragmente itens a qualquer momento, sem esperar pelo horário programado de fragmentação. Para obter detalhes, consulte Fragmentação com o botão direito do mouse na página 41 ou Ativação manual da operação de fragmentação na página 41.
- **Ativar manualmente a purificação de espaço livre**—Ative a purificação de espaço livre a qualquer momento. Para obter detalhes, consulte Ativação manual de purificação de espaço livre na página 42.
- **Visualizar os arquivos de registro**—Visualize os arquivos de registro de fragmentação e purificação de espaço livre, que contêm erros da última operação de fragmentação ou purificação de espaço livre. Para obter detalhes, consulte Visualização de arquivos de log na página 42.

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

Utilização do ícone do File Sanitizer

CUIDADO: Ativos fragmentados não podem ser recuperados. Selecione com cuidado os itens a serem fragmentados manualmente.

Quando uma operação de fragmentação for iniciada manualmente, a lista padrão de fragmentação no visualizador do File Sanitizer é fragmentada (ver Procedimentos de configuração na página 38).

É possível iniciar manualmente uma operação de fragmentação nas seguintes maneiras:

1. Abra o File Sanitizer (ver Inicialização do File Sanitizer na página 38) e clique ou toque em **Fragmentar**.
2. Quando a caixa de diálogo de confirmação for exibida, verifique se os ativos que você deseja fragmentar estão marcados, e então clique ou toque em **OK**.

– ou –

1. Clique com o botão direito ou toque e segure o ícone do **File Sanitizer** na área de trabalho do Windows, e depois clique ou toque em **Fragmentar Agora**.
2. Quando a caixa de diálogo de confirmação for exibida, verifique se os ativos que você deseja fragmentar estão marcados, e então clique ou toque em **Fragmentar**.

Fragmentação com o botão direito do mouse

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

Se a opção **Habilitar fragmentação com o botão direito do mouse** tiver sido selecionada no visualizador do File Sanitizer, é possível fragmentar um ativo da seguinte maneira:

1. Navegue até o documento ou pasta que deseja fragmentar.
2. Clique com o botão direito ou toque e segure o arquivo ou pasta e selecione **HP File Sanitizer – Fragmentar**.

Ativação manual da operação de fragmentação

CUIDADO: Ativos fragmentados não podem ser recuperados. Selecione com cuidado os itens a serem fragmentados manualmente.

Quando uma operação de fragmentação for iniciada manualmente, a lista padrão de fragmentação no visualizador do File Sanitizer é fragmentada (ver Procedimentos de configuração na página 38).

É possível iniciar manualmente uma operação de fragmentação nas seguintes maneiras:

1. Abra o File Sanitizer (ver Inicialização do File Sanitizer na página 38) e clique ou toque em **Fragmentar**.
2. Quando a caixa de diálogo de confirmação for exibida, verifique se os ativos que você deseja fragmentar estão marcados, e então clique ou toque em **OK**.

– ou –

1. Clique com o botão direito ou toque e segure o ícone do **File Sanitizer** na área de trabalho do Windows, e depois clique ou toque em **Fragmentar Agora**.
2. Quando a caixa de diálogo de confirmação for exibida, verifique se os ativos que você deseja fragmentar estão marcados, e então clique ou toque em **Fragmentar**.

Ativação manual de purificação de espaço livre

Quando uma operação de purificação for iniciada manualmente, a lista padrão de fragmentação no visualizador do File Sanitizer é purificada (ver Procedimentos de configuração na página 38).

É possível iniciar manualmente uma operação de purificação nas seguintes maneiras:

1. Abra o File Sanitizer (see Inicialização do File Sanitizer na página 38) e clique ou toque em **Purificar**.
2. Quando a caixa de diálogo de confirmação for exibida, clique ou toque em **OK**.

– ou –

1. Clique com o botão direito ou toque e segure o ícone do **File Sanitizer** na área de trabalho do Windows, e depois clique ou toque em **Purificar Agora**.
2. Quando a caixa de diálogo de confirmação for exibida, clique ou toque em **Purificar**.

Visualização de arquivos de log

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

NOTA: Os arquivos fragmentados ou limpos com êxito não aparecem nos arquivos de registro.

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

- C:\Arquivos de programas\Hewlett-Packard\File Sanitizer*[Nome do usuário]*_ShredderLog.txt
- C:\Arquivos de programas\Hewlett-Packard\File Sanitizer*[Nome do usuário]*_DiskBleachLog.txt

Para sistemas de 64 bits, os arquivos de registro ficam localizados na unidade de disco rígido das seguintes pastas:

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

7 HP Device Access Manager (somente em determinados modelos)

O HP 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 46.

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

- Os perfis de dispositivo são criados para cada usuário a fim de definir os dispositivos aos quais eles possuem ou não possuem permissão de acesso.
- A Autenticação Just In Time (JITA) permite a usuários predefinidos se autenticar para poder ter acesso a dispositivos que, caso contrário, têm acesso negado.
- Os administradores e usuários confiáveis podem ser excluídos das restrições de acesso a dispositivos pelo Device Access Manager adicionando-os ao grupo Administradores de dispositivos. A associação a esse grupo é gerenciada usando as Configurações avançadas.
- O acesso a dispositivos pode ser concedido ou negado com base nas associações dos grupos ou para usuários individuais.
- Para as classes de dispositivos como as unidades de CD-ROM e DVD, o acesso de leitura ou gravação pode ser permitido ou negado separadamente.

O HP Device Acess Manager é configurado automaticamente durante a execução do Assistente de Configuração do HP Client Security, com as seguintes configurações:

- A Mídia Removível da autenticação Just In Time (JITA) é ativada para Administradores e Usuários.
- A política de dispositivos permite acesso total a outros dispositivos.

Inicialização do Device Access Manager

1. Na tela Iniciar, clique ou toque no aplicativo **HP Client Security** (Windows 8).

   – ou –

   Na área de trabalho do Windows, clique ou toque duas vezes no ícone do **HP Client Security** na área de notificação, localizado no lado direito na barra de tarefas.

2. Em **Dispositivos**, clique ou toque em **Permissões de Dispositivos**.

   - Os Usuários padrão podem visualizar suas permissões atuais de acesso aos dispositivos (ver Visualização do Usuário na página 44).
   - Os administradores podem visualizar as permissões de acesso a dispositivos atualmente configuradas para o computador e fazer alterações nelas clicando ou tocando em

Modificar e, depois, digitando a senha do Administrador (ver Visualização do sistema na página 44).

Visualização do Usuário

Quando a **Permissão de Dispositivo**s está selecionada, é exibida a visualização do Usuário. Dependendo da política, os usuários padrão e os administradores podem visualizar suas próprias permissões de acesso por classes de dispositivos ou por dispositivos individuais no computador.

- **Usuário atual**—É exibido o nome do usuário que está com o logon feito no momento.
- **Classe de dispositivo**—São exibidos os tipos de dispositivos.
- **Acesso**—É exibida a sua configuração atual de acesso a tipos de dispositivo ou a dispositivos específicos.
- **Duração**—É exibido o limite de tempo para o acesso a unidades de DVD/CD-ROM ou para unidades de disco removível.
- **Configurações**—Os administradores podem modificar quais unidades terão acesso controlado pelo Device Access Manager.

Visualização do sistema

Na Visualização do sistema, os administradores podem permitir ou negar acesso a dispositivos no computador para o grupo de Usuários ou para o grupo de Administradores.

▲ Os administradores podem acessar a Visualização do sistema clicando ou tocando em **Modificar**, digitando uma senha de administrador e, em seguida, selecionando uma das seguintes opções:

- **Device Access Manager**—Para ligar ou desligar o HP Device Access Manager com autenticação Just In Time, clique ou toque em **Ligar** ou **Desligar**.
- **Usuários e grupos neste PC**—Exibe o Grupo de Usuários ou o Grupo de Administradores que possuem ou não permissão de acesso a determinadas classes de dispositivos.
- **Classe de dispositivo**—Exibe todos os dispositivos e classes de dispositivos que estão instalados ou que podem ter sido instalados anteriormente no sistema. Para expandir a lista, clique no ícone **+**. Todos os dispositivos conectados ao computador são exibidos, e o grupo de administradores e usuários é expandido para mostrar os membros. Para atualizar a lista de dispositivos, clique no ícone da seta girando (atualizar).
    - A proteção é geralmente aplicada a uma classe de dispositivos. Se o acesso for configurado para **Permitir**, o usuário ou grupo selecionado será capaz de acessar qualquer dispositivo desta classe de dispositivos.
    - A proteção também pode ser aplicada a dispositivos específicos.
    - Configure a autenticação Just in time (JITA) e permita que usuários selecionados acessem unidades de DVD/CD-ROM ou unidades de mídias removíveis autenticando a si próprios. Para obter mais informações, consulte Configuração JITA na página 45.
    - Permita ou negue acesso a outras classes de dispositivos, como mídias removíveis (Unidades USB flash, por exemplo), portas paralelas ou seriais, dispositivos Bluetooth®, modems, dispositivos de PCMCIA/ExpressCard, dispositivos 1394, leitor de impressão digital e leitor de smart card. Se o acesso ao leitor de impressão digital e ao leitor de smart card for negado, eles podem ser usados como credenciais de autenticação, mas não poderão ser usados no nível de Política de sessão.

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.

- Quando selecionar uma configuração no nível da Classe de dispositivo ou de Grupo, você deverá escolher se a configuração será aplicada a objetos filhos:

  Sim—A configuração será propagada.

  Não—A configuração não será propagada.

- 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.

NOTA: O grupo Administradores não pode ser adicionado à Lista de usuários.

- **Acesso**—Para permitir ou negar o acesso, clique ou toque na seta para baixo e selecione um dos seguintes tipos de acesso :
  - **Permitir — Acesso total**
  - **Permitir — Somente Leitura**
  - **Permitir – Necessário ter JITA**— Para obter mais informações, consulte Configuração JITA na página 45.

    Se selecionar esse tipo de acesso, em **Duração**, clique ou toque na seta para baixo para selecionar um limite de tempo.
  - **Negar**
- **Duração**—Para selecionar um limite de tempo para o acesso a unidades de DVD/CD-ROM ou a unidades de disco removível, clique ou toque na seta para baixo (consulte Configuração JITA na página 45).

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 habilitados para a JITA poderão acessar alguns dispositivos para os quais políticas criadas na visualização **Configuração de Classe de Dispositivos** sofreram limitações.

O período de autorização da JITA pode ser definido como Ilimitado ou para uma quantidade determinada de minutos. Os usuários com uso ilimitado terão acesso ao dispositivo desde o momento da autenticação até o momento de logoff do sistema.

Se um usuário tiver acesso limitado à JITA, um minuto antes que o período termine, o sistema perguntará ao usuário se deseja estender o período de acesso. Assim que o usuário fizer o logoff do sistema, ou que outro usuário faça o login, o período da JITA é encerrado. 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
- Unidades de disco removíveis

Criação de uma política JITA para um usuário ou grupo

Os Administradores podem permitir acesso a dispositivos para usuários ou para grupos utilizando a autenticação Just in Time (JITA).

1. Abra o **Device Access Manager** e, em seguida, clique ou toque em **Modificar**.
2. Selecione o grupo ou o usuário e, em **Acesso** a **Unidades de disco removível** ou a **Unidades de DVD/CD-ROM**, clique ou toque na seta para baixo e selecione **Permitir – Necessário ter JITA**.
3. Em **Duração**, clique ou toque na seta para baixo para selecionar um período de tempo para o acesso à JITA.

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

Desativação de política 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. Abra o **Device Access Manager** e, em seguida, clique ou toque em **Modificar**.
2. Selecione o grupo ou o usuário e, em **Acesso** a **Unidades de disco removível** ou a **Unidade de DVD/CD-ROM**, clique ou toque na seta para baixo e selecione **Negar**.

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

Configurações

A visualização das **Configurações** permite que os administradores visualizem e modifiquem as unidades cujo acesso é controlado pelo Device Access Manager.

NOTA: É preciso que o Device Access Manager esteja ativado quando a lista de letras de unidades for configurada (consultar Visualização do sistema na página 44).

Classes de dispositivos não gerenciadas

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

- Dispositivos de entrada/saída
  - CD-ROM
  - Unidade de disco
  - Controlador de disquete (FDC)
  - Controlador de disco rígido (HDC)
  - Classe de dispositivos de interface humana (HID)
  - Dispositivos infravermelhos de interface humana
  - Mouse
  - Multiporta serial
  - Teclado
  - Impressoras Plug and play (PnP)

- Impressora
- Upgrade de Impressora

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

8 HP Trust Circles

O HP Trust Circles é um aplicativo de segurança para arquivos e documentos que combina criptografia de arquivos de pastas com uma conveniente capacidade de compartilhamento de documentos dentro de um círculo de confiança. O aplicativo criptografa os arquivos localizados em pastas especificadas pelo usuário, protegendo-os dentro de um círculo de confiança. Uma vez protegidos, os arquivos podem ser usados e compartilhados somente por membros de um círculo de confiança Se um arquivo protegido é recebido por um não-membro, o arquivo permanece criptografado, e o não-membro não tem acesso ao conteúdo.

Abertura do Trust Circles

1. Na Tela Iniciar, clique ou toque no aplicativo **HP Client Security**.

   – ou –

   Na área de trabalho do Windows, clique duas vezes no ícone do **HP Client Security** na área de notificações, na extremidade direita na barra de tarefas.

2. Em **Dados**, clique ou toque em **Trust Circles**.

Passos iniciais

Há dois modos de enviar convites via email e de respondê-los:

- **Usando o Microsoft® Outlook**—O uso do Trust Circles com o Microsoft Outlook automatiza o processo de convite do Trust Circle e de resposta de outros usuários.
- **Usando Gmail, Yahoo, Outlook.com ou outros serviços de email (SMTP)**—Quando você digita o seu nome, endereço de email e senha, o Trust Circles usa o seu serviço de email para enviar convites via email para que membros selecionados entrem no seu círculo de confiança.

Para definir seu perfil básico:

1. Digite o seu nome e endereço de email e, em seguida, clique ou toque em **Avançar**.

   O nome é visível para todos os membros que são convidados para entrar no seu círculo de confiança. O endereço de email é usado para enviar, receber ou responder convites.

2. Digite a senha da conta de email e clique ou toque em **Avançar**.

   Um email-teste será enviado para assegurar que as configurações de email estão corretas.

   NOTA: O computador deve estar conectado a uma rede.

3. No campo **Nome do Círculo de Confiança**, digite um nome para o círculo de confiança e, em seguida, clique ou toque em **Avançar**.

4. Adicione os membros e as pastas e, então, clique ou toque em **Avançar**. O círculo de confiança é criado com todas as pastas selecionadas, e envia convites via email para todos os membros selecionados. Se, por alguma razão, um convite não puder ser enviado, será exibida uma notificação. Os membros podem ser convidados novamente em qualquer momento por meio do visualizador do Trust Circles, clicando em **Seus Círculos de Confiança** e, em seguida, clicando

duas vezes ou tocando duas vezes no círculo de confiança. Para obter mais informações, consulte Trust Circles na página 49.

Trust Circles

Você pode criar um círculo de confiança durante a configuração inicial depois de digitar o seu endereço de email, ou no visualizador do Trust Circle:

▲ No visualizador do Trust Circle, clique ou toque em **Criar Círculo de Confiança** e, em seguida, digite um nome para o círculo de confiança.

- Para adicionar membros ao círculo de confiança, clique ou toque no ícone **M+** ao lado dos **Membros** e, em seguida, siga as instruções na tela.
- Para adicionar pastas ao círculo de confiança, clique ou toque no ícone **+** ao lado das **Pastas** e, em seguida, siga as instruções na tela.

Adição de pastas ao círculo de confiança

Adição de pastas a um novo círculo de confiança:

- Durante a criação de um círculo de confiança, é possível adicionar pastas clicando ou tocando no ícone **+** ao lado das **Pastas**; em seguida, siga as instruções na tela.

  – ou –

- No Windows Explorer, clique com o botão direito do mouse ou toque e segure uma pasta que não ainda seja parte de um círculo de confiança. Selecione **Trust Circle** e, em seguida, selecione **Criar Círculo de Confiança a partir de Pasta**.

DICA: É possível selecionar uma ou mais pastas.

Adição de pastas a um círculo de confiança já existente:

- No visualizador do Trust Circle, clique em **Seus Círculos de Confiança**. Em seguida, clique duas vezes ou toque duas vezes no círculo de confiança já existente para exibir as pastas atuais. Clique ou toque no ícone **+** ao lado das **Pastas** e siga as instruções na tela.

  – ou –

- No Windows Explorer, clique com o botão direito do mouse ou toque e segure uma pasta que ainda não seja parte de um círculo de confiança. Selecione **Trust Circle** e, em seguida, selecione **Adicionar a um Círculo de Confiança existente a partir da Pasta**.

DICA: É possível selecionar uma ou mais pastas.

Uma vez que uma pasta tenha sido adicionada a um círculo de confiança, o Trust Circles automaticamente criptografa a pasta e seus conteúdos. Uma vez que todos os arquivos forem criptografados, será exibida uma notificação. Além disso, é exibido um símbolo de um cadeado verde nos ícones de todas as pastas e arquivos criptografados, indicando que eles estão totalmente protegidos.

Adição de membros a um círculo de confiança

São necessárias três etapas para adicionar membros a um círculo de confiança:

1. **Convidar**—Primeiro, o proprietário do círculo de confiança convida o(s) membro(s). O Convite via email pode ser enviado a vários usuários ou grupos/listas de distribuição.
2. **Aceitar**—O convidado recebe o convite e decide se o aceita ou rejeita. Se o convidado aceitar o convite, uma resposta via email é enviada para o usuário que fez o convite. Se o convite foi enviado para um grupo, cada membro recebe um convite e decide se o aceita ou rejeita.
3. **Registrar**—O usuário que fez o convite tem uma oportunidade final para decidir se quer ou não adicionar o membro ao círculo de confiança. Se o usuário que fez o convite decide registrar o membro, é enviado um email para o convidado acusando o recebimento da resposta. O usuário que fez o convite e o convidado têm a opção de verificar a segurança do processo de Convite. Um código de verificação é exibido para o convidado, que deve lê-lo por telefone para o usuário que fez o convite. Uma vez verificado o código, o usuário que fez o convite pode enviar um email de registro final.

Adição de membros a um novo círculo de confiança:

▲ Durante a criação de um círculo de confiança, é possível adicionar membros clicando ou tocando no ícone **M+** ao lado dos **Membros**; em seguida, siga as instruções na tela.

- Se você está usando Outlook, selecione os contatos do catálogo de endereços do Outlook e, em seguida, clique em **OK**
- Se está usando outro serviço de email, adicione manualmente novos endereços ao Trust Circle, ou recupere-os do endereço de email registrado no Trust Circle.

Adição de membros a um círculo de confiança já existente:

▲ No visualizador do Trust Circle, clique em **Seus Círculos de Confiança**, clique duas vezes ou toque duas vezes no círculo de confiança já existente para exibir os membros atuais, clique ou toque no ícone **M+** ao lado dos **Membros** e siga as instruções na tela.

- Se você está usando Outlook, selecione os contatos do catálogo de endereços do Outlook e, em seguida, clique em **OK**
- Se está usando outro serviço de email, adicione manualmente novos endereços ao Trust Circle, ou recupere-os do endereço de email registrado no Trust Circle.

Adição de arquivos a um círculo de confiança

É possível adicionar arquivos em um círculo de confiança das seguintes maneiras:

- Copie ou mova o arquivo para a pasta de um círculo de confiança já existente.

  – ou –

- No Windows Explorer, clique com o botão direito do mouse ou toque e segure em um arquivo que não esteja atualmente criptografado, selecione **Trust Circle**, e, em seguida, selecione **Criptografar**. Será solicitado que você selecione o círculo de confiança ao qual o arquivo deve ser adicionado.

DICA: É possível selecionar um ou mais arquivos.

Pastas criptografadas

Qualquer membro de um círculo de confiança pode visualizar e editar arquivos que pertençam a este círculo de confiança.

NOTA: O Gerenciador/Leitor do Trust Circle não sincroniza os arquivos entre os membros.

Os arquivos devem ser compartilhados por um método já existente, como provedores de emails, ftp ou armazenamento em nuvem. Os arquivos copiados, movidos ou criados em uma pasta de um círculo de confiança são imediatamente protegidos.

Remoção de pastas do círculo de confiança

A remoção de uma pasta de um círculo de confiança decodifica a pasta e todos os seus conteúdos e remove a sua proteção.

- No visualizador do Trust Circle, clique ou toque em **Seus Círculos de Confiança**, clique duas vezes ou toque duas vezes no círculo de confiança já existente para exibir as pastas atuais e, em seguida, clique ou toque no ícone da **lixeira** ao lado da pasta.

  – ou –

- No Windows Explorer, clique com o botão direito do mouse ou toque e segure uma pasta que já seja parte de um círculo de confiança, selecione **Trust Circle** e, em seguida, selecione **Remover do Círculo de Confiança**.

DICA: É possível selecionar uma ou mais pastas.

Remoção de arquivo do círculo de confiança

Para remover um arquivo de um círculo de confiança, no Windows Explorer, clique com o botão direito do mouse ou toque e segure um arquivo que ainda não esteja criptografado, selecione **Trust Circle**, selecione **Decodificar Arquivo**.

Remoção de membros do círculo de confiança

Um membro que foi completamente registrado não pode ser removido de um círculo de confiança. Uma alternativa seria criar um novo círculo de confiança com todos os outros membros, mover todos os arquivos e pastas ao novo círculo de confiança e excluir o antigo círculo de confiança. Esta ação assegura que nenhum arquivo novo recebido pelos membros será acessível. Contudo, qualquer coisa que já tenha sido compartilhada anteriormente continuará acessível ao membro do antigo círculo de confiança.

Se um membro não foi completamente registrado (seja porque o membro foi convidado há pouco para entrar no círculo de confiança, seja porque não tenha aceitado o convite), é possível removê-lo do círculo de confiança das seguintes maneiras:

- No visualizador do Trust Circle, clique ou toque em **Seus Círculos de Confiança** e, em seguida, clique duas vezes ou toque duas vezes no círculo de confiança para mostrar a lista de membros atuais. Clique ou toque no ícone da **lixeira** ao lado do nome do membro a ser removido.
- No visualizador do Trust Circle, clique ou toque em **Membros** e clique duas vezes ou toque duas vezes no membro, para mostrar os círculos de confiança de que ele faz parte. Clique ou toque no ícone da **lixeira** ao lado de um círculo de confiança para remover o membro desse círculo de confiança.

Exclusão de um círculo de confiança

Para excluir um círculo de confiança, é preciso ser seu proprietário.

▲ No visualizador do Trust Circle, clique ou toque em **Seus Círculos de Confiança**, clique ou toque no ícone da **lixeira** ao lado do círculo de confiança a ser excluído.

Essa ação remove o círculo de confiança da página e envia emails a todos os seus membros, informando que o círculo de confiança foi excluído. Todos os arquivos e pastas que estavam inclusos nesse círculo de confiança serão decodificados.

Preferências de Configuração

No visualizador do Trust Circle, clique ou toque em **Preferências**. Serão exibidas três guias

- **Configurações de email**

Opção	Descrição
Nome de usuário	Será exibido o nome de usuário atualmente em uso. Para modificá-lo, digite um novo nome de usuário na caixa de texto. As modificações são salvas automaticamente.
Endereço de email	Será exibida a conta de email atualmente em uso. Para modificá-la, clique ou toque em **Mudar Configurações de Email** e siga as instruções na tela.
Confirmação de Novo Membro	Selecione uma das seguintes opções: ◦ **Confirmar Automaticamente**—Após o recebimento da aceitação do(s) convidado(s), ele(s) é(são) confirmado(s) no círculo de confiança sem nenhuma entrada manual, e um email de confirmação é enviado ao(s) convidado(s). ◦ **Confirmar Manualmente**—Após o recebimento da aceitação do(s) convidado(s), é necessária entrada manual para registrá-lo(s) no círculo de confiança, e então um email de confirmação é enviado ao(s) convidado(s). ◦ **Pedir Verificação**—Após o recebimento da aceitação do(s) convidado(s), um código de verificação é pedido para registrar completamente o(s) convidado(s). O proprietário do círculo de confiança deve contatar o(s) convidado(s) e checar com ele(s) o código de verificação. Após digitar o código correto, o email de confirmação é enviado.
Autenticação periódica	A autenticação periódica exige que o usuário digite a senha do Windows após um tempo limite especificado (gravado em minutos), e também na execução de operações confidenciais. Esta configuração permite aos usuários a autenticação para ligar e desligar.
Tempo limite para autenticação	Seleciona o período de tempo limite especificado (gravado em minutos) antes que a autenticação seja exigida.
Não mostrar mensagem de confirmação	Marque a caixa de seleção para desativar a exibição das mensagens de confirmação, ou desmarque a caixa de seleção para exibir as mensagens de confirmação.
Desejo ajudar a melhorar o HP Trust Circle por meio de rastreamento de uso anônimo	Selecione a caixa de seleção para participar do programa, ou desmarque a caixa de seleção se não quiser participar.

- **Backup/Restauração**

Opção	Descrição
Backup	Copia os dados do seu aplicativo de Gerenciador/Leitor do Trust Circle (configurações e círculos de confiança) em um arquivo de backup. No caso de quebra ou falha do sistema, você poderá usar este arquivo para restaurar a sua nova instalação do Trust Circles no estado em que o arquivo foi salvo pela última vez. **NOTA:** Somente os dados do aplicativo do Trust Circle são salvos (círculos de segurança, configurações e membros). Não são feitos backups dos arquivos que se encontram nas pastas dos círculos de confiança no momento. O back up desses arquivos deve ser feito separadamente. Para fazer backup das configurações e dos dados de usuário do Trust Circle: **1.** Clique ou toque em **Backup**. **2.** Escolha um nome de arquivo e um diretório para o arquivo de backup e clique ou toque em **Salvar**. **3.** Digite uma senha, confirme-a e clique ou toque em **OK**. Esta senha será pedida para restaurar este arquivo.
Restauração	Restaura as configurações e os círculos de confiança a partir de um arquivo de backup, em geral após uma falha do sistema ou migração para outro computador. Para restaurar as configurações e dados de usuário do Gerenciador do Trust Circle: **1.** Clique ou toque em **Restaurar**. **2.** Navegue até o diretório e nome de arquivo do arquivo de backup e clique ou toque em **Abrir**. **3.** Digite a senha que foi configurada quando o backup foi feito.

- **Sobre**—A versão do software do Gerenciador/Leitor do Trust Circle é exibida. São exibidos links para permitir que você atualize o Gerenciador do Trust Circle para a versão Profissional, ou para exibir a declaração de privacidade da HP.

9 Recuperação em caso de roubo (somente em determinados modelos)

O Computrace (comprado separadamente) permite a você monitorar, gerenciar e rastrear seu computador remotamente.

Uma vez ativado, o Computrace é configurado na Central de Atendimento ao Cliente do Absolute Software. Na Central de Atendimento ao Cliente, o administrador pode configurar o Computrace para monitorar ou gerenciar o computador. Se o sistema for perdido ou roubado, a Central de Atendimento ao Cliente pode ajudar autoridades locais a localizar e recuperar o computador. Se configurado, o Computrace pode continuar a funcionar até mesmo se a unidade de disco rígido for apagada ou substituída.

Para ativar o Computrace:

1. Conecte-se à Internet.
2. Abra o HP Client Security. Para obter mais informações, consulte Abertura do HP Client Security na página 9.
3. 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.

10 Exceções da senha localizada

No nível de Autenticação na inicialização e no nível do HP Drive Encryption, o suporte à localização de senha é limitado. Para obter mais informações, consulte IMEs do Windows não suportados no nível de Autenticação na inicialização ou no nível do Drive Encryption na página 55.

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. Abra o HP Client Security e digite a senha do Windows.

- 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 os caracteres suportados. Para obter mais informações sobre caracteres não compatíveis, consulte Manuseio especial de teclas na página 56.
  2. Abra o HP Client Security e digite a senha do Windows.

IMEs do Windows não suportados no nível de Autenticação na inicialização ou no nível do 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 da Autenticação na inicialização ou no nível do Drive Encryption. Uma senha do Windows não pode ser digitada com um IME na tela de login da Autenticação na Inicialização ou do HP Drive Encryption, e a inserção de uma senha desse modo pode causar o 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 terceiros 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 Client Security poderá suportar a configuração.

AVISO! Quando o HP Client Security é implementado, as senhas inseridas com um IME do Windows são 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 a página de Usuários do HP Client Security (acessada a partir do ícone de **Engrenagem** na Página Inicial) para remover o usuário do HP Client Security, selecionando o layout de teclado desejado no sistema operacional, e, em seguida, executando o Assistente de Configuração do HP Client Security 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 quando a tecla shift é pressionada para letra minúscula e a tecla shift e a tecla caps lock para letra maiúscula caso de autenticação de Inicialização e no HP Drive Encryption. As senhas numéricas devem ser inseridas usando o teclado numérico.

- Coreano

  Quando o 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 direita é pressionada para letra minúscula e a tecla alt à direita e a tecla caps lock para letra maiúscula na autenticação de Inicialização e no HP Drive Encryption.

- Os caracteres não suportados estão listados na seguinte tabela:

Language (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 autenticação de Inicialização.	ç, è, à e é com caps lock são ç, è, à e é no HP Drive Encryption.

Language (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. ◦ As teclas å, ® e Þ na segunda fileira são rejeitadas. ◦ As teclas á, ð e ø na terceira fileira são rejeitadas. ◦ A tecla æ na fileira inferior é rejeitada.	n/d	n/d
Tcheco	◦ A tecla ğ é rejeitada. ◦ A tecla į é rejeitada. ◦ A tecla ų é rejeitada. ◦ As teclas ė, ı e ż são rejeitadas. ◦ As teclas ģ, ķ, ļ, ņ e 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 virtual. ◦ A tecla inativa ţ gera dois caracteres.	n/d
Húngaro	A tecla ż é rejeitada.	A tecla inativa ţ gera dois caracteres.	n/d
Esloveno	A tecla żŽ é rejeitada no Windows, e a tecla alt gera uma tecla inativa 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 que qualquer recurso do Drive Encryption possa ser acessado. Os administradores podem ativar o Drive Encryption com o Assistente de Configuração do HP Client Security ou com o HP Client Security. O processo de ativação consiste em ativar o software, criptografar a unidade e criar a chave de criptografia de backup inicial 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 que verifica se você é a pessoa que diz ser por meio do uso de credenciais, incluindo sua senha do Windows, impressão digital, smart card, um cartão sem contatos ou um cartão de proximidade.

Autenticação Just In Time.
Consulte a Ajuda do software HP Device Access Manager

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.

autenticação na pré-inicialização do Drive Encryption
É a tela de login exibida antes de o Windows ser iniciado. Os usuários devem inserir seu nome de usuário e senha do Windows ou o PIN do smart card, ou fornecer sua impressão digital registrada. Se o login único for selecionado, a inserção da informação correta na tela de login do Drive Encryption permitirá o acesso direto ao Windows, sem que seja necessário efetuar login novamente na tela de login do Windows.

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.

Bluetooth
Tecnologia que usa transmissões de rádio para permitir que computadores, impressoras, mouses, telefones celulares ou outros dispositivos com Bluetooth se comuniquem sem fio a uma curta distância.

cartão de proximidade
Um cartão de plástico que contém um chip de computador que pode ser usado para autenticação em conjunto com outras credenciais para segurança adicional.

cartão sem contatos
Um cartão de plástico que contém um chip de computador que pode ser usado para autenticação.

chip de segurança integrado Trusted Platform Module (TPM)

Um TPM autentica um computador, em vez de um usuário, armazenando informações específicas no sistema host, como chaves de criptografia, certificados digitais e senhas. Um TMP minimiza o risco de que informações do computador sejam comprometidas por roubo ou ataque por um hacker externo.

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.

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
Um usuário autorizado a fazer login em uma rede ou computador específico.

credencial
Uma informação ou dispositivo de hardware específico usado para autenticar um usuário individual.

criptografia por hardware
O uso de unidades de criptografia automática que atendem à especificação OPAL do Trusted Computing Group para gerenciamento desse tipo de unidade a fim de realizar criptografias instantâneas. A criptografia por hardware é instantânea e pode levar somente alguns minutos, mas a criptografia por software pode levar várias horas.

criptografia por software
O uso de software para criptografar o disco rígido setor por setor. Esse processo é mais lento que a criptografia por hardware

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

dispositivo conectado
Um dispositivo de hardware que está conectado a uma porta do computador.

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.

fragmentação automática
Fragmentação programada no File Sanitizer.

fragmentação manual
Fragmentação imediata de um ativo ou de ativos selecionados, que ignora uma fragmentação programada.

fragmentar

A execução de um algoritmo que substitui os dados contidos em um ativo por dados insignificantes.

Gerenciador/Leitor do Trust Circle
O Leitor do Trust Circle só pode aceitar convites enviados por usuários do Gerenciador do Trust Circle. No entanto, o Gerenciador do Trust Circle permite a criação de círculos de confiança. Os recursos incluem o convite para uma pessoa via email para participação em um círculo de confiança e a aceitação de convites para círculos de confiança de outros usuários. Uma vez que um círculo de confiança é estabelecido entre pessoas de confiança, os arquivos protegidos por esse círculo de segurança podem ser compartilhados em segurança.

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 Client Security, um grupo de credenciais e configurações que são tratadas como uma conta ou perfil de um determinado usuário.

impressão digital
Uma cópia digital da imagem da sua impressão digital. A imagem real da sua impressão digital jamais é armazenada pelo HP Client Security.

login
Um objeto dentro do HP Client Security que consiste em um nome de usuário e uma senha (e, possivelmente, outras informações selecionadas) 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.

Página Inicial
Um local central onde é possível acessar e gerenciar os recursos e configurações no HP Client Security.

Pasta do Trust Circle
Qualquer pasta protegida por um círculo de confiança.

PIN
Um número de identificação pessoal de um usuário registrado a ser usado para autenticação.

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.

purificação de espaço livre
A gravação de dados aleatórios sobre ativos excluídos e espaço não utilizado. Esse processo reduz a existência do ativo excluído, tornando o ativo original mais difícil de recuperar.

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.

Single Sign On (login único)
Um recurso que armazena informações de autenticação e permite o uso do HP Client Security para acessar aplicativos da Internet e do Windows que requeiram autenticação por senha.

smart card
Dispositivo de hardware que pode ser usado com um PIN para autenticação.

tela de login do Drive Encryption
Consulte autenticação na pré-inicialização do Drive Encryption.

Trust Circle
Oferece contenção de dados vinculando-os a um grupo definido de usuários de confiança. Previne que os dados caiam em mãos erradas, acidental ou intencionalmente. Com a segurança da tecnologia CryptoMill's Zero Overhead Key Management, os dados são vinculados criptograficamente a um círculo de pessoas de confiança. Isso previne a decodificação dos documentos ou de outras informações confidenciais fora do círculo de confiança

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