HP Client Security

Informação Básica

Primeira edição: agosto de 2013

Número de publicação do documento: 735339-131

Índice

1 Introdução ao HP Client Security Manager

O HP Client Security permite-lhe proteger os seus dados, dispositivo e identidade, aumentando assim a segurança do seu computador.

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

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

NOTA: As instruções neste manual estão escritas segundo o pressuposto que os módulos de software do HP Client Security já estão instalados.

Funcionalidades do HP Client Security

A tabela seguinte descreve as funcionalidades essenciais dos módulos do HP Client Security.

Módulo	Funcionalidades essenciais
HP Client Security Manager	Os administradores podem executar as seguintes funções: • Proteger o seu computador antes de o Windows® iniciar • Proteger a sua conta do Windows utilizando uma autenticação segura • Gerir o seu início de sessão e palavras-passes para websites e aplicações • Alterar facilmente a palavra-passe do seu sistema operativo Windows • Utilizar impressões digitais para segurança e comodidade extras • Configurar um smart card, cartão sem contacto ou cartão de proximidade para autenticação • Utilizar o seu telefone Bluetooth como método de identificação • Definir um PIN para expandir as suas opções de autenticação • Configurar políticas de início de sessão e de sessão • Criar cópias de segurança e restaurar os dados do programa • Adicionar mais aplicações, tais como HP Drive Encryption, HP File Sanitizer, HP Trust Circles, HP Device Access Manager e HP Computrace Os utilizadores gerais podem executar as seguintes funções: • Ver as definições do Estado de encriptação e Device Access Manager. • Ativar o Computrace. • Configurar as Preferências e as opções de Cópia de Segurança e Restauro.
Password Manager	Os utilizadores gerais podem executar as seguintes funções: • Organizar e configurar nomes de utilizador e palavras-passe. • Criar palavras-passe mais seguras para melhorar a segurança das contas de correio eletrónico e contas da Web. O Password Manager preenche e submete automaticamente as informações. • Otimizar o processo de início de sessão com a funcionalidade Início de Sessão Único, que memoriza automaticamente e aplica as credenciais de utilizador. • Marcar uma conta como comprometida, para que possa ser alertado para outra(s) conta(s) com credenciais semelhantes. • Importar dados de início de sessão de um navegador compatível.
HP Drive Encryption (apenas alguns modelos)	• Fornece a encriptação completa e ao nível do volume para a unidade de disco rígido. • Força a autenticação antes de arranque para desencriptar e aceder aos dados. • Oferece a opção de ativar unidades de autoencriptação (apenas alguns modelos).

Módulo	Funcionalidades essenciais
HP Device Access Manager	• Permite aos gestores de TI controlarem o acesso a dispositivos com base em perfis de utilizador. • Impede que utilizadores não autorizados retirem dados utilizando suportes de armazenamento externos e introduzam vírus no sistema partir de suportes de dados externos. • Permite aos administradores desativarem o acesso a dispositivos de comunicação de indivíduos específicos ou grupos de utilizadores.
HP Trust Circles	• Protege ficheiros e documentos. • Encripta ficheiros em pastas especificadas pelo utilizador e protege-os dentro de um círculo de confiança. • Permite que os ficheiros sejam utilizados e partilhados apenas por membros do círculo de confiança.
Recuperação de Roubo (Computrace, adquirido em separado)	• Requer a compra separada de subscrições de controlo e rastreio para ser ativado. • Fornece o rastreio de ativos protegidos. • Monitoriza a atividade de utilizadores, assim como alterações no hardware e software. • Permanece ativo mesmo se a unidade de disco rígido for reformatada ou substituída.

Descrição do produto HP Client Security e exemplos de utilização comum

A maioria dos produtos HP Client Security possui autenticação de utilizador (normalmente uma palavra-passe) e uma cópia de segurança administrativa para obter o acesso se as palavras-passe forem perdidas, esquecidas ou não estiverem disponíveis ou sempre que a segurança empresarial necessitar do acesso.

NOTA: Alguns dos produtos HP Client Security estão concebidos para restringir o acesso a dados. Os dados devem ser encriptados quando são tão importantes que o utilizador prefira perder as informações a vê-las comprometidas. Recomenda-se que seja criada uma cópia de segurança de todos os dados num local seguro.

Password Manager

O Password Manager armazena nomes de utilizador e palavras-passe e pode ser utilizado para:

- Guardar nomes de início de sessão e palavras-passe para o acesso à Internet ou ao correio eletrónico.
- Iniciar automaticamente a sessão do utilizador num web site ou correio eletrónico.
- Gerir e organizar autenticações.
- Selecionar um ativo da Web ou rede e aceder diretamente à hiperligação.
- Ver nomes e palavras-passe sempre que necessário.

- Marcar uma conta como comprometida, para que possa ser alertado para outra(s) conta(s) com credenciais semelhantes.
- Importar dados de início de sessão de um navegador compatível.

Exemplo 1: Uma agente de aquisições de um grande fabricante faz a maior parte das suas transações empresariais através da Internet. Também visita frequentemente vários web sites populares que necessitam de informações de inicio de sessão. Ela conhece as questões de segurança, por isso não utiliza a mesma palavra-passe em todas as contas. A agente de aquisições decidiu utilizar o Password Manager para fazer a correspondência entre as várias hiperligações da Web e os vários nomes de utilizador e palavras-passe. Quando ela inicia sessão num web site, o Password Manager apresenta automaticamente as credenciais. Se ela quiser ver os nomes de utilizador e as palavras-passe, o Password manager pode ser configurado para as apresentar.

O Password Manager também pode ser utilizado para gerir e organizar as autenticações. Esta ferramenta vai permitir ao utilizador selecionar um ativo da Web ou rede e aceder diretamente à hiperligação. O utilizador também pode visualizar os nomes de utilizador e as palavras-passe sempre que necessário.

Exemplo 2: Um funcionário empenhado foi promovido e agora vai gerir todo o departamento de contabilidade. A equipa tem de iniciar sessão em várias contas de cliente na Web, cada uma utilizando diferentes informações de início de sessão. As informações de início de sessão têm de ser partilhadas com outros funcionários, por isso a confidencialidade é essencial. O funcionário decide organizar todas as hiperligações da Web, ou nomes de utilizador da empresa e as palavras-passe no Password Manager. No final o funcionário implementa o Password Manager junto dos funcionários para que estes possam trabalhar em contas Web e sem terem de saber as credenciais de início de sessão que estão a utilizar.

HP Drive Encryption (apenas alguns modelos)

O HP Drive Encryption é utlizado para restringir o acesso aos dados em toda a unidade de disco rígido ou numa unidade secundária. O Drive Encryption também pode gerir unidades de autoencriptação.

Exemplo 1: Um médico quer certificar-se de que apenas ele pode aceder aos dados na unidade de disco rígido do seu computador. O médico ativa o Drive Encryption, que requer a autenticação antes de arranque antes do início de sessão no Windows. Depois de configurado, não é possível aceder à unidade de disco rígido sem uma palavra-passe antes que o sistema operativo inicie. O médico pode otimizar ainda mais a segurança da unidade se escolher encriptar os dados com a opção de unidade de autoencriptação.

Exemplo 2: Um administrador hospitalar pretende garantir que apenas os médicos e pessoal autorizado podem aceder aos dados no computador local, sem terem de partilhar palavras-passe pessoais. O departamento de TI adiciona o administrador, os médicos e o pessoal autorizado como utilizadores do Drive Encryption. Agora, apenas o pessoal autorizado pode arrancar o computador ou domínio utilizando o respetivo nome de utilizador e palavra-passe.

HP Device Access Manager (apenas alguns modelos)

O HP Device Access Manager permite a um administrador restringir e gerir o acesso a hardware. O Device Access Manager pode ser utilizado para bloquear o acesso não autorizado a unidades flash USB onde os dados possam ser copiados. Também pode restringir o acesso a unidades de CD/DVD, controlar dispositivos USB, ligações de rede, etc. Um exemplo poderia ser uma situação na qual os vendedores externos precisem de acesso aos computadores da empresa mas quer não possam copiar os dados para uma unidade USB.

Exemplo 1: Um gestor de uma empresa de fornecimento médico trabalha frequentemente com registos médicos pessoais, assim como informações comerciais. Os funcionários precisam de

acesso a estes dados, mas é extremamente importante que os dados não sejam removidos do computador através de uma unidade USB ou de qualquer outro suporte de armazenamento externo. A rede é segura, mas oc computadores possuem gravadores de CD e portas USB que podem permitir que os dados sejam copiados ou roubados. O gestor utiliza o Device Access Manager para desativar as portas USB e os gravadores de CD para que não possam ser utilizados. Apesar de as portas USB estarem desbloqueadas, o rato e o teclado continuarão a funcionar.

Exemplo 2: Uma empresa de seguros não quer que os seus funcionários instalem ou transfiram software ou dados pessoais de casa. Alguns funcionários precisam de acesso às portas USB de todos os computadores. O gestor de TI utiliza o Device Access Manager para permitir o acesso a alguns funcionários e a bloquear o acesso externo a outros.

Computrace (adquirido em separado)

O Computrace (adquirido em separado) é um serviço que pode rastrear a localização de um computador roubado sempre que o utilizador acede à Internet. O Computrace também pode ajudar a gerir e localizar computadores à distância, assim como monitorizar a utilização e as aplicações do computador.

Exemplo 1: O diretor de uma escola pediu ao departamento de TI que monitorize todos os computadores da escola. Depois de fazer o inventário dos computadores, o administrador de TI registou todos os computadores no Computrace para que estes possam ser rastreados no caso de alguma vez serem roubados. Recentemente, a escola descobriu que vários computadores tinha desaparecido, por isso o administrador de TI alertou as autoridades e os representantes do Computrace. Os computadores foram localizados e devolvidos à escola pelas autoridades.

Exemplo 2: Uma agência imobiliária precisa de gerir e atualizar todos os computadores por todo o mundo. Eles utilizam o Computrace para monitorizar e atualizar os computadores sem terem de enviar um técnico de TI pessoalmente a cada computador.

Alcançar objetivos essenciais de segurança

Os módulos do HP Client Security podem trabalhar em conjunto para fornecer uma solução para diversas questões de segurança, incluindo objetivos essenciais de segurança:

- Proteger contra roubo direcionado
- Restringir o acesso a dados sensíveis
- Prevenir o acesso não autorizado a partir de localizações internas ou externas
- Criar políticas de palavras-passe seguras

Proteger contra roubo direcionado

Um exemplo de roubo direcionado seria o roubo de um computador com dados confidenciais e informações de cliente no ponto de verificação de segurança de um aeroporto. As seguintes funcionalidades ajudam a proteger contra o roubo direcionado:

- A funcionalidade de autenticação antes de arranque, se ativada, ajuda a impedir o acesso ao sistema operativo.
  - HP Client Security—Ver HP Client Security na página 13.
  - HP Drive Encryption—Ver HP Drive Encryption (apenas alguns modelos) na página 31.
- A encriptação ajuda a garantir que não possível aceder aos dados mesmo se a unidade de disco rígido for removida instalada num sistema não seguro.
- O Computrace pode rastrear a localização do computador após o roubo.
  - Computrace—Ver Recuperação de roubo (apenas alguns modelos) na página 55.

Restringir o acesso a dados sensíveis

Imagine que um auditor contratado está a trabalhar no local e tem acesso a um computador para rever dados financeiros sensíveis. O auditor não deve poder imprimir os ficheiros ou guardá-lo num dispositivo gravável, como um CD. A seguinte funcionalidade ajuda a restringir o acesso aos dados:

- O HP Device Access Manager permite aos gestores de TI restringirem o acesso a dispositivos de comunicação de forma que não seja possível copiar informações sensíveis da unidade de disco rígido. Consulte Vista Sistema na página 45.

Prevenir o acesso não autorizado a partir de localizações internas ou externas

O acesso não autorizado a um computador empresarial não seguro implica um risco muito elevado para os recursos de rede empresarial, tais como informações dos serviços financeiros, um executivo, ou a equipa de Investigação e Desenvolvimento, e para informações privadas, tais como registos hospitalares e registos financeiros pessoais. As seguintes funcionalidades ajudam a prevenir o acesso não autorizado:

- A funcionalidade de autenticação antes de arranque, se ativada, ajuda a impedir o acesso ao sistema operativo. Consulte HP Drive Encryption (apenas alguns modelos) na página 31.
- O HP Client Security ajuda a garantir que um utilizador não autorizado não consegue obter palavras-passe ou aceder a aplicações protegidas por palavra-passe. Consulte HP Client Security na página 13.
- O HP Device Access Manager permite aos gestores de TI restringirem o acesso a dispositivos graváveis de forma que não seja possível copiar informações sensíveis da unidade de disco rígido. Consulte HP Device Access Manager (apenas alguns modelos) na página 44.

Criar políticas de palavras-passe seguras

Se for implementada uma política empresarial que requeira a utilização de uma política de palavras-passe para dezenas de aplicações baseadas na Web e bases de dados, o Password Manager oferece um repositório protegido para as palavras-passe e a conveniência do Início de Sessão Único. Consulte Password Manager na página 19.

Elementos adicionais de segurança

Atribuição de funções de segurança

Na gestão da segurança informática (especialmente para organizações de grande dimensão), uma prática importante é a divisão de responsabilidades e direitos entre os diferentes tipos de administradores e utilizadores.

NOTA: Numa organização de pequena dimensão ou para uso individual, estas funções podem ser detidas pela mesma pessoa.

No HP Client Security, as funções e responsabilidades de segurança podem ser divididas da seguinte forma:

- Gestor de Segurança - define o nível de segurança da empresa ou rede e determina as funcionalidades de segurança a implementar, tais como o Drive Encryption.

  NOTA: Muitas das funcionalidades do HP Client Security podem ser personalizadas pelo gestor de segurança em colaboração com a HP. Para obter mais informações, visite http://www.hp.com.

- Administrador de TI - aplica e gere as funcionalidades de segurança definidas pelo gestor de segurança. Também ativa e desativa algumas funcionalidades. Por exemplo, se o gestor de segurança decidiu implementar smart cards, o administrador de TI pode ativar o modo palavra-passe e o modo smart card.
- Utilizador - utiliza as funcionalidades de segurança. Por exemplo, se o gestor de segurança e o administrador de TI ativaram o modo smart card para o sistema, o utilizador pode configurar o PIN do smart card e utilizá-lo para a autenticação.

CUIDADO: Recomenda-se que os administradores sigam as "melhores práticas" na restrição dos privilégios do utilizador final e na restrição do acesso dos utilizadores.

Não devem ser concedidos privilégios administrativos a utilizadores não autorizados.

Gerir as palavras-passe do HP Client Security

A maioria das funcionalidades do HP Client Security estão protegidas por palavra-passe. A tabela seguinte lista as palavras-passe utilizadas mais frequentemente, o módulo de software onde a palavra-passe está configurada e a função da palavra-passe.

As palavras-passe que são configuradas e utilizadas apenas por administradores de TI também estão indicadas nesta tabela. Todas as restantes palavras-passe podem ser configuradas por utilizadores normais ou administradores.

Palavra-passe do HP Client Security	Configurada no seguinte módulo	Função
Palavra-passe de início de sessão do Windows	Painel de Controlo do Windows ou HP Client Security	Pode ser utilizado para o início de sessão manual e para autenticação para aceder às várias funcionalidades do HP Client Security.

Palavra-passe do HP Client Security	Configurada no seguinte módulo	Função
Palavra-passe da Cópia de Segurança e Recuperação do HP Client Security	HP Client Security, por utilizador individual	Protege o acesso ao ficheiro da Cópia de Segurança e Recuperação do HP Client Security.
PIN do Smart Card	Credential Manager	Pode ser utilizado como autenticação multifator. Pode ser utilizado como autenticação do Windows. Autentica utilizadores do Drive Encryption, se o smart card estiver selecionado.

Criar uma palavra-passe segura

Ao criar palavras-passe, tem de seguir todas as especificações definidas pelo programa. No entanto, deve considerar as seguintes orientações para o ajudar a criar palavras-passe seguras e reduzir as hipóteses de a sua palavra-passe ficar comprometida:

- Utilize palavras-passe com mais de 6 carateres, de preferência mais de 8.
- Misture letras maiúsculas e minúsculas na sua palavra-passe.
- Sempre que possível, misture carateres alfanuméricos e inclua carateres especiais e marcas de pontuação.
- Substitua as letras de uma palavra-chave por carateres especiais ou números. Por exemplo, pode utilizar o número 1 para as letras I ou L.
- Combine palavras de 2 ou mais idiomas.
- Divida uma palavra ou frase com números ou carateres especiais no meio, por exemplo: “Maria2-2Gato45.”
- Não utilize uma palavra-passe que esteja no dicionário.
- Não utilize o seu nome na palavra-passe, ou outras informações pessoais, tais como a data de nascimento, nomes de animais de estimação ou nome da mãe, mesmo se os escrever ao de trás para a frente.
- Mude frequentemente as palavras-passe. Pode alterar apenas alguns carateres na palavra--passe.
- Se escrever a sua palavra-passe, não a guarde num local normalmente visível próximo do computador.
- Não guarde a palavra-passe num ficheiro, tal como numa mensagem de correio eletrónico, do computador.
- Não partilhe contas ou divulgue a sua palavra-passe.

Efetuar a cópia de segurança das credenciais e definições

Pode utilizar a ferramenta de Cópia de Segurança e Restauro do HP Client Security como localização central a partir da qual pode efetuar a cópia de segurança e o restauro das credenciais de segurança de alguns dos módulos do HP Client Security instalados.

2 Informação básica

A fim de configurar o HP Client Security para utilização com as suas credenciais, inicie o HP Client Security de uma das seguintes formas. Assim que o assistente tiver sido concluído por um utilizador, não pode ser iniciado novamente por esse utilizador.

1. No ecrã Iniciar ou Aplicações, clique ou toque na aplicação **HP Client Security** (Windows 8).

   – ou –

   No ambiente de trabalho do Windows, clique ou toque em **HP Client Security Gadget** (Windows 7).

   – ou –

   No ambiente de trabalho do Windows, clique duas vezes ou toque duas vezes no ícone **HP Client Security** na área de notificação, situada na extremidade direita da barra de tarefas.

   – ou –

   No ambiente de trabalho do Windows, clique 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 página de boas-vindas apresentada.

3. Leia o ecrã de boas-vindas, verifique a sua identidade escrevendo a sua palavra-passe do Windows e clique ou toque em **Seguinte**.

   É-lhe pedido que crie uma palavra-passe, se ainda não tiver criado uma palavra-passe do Windows. É necessária uma palavra-passe do Windows para proteger a sua conta do Windows contra o acesso por pessoas não autorizadas e para utilizar as funcionalidades do HP Client Security.

4. Na página HP SpareKey, selecione três perguntas de segurança. Introduza uma resposta para cada pergunta e em seguida clique em **Seguinte**. Também são permitidas perguntas personalizadas. Para obter mais informações, consulte HP SpareKey – Recuperação da palavra-passe na página 15.

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

6. Na página Encriptação de dados, ative a encriptação, crie a cópia de segurança da chave e em seguida clique ou toque em **Seguinte**. Para mais informações, consulte a Ajuda do software HP Drive Encryption.

NOTA: Isto aplica-se a um cenário em que o utilizador é um administrador e o assistente de configuração do HP Client Security não foi configurado previamente por um administrador.

7. Na última página do assistente, clique ou toque em **Concluir**.

   Esta página fornece o estado das funcionalidades e credenciais.

8. O assistente de configuração do HP Client Security assegura a ativação das funcionalidades Just In Time Authentication e File Sanitizer. Para mais informações, consulte a Ajuda do software HP Device Access Manager e a Ajuda do software HP File Sanitizer.

NOTA: Isto aplica-se a um cenário em que o utilizador é um administrador e o assistente de configuração do HP Client Security não foi configurado previamente por um administrador.

Abrir o HP Client Security

Pode abrir a aplicação HP Client Security através de uma das seguintes formas:

NOTA: É necessário concluir o assistente de configuração do HP Client Security antes de ser possível iniciar a aplicação HP Client Security.

- No ecrã Iniciar ou Aplicações, clique ou toque na aplicação **HP Client Security**.

  – ou –

  No ambiente de trabalho do Windows, clique ou toque em **HP Client Security Gadget** (Windows 7).

  – ou –

  No ambiente de trabalho do Windows, clique duas vezes ou toque duas vezes no ícone **HP Client Security** na área de notificação, situada na extremidade direita da barra de tarefas.

  – ou –

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

3 Guia de Configuração Rápida para Pequenas Empresas

Este capítulo destina-se a demonstrar os passos básicos para ativar as opções mais comuns e úteis do HP Client Security para Pequenas Empresas. Com as várias ferramentas e opções deste software, poderá otimizar as suas preferências e configurar o seu controlo de acesso. O essencial deste Guia de Configuração Rápida consiste em colocar cada módulo em execução, da forma mais fácil e rápida. Para obter informações adicionais, selecione o módulo que lhe interessa e de seguida clique no botão **?** ou Ajuda no canto superior direito. O botão vai apresentar automaticamente informações para o ajudar na janela atualmente aberta.

Informação básica

1. No ambiente de trabalho do Windows, abra o HP Client Security fazendo duplo clique no ícone do **HP Client Security** na área de notificação, situada na extremidade direita da barra de tarefas.
2. Introduza a sua palavra-passe do Windows ou crie uma palavra-passe do Windows.
3. Conclua a configuração do HP Client Security Manager.

Para configurar o HP Client Security para exigir autenticação apenas uma vez durante o início de sessão do Windows, consulte Funcionalidades de segurança na página 28.

Password Manager

Todos nós temos imensas palavras-passe - especialmente se acedemos regularmente a web sites ou utilizamos aplicações que exigem o início de sessão. O utilizador normal ou utiliza a mesma palavra-passe para todas as aplicações e web sites ou é criativo e esquece rapidamente a palavra-passe de cada aplicação.

O Password Manager pode memorizar automaticamente as suas palavras-passe ou dar-lhe a possibilidade de identificar que sites deve memorizar e omitir. Assim que inicia sessão no computador, o Password Manager vai fornecer-lhe as suas palavras-passe ou credenciais para as aplicações ou web sites participantes.

Quando acede a uma aplicação ou a um web site que necessite de credenciais, o Password Manager vai reconhecer automaticamente o site e perguntar-lhe se pretende que o software memorize as suas informações. Se pretender excluir determinados sites, pode recusar o pedido.

Para começar a guardar localizações na web, nomes de utilizador e palavras-passe:

1. Por exemplo, navegue para um web site ou aplicação participante e depois clique no ícone do Password Manager no canto superior esquerdo da página Web para adicionar a autenticação Web.
2. Dê um nome à hiperligação (opcional) e introduza um nome de utilizador e uma palavra-passe no Password manager.

3. Quando terminar, clique no botão **OK**.
4. O Password Manager também pode guardar o seu nome de utilizador e palavra-passe para partilhas de rede ou unidades de rede mapeadas.

Ver e gerir as autenticações guardadas no Password Manager

O Password Manager permite-lhe visualizar, gerir, fazer a cópia de segurança e iniciar as suas autenticações a partir de uma localização central. O Password Manager também suporta o início de locais guardados a partir do Windows.

Para abrir o Password Manager, utilize a combinação de teclas do teclado Ctrl+tecla do Windows+h para abrir o Password Manager e de seguida clique em **Iniciar sessão** para iniciar e autenticar o atalho guardado.

A opção **Editar** do Password Manager permite-lhe visualizar e modificar o nome, o nome de início sessão e até revelar as palavras-passe.

O HP Client Security para Pequenas Empresas permite efetuar a cópia de segurança de todas as credenciais e definições e/ou copiá-las para outro computador.

HP Device Access Manager

O Device Access Manager pode ser utilizado para restringir a utilização de vários dispositivos de armazenamento internos e externos para que os seus dados permaneçam seguros na unidade de disco rígido, nunca saindo das suas instalações. Um exemplo seria permitir a um utilizador aceder aos seus dados mas impedi-los de copiá-los para um CD, leitor de música pessoal ou dispositivo de memória USB.

1. Abra o **Device Access Manager** (consulte Abrir o Device Access Manager na página 44).

   É apresentado o acesso do utilizador atual.

2. Para alterar o acesso de utilizadores, grupos ou dispositivos, clique ou toque em **Alterar**. Para obter mais informações, consulte Vista Sistema na página 45.

HP Drive Encryption

O HP Drive Encryption é utilizado para proteger os seus dados, encriptando toda a unidade de disco rígido. Os dados na sua unidade de disco rígido permanecerão protegidos se o seu PC for roubado e/ou se a unidade de disco rígido for removida do computador original e colocada noutro computador.

Um benefício de segurança adicional é que o Drive Encryption exige que se autentique corretamente utilizando o seu nome de utilizador e palavra-passe antes de o sistema operativo iniciar. Este processo chama-se autenticação antes de arranque.

Para tornar tudo ainda mais fácil, os vários módulos de software sincronizam automaticamente as palavras-passe, incluindo as contas de utilizador do Windows, os domínios de autenticação, o HP Drive Encryption, o Password Manager e o HP Client Security.

Para configurar o HP Drive Encryption durante a configuração inicial com o assistente de Configuração do HP Client Security, consulte Informação básica na página 9.

4 HP Client Security

A página inicial do HP Client Security é a localização central para fácil acesso às funcionalidades, aplicações e definições do HP Client Security. A página inicial está dividida em três secções:

- **DADOS** – Fornece acesso a aplicações utilizadas para gerir a segurança dos dados.
- **DISPOSITIVO** – Fornece acesso a aplicações utilizadas para gerir a segurança dos dispositivos.
- **IDENTIDADE** – Fornece registo e gestão de credenciais de autenticação.

Mova o cursor sobre o mosaico de uma aplicação para visualizar uma descrição da mesma.

O HP Client Security poderá fornecer ligações para definições do utilizador e administrativas no fundo de uma página. O HP Client Security fornece acesso a definições e funcionalidades avançadas tocando ou clicando no ícone da **engrenagem** (definições).

Funcionalidades, aplicações e definições de identidade

As funcionalidades, aplicações e definições de identidade fornecidas pelo HP Client Security ajudam-no a gerir vários aspetos da sua identidade digital. Clique ou toque num dos seguintes mosaicos na página inicial do HP Client Security e em seguida introduza a sua palavra-passe do Windows:

- **Impressões digitais** – Regista e gere a sua credencial de impressão digital.
- **SpareKey** – Configura e gere a sua credencial HP SpareKey, que pode ser utilizada para iniciar sessão no seu computador se as outras credenciais foram perdidas ou colocadas fora do sítio. Permite-lhe igualmente repor a sua palavra-passe esquecida.
- **Palavra-passe do Windows** – Fornece acesso fácil para alterar a sua palavra-passe do Windows.
- **Dispositivos Bluetooth** – Permite-lhe registar e gerir os seus dispositivos Bluetooth.
- **Cartões** – Permite-lhe registar e gerir os seus smart cards, cartões sem contactos e cartões de proximidade.
- **PIN** – Permite-lhe registar e gerir a sua credencial PIN.
- **RSA SecurID** – Permite-lhe registar e gerir a sua credencial RSA SecurID (se a configuração adequada estiver implementada).
- **Gestor de palavras-passes** – Permite-lhe gerir palavras-passes para as suas contas online e aplicações.

Impressões digitais

O assistente de configuração do HP Client Security guia-o ao longo do processo de configuração, ou “registo”, das suas impressões digitais.

Pode também registar ou eliminar as suas impressões digitais na página Impressões digitais, à qual pode aceder clicando ou tocando no ícone **Impressões digitais** na página inicial do HP Client Security.

1. Na página Impressões digitais, deslize um dedo até ser registado com êxito.

   O número de dedos necessários para ser registado é indicado na página. Os dedos indicador ou do meio são preferíveis.

2. Para eliminar impressões digitais previamente registadas, clique ou toque em **Eliminar**.
3. Para registar dedos adicionais, clique ou toque em **Registar uma impressão digital adicional**.
4. Clique ou toque em **Guardar** antes de sair da página.

⚠ **CUIDADO:** Quando regista impressões digitais através do assistente, as informações das impressões digitais apenas são guardadas depois de clicar em **Seguinte**. Se deixar o computador inativo durante algum tempo, ou fechar o programa, as alterações que efetuou **não** são guardadas.

- Para aceder às Definições administrativas de impressões digitais, onde os administradores podem especificar o registo, a precisão e outras definições, clique ou toque em **Definições administrativas** (requer privilégios administrativos).
- Para aceder às Definições do utilizador de impressões digitais, onde pode especificar definições que determinam o aspeto e o comportamento do reconhecimento de impressões digitais, clique ou toque em **Definições do utilizador**.

Definições administrativas de impressões digitais

Os administradores podem especificar o registo, a precisão e outras definições para um leitor. São necessários privilégios administrativos.

- Para aceder às Definições administrativas para a credencial de impressão digital, clique ou toque em **Definições administrativas** na página Impressões digitais.

- **Registo de utilizador** – Escolha o número mínimo e máximo de impressões digitais que um utilizador tem permissão para registar.
- **Reconhecimento** – Mova o cursor de deslocamento para ajustar a sensibilidade do leitor de impressões digitais quando deslizar o dedo.

  Se a sua impressão digital não for reconhecida de forma consistente, poderá necessitar de uma definição de reconhecimento mais baixa. Uma definição mais alta aumenta a sensibilidade a variações nas passagens de impressões digitais e, por conseguinte, diminui a possibilidade de uma falsa aceitação. A definição **Média-Alta** fornece uma boa combinação de segurança e comodidade.

Definições do utilizador de impressões digitais

Na página Definições do utilizador de impressões digitais, pode especificar definições que determinam o aspeto e o comportamento do reconhecimento de impressões digitais.

▲ Para aceder às Definições do utilizador para a credencial de impressão digital, clique ou toque em **Definições do utilizador** na página Impressões digitais.

- **Ativar o retorno de som** – Por predefinição, o HP Client Security fornece-lhe um retorno de áudio quando uma impressão digital foi passada, reproduzindo diferentes sons para eventos específicos do programa. Pode atribuir novos sons a estes eventos através do separador Sons na definição Som no Painel de Controlo do Windows, ou, para desativar o retorno de som, desmarque a caixa de verificação.
- **Mostrar retorno da qualidade de leitura** – Para visualizar todas as passagens, independentemente da qualidade, marque a caixa de verificação. Para visualizar apenas passagens de boa qualidade, desmarque a caixa de verificação.

HP SpareKey – Recuperação da palavra-passe

O HP SpareKey permite-lhe aceder ao seu computador (em plataformas suportadas) respondendo a três perguntas de segurança.

O HP Client Security pede-lhe para configurar a sua HP SpareKey pessoal durante a configuração inicial no assistente de configuração do HP Client Security.

Para configurar a sua HP SpareKey:

1. na página HP SpareKey do assistente, selecione três perguntas de segurança e em seguida introduza uma resposta para cada pergunta.

   Pode selecionar uma pergunta a partir de uma lista predefinida ou escrever a sua própria pergunta.

2. Clique ou toque em **Registar**.

Para eliminar a sua HP SpareKey:

▲ Clique ou toque em **Eliminar a sua SpareKey**.

Depois de configurar a sua SpareKey, pode aceder ao seu computador utilizando a sua SpareKey a partir de um ecrã de início de sessão de autenticação na ligação ou do ecrã de boas-vindas do Windows.

Pode selecionar diferentes perguntas ou alterar as suas respostas na página SpareKey, à qual pode aceder a partir do mosaico Recuperação da palavra-passe na página inicial do HP Client Security.

Para aceder às Definições do HP SpareKey, onde um administrador pode especificar definições relacionadas com a credencial HP SpareKey, clique em **Definições** (requer privilégios administrativos).

Definições do HP SpareKey

Na página Definições da HP SpareKey, pode especificar definições que determinam o comportamento e a utilização da credencial HP SpareKey.

▲ Para iniciar a página Definições da HP SpareKey, clique ou toque em **Definições** na página HP SpareKey (requer privilégios administrativos).

Os administradores podem selecionar as seguintes definições:

- Especifique as perguntas que são apresentadas a cada utilizador durante a configuração da HP SpareKey.
- Adicione até três perguntas de segurança personalizadas para incluir na lista apresentada aos utilizadores.
- Escolha se deve permitir ou não que os utilizadores escrevam as suas próprias perguntas de segurança.
- Especificar que ambientes de autenticação (Windows ou autenticação na ligação) permitem a utilização da HP SpareKey para a recuperação da palavra-passe.

Palavra-passe do Windows

O HP Client Security torna mais simples e mais rápido alterar a sua palavra-passe do Windows do que alterá-la através do Painel de Controlo do Windows.

Selecione Criar palavra-passe do Windows.

1. Na página inicial do HP Client Security, clique ou toque em **Palavra-passe do Windows**.
2. Introduza a sua palavra-passe correta na caixa de texto **Palavra-passe atual do Windows**.
3. Escreva uma nova palavra-passe na caixa de texto **Nova palavra-passe do Windows** e em seguida escreva-a novamente na caixa de texto **Confirmar a nova palavra-passe**.
4. Clique ou toque em **Alterar** para alterar imediatamente a sua palavra-passe atual para a nova palavra-passe que introduziu.

Dispositivos Bluetooth

Se o administrador tiver ativado o Bluetooth como uma credencial de autenticação, pode definir um telefone Bluetooth em conjunto com outras credenciais para segurança adicional.

NOTA: Apenas são suportados dispositivos de telefone Bluetooth.

1. Certifique-se de que a funcionalidade Bluetooth está ativada no computador e que o telefone Bluetooth está configurado para o modo de deteção. Para ligar o telefone, poderá ser necessário escrever um código gerado automaticamente no dispositivo Bluetooth. Consoante as definições de configuração do dispositivo Bluetooth, poderá ser necessário comparar os códigos de emparelhamento entre o computador e o telefone.
2. Para registar o telefone, selecione-o e em seguida clique ou toque em **Registar**.

Para aceder à página Definições dos dispositivos Bluetooth na página 16 onde um administrador pode especificar definições para dispositivos Bluetooth, clique ou **Definições** (requer privilégios administrativos).

Definições dos dispositivos Bluetooth

Os administradores podem especificar as seguintes definições que determinam o comportamento e a utilização de credenciais de dispositivos Bluetooth:

Autenticação silenciosa

- **Utilize automaticamente o seu dispositivo Bluetooth registado ligado durante a verificação da sua identidade** – Marque a caixa de verificação para permitir que os

utilizadores utilizem a credencial Bluetooth para autenticação sem exigir qualquer ação do utilizador ou desmarque a caixa de verificação para desativar esta opção.

Proximidade do Bluetooth

- **Bloqueie o computador quando o seu dispositivo Bluetooth registado ficar fora do alcance do computador** – Marque a caixa de verificação para bloquear o computador quando um dispositivo Bluetooth que foi ligado fica fora do alcance, ou marque a caixa de verificação para desativar esta opção.

NOTA: O módulo Bluetooth no seu computador deve suportar esta capacidade para tirar partido desta funcionalidade.

Cartões

O HP Client Security suporta vários tipos de cartões de identificação diferentes, os quais são cartões de plástico pequenos contendo um chip informático. Estes incluem smart cards, cartões sem contactos e cartões de proximidade. Se um destes cartões, e o leitor de cartões adequado, for ligado ao computador, se o administrador instalou o controlador associado do fabricante e se o administrador ativou o cartão como uma credencial de autenticação, pode utilizar o cartão como uma credencial de autenticação.

Para os smart cards, o fabricante deve fornecer ferramentas para instalar um certificado de segurança e gestão de PIN que o HP Client Security utiliza no seu algoritmo de segurança. O número e o tipo de caracteres utilizados como PIN poderá variar. Um administrador deve inicializar o smart card antes de poder ser utilizado.

O HP Client Security suporta os seguintes formatos de smart card:

- CSP
- PKCS11

O HP Client Security suporta os seguintes tipos de cartões sem contactos:

- Cartões de memória iCLASS HID sem contactos
- Cartões de memória sem contactos MiFare Classic 1k, 4k e mini

O HP Client Security suporta os seguintes cartões de proximidade:

- Cartões de proximidade HID

Para registar um smart card:

1. Insira o cartão num leitor de smart card ligado.
2. Quando o cartão for reconhecido, introduza o PIN do cartão e em seguida clique ou toque em **Registar**.

Para alterar o PIN de um smart card:

1. Insira o cartão num leitor de smart card ligado.
2. Quando o cartão for reconhecido, introduza o PIN do cartão e em seguida clique ou toque em **Autenticar**.
3. Clique ou toque em **Alterar PIN** e em seguida introduza o novo PIN.

Para registar um cartão sem contactos ou cartão de proximidade:

1. Coloque o cartão no ou muito perto do leitor adequado.
2. Quando o cartão for reconhecido, clique ou toque em **Registar**.

Para eliminar um cartão registado:

1. Apresente o cartão ao leitor.
2. Apenas para smart cards, introduza o PIN atribuído do cartão e em seguida clique ou toque em **Autenticar**.
3. Clique ou toque em **Eliminar**.

Depois de o cartão ser registado, os detalhe do cartão são apresentados em **Cartões registados**. Quando um cartão é eliminado, é removido da lista.

Para aceder às Definições de Cartão de proximidade, Cartão sem contactos e Smart card, onde os administradores podem especificar definições relacionadas com as credenciais de cartões, clique ou toque em **Definições** (requer privilégios administrativos).

Definições de Cartão de proximidade, Cartão sem contactos e Smart card

para aceder às definições para um cartão, clique ou toque no cartão na lista e em seguida clique ou toque na seta apresentada.

Para alterar o PIN de um smart card:

1. Apresente o cartão ao leitor
2. Introduza o PIN atribuído do cartão e em seguida clique ou toque em **Continuar**.
3. Introduza e confirme o novo PIN e em seguida clique ou toque em **Continuar**.

Para inicializar o PIN de um smart card:

1. Apresente o cartão ao leitor
2. Introduza o PIN atribuído do cartão e em seguida clique ou toque em **Continuar**.
3. Introduza e confirme o novo PIN e em seguida 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. Introduza o PIN atribuído do cartão (apenas para smart cards) e em seguida clique ou toque em **Continuar**.
3. Clique ou toque em **Sim** para confirmar a eliminação.

PIN

Se o administrador tiver ativado um PIN como uma credencial de autenticação, pode configurar um PIN em conjunto com outras credenciais para maior segurança.

Para configurar um novo PIN:

- Introduza o PIN, introduza-o novamente para confirmá-lo e em seguida clique ou toque em **Aplicar**.

Para eliminar um PIN:

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

Para aceder às Definições do PIN, onde os administradores podem especificar definições relacionadas com as credenciais de PIN, clique ou toque em **Definições** (requer privilégios administrativos).

Definições de PIN

Na página Definições de PIN, pode especificar os comprimentos mínimo e máximo aceitáveis para a credencial PIN.

RSA SecurID

Se o administrador tiver ativado RSA como uma credencial de autenticação, e as condições seguintes são verdadeiras, pode registar ou eliminar uma credencial RSA SecurID.

NOTA: É necessária a configuração adequada.

- Deverá ter sido criado o utilizador num servidor RSA.
- O token RSA SecurID atribuído ao utilizador e ao computador devem ter sido adicionados ao domínio do servidor RSA.
- O software SecurID está instalado no computador
- Está disponível uma ligação ao servidor RSA devidamente configurada.

Para registar uma credencial RSA SecurID:

▲ Introduza o seu nome de utilizador e código de acesso RSA SecurID (código token ou PIN +código token de RSA SecurID, consoante o seu ambiente) e em seguida clique em **Aplicar**.

Após o registo com êxito, é apresentada uma mensagem, “A sua credencial RSA SecurID foi registada com êxito”, e o botão Eliminar é ativado.

Para eliminar uma credencial RSA SecurID:

▲ Clique em **Eliminar** e em seguida selecione **Sim** na caixa de diálogo pop-up que pergunta “Tem a certeza de que pretende eliminar a sua credencial RSA SecurID?”

Password Manager

Iniciar sessão em websites e aplicações é mais fácil do que nunca quando utiliza o Password Manager. Pode criar palavras-passes mais seguras que não tem de anotar ou memorizar, e em seguida iniciar sessão de forma fácil e rápida com uma impressão digital, smart card, cartão de proximidade, cartão sem contactos, telefone Bluetooth, PIN, credencial RSA ou a sua palavra-passe do Windows.

NOTA: Devido à estrutura em constante mudança dos ecrãs de início de sessão da Web, o Password Manager poderá não conseguir suportar todos os websites permanentemente.

O Password Manager oferece as seguintes opções:

Página Password Manager

- Clique ou toque numa conta para iniciar automaticamente uma página Web ou aplicação e inicie sessão.
- Utilize categorias para organizar as suas contas.

Força da palavra-passe

- Veja de relance se alguma das suas palavras-passes é um risco de segurança.
- Quando adicionar dados de início de sessão, verifique a força de palavras-passes individuais utilizadas para websites e aplicações.
- A força da palavra-passe é ilustrada por indicadores de estado vermelhos, amarelos ou verdes.

O ícone **Password Manager** é apresentado no canto superior esquerdo de uma página Web ou no ecrã de início de sessão de uma aplicação. Quando um início de sessão ainda não tiver sido criado para esse website ou aplicação, é apresentado um sinal mais no ícone.

▲ Clique ou toque no ícone **Password Manager** para visualizar um menu de contexto onde pode escolher entre as seguintes opções:

- Adicionar [umdominio.com] ao Password Manager
- Abrir o Password Manager
- Definições dos ícones
- Ajuda

Para as páginas Web ou programas onde ainda não foi criado um início de sessão

São apresentadas as seguintes opções no menu de contexto:

- **Adicionar [umdominio.com] ao Password Manager** – Permite-lhe adicionar um início de sessão ao ecrã de início de sessão atual.
- **Abrir o Password Manager** – Inicia o Password Manager.
- **Definições dos ícones** – Permite-lhe especificar condições segundo as quais o ícone **Password Manager** é apresentado.
- **Ajuda** – Apresenta a Ajuda do HP Client Security.

Para as páginas Web ou programas onde já foi criado um início de sessão

São apresentadas as seguintes opções no menu de contexto:

- **Preencher dados de início de sessão** – Apresenta uma página **Verificar a sua identidade**. Se forem autenticados com êxito, os seus dados de início de sessão são colocados nos campos de início de sessão e em seguida a página é enviada (se o envio foi especificado quando o início de sessão foi criado ou editado pela última vez).
- **Editar início de sessão** – Permite-lhe editar os seus dados de início de sessão para este website.
- **Adicionar início de sessão** – Permite-lhe adicionar uma conta ao Password Manager.
- **Abrir o Password Manager** – Inicia o Password Manager.
- **Ajuda** – Apresenta a Ajuda do HP Client Security.

NOTA: O administrador deste computador poderá ter configurado o HP Client Security para exigir mais do que uma credencial ao verificar a sua identidade.

Adicionar inícios de sessão

Pode adicionar facilmente um início de sessão para um website ou programa introduzindo uma vez as informações de início de sessão. A partir daqui, o Password Manager introduz automaticamente

as informações por si. Pode utilizar estes inícios de sessão depois de navegar até ao website ou programa.

Para adicionar um início de sessão:

1. Abra o ecrã de início de sessão de um website ou programa.
2. Clique ou toque no ícone **Password Manager** e em seguida clique ou toque numa das seguintes opções, consoante o ecrã de início de sessão pertence a um website ou um programa:
   - Para um website, clique ou toque em **Adicionar [nome de domínio] ao Password Manager**.
   - Para um programa, clique ou toque em **Adicionar este ecrã de início de sessão ao Password Manager**.
3. Introduza os seus dados do início de sessão. Os campos de início de sessão no ecrã, e os campos correspondentes na caixa de diálogo, estão identificados por uma margem cor de laranja a negrito.
   a. Para popular um campo de início de sessão com uma das escolhas pré-formatadas, clique ou toque nas setas à direita do campo.
   b. Para ver a palavra-passe para este início de sessão, clique ou toque em **Mostrar palavra--passe**.
   c. Para que os campos de início de sessão sejam preenchidos, mas não enviados, desmarque a caixa de verificação **Enviar dados de início de sessão automaticamente**.
   d. Clique ou toque em **OK** para selecionar o método de autenticação que pretende utilizar (impressões digitais, smart card, cartão de proximidade, cartão sem contactos, telefone Bluetooth, PIN ou palavra-passe) e em seguida inicie sessão com o método de autenticação selecionado.

      O sinal mais é removido do ícone do **Password Manager** para o informar de que o início de sessão foi criado.
   e. Se o Password Manager não detetar os campos de início de sessão, clique ou toque em **Mais campos**.
      - Selecione a caixa de verificação para cada campo necessário para o início de sessão, ou desmarque na caixa de verificação quaisquer campos que não sejam necessários para o início de sessão.
      - Clique ou toque em **Fechar**.

Cada vez que acede a esse website ou abre esse programa, o ícone do **Password Manager** é apresentado no canto superior esquerdo de um website ou no ecrã de início de sessão de uma aplicação, indicando que pode utilizar as suas credenciais registadas para iniciar sessão.

Editar inícios de sessão

Para editar um início de sessão:

1. Abra o ecrã de início de sessão de um website ou programa.
2. Para visualizar uma caixa de diálogo onde pode editar as suas informações de início de sessão, clique ou toque no ícone do **Password Manager** e em seguida clique ou toque em **Editar início de sessão**.

   Os campos de início de sessão no ecrã, e os campos correspondentes na caixa de diálogo, estão identificados por uma margem cor de laranja a negrito.

   Pode também editar informações da conta a partir da página Password Manager clicando ou tocando no início de sessão para visualizar as opções de edição e em seguida selecionando **Editar**.
3. Edite as suas informações de início de sessão.
   - Para editar o **Nome da conta**, introduza um novo nome no campo.
   - Para adicionar ou editar o nome de uma **Categoria**, introduza ou modifique o nome no campo **Categoria**.
   - Para selecionar um campo de início de sessão **Nome de utilizador** com uma das escolhas pré-formatadas, clique ou toque na seta para baixo à direita do campo.

     As escolhas pré-formatadas apenas estão disponíveis quando edita o início de sessão a partir do comando Editar no menu de contexto do ícone do Password Manager.
   - Para selecionar um campo de início de sessão **Palavra-passe** com uma das escolhas pré--formatadas, clique ou toque na seta para baixo à direita do campo.

     As escolhas pré-formatadas apenas estão disponíveis quando edita o início de sessão a partir do comando Editar no menu de contexto do ícone do Password Manager.
   - Para adicionar mais campos do ecrã ao seu início de sessão, clique ou toque em **Mais campos**.
   - Para ver a palavra-passe para este início de sessão, clique ou toque no ícone **Mostrar palavra-passe**.
   - Para que os campos de início de sessão sejam preenchidos, mas não enviados, desmarque a caixa de verificação **Enviar dados de início de sessão automaticamente**.
   - Para marcar este início de sessão como tendo uma palavra-passe comprometida, marque a caixa de verificação **Esta palavra-passe está comprometida**.

     Depois de as alterações serem guardadas, todos os outros inícios de sessão que partilham a mesma palavra-passe também serão marcados como comprometidos. Pode então visitar cada conta afetada e alterar as palavras-passes conforme necessário.
4. Clique ou toque em **OK**.

Utilizar o menu Ligações rápidas do Password Manager

O Password Manager fornece uma forma rápida e fácil de iniciar os websites e programas para os quais criou inícios de sessão. Faça duplo clique ou faça duplo toque no início de sessão de um website ou programa no menu **Ligações rápidas do Password Manager**, ou na página Password Manager no HP Client Security, para abrir o ecrã de início de sessão e em seguida preencha os seus dados de início de sessão.

Quando cria um início de sessão, é adicionado automaticamente ao seu menu **Ligações rápidas** do Password Manager.

Para visualizar o menu **Ligações rápidas**:

▲ Prima a combinação de teclas de atalho do **Password Manager**. (A predefinição é ctrl+tecla do Windows+h). Para alterar a combinação de teclas de atalho, na página inicial do HP Client Security, clique em **Password Manager** e em seguida clique ou toque em **Definições**.

Organizar os inícios de sessão em categorias

Crie uma ou mais categorias para manter os seus inícios de sessão em ordem.

Para atribuir um início de sessão a uma categoria:

1. Na página inicial do HP Client Security, clique ou toque em **Password Manager**.
2. Clique ou toque numa entrada de conta e em seguida clique ou toque em **Editar**.
3. No campo **Categoria**, introduza um nome de categoria.
4. Clique ou toque em **Guardar**.

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 numa 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 **Guardar**.

Para mudar o nome de uma categoria:

1. Na página inicial do HP Client Security, clique ou toque em **Password Manager**.
2. Clique ou toque numa entrada de conta e em seguida clique ou toque em **Editar**.
3. No campo **Categoria**, mude o nome da categoria.
4. Clique ou toque em **Guardar**.

Gerir os seus inícios de sessão

O Password Manager facilita a gestão das suas informações de início de sessão para nomes de utilizadores, palavras-passes e contas com vários inícios de sessão a partir de uma localização central.

Os seus inícios de sessão são indicados na página Password Manager.

Para gerir os seus inícios de sessão:

1. Na página inicial do HP Client Security, clique ou toque em **Password Manager**.
2. Clique ou toque num início de sessão existente e em seguida selecione uma das opções seguintes e siga as instruções apresentadas no ecrã:
   - **Editar** – Edite um início de sessão. Para obter mais informações, consulte Editar inícios de sessão na página 22.
   - **Iniciar sessão** – Inicie sessão na conta selecionada.
   - **Eliminar** – Elimine o início de sessão da conta selecionada.

Para adicionar um novo início de sessão a um website ou programa:

1. Abra o ecrã de início de sessão do website ou programa.
2. Clique ou toque no ícone do **Password Manager** para visualizar o menu de contexto.
3. Clique ou toque em **Adicionar início de sessão** e siga as instruções apresentadas no ecrã.

Avaliar a força da sua palavra-passe

A utilização de palavras-passes seguras para iniciar sessão nos seus websites e programas é um aspeto importante de proteção da sua identidade.

O Password Manager torna mais fácil monitorizar e melhorar a sua segurança com a análise instantânea e automática de cada uma das palavras-passes utilizadas para iniciar sessão nos seus websites e programas.

À medida que introduz uma palavra-passe durante a criação do início de sessão do Password Manager para uma conta, é mostrada uma barra colorida por baixo da palavra-passe para indicar a força da palavra-passe. As cores indicam os seguintes valores:

- **Vermelho** – Fraca
- **Amarelo** – Razoável
- **Verde** – Segura

Definições dos ícones do Password Manager

O Password Manager tenta identificar ecrãs de início de sessão para websites e programas. Quando deteta um ecrã de início de sessão para o qual não criou um início de sessão, o Password Manager pede-lhe para adicionar um início de sessão para o ecrã apresentando o ícone do **Password Manager** com um sinal mais.

1. Clique ou toque no ícone e em seguida clique ou toque em **Definições dos ícones** para personalizar a forma como o Password Manager trata possíveis sites de início de sessão.
   - **Pedir para adicionar inícios de sessão para ecrãs de início de sessão** – Clique ou toque nesta opção para que o Password Manager lhe peça para adicionar um início de sessão quando é apresentado um ecrã de início de sessão que ainda não tenha um início de sessão configurado.
   - **Excluir este ecrã** – Marque a caixa de verificação para que o Password Manager não lhe peça para adicionar um início de sessão para este ecrã de início de sessão.
   - **Não pedir para adicionar inícios de sessão para ecrãs de início de sessão** – Selecione o botão de rádio.
2. Para adicionar um início de sessão para um ecrã que tenha sido excluído anteriormente:
   a. Inicie sessão no website anteriormente excluído.
   b. Para que o Password Manager memorize a palavra-passe para este site, clique ou toque em **Lembrar** na caixa de diálogo pop-up para guardar a palavra-passe e criar um início de sessão para o ecrã.
3. Para aceder a definições adicionais do Password Manager, clique ou toque no ícone do Password Manager, clique ou toque em **Abrir o Password Manager** e em seguida clique ou toque em **Definições** na página Password Manager.

Importar e exportar inícios de sessão

Na página Importar e exportar do HP Password Manager, pode importar inícios de sessão guardados por browsers no seu computador. Também pode importar dados a partir de um ficheiro de cópia de segurança do HP Client Security e exportar dados para um ficheiro de cópia de segurança do HP Client Security.

- ▲ Para iniciar a página Importar e exportar, clique ou toque em **Importar e exportar** na página Password Manager.

Para importar palavras-passes de um browser:

1. Clique ou toque no browser a partir do qual pretende importar palavras-passes (apenas são apresentados os browsers instalados).
2. Desmarque a caixa de verificação de quaisquer contas para as quais não pretende importar palavras-passes.
3. Clique ou toque em **Importar**.

A importação de dados de, ou a exportação de dados para, um ficheiro de cópia de segurança do HP Client Security pode ser realizada através das ligações associadas (em **Outras opções)** na página Importar e exportar.

NOTA: Esta funcionalidade apenas importa e exporta dados do Password Manager. Para mais informações sobre criar cópias de segurança e restaurar dados adicionais do HP Client Security, consulte Criar cópias de segurança e restaurar os seus dados na página 29.

Para importar dados de um ficheiro de cópia de segurança do HP Client Security:

1. Na página Importar e exportar do HP Password Manager, clique ou toque em **Importar dados a partir de um ficheiro de cópia de segurança do HP Client Security**.
2. Verifique a sua identidade.
3. Selecione o ficheiro de cópia de segurança previamente criado ou introduza o caminho no campo fornecido e em seguida clique ou toque em **Procurar**.
4. Introduza a palavra-passe utilizada para proteger o ficheiro e em seguida clique ou toque em **Seguinte**.
5. Clique ou toque em **Restaurar**.

Para exportar dados para um ficheiro de cópia de segurança do HP Client Security:

1. Na página Importar e exportar do HP Password Manager, clique ou toque em **Exportar dados para um ficheiro de cópia de segurança do HP Client Security**.
2. Verifique a sua identidade e em seguida clique ou toque em **Seguinte**.
3. Introduza um nome para o ficheiro de cópia de segurança. Por predefinição, o ficheiro é guardado na sua pasta Documentos. Para especificar uma localização diferente, clique ou toque em **Procurar**.
4. Introduza e confirme uma palavra-passe para proteger o ficheiro e em seguida clique ou toque em **Guardar**.

Definições

Pode especificar definições para personalizar o Password Manager:

- **Pedir para adicionar inícios de sessão para ecrãs de início de sessão** – O ícone do **Password Manager** com um sinal mais é apresentado sempre que é detetado um website ou programa, indicando que pode adicionar um início de sessão para este ecrã no menu **Inícios de sessão**.

  Para desativar esta funcionalidade, desmarque a caixa de verificação ao lado de **Pedir para adicionar inícios de sessão para ecrãs de início de sessão**.

- **Abrir o Password Manager com Ctrl+Win+h** – A tecla de atalho predefinida que abre o menu **Ligações rápidas do Password Manager** é Ctrl+tecla do Windows+h.

  Para alterar a tecla de atalho, clique ou toque nesta opção e em seguida introduza uma nova combinação de teclas. As combinações poderão incluir uma ou mais das seguintes: ctrl, alt, ou shift, e qualquer tecla alfabética ou numérica.

  As combinações reservadas para o Windows ou aplicações do Windows não podem ser utilizadas.

- Para repor os valores predefinidos de fábrica, clique ou toque em **Restaurar predefinições**.

Definições avançadas

Os administradores podem aceder às seguintes opções selecionando o ícone da **engrenagem** (definições) na página inicial do HP Client Security.

- **Políticas de administradores** – Permite-lhe configurar políticas de início de sessão e de sessão para administradores.
- **Políticas de utilizadores padrões** – Permite-lhe configurar políticas de início de sessão e de sessão para utilizadores padrões.
- **Funcionalidades de segurança** – Permite-lhe aumentar a segurança do computador protegendo a sua conta do Windows através de uma autenticação segura e/ou ativando a autenticação antes do arranque do Windows.
- **Utilizadores** – Permite-lhe gerir utilizadores e as respetivas credenciais.
- **As minhas políticas** – Permite-lhe rever as suas políticas de autenticação e o estado de registo.
- **Cópia de segurança e restauro** – Permite-lhe criar uma cópia de segurança ou restaurar dados do HP Client Security.
- **Acerca do HP Client Security** – Apresenta informações da versão acerca do HP Client Security Manager.

Políticas de administradores

Pode configurar políticas de início de sessão e de sessão para administradores deste computador. As políticas de início de sessão definidas aqui determinam as credenciais exigidas para um administrador local ao iniciar sessão no Windows. As políticas de sessão definidas aqui determinam as credenciais exigidas para um administrador local verificar a identidade numa sessão no Windows.

Por predefinição, todas as políticas novas ou alteradas são aplicadas imediatamente depois de tocar ou clique em **Aplicar**.

Para adicionar uma nova política:

1. Na página inicial do HP Client Security, clique ou toque no ícone da **engrenagem**.
2. Na página Definições avançadas, clique ou toque em **Políticas de administradores**.
3. Clique ou toque em **Adicionar nova política**.
4. Clique nas setas para baixo para selecionar credenciais principais e secundárias (opcionais) para a nova política e em seguida clique ou toque em **Adicionar**.
5. Clique em **Aplicar**.

Para retardar a aplicação de uma política nova ou alterada:

1. Clique ou toque em **Aplicar esta política imediatamente**.
2. Selecione **Aplicar esta política na data específica**.
3. Introduza uma data ou utilize o calendário pop-up para selecionar a data em que esta política deve ser aplicada.
4. Caso pretenda, selecione quando lembrar os utilizadores acerca da nova política.
5. Clique em **Aplicar**.

Políticas de utilizadores padrões

Pode configurar políticas de início de sessão e de sessão para utilizadores padrões deste computador. As políticas de início de sessão definidas aqui determinam as credenciais exigidas para um utilizador padrão ao iniciar sessão no Windows. As políticas de sessão definidas aqui determinam as credenciais exigidas para um utilizador padrão verificar a identidade numa sessão no Windows.

Por predefinição, todas as políticas novas ou alteradas são aplicadas imediatamente depois de tocar ou clique em **Aplicar**.

Para adicionar uma nova política:

1. Na página inicial do HP Client Security, clique ou toque no ícone da **engrenagem**.
2. Na página Definições avançadas, clique ou toque em **Políticas de utilizadores padrões**.
3. Clique ou toque em **Adicionar nova política**.
4. Clique nas setas para baixo para selecionar credenciais principais e secundárias (opcionais) para a nova política e em seguida clique ou toque em **Adicionar**.
5. Clique em **Aplicar**.

Para retardar a aplicação de uma política nova ou alterada:

1. Clique ou toque em **Aplicar esta política imediatamente**.
2. Selecione **Aplicar esta política na data específica**.
3. Introduza uma data ou utilize o calendário pop-up para selecionar a data em que esta política deve ser aplicada.
4. Caso pretenda, selecione quando lembrar os utilizadores acerca da nova política.
5. Clique em **Aplicar**.

Funcionalidades de segurança

Pode ativar funcionalidades de segurança do HP Client Security que ajudam a proteger contra o acesso não autorizado ao computador.

Para configurar funcionalidades de segurança:

1. Na página inicial do HP Client Security, clique ou toque no ícone da **engrenagem**.
2. Na página Definições avançadas, clique ou toque em **Funcionalidades de segurança**.
3. Ative funcionalidades de segurança marcando as caixas de verificação e em seguida clique ou toque em **Aplicar**. Quanto mais funcionalidades selecionar, mais seguro estará o seu computador.

   Estas definições aplicam-se a todos os utilizadores.

   - **Segurança de início de sessão do Windows** – Protege as suas contas do Windows ao exigir a utilização de credenciais do HP Client Security para o acesso.
   - **Segurança de pré-arranque (autenticação na ligação)** – Protege o seu computador antes do arranque do Windows. Esta seleção não está disponível se não for suportada pelo BIOS.
   - **Permitir início de sessão de passo único** – Esta definição permite ignorar o início de sessão do Windows se foi previamente realizada a autenticação ao nível da autenticação na ligação ou do Drive Encryption.
4. Clique ou toque em **Utilizadores** e em seguida clique ou toque no mosaico do utilizador.

Utilizadores

Pode monitorizar e gerir os utilizadores do HP Client Security deste computador.

Para adicionar outro utilizador Windows ao HP Client Security:

1. Na página inicial do HP Client Security, clique ou toque no ícone da **engrenagem**.
2. Na página Definições avançadas, clique ou toque em **Utilizadores**.
3. Clique ou toque em **Adicionar outro utilizador Windows ao HP Client Security**.
4. Introduza o nome do utilizador que pretende adicionar e em seguida clique ou toque em **OK**.
5. Introduza a palavra-passe do Windows do utilizador.

   Na página Utilizador é apresentado um mosaico para o utilizador adicionado.

Para eliminar um utilizador Windows do HP Client Security:

1. Na página inicial do HP Client Security, clique ou toque no ícone da **engrenagem**.
2. Na página Definições avançadas, clique ou toque em **Utilizadores**.
3. Clique ou toque no nome do utilizador que pretende eliminar.
4. Clique ou toque em **Eliminar utilizador** e em seguida clique ou toque em **Sim** para confirmar.

Para visualizar um resumo das políticas de início de sessão e de sessão aplicadas a um utilizador:

▲ Clique ou toque em **Utilizadores** e em seguida clique ou toque no mosaico do utilizador.

As minhas políticas

Pode visualizar as suas políticas de autenticação e o estado de registo. A página As minhas políticas também fornece ligações para as páginas Políticas de administradores e Políticas de utilizadores padrões.

1. Na página inicial do HP Client Security, clique ou toque no ícone da **engrenagem**.
2. Na página Definições avançadas, clique ou toque em **As minhas políticas**.

   São apresentadas as políticas de início de sessão e de sessão aplicadas ao utilizador atualmente com sessão iniciada.

A página As minhas políticas também fornece ligações para Políticas de administradores na página 26 e Políticas de utilizadores padrões na página 27.

Criar cópias de segurança e restaurar os seus dados

Recomenda-se que crie cópias de segurança regularmente dos seus dados do HP Client Security. A frequência da cópia de segurança depende da frequência com que os dados mudam. Por exemplo, se adicionar novos inícios de sessão diariamente, deve criar cópias de segurança dos seus dados diariamente.

As cópias de segurança também são designadas como importar e exportar.

NOTA: Apenas é criada uma cópia de segurança do Password Manager por esta funcionalidade. O Drive Encryption tem um método de cópia de segurança independente. O Device Access Manager e as informações de autenticação de impressões digitais não são copiados.

O HP Client Security deve estar instalado em qualquer computador que vá receber dados copiados antes que os dados possam ser restaurados a partir do ficheiro de cópia de segurança.

Para criar uma cópia de segurança dos seus dados:

1. Na página inicial do HP Client Security, clique ou toque no ícone da **engrenagem**.
2. Na página Definições avançadas, clique ou toque em **Políticas de administradores**.
3. Clique ou toque em **Cópia de segurança e restauro**.
4. Clique ou toque em **Cópia de segurança** e em seguida verifique a sua identidade.
5. Selecione o módulo que pretende incluir na cópia de segurança e em seguida clique ou toque em **Seguinte**.
6. Introduza um nome para o ficheiro de armazenamento. Por predefinição, o ficheiro é guardado na sua pasta Documentos. Para especificar uma localização diferente, clique ou toque em **Procurar**.
7. Introduza e confirme uma palavra-passe para proteger o ficheiro.
8. Clique ou toque em **Guardar**.

Para restaurar os seus dados:

1. Na página inicial do HP Client Security, clique ou toque no ícone da **engrenagem**.
2. Na página Definições avançadas, clique ou toque em **Políticas de administradores**.
3. Clique ou toque em **Cópia de segurança e restauro**.
4. Selecione **Restaurar** e em seguida verifique a sua identidade.

5. Selecione o ficheiro de armazenamento previamente criado. Introduza o caminho no campo fornecido. Para especificar uma localização diferente, clique ou toque em **Procurar**.
6. Introduza a palavra-passe utilizada para proteger o ficheiro e em seguida clique ou toque em **Seguinte**.
7. Selecione os módulos para os quais pretende restaurar dados.
8. Clique ou toque em **Restaurar**.

5 HP Drive Encryption (apenas alguns modelos)

O HP Drive Encryption fornece uma proteção de dados total ao encriptar os dados do seu computador. Quando o Drive Encryption está ativado, deve iniciar sessão no ecrã de início de sessão do Drive Encryption, que é apresentado antes de o sistema operativo Windows® ser iniciado.

O ecrã inicial do HP Client Security permite aos administradores do Windows ativar o Drive Encryption, criar a cópia de segurança da chave de encriptação e marcar ou desmarcar uma ou mais unidades para encriptação. Para mais informações, consulte a Ajuda do software HP Client Security.

É possível realizar as seguintes tarefas com o Drive Encryption:

- Selecionar definições do Drive Encryption:
  - Encriptar ou desencriptar unidades ou partições individuais utilizando a encriptação por software
  - Encriptar ou desencriptar unidades de autoencriptação individuais utilizando a encriptação por hardware
  - Adicionar segurança extra ao desativar o modo de Suspensão ou de Espera para garantir que é sempre exigida a autenticação de pré-arranque do Drive Encryption

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

- Criar chaves de cópia de segurança
- Recuperar o acesso a um computador encriptado utilizando chaves de cópia de segurança e a HP SpareKey
- Ativar a autenticação de pré-arranque do Drive Encryption utilizando uma palavra-passe, impressão digital registada ou PIN para cartões smart card selecionados

Abrir o Drive Encryption

Os administradores podem aceder ao Drive Encryption abrindo o HP Client Security:

1. No ecrã Iniciar, clique ou toque na aplicação **HP Client Security** (Windows 8).

   – ou –

   No ambiente de trabalho do Windows, clique duas vezes ou toque duas vezes no ícone **HP Client Security** na área de notificação, situada na extremidade direita da barra de tarefas.

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

Tarefas gerais

Ativar o Drive Encryption para unidades de disco rígido padrões

As unidades de disco rígido padrões são encriptadas utilizando a encriptação por software. Siga estes passos para encriptar uma unidade ou partição de disco:

1. Inicie o **Drive Encryption**. Para obter mais informações, consulte Abrir o Drive Encryption na página 31.
2. Marque a caixa de verificação da unidade ou partição que pretende encriptar e clique ou toque em **Chave de cópia de segurança**.

NOTA: Para uma maior segurança, marque a caixa de verificação **Desativar o modo de Suspensão para maior segurança**. Quando desativa o modo de Suspensão, não há absolutamente qualquer risco de que as credenciais utilizadas para desbloquear a unidade sejam armazenadas na memória.

3. Selecione uma ou mais das opções de cópia de segurança e em seguida clique ou toque em **Criar cópia de segurança**. Para obter mais informações, consulte Criar cópia de segurança das chaves de encriptação na página 35.
4. Pode continuar a trabalhar enquanto é criada a cópia de segurança da chave de encriptação. Não reinicie o computador.

NOTA: É-lhe pedido para reiniciar o computador. Depois de reiniciar, é apresentado o ecrã de pré-arranque da encriptação da unidade, que requer a autenticação antes de o Windows iniciar.

O Drive Encryption foi ativado. A encriptação das partições de unidade selecionadas poderá demorar várias horas, consoante o número e o tamanho das partições.

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

Ativar o Drive Encryption para unidades de autoencriptação

As unidades de autoencriptação que cumprem a especificação OPAL do Trusted Computing Group para a gestão de unidades de autoencriptação podem ser encriptadas utilizando a encriptação por software ou a encriptação por hardware. A encriptação por hardware é muito mais rápida do que a encriptação por software. No entanto, não pode escolher as partições de disco a encriptar. É encriptado o disco inteiro, incluindo quaisquer partições de disco.

Para encriptar partições específicas, deve utilizar a encriptação por software. Certifique-se de que marca a caixa de verificação **Permitir a encriptação por hardware apenas para unidades de autoencriptação (SED)**.

Siga estes passos para ativar o Drive Encryption para unidades de autoencriptação:

1. Inicie o **Drive Encryption**. Para obter mais informações, consulte Abrir o Drive Encryption na página 31.
2. Marque a caixa de verificação da unidade que pretende encriptar e clique ou toque em **Chave de cópia de segurança**.

NOTA: Para uma maior segurança, marque a caixa de verificação **Desativar o modo de Suspensão para maior segurança**. Quando desativa o modo de Suspensão, não há absolutamente qualquer risco de que as credenciais utilizadas para desbloquear a unidade sejam armazenadas na memória.

3. Selecione uma ou mais das opções de cópia de segurança e em seguida clique ou toque em **Criar cópia de segurança**. Para obter mais informações, consulte Criar cópia de segurança das chaves de encriptação na página 35.

4. Pode continuar a trabalhar enquanto é criada a cópia de segurança da chave de encriptação. Não reinicie o computador.

NOTA: No caso das unidades de autoencriptação, é-lhe pedido para encerrar o computador.

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

Desativar o Drive Encryption

1. Inicie o **Drive Encryption**. Para obter mais informações, consulte Abrir o Drive Encryption na página 31.

2. Desmarque a caixa de verificação de todas as unidades encriptadas e em seguida clique ou toque em **Aplicar**.

   A desativação do Drive Encryption começa.

NOTA: Se foi utilizada a encriptação por software, começa a desencriptação. Poderá demorar várias horas, consoante o tamanho das partições da unidade de disco rígido encriptada. Quando a desencriptação está concluída, o Drive Encryption é desativado.

Se foi utilizada a desencriptação por hardware, a unidade é desencriptada instantaneamente, sendo o Drive Encryption desativado alguns minutos depois.

Assim que o Drive Encryption for desativado, ser-lhe-á pedido para encerrar o computador, no caso da encriptação por hardware, ou para reiniciar o computador, no caso da encriptação por software.

Iniciar sessão depois de ativar o Drive Encryption

Quando liga o computador depois de ativar o Drive Encryption e de a sua conta de utilizador ser registada, deve iniciar sessão no ecrã de início de sessão do Drive Encryption:

NOTA: Quando reativa o computador a partir do modo de Suspensão ou de Espera, não é apresentada a autenticação de pré-arranque do Drive Encryption para a encriptação por software ou encriptação por hardware. A encriptação por hardware fornece a opção **Desativar o modo de Suspensão para maior segurança**.

Quando reativa o computador a partir do modo de Hibernação, é apresentada a autenticação de pré--arranque do Drive Encryption para a encriptação por software ou encriptação por hardware.

NOTA: Se o administrador do Windows tiver ativado a segurança de pré-arranque do BIOS no HP Client Security e o One-Step Logon estiver ativado (por predefinição), pode iniciar sessão no computador imediatamente depois de autenticar o pré-arranque do BIOS, sem necessitar de voltar a autenticar -seno ecrã de início de sessão do Drive Encryption.

Início de sessão de utilizador simples:

- Na página **Início de sessão**, introduza a sua palavra-passe do Windows, PIN de smart card, SpareKey ou deslize um dedo registado.

Início de sessão de vários utilizadores:

1. Na página **Selecionar utilizador para iniciar sessão**, selecione o utilizador para iniciar sessão na lista pendente e clique ou toque em **Seguinte**.
2. Na página **Início de sessão**, introduza a sua palavra-passe do Windows, PIN de smart card ou deslize um dedo registado.

NOTA: São suportados os seguintes cartões smart card:

Cartões smart card suportados

- Gemalto Cyberflex Access 64k V2c

NOTA: Se for utilizada a chave de recuperação para iniciar sessão no ecrã de início de sessão do Drive Encryption, são exigidas credenciais adicionais no início de sessão do Windows para aceder às contas de utilizadores.

Encriptar unidades de disco rígido adicionais

Recomendamos vivamente que utilize o HP Drive Encryption para proteger os seus dados ao encriptar a sua unidade de disco rígido. Após a ativação, quaisquer unidades de disco rígido adicionadas ou partições criadas podem ser encriptadas seguindo estes passos:

1. Inicie o **Drive Encryption**. Para obter mais informações, consulte Abrir o Drive Encryption na página 31.
2. NO caso das unidades com encriptação por software, selecione as partições de unidade a encriptar.

NOTA: Isto aplica-se igualmente num cenário de várias unidades em que estão presentes uma ou mais unidades de disco rígido padrões e uma ou mais unidades de autoencriptação.

– ou –

▲ Para as unidades com encriptação por hardware, selecione as unidades adicionais a encriptar.

Tarefas avançadas

Gerir o Drive Encryption (tarefa de administrador)

Os administradores podem utilizar o Drive Encryption para ver e alterar o estado da encriptação (Não encriptada ou Encriptada) de todas as unidades de disco rígido do computador.

- Se o estado for Ativado, o Drive Encryption foi ativado e configurado. A unidade apresenta um dos seguintes estados:

Encriptação por software

  - Não encriptada
  - Encriptada
  - Encriptar
  - Desencriptar

Encriptação por hardware

- Encriptada
- Não encriptada (para unidades adicionais)

Encriptar ou desencriptar partições de unidades individuais (apenas encriptação por software)

Os administradores podem utilizar o Drive Encryption para encriptar uma ou mais partições de unidades de disco rígido no computador ou desencriptar quaisquer partições de unidades que já tenham sido encriptadas.

1. Inicie o **Drive Encryption**. Para obter mais informações, consulte Abrir o Drive Encryption na página 31.
2. Em **Estado da unidade**, marque ou desmarque a caixa de verificação ao lado de cada partição de unidade de disco rígido que pretende encriptar ou desencriptar e em seguida clique ou toque em **Aplicar**.

NOTA: Quando uma partição está a ser encriptada ou desencriptada, uma barra de progresso mostra a percentagem de encriptação da partição.

NOTA: As partições dinâmicas não são suportadas. Se uma partição for apresentada como disponível, mas não for possível encriptá-la quando selecionada, essa partição é dinâmica. Uma partição dinâmica resulta de reduzir uma partição para criar uma nova partição em Gestão de Discos.

É apresentado um aviso se uma partição for convertida para partição dinâmica.

Gestão dos discos

- **Alcunha** – Pode dar nomes às suas unidades ou partições para facilitar a identificação.
- **Unidades desligadas** – O Drive Encryption consegue rastrear discos que são removidos do computador. Um disco que seja removido do computador é transferido automaticamente para a lista Desligadas. Se o disco for devolvido ao sistema, voltará a aparecer na lista Ligadas.
- Se já não necessitar de rastrear ou gerir a unidade desligada, pode remover a unidade desligada da lista Desligadas.
- O Drive Encryption permanece ativado até que todas as caixas de verificação de todas as unidades ligadas sejam desmarcadas e que a lista Desligadas esteja vazia.

Cópia de segurança e recuperação (tarefa de administrador)

Quando o Drive Encryption é ativado, os administradores podem utilizar a página Cópia de segurança da chave de encriptação para criar cópias de segurança das chaves de encriptação para suportes amovíveis e executar uma recuperação.

Criar cópia de segurança das chaves de encriptação

Os administradores podem criar uma cópia de segurança da chave de encriptação de uma unidade encriptada num dispositivo de armazenamento amovível.

CUIDADO: Certifique-se de que mantém num local seguro o dispositivo de armazenamento que contém a cópia de segurança da chave, pois, na eventualidade de se esquecer da sua palavra--passe, perder o seu smart card ou não ter um dedo registado, este dispositivo fornece o seu único acesso ao computador. O local de armazenamento também deve ser seguro porque o dispositivo de armazenamento permite o acesso ao Windows.

1. Inicie o **Drive Encryption**. Para obter mais informações, consulte Abrir o Drive Encryption na página 31.
2. Marque a caixa de verificação de uma unidade e em seguida clique ou toque em **Criar cópia de segurança da chave**.
3. Em **Criar chave de recuperação do HP Drive Encryption**, selecione uma ou mais das seguintes opções:
   - **Armazenamento amovível** – Marque a caixa de verificação e em seguida selecione o dispositivo de armazenamento onde será guardada a chave de encriptação.
   - **SkyDrive** – Marque a caixa de verificação. Deve estar ligado à Internet. Inicie sessão no Microsoft SkyDrive e em seguida clique ou toque em **Sim**.

     NOTA: Para utilizar a chave de cópia de segurança do HP Drive Encryption que está armazenada no SkyDrive, deve transferi-la do SkyDrive para um dispositivo de armazenamento amovível e em seguida inserir o dispositivo de armazenamento no computador.
   - **TPM** (apenas modelos selecionados) – Permite-lhe recuperar os seus dados utilizando a sua palavra-passe TPM.

     CUIDADO: Se TPM for limpo ou o computador for danificado, perderá o acesso à cópia de segurança. Se for selecionado este método, deve ser selecionado também outro método de cópia de segurança.
4. Clique ou toque em **Criar cópia de segurança**.

   A chave de encriptação é guardada no dispositivo de armazenamento que selecionou.

Recuperar o acesso a um computador ativado utilizando chaves de cópia de segurança

Os administradores podem efetuar uma recuperação utilizando a chave do Drive Encryption copiada para um dispositivo de armazenamento amovível na ativação ou selecionando a opção **Chave de cópia de segurança** no Drive Encryption.

1. Insira o dispositivo de armazenamento amovível que contém a sua chave de cópia de segurança.
2. Ligue o computador.
3. Quando surgir a caixa de diálogo de início de sessão do HP Drive Encryption, clique ou toque em **Recuperação**.
4. Introduza o caminho ou nome do ficheiro que contém a sua chave de cópia de segurança e em seguida clique ou toque em **Recuperação**.
5. Quando surgir a caixa de diálogo de confirmação, clique ou toque em **OK**.

   É apresentado o ecrã de início de sessão do Windows.

NOTA: Se for utilizada a chave de recuperação para iniciar sessão no ecrã de início de sessão do Drive Encryption, são exigidas credenciais adicionais no início de sessão do Windows para aceder às contas de utilizadores. Recomendamos vivamente que reponha a sua palavra-passe depois de efetuar uma recuperação.

Efetuar uma recuperação com a HP SpareKey

A recuperação com a SpareKey no pré-arranque do Drive Encryption exige que responda corretamente a perguntas de segurança antes de poder aceder ao computador. Para mais informações sobre como configurar a recuperação com a SpareKey, consulte a Ajuda do software HP Client Security.

Para efetuar uma recuperação com a HP SpareKey caso se esqueça da palavra-passe:

1. Ligue o computador.
2. Quando surgir o ecrã do HP Drive Encryption, navegue até ao ecrã de início de sessão do utilizador.
3. Clique em **SpareKey**.

   NOTA: Se a sua SpareKey não foi inicializada no HP Client Security, o botão **SpareKey** não está disponível.

4. Escreva respostas corretas às perguntas apresentadas e em seguida clique em **Iniciar sessão**.

   É apresentado o ecrã de início de sessão do Windows.

NOTA: Se for utilizada a SpareKey para iniciar sessão no ecrã de início de sessão do Drive Encryption, são exigidas credenciais adicionais no início de sessão do Windows para aceder às contas de utilizadores. Recomendamos vivamente que reponha a sua palavra-passe depois de efetuar uma recuperação.

6 HP File Sanitizer (apenas alguns modelos)

O File Sanitizer permite-lhe triturar recursos em segurança (por exemplo: informações ou ficheiros pessoais, dados relacionados com o histórico ou a Internet ou outros componentes de dados) na unidade de disco rígida interna do computador e eliminar definitivamente os dados da unidade de disco rígido interna do computador de forma periódica.

Não é possível utilizar o File Sanitizer para limpar os seguintes tipos de unidades:

- Unidades de estado sólido (SSD), incluindo volumes RAID que abarcam um dispositivo SSD
- Unidades externas ligadas via interface USB, FireWire ou eSATA

Se for tentada uma operação de trituração ou eliminação definitiva num SSD, é apresentada uma mensagem de aviso e a operação não é executada.

Trituração

A trituração é diferente de uma ação de eliminação padrão do Windows®. Quando tritura um recurso utilizando o File Sanitizer, os ficheiros são substituídos por dados sem sentido, tornando virtualmente impossível recuperar o recurso original. Uma simples ação de eliminação do Windows poderá deixar o ficheiro (ou recurso) intacto na unidade de disco rígido ou num estado em que possam ser utilizados métodos forenses para recuperá-lo.

Pode agendar uma hora de trituração futura, ou pode ativar manualmente a trituração selecionando o ícone do **File Sanitizer** no ecrã inicial do HP Client Security ou utilizando o ícone do **File Sanitizer** no ambiente de trabalho do Windows. Para mais informações, consulte Definir um agendamento de trituração na página 40, Trituração com clique do botão direito do rato na página 42 ou Iniciar manualmente uma operação de trituração na página 42.

NOTA: Um ficheiro .dll só é triturado e removido do sistema se tiver sido movido para a Reciclagem.

Eliminação definitiva do espaço livre

A eliminação de um recurso no Windows não remove completamente os conteúdos do recurso da unidade de disco rígido. O Windows elimina apenas a referência ao recurso ou a respetiva localização na unidade de disco rígido. O conteúdo do recurso ainda permanece na unidade de disco rígido até outro recurso substituir essa mesma área na unidade de disco rígido com novas informações.

A eliminação definitiva permite-lhe escrever em segurança dados aleatórios por cima de recursos eliminados, impedindo os utilizadores de ver os conteúdos originais do recurso eliminado.

NOTA: A eliminação definitiva não fornece segurança adicional para recursos triturados.

Pode definir a hora para uma eliminação definitiva futura ou ativar manualmente a eliminação definitiva de recursos previamente triturados selecionando o ícone do **File Sanitizer** no ecrã inicial do HP Client Security ou utilizando o ícone do **File Sanitizer** no ambiente de trabalho do Windows. Para mais informações, consulte Definir um agendamento de eliminação definitiva do espaço livre

na página 41, Iniciar manualmente a eliminação definitiva na página 43 ou Utilizar o ícone do File Sanitizer na página 42.

Abrir o File Sanitizer

1. No ecrã Iniciar, clique ou toque na aplicação **HP Client Security** (Windows 8).

   – ou –

   No ambiente de trabalho do Windows, clique duas vezes ou toque duas vezes no ícone **HP Client Security** na área de notificação, situada na extremidade direita da 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** no ambiente de trabalho do Windows.

– ou –

▲ Clique com o botão direito do rato ou toque continuamente no ícone do **File Sanitizer** no ambiente de trabalho do Windows e em seguida selecione **Abrir o File Sanitizer**.

Procedimentos de configuração

Trituração – O File Sanitizer elimina ou tritura em segurança as categorias de recursos selecionadas.

1. Em **Trituração**, marque a caixa de verificação para cada tipo de ficheiro a triturar ou desmarque a caixa caso não pretenda triturar esses ficheiros.

   - **Reciclagem** – Tritura todos os itens existentes na Reciclagem.
   - **Ficheiros temporários do sistema** – Tritura todos os ficheiros encontrados na pasta temporária do sistema. As seguintes variáveis são procuradas pela ordem que se segue e o primeiro caminho encontrado é considerado como a pasta de sistema:
     - TMP
     - TEMP
   - **Ficheiros temporários da Internet** – Tritura cópias de páginas Web, imagens e conteúdos multimédia que são guardados pelos browsers para uma visualização mais rápida.
   - **Cookies** – Tritura todos os ficheiros armazenados num computador por websites para guardar preferências, tais como informações de início de sessão.

2. Para iniciar a trituração, clique ou toque em **Triturar**.

Eliminação definitiva – Escreve dados aleatórios para libertar espaço e impede a recuperação dos itens eliminados.

▲ Para iniciar a eliminação definitiva, clique ou toque em **Eliminar definitivamente**.

Opções do File Sanitizer – Marque a caixa de verificação para ativar cada uma das seguintes opções ou desmarque a caixa de verificação para desativar uma opção:

- **Ativar ícone no ambiente de trabalho** – Apresenta o ícone do File Sanitizer no Ambiente de Trabalho do Windows.
- **Ativar clique com o botão direito** – Permite-lhe clicar com o botão direito do rato ou tocar continuamente num recurso e em seguida selecionar **HP File Sanitizer – Triturar**.
- **Solicitar a palavra-passe do Windows antes da trituração manual** – Requer a autenticação com a palavra-passe do Windows antes de triturar manualmente um item.
- **Triturar cookies e ficheiros temporários da Internet ao fechar o browser** – Tritura todos os recursos relacionados com a Internet, tais como o histórico de URL do browser, quando fecha um browser de Internet.

Definir um agendamento de trituração

Pode agendar uma hora para executar a trituração automaticamente ou pode também triturar recursos manualmente em qualquer altura. Para obter mais informações, consulte Procedimentos de configuração na página 39.

1. Abra o File Sanitizer e clique ou toque em **Definições**.
2. Para agendar uma hora futura para triturar recursos selecionados, em **Agendamento de trituração** selecione **Nunca**, **Uma vez**, **Diariamente**, **Semanalmente** ou **Mensalmente** e em seguida selecione um dia e uma hora:
   a. Clique ou toque no campo da hora, minutos ou AM/PM.
   b. Desloque o ecrã até visualizar o valor pretendido ao mesmo nível dos outros campos.
   c. Clique ou toque no espaço branco à volta dos campos de definição da hora.
   d. Repita para cada campo até ter selecionado o agendamento correto.
3. São indicados os quatro tipos de recursos seguintes:
   - **Reciclagem** – Tritura todos os itens existentes na Reciclagem.
   - **Ficheiros temporários do sistema** – Tritura todos os ficheiros encontrados na pasta temporária do sistema. As seguintes variáveis são procuradas pela ordem que se segue e o primeiro caminho encontrado é considerado como a pasta de sistema:
     - TMP
     - TEMP
   - **Ficheiros temporários da Internet** – Tritura cópias de páginas Web, imagens e conteúdos multimédia que são guardados pelos browsers para uma visualização mais rápida.
   - **Cookies** – Tritura todos os ficheiros armazenados num computador por websites para guardar preferências, tais como informações de início de sessão.

   Se forem marcados, estes recursos serão triturados na hora agendada.
4. Para selecionar recursos personalizados adicionais para triturar:
   a. Em **Lista de trituração agendada**, clique ou toque em **Adicionar pasta** e navegue até ao ficheiro ou pasta.
   b. Clique ou toque em **Abrir** e depois clique ou toque em **OK**.

Para remover um recurso da Lista de trituração agendada, desmarque a caixa de verificação do recurso.

Definir um agendamento de eliminação definitiva do espaço livre

A eliminação definitiva não fornece segurança adicional para recursos triturados.

1. Abra o File Sanitizer e clique ou toque em **Definições**.
2. Para agendar uma hora futura para eliminar definitivamente os dados da unidade de disco rígido, em **Agendamento de eliminação definitiva** selecione **Nunca**, **Uma vez**, **Diariamente**, **Semanalmente** ou **Mensalmente** e em seguida selecione um dia e uma hora.
   a. Clique ou toque no campo da hora, minutos ou AM/PM.
   b. Desloque o ecrã até visualizar a hora pretendida ao mesmo nível dos outros campos.
   c. Clique ou toque no espaço branco à volta dos campos de definição da hora.
   d. Repita até ter selecionado o agendamento correto.

NOTA: A operação de eliminação definitiva pode demorar muito tempo. Certifique-se de que o computador está ligado à alimentação CA. Embora a eliminação definitiva seja realizada em segundo plano, a utilização acrescida do processador poderá afetar o desempenho do computador. É possível executar a eliminação definitiva depois do horário normal de trabalho ou quando o computador não está a ser utilizado.

Proteger ficheiros contra a trituração

Para proteger ficheiros ou recursos contra a trituração:

1. Abra o File Sanitizer e clique ou toque em **Definições**.
2. Em **Lista Nunca triturar**, clique ou toque em **Adicionar pasta** e navegue até ao ficheiro ou pasta.
3. Clique ou toque em **Abrir** e depois clique ou toque em **OK**.

NOTA: Os ficheiros nesta lista estarão protegidos enquanto constarem da lista.

Para remover um recurso da lista de exclusões, desmarque a caixa de verificação do recurso.

Tarefas gerais

Utilize o File Sanitizer para realizar as seguintes tarefas:

- **Utilizar o ícone do File Sanitizer para iniciar a trituração** – Arraste ficheiros para o ícone do **File Sanitizer** no ambiente de trabalho do Windows. Para mais informações, consulte Utilizar o ícone do File Sanitizer na página 42.
- **Triturar manualmente um ficheiro específico ou todos os recursos selecionados** – Triture itens em qualquer altura sem esperar por uma hora de trituração agendada. Para mais informações, consulte Trituração com clique do botão direito do rato na página 42 ou Iniciar manualmente uma operação de trituração na página 42.

- **Ativar manualmente a eliminação definitiva** – Ative a eliminação definitiva em qualquer altura. Para mais informações, consulte Iniciar manualmente a eliminação definitiva na página 43.
- **Ver os ficheiros de registo** – Veja os ficheiros de registo da trituração e da eliminação definitiva, os quais contêm quaisquer erros ou falhas da última operação de trituração ou eliminação definitiva. Para mais informações, consulte Ver os ficheiros de registo na página 43.

NOTA: A operação de trituração ou eliminação definitiva pode demorar muito tempo. Embora a trituração e a eliminação definitiva sejam realizadas em segundo plano, a utilização acrescida do processador poderá afetar o desempenho do computador.

Utilizar o ícone do File Sanitizer

CUIDADO: Não é possível recuperar ativos eliminados profundamente. Pondere cuidadosamente que itens seleciona para trituração manual.

Quando inicia uma operação de trituração manualmente, a lista de trituração padrão na vista do File Sanitizer é triturada (ver Procedimentos de configuração na página 39).

Pode iniciar uma operação de trituração manualmente através de uma das seguintes formas:

1. Abra o File Sanitizer (ver Abrir o File Sanitizer na página 39) e clique ou toque em **Triturar**.
2. Quando a caixa de diálogo de confirmação surgir, certifique-se de que os recursos que pretende triturar estão marcados e em seguida clique ou toque em **OK**.

– ou –

1. Clique com o botão direito do rato ou toque continuamente no ícone do **File Sanitizer** no ambiente de trabalho do Windows e em seguida clique ou toque em **Triturar agora**.
2. Quando a caixa de diálogo de confirmação surgir, certifique-se de que os recursos que pretende triturar estão marcados e em seguida clique ou toque em **Triturar**.

Trituração com clique do botão direito do rato

CUIDADO: Não é possível recuperar ativos eliminados profundamente. Pondere cuidadosamente que itens seleciona para trituração manual.

Se a opção **Ativar trituração com o botão direito** tiver sido selecionada na vista do File Sanitizer, pode triturar um recurso como se segue:

1. Navegue até ao documento ou pasta que pretende triturar.
2. Clique com o botão direito do rato ou toque continuamente no ficheiro ou pasta e em seguida selecione **HP File Sanitizer – Triturar**.

Iniciar manualmente uma operação de trituração

CUIDADO: Não é possível recuperar ativos eliminados profundamente. Pondere cuidadosamente que itens seleciona para trituração manual.

Quando inicia uma operação de trituração manualmente, a lista de trituração padrão na vista do File Sanitizer é triturada (ver Procedimentos de configuração na página 39).

Pode iniciar uma operação de trituração manualmente através de uma das seguintes formas:

1. Abra o File Sanitizer (ver Abrir o File Sanitizer na página 39) e clique ou toque em **Triturar**.
2. Quando a caixa de diálogo de confirmação surgir, certifique-se de que os recursos que pretende triturar estão marcados e em seguida clique ou toque em **OK**.

– ou –

1. Clique com o botão direito do rato ou toque continuamente no ícone do **File Sanitizer** no ambiente de trabalho do Windows e em seguida clique ou toque em **Triturar agora**.
2. Quando a caixa de diálogo de confirmação surgir, certifique-se de que os recursos que pretende triturar estão marcados e em seguida clique ou toque em **Triturar**.

Iniciar manualmente a eliminação definitiva

Quando inicia uma operação de eliminação definitiva manualmente, a lista de trituração padrão na vista do File Sanitizer é eliminada definitivamente (ver Procedimentos de configuração na página 39).

Pode iniciar uma operação de eliminação definitiva manualmente através de uma das seguintes formas:

1. Abra o File Sanitizer (ver Abrir o File Sanitizer na página 39) e clique ou toque em **Eliminar definitivamente**.
2. Quando surgir a caixa de diálogo de confirmação, clique ou toque em **OK**.

– ou –

1. Clique com o botão direito do rato ou toque continuamente no ícone do **File Sanitizer** no ambiente de trabalho do Windows e em seguida clique ou toque em **Eliminar definitivamente agora**.
2. Quando surgir a caixa de diálogo de confirmação, clique ou toque em **Eliminar definitivamente**.

Ver os ficheiros de registo

Sempre que é executada uma operação de trituração ou de eliminação definitiva, são gerados ficheiros de registo de quaisquer erros ou falhas. Os ficheiros de registo são sempre atualizados de acordo com a última operação de trituração ou de eliminação definitiva.

NOTA: Os ficheiros que foram triturados ou eliminados definitivamente com êxito não aparecem nos ficheiros de registo.

É criado um ficheiro de registo para operações de trituração e outro para as operações de eliminação definitiva. Ambos os ficheiros estão localizados na unidade de disco rígido nas seguintes pastas:

- C:\Program Files\Hewlett-Packard\File Sanitizer*[Nome de utilizador]*_ShredderLog.txt
- C:\Program Files\Hewlett-Packard\File Sanitizer*[Nome de utilizador]*_DiskBleachLog.txt

Nos sistemas de 64 bits, os ficheiros estão localizados na unidade de disco rígido nas seguintes pastas:

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

7 HP Device Access Manager (apenas alguns modelos)

O HP Device Access Manager controla o acesso aos dados ao desativar dispositivos de transferência de dados.

NOTA: Alguns dispositivos de interface/introdução humana, tais como um rato, teclado e painel táctil e leitor de impressões digitais não são controlados pelo Device Access Manager. Para obter mais informações, consulte Classes de dispositivos não geridas na página 47.

Os administradores de sistemas operativos Windows® utilizam o HP Device Access Manager para controlar o acesso aos dispositivos num sistema e para proteção contra o acesso não autorizado:

- São criados perfis de dispositivos para utilizadores locais, a fim de definir os dispositivos aos quais têm ou não permissão para aceder.
- A autenticação Just In Time Authentication (JITA) permite que utilizadores predefinidos se autentiquem a eles próprios para acederem a dispositivos que não poderiam de outra forma.
- Podem ser excluídos administradores e utilizadores fidedignos das restrições sobre o acesso a dispositivos impostas pelo Device Access Manager adicionando-os ao grupo de Administradores do Dispositivo. A associação a este grupo é gerida utilizando as definições Avançadas.
- O acesso aos dispositivos pode ser concedido ou recusado com base na associação aos grupos ou para utilizadores individuais.
- Para as classe de dispositivo, tais como unidades de CD-ROM unidades de DVD, o acesso de leitura e o acesso de escrita pode ser permitido ou recusado em separado.

O HP Device Access Manager é configurado automaticamente com as seguintes definições durante a conclusão do assistente de configuração do HP Client Security:

- São ativados suportes amovíveis de autenticação Just In Time Authentication (JITA) para administradores e utilizadores.
- A política de dispositivos permite o acesso total a outros dispositivos.

Abrir o Device Access Manager

1. No ecrã Iniciar, clique ou toque na aplicação **HP Client Security** (Windows 8).

   – ou –

   No ambiente de trabalho do Windows, clique duas vezes ou toque duas vezes no ícone **HP Client Security** na área de notificação, situada na extremidade direita da barra de tarefas.

2. Em **Dispositivos**, clique ou toque em **Permissões dos dispositivos**.

   - Os utilizadores padrões podem ver o respetivo acesso atual aos dispositivos (ver Vista de utilizador na página 45).
   - Os administradores podem ver e fazer alterações no acesso aos dispositivos que está configurado atualmente para o computador clicando ou tocando em **Alterar** e introduzindo em seguida a palavra-passe de administrador (ver Vista Sistema na página 45).

Vista de utilizador

Quando a opção **Permissões dos dispositivos** é selecionada, a vista Utilizador é apresentada. Consoante a política, os utilizadores padrões e os administradores podem ver o seu próprio acesso para classes de dispositivos ou dispositivos individuais neste computador.

- **Utilizador atual** – É apresentado o nome do utilizador atualmente com sessão iniciada.
- **Classes de dispositivos** – São apresentados os tipos de dispositivos.
- **Acesso** – É apresentado o seu acesso configurado atualmente a tipos de dispositivos ou dispositivos específicos.
- **Duração** – É apresentado o limite de tempo do seu acesso a unidades de CD/DVD-ROM ou unidades de disco rígido amovíveis.
- **Definições** – Os administradores podem alterar as unidades cujo acesso é controlado pelo Device Access Manager.

Vista Sistema

Na vista Sistema, os administradores podem permitir ou recusar o acesso a dispositivos neste computador para o grupo de utilizadores ou de administradores.

▲ Os administradores podem aceder à vista Sistema clicando ou tocando em **Alterar**, introduzindo uma palavra-passe de administrador e selecionando depois as seguintes opções:

- **Device Access Manager** – Para ativar o desativar o HP Device Access Manager com a autenticação Just In Time Authentication, clique ou toque em **Ligar** ou **Desligar**.
- **Utilizadores e grupos neste computador** – Mostra o grupo de utilizadores ou de administradores com acesso autorizado ou recusado às classes de dispositivos selecionadas.
- **Classes de dispositivos** – Mostra as classes de dispositivos e os dispositivos que estão instalados no sistema ou que possam ter estado instalados no sistema anteriormente. Para expandir a lista, clique no ícone **+**. São mostrados todos os dispositivos ligados ao computador e os grupos de Administradores e Utilizadores são expandidos para mostrar a respetiva associação. Para atualizar a lista de dispositivos, clique no ícone da seta redonda (atualizar).
  - A proteção é normalmente aplicada a uma classe de dispositivos. Se o acesso estiver definido para **Permitir**, o utilizador ou grupo selecionado poderá aceder a qualquer dispositivo na classe de dispositivos.
  - A proteção também pode ser aplicada a dispositivos específicos.
  - Configure a autenticação Just In Time Authentication, permitindo que utilizadores selecionados acedam a unidades de DVD/CD-ROM ou unidades de disco amovíveis autenticando-se a eles próprios. Para obter mais informações, consulte Configuração da JITA na página 46.
  - Permita ou recuse o acesso a outras classes de dispositivos, tais como suportes amovíveis (por exemplo: unidades flash USB), portas série e paralelas, dispositivos Bluetooth®, dispositivos de modem, dispositivos PCMCIA/ExpressCard, dispositivos 1394, leitores de impressões digitais e leitores de smart cards. Se o leitor de impressões digitais e o leitor de smart cards forem recusados, podem ser utilizados como credenciais de autenticação, mas não podem ser utilizados ao nível da política de sessão.

NOTA: Se forem utilizados dispositivos Bluetooth como credenciais de autenticação, o acesso a dispositivos Bluetooth não deve ser restringido na política do Device Access Manager.

- Quando seleciona uma definição ao nível do grupo ou da classe de dispositivos e lhe for perguntado se pretende aplicar a definição a objetos subordinados:

  Sim – A definição será propagada.

  Não – A definição não será propagada.

- Algumas classes de dispositivos, tais como DVD e CD-ROM, poderão ser controlados adicionalmente permitindo ou recusando o acesso separadamente para operações de leitura e escrita.

NOTA: O grupo de administradores não pode ser adicionado à lista de utilizadores.

- **Acesso** – Clique ou toque na seta para baixo e em seguida selecione um dos seguintes tipos de acesso para permitir ou recusar o acesso:
  - **Permitir – Acesso total**
  - **Permitir – Só de leitura**
  - **Permitir – Autenticação JITA obrigatória** – Para mais informações, consultar Configuração da JITA na página 46.

    Se este tipo de acesso for selecionado, em **Duração** clique ou toque na seta para baixo para selecionar um limite de tempo.
  - **Recusar**
- **Duração** – Clique ou toque na seta para baixo para selecionar um limite de tempo para aceder a unidades de CD/DVD-ROM ou unidades de discos amovíveis (ver Configuração da JITA na página 46).

Configuração da JITA

A configuração JITA permite ao administrador ver e modificar listas de utilizadores e grupos aos quais é permitido aceder a dispositivos utilizando a autenticação Just In Time Authentication (JITA).

Os utilizadores com capacidade JITA poderão aceder a alguns dispositivos para os quais as políticas criadas na vista **Configuração da classe de dispositivos** foram restringidas.

O período JITA pode ser autorizado para um número definido de minutos ou Ilimitado. Os utilizadores ilimitados terão acesso ao dispositivo a partir do momento em que se autenticam até ao momento em que terminam a sessão no sistema.

Se for atribuído ao utilizador um período JITA limitado, um minuto antes de o período JITA expirar, é perguntado ao utilizador se pretende prolongar o acesso. Assim que o utilizador termina sessão no sistema ou outro utilizador inicia sessão, o período JITA expira. na vez seguinte que o utilizador iniciar sessão para aceder a um dispositivo com capacidade JITA, é apresentado um pedido de introdução das credenciais.

A JITA está disponível para as seguintes classes de dispositivos:

- Unidades de DVD/CD-ROM
- Unidades de discos amovíveis

Criar uma política JITA para um utilizador ou grupo

Os administradores podem permitir que os utilizadores acedam a dispositivos utilizando a autenticação Just In Time Authentication (JITA).

1. Inicie o **Device Access Manager** e em seguida clique ou toque em **Alterar**.
2. Selecione o utilizador ou grupo e em seguida, em **Acesso** para **Unidades de discos amovíveis** ou **Unidades de DVD/CD-ROM**, clique ou toque na seta para baixo e selecione **Permitir – Autenticação JITA obrigatória**.
3. Em **Duração**, clique ou toque na seta para baixo para baixo para selecionar um período de tempo para o acesso JITA.

O utilizador deve terminar sessão e em seguida iniciar sessão novamente para que a nova definição JITA seja aplicada.

Desativar uma política JITA para um utilizador ou grupo

Os administradores podem desativar o acesso de utilizadores ou grupos aos dispositivos utilizando a autenticação Just In Time Authentication.

1. Inicie o **Device Access Manager** e em seguida clique ou toque em **Alterar**.
2. Selecione o utilizador ou grupo e em seguida, em **Acesso** para **Unidades de discos amovíveis** ou **Unidades de DVD/CD-ROM**, clique ou toque na seta para baixo e em seguida selecione **Recusar**.

Quando o utilizador inicia sessão e tenta aceder ao dispositivo, o acesso é negado.

Definições

A vista **Definições** permite aos administradores ver e alterar as unidades cujo acesso é controlado pelo Device Access Manager.

NOTA: O Device Access Manager deve estar ativado quando a lista de letras de unidades é configurada (ver Vista Sistema na página 45).

Classes de dispositivos não geridas

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

- Dispositivos de entrada/saída
  - CD-ROM
  - Unidades de disco
  - Controladores de disquetes (FDC)
  - Controladores de disco rígido (HDC)
  - Classe de dispositivos de interface humana (HID)
  - Dispositivos de interface humana infravermelhos
  - Rato
  - Múltiplas portas série
  - Teclado

- Impressoras Plug & Play
- Impressora
- Atualização de impressora

- Energia
  - Suporte de gestão de energia avançada (APM)
  - Bateria
- Diversos
  - Computador
  - Descodificador
  - Ecrã
  - unidade de visualização unificada Intel®
  - Legacard
  - Controlador de multimédia
  - Modificador de suporte de dados
  - 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 do volume

8 HP Trust Circles

O HP Trust Circles é uma aplicação de segurança de ficheiros e documentos que alia a encriptação de pastas e ficheiros à cómoda capacidade de partilha de documentos num círculo de confiança. A aplicação encripta ficheiros em pastas especificadas pelo utilizador, protegendo-as dentro de um círculo de confiança. Uma vez protegidos, os ficheiros podem ser utilizados e partilhados apenas pelos membros do círculo de confiança. Se um ficheiro protegido por recebido por alguém que não faça parte do círculo de confiança, o ficheiro permanece encriptados e essa pessoa não consegue aceder ao conteúdo.

Abrir o Trust Circles

1. No ecrã Iniciar, clique ou toque na aplicação **HP Client Security**.

   – ou –

   No ambiente de trabalho do Windows, faça duplo clique ou no ícone **HP Client Security** na área de notificação, situada na extremidade direita da barra de tarefas.

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

Informação básica

Existem duas formas de enviar convites por correio eletrónico e de lhes responder:

- **Utilizar o Microsoft® Outlook** – A utilização do Trust Circles com o Microsoft Outlook automatiza o processamento de quaisquer convites do Trust Circles e respostas a outros utilizadores do Trust Circles.
- **Utilizar o Gmail, Yahoo, Outlook.com ou outros serviços de correio eletrónico (SMTP)** – Quando introduz o seu nome, endereço eletrónico e palavra-passe, o Trust Circles utiliza o seu serviço de correio eletrónico para enviar convites por correio eletrónico aos membros selecionados para aderirem ao seu círculo de confiança.

Para configurar o seu perfil básico:

1. Introduza o seu nome e o endereço eletrónico e em seguida clique ou toque em **Seguinte**.

   O nome é visível a qualquer membros que são convidados para aderirem ao seu círculo de confiança. O endereço eletrónico é utilizado para enviar, receber ou responder a convites.

2. Introduza a palavra-passe da conta de correio eletrónico e em seguida clique ou toque em **Seguinte**.

   É enviada uma mensagem de correio eletrónico de teste para garantir que as definições de correio eletrónico estão corretas.

   NOTA: O computador deve estar ligado a uma rede.

3. No campo **Nome do círculo de confiança**, introduza um nome para o círculo de confiança e em seguida clique ou toque em **Seguinte**.

4. Adicione membros e pastas e em seguida clique ou toque em **Seguinte**. O círculo de confiança é criado com as pastas que foram selecionadas e envia notificações por correio eletrónico a

quaisquer membros selecionados. Se, por qualquer motivo, não for possível enviar um convite, é apresentada uma notificação. Os membros podem ser convidados novamente em qualquer altura a partir da vista Círculo de confiança clicando em **Os seus círculos de confiança** e em seguida fazendo duplo clique ou duplo toque no círculo de confiança. Para obter mais informações, consulte Trust Circles na página 50.

Trust Circles

Pode criar um círculo de confiança durante a configuração inicial depois de introduzir o seu endereço eletrónico ou na vista Círculo de confiança:

▲ Na vista Círculo de confiança, clique ou toque em **Criar círculo de confiança** e introduza um nome para o círculo de confiança.

- Para adicionar membros ao círculo de confiança, clique ou toque no ícone **M+** ao lado de **Membros** e siga as instruções apresentadas no ecrã.
- Para adicionar pastas ao círculo de confiança, clique ou toque no ícone **+** ao lado de **Pastas** e siga as instruções apresentadas no ecrã.

Adicionar pastas a um círculo de confiança

Adicionar pastas a um novo círculo de confiança:

- Durante a criação de um círculo de confiança, pode adicionar pastas clicando ou tocando no ícone **+** ao lado de **Pastas** e seguindo as instruções apresentadas no ecrã.

  – ou –

- No Explorador do Windows, faça duplo clique ou toque continuamente numa pasta que não faça parte de um círculo de confiança, selecione **Círculo de confiança** e em seguida selecione **Criar círculo de confiança a partir de pasta**.

SUGESTÃO: Pode selecionar uma ou mais pastas.

Adicionar pastas a um círculo de confiança existente:

- Na vista Círculo de confiança, clique em **Os seus círculos de confiança**, faça duplo clique ou duplo toque no círculo de confiança existente para visualizar as pastas atuais, clique ou toque no ícone **+** ao lado de **Pastas** e siga as instruções apresentadas no ecrã.

  – ou –

- No Explorador do Windows, faça duplo clique ou toque continuamente numa pasta que não faça parte de um círculo de confiança, selecione **Círculo de confiança** e em seguida selecione **Adicionar a círculo de confiança a partir de pasta**.

SUGESTÃO: Pode selecionar uma ou mais pastas.

Depois de uma pasta ter sido adicionada a um círculo de confiança, o Trust Circles encripta a pasta e o respetivo conteúdo automaticamente. Quando todos os ficheiros estiverem encriptados, é apresentada uma notificação. Além disso, um símbolo de cadeado verde é apresentado em todos os ícones de pastas encriptadas e ícones de ficheiros dentro das pastas para indicar que estão completamente protegidos.

Adicionar membros a um círculo de confiança

São necessários três passos para adicionar membros a um círculo de confiança:

1. **Convidar** – Em primeiro lugar, o titular do círculo de confiança convida o(s) membro(s). O convite por correio eletrónico pode ser enviado a vários utilizadores ou listas/grupos de distribuição.
2. **Aceitar** – O convidado recebe o convite e decide se aceita ou recusa. Se o convidado aceitar o convite, é enviada uma resposta por correio eletrónico ao autor do convite. Se o convite foi enviado a um grupo, cada membro recebe um convite e decide se aceita ou recusa.
3. **Registar** – O autor do convite tem uma última oportunidade para decidir se deve adicionar o membro ao círculo de confiança. Se o autor do convite decidir registar o membro, é enviada uma mensagem de correio eletrónico ao convidado a confirmar a resposta. O autor do convite e o convidado podem verificar opcionalmente a segurança do processo de convite. É apresentado um código de verificação para o convidado, que deve ser lido ao autor do convite pelo telefone. Depois de o código ter sido verificado, o autor do convite pode enviar a mensagem de correio eletrónico final de registo.

Adicionar membros a um novo círculo de confiança:

▲ Durante a criação de um círculo de confiança, pode adicionar membros clicando ou tocando no ícone **M+** ao lado de **Membros** e seguindo as instruções apresentadas no ecrã.

- Se utiliza o Outlook, selecione contactos no livro de endereços do Outlook e clique em **OK**
- Se utiliza outro serviço de correio eletrónico, introduza manualmente novos endereços eletrónicos no círculo de confiança ou pode recuperá-los a partir do endereço eletrónico registado no círculo de confiança.

Adicionar membros a um círculo de confiança existente:

▲ Na vista Círculo de confiança, clique em **Os seus círculos de confiança**, faça duplo clique ou duplo toque no círculo de confiança existente para visualizar os membros atuais, clique ou toque no ícone **M+** ao lado de **Membros** e siga as instruções apresentadas no ecrã.

- Se utiliza o Outlook, selecione contactos no livro de endereços do Outlook e clique ou toque em **OK**.
- Se utiliza outro serviço de correio eletrónico, introduza manualmente novos endereços eletrónicos no círculo de confiança ou pode recuperá-los a partir do endereço eletrónico registado no círculo de confiança.

Adicionar ficheiros a um círculo de confiança

Pode adicionar ficheiros a um círculo de confiança através de uma das seguintes formas:

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

  – ou –

- No Explorador do Windows, clique com o botão direito ou toque continuamente num ficheiro que não esteja encriptado atualmente, selecione **Círculo de confiança** e em seguida selecione **Encriptar**. Ser-lhe-á pedido para selecionar o círculo de confiança ao qual o ficheiro deve ser adicionado.

SUGESTÃO: Pode selecionar um ou mais ficheiros.

Pastas encriptadas

Qualquer membro de um círculo de confiança pode ver e editar ficheiros que pertencem a esse círculo de confiança.

NOTA: O Gestor/leitor de círculos de confiança não sincroniza ficheiros entre os membros.

Os ficheiros devem ser partilhados através dos meios existentes, tais como correio eletrónico, FTP ou fornecedores de armazenamento na nuvem. Os ficheiros copiados para, movidos para ou criados numa pasta de círculo de confiança ficam protegidos imediatamente.

Remover pastas de um círculo de confiança

Remover uma pasta de um círculo de confiança desencripta a pasta e o respetivo conteúdo e remove a sua proteção.

- Na vista Círculo de confiança, clique ou toque em **Os seus círculos de confiança**, faça duplo clique ou duplo toque no círculo de confiança existente para visualizar as pastas atuais e em seguida clique ou toque no ícone da **lata de lixo** ao lado dessa pasta.

  – ou –

- No Explorador do Windows, faça duplo clique ou toque continuamente numa pasta que faça parte atualmente de um círculo de confiança, selecione **Círculo de confiança** e em seguida selecione **Remover do círculo de confiança**.

SUGESTÃO: Pode selecionar uma ou mais pastas.

Remover um ficheiro de um círculo de confiança

Para remover um ficheiro de um círculo de confiança, no Explorador do Windows clique com o botão direito do rato ou toque continuamente num ficheiro que esteja encriptado atualmente e selecione **Círculo de confiança**, seguido de **Desencriptar ficheiro**.

Remover membros de um círculo de confiança

Um membro que tenha sido registado completamente 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 ficheiros e pastas para o novo círculo de confiança e em seguida eliminar o círculo de confiança antigo. Isto irá assegurar que quaisquer novos ficheiros que o membro receba não estarão acessíveis, mas tudo o que tenha sido partilhado previamente permanecerá acessível ao membro do círculo de confiança antigo.

Se o membro não foi registado completamente (o membro foi convidado a aderir ao círculo de confiança ou não aceitou o convite do círculo de confiança), pode remover o membro do círculo de confiança através de uma das seguintes formas:

- Na vista Círculo de confiança, clique ou toque em **os seus círculos de confiança** e em seguida faça duplo clique ou duplo toque no círculo de confiança para mostrar a lista atual de membros. Clique ou toque no ícone da **lata de lixo** ao lado do nome do membro a remover.
- Na vista Círculo de confiança, clique ou toque em **Membros** e em seguida faça duplo clique ou duplo toque no membro para mostrar os círculos de confiança dos quais é membro. Clique ou toque no ícone da **lata de lixo** ao lado de um círculo de confiança para remover o membro desse círculo de confiança.

Eliminar um círculo de confiança

Para eliminar um círculo de confiança, é necessário ser-se o titular.

▲ Na vista Círculo de confiança, clique ou toque em **Os seus círculos de confiança** e em seguida clique ou toque no ícone da **lata de lixo** ao lado do círculo de confiança a eliminar.

Isto remove o círculo de confiança da página e envia mensagens de correio eletrónico a todos os membros do círculo de confiança para os informar de que o círculo de confiança foi eliminado. Quaisquer ficheiros ou pastas que estavam incluídos nesse círculo de confiança são desencriptados.

Definir preferências

Na vista Círculo de confiança, clique ou toque em **Preferências**. São apresentados três separadores

- **Definições de correio eletrónico**

Opção	Descrição
Nome de utilizador	É apresentado o nome de utilizador atualmente em uso. Para alterá-lo, introduza um novo nome de utilizador na caixa de texto. As alterações são guardadas automaticamente.
Endereço eletrónico	É apresentada a conta de correio eletrónico utilizada atualmente. Para alterá-la, clique ou toque em **Alterar definições de correio eletrónico** e sigas as instruções apresentadas no ecrã.
Confirmação de novo membro	Selecione entre as seguintes opções: ◦ **Confirmar automaticamente** – Depois de receber a aceitação dos convidados, estes são confirmados no círculo de confiança sem qualquer introdução manual, sendo-lhes enviada uma mensagem de correio eletrónico de confirmação. ◦ **Confirmar manualmente** – Depois de receber a aceitação dos convidados, é necessário efetuar a introdução manual para registar os novos membros no círculo de confiança, sendo-lhes enviada em seguida uma mensagem de correio eletrónico de confirmação. ◦ **Solicitar verificação** – Depois de receber a aceitação dos convidados, é necessário um código de verificação para registar completamente os convidados. O titular do círculo de confiança deve contactar os convidados e obter deles o código de verificação. Depois de introduzir o código correto, são enviadas as mensagens de correio eletrónico de confirmação.
Autenticação periódica	A autenticação periódica requer que o utilizador introduza a palavra-passe do Windows depois do tempo limite especificado (registado em minutos) e também ao realizar operações sensíveis. Esta definição permite ativar ou desativar a autenticação dos utilizadores.
Tempo limite de autenticação	Selecione o período de tempo limite especificado (registado em minutos) antes de ser necessário efetuar a autenticação.
Não mostrar a mensagem de confirmação	Marque a caixa de verificação para desativar a apresentação de mensagens de confirmação ou desmarque a caixa de verificação para visualizar mensagens de confirmação.
Quero ajudar a melhorar o HP Trust Circle através do controlo de utilização anónimo	Marque a caixa de verificação para participar no programa ou desmarque a caixa de verificação caso não queira participar.

- **Cópia de segurança / Restauro**

Opção	Descrição
Cópia de segurança	Copia os seus dados (definições e círculos de confiança) da aplicação Gestor/leitor do círculo de confiança para um ficheiro de cópia de segurança. Na eventualidade de uma falha do sistema, pode utilizar este ficheiro para restaurar a sua nova instalação do Trust Circles para o estado guardado no ficheiro. **NOTA:** Apenas são guardados os dados da aplicação do seu círculo de confiança (círculos de confiança, definições e membros). Os ficheiros nas pastas do círculo de confiança não são copiados. Esses ficheiros devem ser copiados à parte. Para criar a cópia de segurança das definições e dados de utilizador do círculo de confiança: **1.** Clique ou toque em **Criar cópia de segurança**. **2.** Escolha um nome de ficheiro e um diretório para o ficheiro de cópia de segurança e em seguida clique ou toque em **Guardar**. **3.** Introduza uma palavra-passe, confirme-a e em seguida clique ou toque em **OK**. Esta palavra-passe será necessária para restaurar o ficheiro.
Restaurar	Restaura definições e círculos de confiança a partir de um ficheiro de cópia de segurança, normalmente depois de uma falha do sistema ou migração para outro computador. Para restaurar as definições e dados de utilizador do Gestor de círculos de confiança: **1.** Clique ou toque em **Restaurar**. **2.** Navegue até ao diretório e nome de ficheiro do ficheiro de cópia de segurança e em seguida clique ou toque em **Abrir**. **3.** Introduza a palavra-passe que foi configurada ao criar a cópia de segurança.

- **Acerca de** É apresentada a versão do software do Gestor/Leitor de círculos de confiança. São apresentadas ligações que lhe permitem atualizar o Gestor de círculos de confiança para a versão Pro ou visualizar a declaração de privacidade da HP.

9 Recuperação de roubo (apenas alguns modelos)

O Computrace (comprado em separado) permite-lhe monitorizar, gerir e rastrear à distância o seu computador.

Depois de ativado , Computrace é configurado a partir do Centro de Cliente Absolute Software. A parir do Centro de Cliente, o administrador pode configurar o Computrace para monitorizar ou gerir o computador. Se o sistema for perdido ou roubado, o Centro de Cliente pode auxiliar as autoridades locais a localizar e recuperar o computador. Se estiver configurado, o Computrace pode continuar a funcionar mesmo se a unidade de disco rígido for apagada ou substituída.

Para ativar o Computrace:

1. Estabeleça a ligação à Internet.
2. Abra o HP Client Security. Para obter mais informações, consulte Abrir o HP Client Security na página 10.
3. Clique em **Recuperação de roubo**.
4. Para iniciar o Assistente de Ativação do Computrace, clique em **Introdução**.
5. Introduza as suas informações de contacto e informações de pagamento com cartão de crédito, ou introduza a Chave de produto previamente adquirida.

O Assistente de Ativação processa se forma segura a transação e configura a sua conta de utilizador no web site do Centro de Cliente Absolute Software. Quando terminar, recebe uma mensagem de correio eletrónico com as suas informações de conta no centro de Cliente.

Se tiver executado anteriormente o Assistente de Ativação do Computrace e já possuir uma conta de utilizador do centro de Cliente, pode adquirir licenças adicionais contactando o seu representante de conta da HP.

Para iniciar sessão no centro de Cliente:

1. Visite https://cc.absolute.com/.
2. Nos campos **ID de início de sessão** e **Palavra-passe**, introduza as credenciais que recebeu na mensagem de confirmação e de seguida clique em **Iniciar sessão**.

No Centro de Cliente, pode:

- Monitorizar os seus computadores.
- Proteger os seus dados à distância.
- Comunicar o roubo de qualquer computador protegido pelo Computrace.

▲ Clique em **Saber mais** para obter mais informações sobre o Computrace.

10 Exceções de palavras-passes localizadas

Ao nível da autenticação na ligação e do HP Drive Encryption, o suporte de localização da palavra-passe é limitado. Para obter mais informações, consulte IME do Windows não suportados ao nível da autenticação na ligação ou do Drive Encryption na página 56.

O que fazer quando uma palavra-passe é rejeitada

As palavras-passes podem ser rejeitadas pelas seguintes razões:

- Um utilizador está a utilizar um IME que não é suportado. Este é um problema comum com idiomas de byte duplo (coreano, japonês, chinês). Para resolver este problema:

  1. Utilizando o **Painel de Controlo**, adicione um esquema do teclado suportado (adicione teclados norte-americanos/ingleses no idioma de teclado chinês).
  2. Defina o teclado suportado para introdução padrão.
  3. Inicie o HP Client Security e em seguida introduza a palavra-passe do Windows.

- Um utilizador está a utilizar um carácter que não é suportado. Para resolver este problema:

  1. Altere a palavra-passe do Windows para utilizar apenas caracteres suportados. Para mais informações sobre caracteres não suportados, consulte Tratamento de teclas especiais na página 57.
  2. Inicie o HP Client Security e em seguida introduza a palavra-passe do Windows.

IME do Windows não suportados ao nível da autenticação na ligação ou do Drive Encryption

No Windows, o utilizador pode escolher um IME (editor do método de introdução) para introduzir caracteres e símbolos complexos, tais como caracteres japoneses e chineses, utilizando um teclado ocidental padrão.

Os IME do Windows não são suportados ao nível da autenticação na ligação ou do Drive Encryption. Não é possível introduzir uma palavra-passe do Windows com um IME no ecrã de início de sessão da autenticação na ligação ou do HP Drive Encryption, e fazê-lo poderá resultar numa situação de bloqueio. Em alguns casos, o Microsoft® Windows não apresenta o IME quando o utilizador introduz a palavra-passe.

A solução consiste em mudar para um dos esquemas de teclado suportados que traduz para o esquema de teclado 00000411:

- Microsoft IME para japonês
- O esquema de teclado japonês
- Office 2007 IME para japonês – Se a Microsoft ou um terceiro utiliza o termo IME ou editor do método de introdução, o método de introdução poderá não ser na verdade um IME. Isto pode causar confusão, mas o software lê a representação de código hexadecimal. Desta forma, se

um IME mapeia para um esquema de teclado suportado, então o HP Client Security suporta a configuração.

AVISO! Quando o HP Client Security é implementado, as palavras-passes introduzidas com um IME do Windows serão rejeitadas.

Alterações de palavras-passes utilizando esquemas de teclado que também são suportados

Se a palavra-passe for definida inicialmente com um esquema de teclado, tal como Inglês dos EUA (409) e em seguida o utilizador alterar a palavra-passe utilizando um esquema de teclado diferente que também é suportado, tal como Latino-americano (080A), a alteração da palavra-passe funcionará com o HP Drive Encryption, mas falhará no BIOS se o utilizador utilizar caracteres que existem no último, mas não no primeiro (por exemplo, ē).

NOTA: Os administradores podem resolver este problema utilizando a página Utilizadores do HP Client Security (acessível a partir do ícone da **engrenagem** na página inicial) para remover o utilizador do HP Client Security, selecionando o esquema de teclado pretendido no sistema operativo e em seguida executando novamente o assistente de configuração do HP Client Security para o mesmo utilizador. O BIOS armazena o esquema de teclado pretendido, e as palavras-passes que podem ser escritas com este esquema de teclado serão definidas corretamente no BIOS.

Outro problema potencial é a utilização de diferentes esquemas de teclado que podem todos produzir os mesmos caracteres. Por exemplo, tanto o esquema de teclado EUA Internacional (20409) como o esquema de teclado Latino-americano (080A) podem produzir o carácter é, embora possam ser necessárias sequências diferentes de batimentos de teclas. Se uma palavra-passe for definida inicialmente com o esquema de teclado latino-americano, então o esquema de teclado Latino-americano é definido no BIOS, mesmo que a palavra-passe seja alterada posteriormente utilizando o esquema de teclado EUA Internacional.

Tratamento de teclas especiais

- Chinês, eslovaco, francês do Canadá e checo

  Quando um utilizador seleciona um dos esquemas de teclado anteriores e depois introduz uma palavra-passe (por exemplo, abcdef), a mesma palavra-passe deve ser introduzida enquanto é premida a tecla shift para minúsculas e as teclas shift e caps lock para maiúsculas na autenticação na ligação ou do Drive Encryption. As palavras-passes numéricas devem ser introduzidas utilizando o teclado numérico.

- Coreano

  Quando um utilizador seleciona um esquema de teclado coreano compatível e depois introduz uma palavra-passe, a mesma palavra-passe deve ser introduzida enquanto é premida a tecla alt para minúsculas e a tecla alt direita e a tecla caps lock para maiúsculas na autenticação na ligação ou do Drive Encryption.

- Os caracteres não suportados são indicados na tabela seguinte:

Idioma	Windows	BIOS	Drive Encryption
Árabe	As teclas ﻯ ,ﻰ, e ﻯ geram dois caracteres.	As teclas ﻯ ,ﻰ, e ﻯ geram um carácter.	As teclas ﻯ ,ﻰ, e ﻯ geram um carácter.
Francês do Canadá	ç, è, à, é com caps lock são Ç, È, À, É no Windows.	ç, è, à, é com caps lock são ç, è, à, é na autenticação na ligação.	ç, è, à, e é com caps lock são ç, è, à, é no HP Drive Encryption.

Idioma	Windows	BIOS	Drive Encryption
Espanhol	40a não é suportado. Apesar disso, funciona porque o software converte-a para c0a. No entanto, devido a diferenças subtis entre os esquemas de teclado, recomenda-se que os utilizadores de língua espanhol mudem o seu esquema de teclado Windows para 1040a (Variante espanhola) ou 080a (Latino-americano).	n/a	n/a
EUA Internacional	◦ As teclas ¡, ¤, ‘, ’, ¥ e × na fila superior são rejeitadas. ◦ As teclas å, ® e Þ na segunda fila são rejeitadas. ◦ As teclas á, ð e ø na terceira fila são rejeitadas. ◦ A tecla æ na fila inferior é rejeitada.	n/a	n/a
Czech	◦ 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/a	n/a
Eslovaco	A tecla ż é rejeitada.	◦ As teclas š, ś e ş são rejeitadas quando escritas, mas são aceites quando introduzidas com o teclado virtual ◦ A tecla morta ţ gera dois caracteres.	n/a
Hungarian	A tecla ż é rejeitada.	A tecla ţ gera dois caracteres.	n/a
Slovenian	A tecla żŻ é rejeitada no Windows e a tecla alt gera uma tecla morta no BIOS.	As teclas ú, Ú, ů, Ů, ş, Ş, ś, Ś, š e Š são rejeitadas no BIOS.	n/a
Japonês	Quando disponível, o Microsoft Office 2007 IME é uma escolha melhor. Apesar do nome IME, é na verdade o esquema de teclado 411, que é suportado.	n/a	n/a

Glossário

administrador
Consulte *administrador do Windows*.

administrador do Windows
Um utilizador com direitos plenos para modificar permissões e gerir outros utilizadores.

ativação
A tarefa que é necessário concluir antes que quaisquer funcionalidades do Drive Encryption fiquem acessíveis. Os administradores podem ativar o Drive Encryption com o assistente de configuração do HP Client Security ou HP Client Security. O processo de ativação consiste em ativar o software, encriptar a unidade e criar a cópia de segurança da chave de encriptação inicial num dispositivo de armazenamento amovível.

ativo
Um componente de dados que consiste em informações ou ficheiros pessoais, dados relacionados com o histórico ou a Internet, etc., o qual está localizado na unidade de disco rígido.

autenticação
O processo de verificar se é a pessoa que afirma ser, através da utilização de credenciais, incluindo a sua palavra-passe do Windows, a sua impressão digital, um smart card, um cartão sem contactos ou um cartão de proximidade.

autenticação de pré-arranque do Drive Encryption
Um ecrã de início de sessão que é apresentando antes de iniciar o Windows. Os utilizadores devem introduzir o respetivo nome de utilizador e palavra-passe do Windows ou o PIN do smart card ou deslizar um dedo registado. Se for selecionado o início de sessão de passo único, então introduzir as informações corretas no ecrã de início de sessão do Drive Encryption permite o acesso direto ao Windows sem ter de iniciar sessão novamente no ecrã de início de sessão do Windows.

autenticação na ligação
Uma funcionalidade de segurança que exige alguma forma de autenticação, por exemplo um smart card, chip de segurança ou palavra-passe, quando o computador arranca.

Bluetooth
Tecnologia que utiliza radiotransmissões para ativar computadores, impressoras, ratos, telemóveis e outros dispositivos com capacidade Bluetooth para a comunicação sem fios numa distância curta.

cartão de proximidade
Um cartão de plástico com um chip informático que pode ser utilizado para autenticação em conjunto com outras credenciais para maior segurança.

Cartão ID
Uma miniaplicação do Windows que serve para identificar o seu ambiente de trabalho com o seu nome de utilizador e imagem escolhida.

cartão sem contactos
Um cartão de plástico com um chip informático que pode ser utilizado para autenticação.

chip de segurança incorporado Trusted Platform Module (TPM)
A aplicação TPM autentica um computador, em vez de um utilizador, armazenando informações específicas ao sistema anfitrião, tais como chaves de encriptação, certificados digitais e palavras-passe. Uma TPM minimiza o risco de as informações no computador serem comprometidas pelo roubo físico ou ocorrer um ataque por um hacker externo.

Círculo de confiança
Fornece contenção de dados ao associar os dados a um grupo de definido de utilizadores fidedignos. Isto impede que os dados caiam nas mãos erradas, quer acidentalmente, quer intencionalmente. Protegidos com a tecnologia Zero Overhead Key Management da CryptoMill, os dados são associados criptograficamente a um círculo de confiança. Isto impede a desencriptação de documentos ou outras informações sensíveis fora do círculo de confiança

classe de dispositivo
Todos os dispositivos de um tipo específico, tais como unidades.

conta de rede
Uma conta de utilizador ou administrador do Windows, num computador local, num grupo de trabalho ou num domínio.

Conta de utilizador do Windows
Um utilizador que está autorizado a iniciar sessão numa rede ou num computador individual.

cópia de segurança
Utilizar a funcionalidade de cópia de segurança para guardar uma cópia de informações importantes de um programa numa localização fora do programa. Pode em seguida ser utilizada para restaurar as informações posteriormente no mesmo computador ou noutro.

credencial
Uma peça de informação específica ou um dispositivo de hardware utilizado para autenticar um utilizador individual.

desencriptação
Um procedimento utilizado em criptografia para converter dados encriptados em texto simples.

dispositivo ligado
Um dispositivo de hardware que está ligado a uma porta no computador.

domínio
Um conjunto de computadores que fazem parte de uma rede e partilham uma base de dados de diretório comum. Os domínios têm nomes exclusivos e cada um possui as suas próprias regras e procedimentos.

Drive Encryption
Protege os seus dados encriptando as suas unidades de disco rígido, impossibilitando a leitura das informações por pessoas sem a devida autorização.

DriveLock
Uma funcionalidade de segurança que associa a unidade de disco rígido a um utilizador e exige que o utilizador escreva corretamente a palavra-passe DriveLock quando o computador arranca.

ecrã de início de sessão do Drive Encryption
Ver Autenticação de pré-arranque do Drive Encryption.

eliminação definitiva do espaço livre
A escrita de dados aleatórios por cima de recursos eliminados e espaço não utilizado. Este processo reduz a existência do recurso eliminado para que seja mais difícil recuperar o recurso original.

encriptação
Um procedimento, tal como a utilização de um algoritmo, implementando na criptografia para converter texto simples em texto cifrado de forma a impedir que destinatários não autorizados leiam esses dados. Há vários tipos de encriptação de dados e estes são a base da segurança de rede. Os tipos comuns incluem a norma DES (Data Encryption Standard) e a encriptação de chave pública.

encriptação por hardware
A utilização de unidades de autoencriptação que cumprem a especificação OPAL do Trusted Computing Group para a gestão de unidades de autoencriptação para concluir a encriptação instantânea. A encriptação por

hardware é instantânea e poderá demorar apenas alguns minutos, mas a encriptação por software poderá demorar várias horas.

encriptação por software
A utilização de software para encriptar a unidade de disco rígido setor por setor. Este processo é mais lento do que a encriptação por hardware

Gestor/Leitor do círculo de confiança
O Leitor de círculos de confiança apenas pode aceitar convites enviados por utilizadores do círculo de confiança. No entanto, o Gestor de círculos de confiança permite a criação de círculos de confiança. As funcionalidades incluem convidar alguém por correio eletrónico para um círculo de confiança e aceitar convites para círculos de confiança de outras pessoas. Assim que é estabelecido um círculo de confiança entre pares, os ficheiros protegidos por esse círculo de confiança podem ser partilhados em segurança.

grupo
Um grupo de utilizadores que têm o mesmo nível de acesso ou recusa em relação a uma classe de dispositivos ou a um dispositivo específico.

identidade
No HP Client Security, um grupo de credenciais e definições que é gerido como uma conta ou um perfil para um determinado utilizador.

impressão digital
Uma extração digital da imagem da sua impressão digital. A imagem real da sua impressão digital nunca é armazenada pelo HP Client Security.

início de sessão
Um objeto dentro do HP Client Security que consiste num nome de utilizador e numa palavra-passe (e possivelmente outras informações selecionadas) que pode ser utilizado para iniciar sessão em websites ou outros programas.

Início de sessão único
Uma funcionalidade que armazena informações de autenticação e permite-lhe utilizar o HP Client Security para aceder à Internet e a aplicações do Windows que exigem a autenticação por palavra-passe.

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

método de início de sessão em segurança
O método utilizado para iniciar a sessão no computador.

Página inicial
Uma localização central onde pode aceder e gerir as funcionalidades e definições no HP Client Security.

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

PIN
Um número de identificação pessoal para um utilizador registado para ser utilizado para autenticação.

PKI
A norma de Infraestrutura de chave pública que define as interface para criar, utilizar e administrar certificados e chaves criptográficas.

política de controlo de acesso aos dispositivos
A lista de dispositivos para os quais o acesso do utilizador é permitido ou recusado.

Recuperação da HP SpareKey
A capacidade de aceder ao seu computador respondendo corretamente a perguntas de segurança.

reiniciar

O processo de reiniciar o computador.

restaurar
Um processo que copia informações do programa a partir de um ficheiro de cópia de segurança previamente guardado para o programa.

Sistema de encriptação de ficheiros (EFS)
Um sistema que encripta todos os ficheiros e subpastas na pastas selecionada.

smart card
Um dispositivo de hardware que pode ser utilizado com um PIN para autenticação.

token de recuperação de emergência
Uma área de armazenamento seguro que permite a reencriptação das Teclas de Utilizador Básico a partir de uma tecla de proprietário da plataforma para outra.

trituração automática
Trituração agendada por si no File Sanitizer.

trituração manual
Trituração imediata de um ou mais recursos selecionados, a qual substitui uma trituração agendada.

triturar
A execução de um algoritmo que substitui os dados contidos num recurso por dados sem sentido.

utilizador
Qualquer pessoa registada no Drive Encryption. Os utilizadores não administradores têm direitos limitados no Drive Encryption. Apenas se podem registar (com a aprovação do administrador) e iniciar sessão.

Windows Logon Security
Protege as suas contas do Windows exigindo a utilização de credenciais específicas para fins de acesso.

Índice Remissivo